Florida Cyber-Security Manual

Secure Florida
Legal Notices

C-SAFE CC License Version 1.1

Highlighted License Terms:

**Attribution.** The licensor (Secure Florida) permits others to copy, distribute, display, and perform the work. In return, licensees (you) must give credit to the Secure Florida and the original author(s) of the material you use.

**Noncommercial.** The licensor permits others to copy, distribute, display, and perform the work. In return, licensees may not use the work for commercial purposes—unless they get the licensor’s permission.

**Share Alike.** The licensor permits others to distribute original or derivative works, but only under a license identical to the one that governs the licensor’s work. Derivative works are C-SAFE materials that have been edited, translated, combined with someone else’s materials, reformatted, or changed in any other way.

**Exceptions.** Certain elements (selected photos, graphs, text quotes) included in the Florida Cyber-Security Manual have been acquired from sources outside Secure Florida. Note: you must contact the copyright owner to get permission for non-fair use purposes if you wish to copy, distribute, display, or perform an element that is not covered under the C-SAFE CC license.

The C-SAFE CC license follows the Creative Commons licensing standards <www.creativecommons.org>.

The legal code for the C-SAFE CC license can found at the Secure Florida website <www.secureflorida.org>.

November 2004
The C-SAFE Program and the Florida Cyber-Security Manual

Sponsored by

Florida Department of Law Enforcement <www.fdle.state.fl.us>
Secure Florida <www.secureflorida.org>
Florida Cybersecurity Institute <www.fci.fsu.edu>

C-SAFE Lectures
Secure Florida Handbook
C-SAFE Train the Trainer (T3) Program
Designed and Developed by
Bob Breeden, FDLE
Mary McLaughlin, FDLE
Neil Sindicich, FDLE
Andrew Valentine, FDLE

~

Florida Cyber-Security Manual
Researched and Written by
Judie Mulholland, FCI

Version 1.1
Creative Commons License
Some Rights Reserved
# Table of Contents

List of Tables xi
List of Figures xi
Disclaimer xii

## Part I – Fundamentals

Overview 2
  Objectives 2
  Caveats 3
  Outline 4
  References 5

Security 6
  Definition 6
  Elements of Security 7
  Verification Processes 9
  Threats 9
  Critical Success Factors 12
  References 14

Attacks 17
  Definition 17
  Vectors vs. Payloads 19
  Types of Attacks 20
  Anatomy of an Attack 23
  References 24

Networks 27
  Definition 27
  Network Components 29
  Internet Backbone 30
  Internet Addresses 30
  Secure Sockets Layer (SSL) 32
  Network Tools 33
  Network Toolkit 34
  References 35

## Part II – Network-related Threats

Denial of Service 40
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Definition</td>
<td>40</td>
</tr>
<tr>
<td>DoS Structure</td>
<td>41</td>
</tr>
<tr>
<td>Implications</td>
<td>43</td>
</tr>
<tr>
<td>Zombies</td>
<td>44</td>
</tr>
<tr>
<td>Countermeasures</td>
<td>44</td>
</tr>
<tr>
<td>References</td>
<td>45</td>
</tr>
<tr>
<td>E-mail</td>
<td>46</td>
</tr>
<tr>
<td>Definition</td>
<td>46</td>
</tr>
<tr>
<td>E-mail Security</td>
<td>47</td>
</tr>
<tr>
<td>“Suspicious E-mails”</td>
<td>48</td>
</tr>
<tr>
<td>E-mail Threats</td>
<td>49</td>
</tr>
<tr>
<td>E-mail Attack Vectors</td>
<td>50</td>
</tr>
<tr>
<td>Attachments</td>
<td>50</td>
</tr>
<tr>
<td>Handling Attachments</td>
<td>51</td>
</tr>
<tr>
<td>Precautions</td>
<td>52</td>
</tr>
<tr>
<td>FYI</td>
<td>53</td>
</tr>
<tr>
<td>Liability</td>
<td>53</td>
</tr>
<tr>
<td>E-mail at Work</td>
<td>54</td>
</tr>
<tr>
<td>The KRESV Test</td>
<td>55</td>
</tr>
<tr>
<td>References</td>
<td>55</td>
</tr>
<tr>
<td>Spam</td>
<td>57</td>
</tr>
<tr>
<td>Definition</td>
<td>57</td>
</tr>
<tr>
<td>Who are the Spammers</td>
<td>58</td>
</tr>
<tr>
<td>Components</td>
<td>59</td>
</tr>
<tr>
<td>Recognizing Spam</td>
<td>62</td>
</tr>
<tr>
<td>Tips for Fighting Spam</td>
<td>62</td>
</tr>
<tr>
<td>References</td>
<td>62</td>
</tr>
<tr>
<td>Spoofing</td>
<td>67</td>
</tr>
<tr>
<td>Definition</td>
<td>67</td>
</tr>
<tr>
<td>Types of Spoofing</td>
<td>67</td>
</tr>
<tr>
<td>Joe Job</td>
<td>69</td>
</tr>
<tr>
<td>Social Engineering</td>
<td>70</td>
</tr>
<tr>
<td>Spotting Spoofed Webpages</td>
<td>71</td>
</tr>
<tr>
<td>Spotting Spoofed E-mails</td>
<td>72</td>
</tr>
<tr>
<td>Cloaking Techniques</td>
<td>74</td>
</tr>
<tr>
<td>Viewing Headers</td>
<td>77</td>
</tr>
<tr>
<td>E-mail Protocols</td>
<td>79</td>
</tr>
<tr>
<td>Decoding E-mail Headers</td>
<td>81</td>
</tr>
<tr>
<td>References</td>
<td>84</td>
</tr>
<tr>
<td>Topic</td>
<td>Page</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Anti-Trojan Software</td>
<td>127</td>
</tr>
<tr>
<td>Online Scanning Tests</td>
<td>127</td>
</tr>
<tr>
<td>Don’t Be Duped</td>
<td>128</td>
</tr>
<tr>
<td>References</td>
<td>129</td>
</tr>
<tr>
<td>Spyware</td>
<td>131</td>
</tr>
<tr>
<td>Definition</td>
<td>131</td>
</tr>
<tr>
<td>Earmarks of Spyware</td>
<td>132</td>
</tr>
<tr>
<td>Ethical Conduct</td>
<td>133</td>
</tr>
<tr>
<td>Detection and Removal</td>
<td>134</td>
</tr>
<tr>
<td>Anti-Spyware Tools</td>
<td>136</td>
</tr>
<tr>
<td>Spyware Removal Tips</td>
<td>136</td>
</tr>
<tr>
<td>Spyware Prevention</td>
<td>137</td>
</tr>
<tr>
<td>References</td>
<td>139</td>
</tr>
<tr>
<td>Blended Threats</td>
<td>142</td>
</tr>
<tr>
<td>Definition</td>
<td>142</td>
</tr>
<tr>
<td>Recent Trends</td>
<td>143</td>
</tr>
<tr>
<td>Worse Case Scenario</td>
<td>145</td>
</tr>
<tr>
<td>Taking Precautions</td>
<td>146</td>
</tr>
<tr>
<td>References</td>
<td>147</td>
</tr>
<tr>
<td>Part IV – Asset-related Threats</td>
<td>149</td>
</tr>
<tr>
<td>Internet Cons</td>
<td>150</td>
</tr>
<tr>
<td>Definition</td>
<td>150</td>
</tr>
<tr>
<td>Trends</td>
<td>150</td>
</tr>
<tr>
<td>Scam Artists</td>
<td>152</td>
</tr>
<tr>
<td>Reporting a Scam</td>
<td>153</td>
</tr>
<tr>
<td>References</td>
<td>153</td>
</tr>
<tr>
<td>Nigerian Scam</td>
<td>155</td>
</tr>
<tr>
<td>Definition</td>
<td>155</td>
</tr>
<tr>
<td>Gist of a Nigerian Scam</td>
<td>157</td>
</tr>
<tr>
<td>References</td>
<td>158</td>
</tr>
<tr>
<td>Phishing</td>
<td>159</td>
</tr>
<tr>
<td>Definition</td>
<td>159</td>
</tr>
<tr>
<td>How Phishing Works</td>
<td>160</td>
</tr>
<tr>
<td>Rising Number of Attacks</td>
<td>162</td>
</tr>
<tr>
<td>You May be a Victim If...</td>
<td>163</td>
</tr>
<tr>
<td>Prevention Measures</td>
<td>164</td>
</tr>
<tr>
<td>Unearthing a Phishing Scheme</td>
<td>165</td>
</tr>
<tr>
<td>Inspecting URLs</td>
<td>167</td>
</tr>
</tbody>
</table>
Checking Source Code | 168  
Tracking Down Rogue Servers | 169  
Avoid Getting Hooked | 170  
Business Countermeasures | 172  
References | 174  

### Auction Fraud

- Definition | 177  
- Online vs. Offline | 179  
- Types of Auction Fraud | 179  
- Auction Fraud Victims | 184  
- Cautionary Note | 185  
- Safe Bidding | 185  
- References | 187  

### Identity Theft

- Definition | 190  
- Looting Information | 191  
- Victimization | 193  
- Remedies | 194  
- Dealing w/ Credit Agencies | 194  
- Situation in Florida | 197  
- Preventative Measures | 197  
- References | 200  

### Urban Legends...

- Definition | 203  
- Chain Letters | 204  
- Urban Legends | 205  
- Rumors | 206  
- Hoaxes | 207  
- Security Issues | 209  
- Bogus E-mails | 209  
- Sample Letters | 210  
- Fear Factor | 211  
- Fact Checking | 212  
- Hidden Costs | 212  
- References | 214  

### Part V – Behavior-related Threats

- Wireless | 218  
- Definition | 218  
- 802.11 Standard | 218
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wireless Set Up</td>
<td>220</td>
</tr>
<tr>
<td>Security Risks</td>
<td>222</td>
</tr>
<tr>
<td>Wireless Attacks</td>
<td>224</td>
</tr>
<tr>
<td>Securing WLANS</td>
<td>226</td>
</tr>
<tr>
<td>References</td>
<td>228</td>
</tr>
<tr>
<td>Instant Messaging</td>
<td>230</td>
</tr>
<tr>
<td>Definition</td>
<td>230</td>
</tr>
<tr>
<td>How IM Works</td>
<td>231</td>
</tr>
<tr>
<td>IM Services</td>
<td>232</td>
</tr>
<tr>
<td>IM Threats</td>
<td>232</td>
</tr>
<tr>
<td>The Future</td>
<td>235</td>
</tr>
<tr>
<td>References</td>
<td>235</td>
</tr>
<tr>
<td>Chat Rooms</td>
<td>237</td>
</tr>
<tr>
<td>Definition</td>
<td>238</td>
</tr>
<tr>
<td>Chat Room Basics</td>
<td>242</td>
</tr>
<tr>
<td>Online Predators</td>
<td>243</td>
</tr>
<tr>
<td>Danger Online</td>
<td>243</td>
</tr>
<tr>
<td>Warning Signs</td>
<td>243</td>
</tr>
<tr>
<td>Safe Chatting</td>
<td>245</td>
</tr>
<tr>
<td>The CHAT Test</td>
<td>247</td>
</tr>
<tr>
<td>References</td>
<td>247</td>
</tr>
<tr>
<td>Cyberstalking</td>
<td>249</td>
</tr>
<tr>
<td>Definition</td>
<td>249</td>
</tr>
<tr>
<td>Online vs. Offline Stalking</td>
<td>250</td>
</tr>
<tr>
<td>Nature and Extent</td>
<td>252</td>
</tr>
<tr>
<td>Stalker Motivation</td>
<td>253</td>
</tr>
<tr>
<td>Cyberstalking Toll</td>
<td>254</td>
</tr>
<tr>
<td>Avoid Becoming a Victim</td>
<td>255</td>
</tr>
<tr>
<td>Anti-Cyberstalking Tips</td>
<td>255</td>
</tr>
<tr>
<td>References</td>
<td>257</td>
</tr>
<tr>
<td>P2P File Sharing</td>
<td>259</td>
</tr>
<tr>
<td>Definition</td>
<td>259</td>
</tr>
<tr>
<td>How P2P Works</td>
<td>259</td>
</tr>
<tr>
<td>Exemplars</td>
<td>260</td>
</tr>
<tr>
<td>Why P2P is Dangerous</td>
<td>263</td>
</tr>
<tr>
<td>Computer Check</td>
<td>264</td>
</tr>
<tr>
<td>How NOT to Get Sued...</td>
<td>265</td>
</tr>
<tr>
<td>Legal Implications</td>
<td>267</td>
</tr>
<tr>
<td>Down- / Up-loading</td>
<td>267</td>
</tr>
</tbody>
</table>
The LOCATE Test
References

Harmful Content
Definition
Offensive Content
Illegal Content
Avoiding Inappropriate Content
Tips for Safe Viewing
The Basics of Content Filtering
Internet Filtering Programs
No Tool is Perfect
References

Part VI – Additional Safeguards

Passwords
Definition
Password Security
Password Vulnerability
Password Attacks
Password Rules
How to Make Strong Passwords
For Added Protection
Managing Passwords
Password Protected Screensavers
References

Firewalls
Definition
Types of Firewalls
Ports
How Firewalls Work
Limitations of Firewalls
The PORT Test
References

Maintenance
Definition
Weekly Tasks
Semi-Annual Tasks
Hard Drive Disposal
Backups 317
Backup Principles 319
Storing Assets 321
The FORMS Test 321
Patches 323
The Attack-and-Patch Cycle 323
Patch Management 325
The BUT Test 326
Policies 327
Best Practices 329
References 331

Glossary 336
Index 341
# List of Tables

1. Authentication Procedures  
21
2. Attack Vectors  
21
3. Basic Network Tools  
38
4. Virus Types  
94
5. Internet Cons  
151
6. Florida ID Theft Victims  
198
7. Strong Passwords  
294
8. TCP/IP Services and Ports  
305
List of Figures

1  DoS Configuration  42
2  Malware Trends  144
3  Sample Nigerian Scam Letter  156
4  Phishing Attack Trends  163
5  ID Theft (National) Trends  199
6  Wireless Communication Modes  219
7  Warchalking Symbols  225
8  A Generic Firewall Set Up  303
9  The Bathtub Curve  319
Disclaimer

For current, revised up-dates and advisories, please visit on a regular basis, the Secure Florida website <www.secureflorida.org>. Our mission is to provide information and solutions dealing with computer technology issues to the citizens of the State of Florida.

The information contained in the C-SAFE Training materials and the Florida Cyber-Security Manual deals with computer technology issues. Due to the rapidly changing nature of computer technology and our reliance on information provided by outside sources, Secure Florida does not warranty or guarantee the accuracy or availability of the content referenced in the printed documents, located on the website or any references made to sites to which we link.

In no event will Secure Florida be held liable to any party for any damages arising in any way out of the availability, use, reliance or inability to use Secure Florida website, or for any claim attributable to errors, omissions, or other inaccuracies in, or destructive properties of, any information provided by or through the Secure Florida website and the C-SAFE training and educational materials.

Secure Florida does not endorse or recommend any specific product or vendor. We present answers to informal security questions and solutions to problems. All products discussed or referenced, and all websites cited, are to be considered as examples only.

Secure Florida has provided links and pointers to Internet sites maintained by third parties. Secure Florida does not operate or control in any respect any information, products or services on these third-party sites. Secure Florida does not endorse these sites or any of their sponsors. The materials in this site and the third-party sites are provided "as is" and without warranties of any kind either express or implied. To the fullest extent permissible pursuant to applicable law, Secure Florida disclaims all warranties, express or implied, including, but not limited to, implied warranties of merchantability and fitness for a particular purpose. Secure Florida does not warrant that the functions contained in the materials will be uninterrupted or error-free, that defects will be corrected, or that this site, including bulletin boards, or the server that makes it available, are free of viruses or other harmful components. Secure Florida does not warrant or make any representations regarding the use or the results of the use of the materials in this site or in third-party sites in terms of their correctness, accuracy, timeliness, reliability, or otherwise. You (and not Secure Florida) assume the entire cost of all necessary maintenance, repair, or correction.

This agreement shall be governed by and construed in accordance with the laws of the State of Florida without giving effect to any principles or conflicts of law.

Part I

Fundamentals
Overview

Objectives

The C-SAFE Program and the *Florida Cyber-Security Manual* have three main goals: (i) to increase your awareness about cyber-security issues and what steps you can take to safeguard your network, your computer and your assets; (ii) to share the latest information on state-of-the-art tools and techniques that will help reduce your risk of becoming a victim of cybercrime; and finally, (iii) to introduce you to a virtual treasure trove of online resources that can be found at the Secure Florida website <www.secureflorida.org>.

To keep informed about technical and legal issues concerning Florida residents, we encourage you to visit the Secure Florida website on a regular basis. Better still, register to become a member of Secure Florida and security news and advisories will be sent directly to your e-mail account.

Secondly, we would like you to know that we have developed the C-SAFE Program in the hopes that you will share what you learn—with family, colleagues, and friends—so they too can begin the process of becoming safe and secure “cyber” citizens.

Finally, we are always happy to obtain feedback about the C-SAFE Program, the Secure Florida website and the training materials we are in the process of developing. 
If you have suggestions on how we might improve any of our deliverables, we would very much like to hear from you. Likewise, if you find any errors, omissions, or discrepancies, we would appreciate it, if you bring those to our attention too. To find out how you can to contact us, please visit the Secure Florida web site <www.secureflorida.org>.

Caveats

Not surprisingly, we are very enthusiastic about the C-SAFE Program and the range of resources that we have been able to compile on your behalf. However, we would be remiss if we didn’t point out a number of caveats.

The first thing to keep in mind as you work through the Florida Cyber-Security Manual is the adage: “there is no there, there.” Instead of treating security as a destination, an end-point or a fait accompli—as we were inclined to do in the past—we now need to think of security as an on-going process. In a post-9/11 world, we need to be constantly on the look out for recurring vulnerabilities and new threats.

Unfortunately, this raises the second caveat. While we have tried to be comprehensive without being overwhelming, each section in the Florida Cyber-Security Manual is presented as a stand-alone document. To the extent possible, we have tried to limit any context-specific cross-references and in the instances where it couldn’t be avoided, we have made a notation that points you to the corresponding section(s). As such, there is no need to read the manual sequentially. Secondly, be aware that C-SAFE is a work-in-progress and we will be updating our materials with each new iteration of the program which explains why, in addition to having you visit the Secure Florida website on a regular basis, we have included a
version number so you can more easily keep track of any additions/revisions.

Thirdly, by the time you read this, you will no doubt discover that some of the links are broken or some of the websites/webpages have been (re)moved. For that reason, we recommend that if you want to learn more on a particular topic, you start your inquiry by visiting the Secure Florida website. Not only can all of the URLs listed in the manual be readily accessed at <www.secureflorida.org> but new ones (that have not been included in this version of the manual) are being added every day.

Outline

The Florida Cyber-Security Manual is organized into six sections. Section one provides an overview of cybercrime and security issues.

Section two focuses on network-related threats. The topics covered are denial of service (DoS) attacks, spoofing, e-mail spam and how to read e-mail headers.

Section three looks at computer-based risks. Here, the focus is on the types of attacks most commonly associated with malware (e.g., viruses and worms), underware (e.g., Trojan Horses, spyware) and blended threats.

In section four, asset-related threats, the major concern for most Florida residents who use the Internet is identity theft. In order to understand why anyone would want to steal your identity, we review the various scams that have been perpetrated in this state and what you can do to minimize your risk profile. Topping the list of Internet cons covered are: (i) Nigerian scams, (ii) phishing, (iii) auction fraud and (iv) identity theft. Then we cover urban legends, rumors and hoaxes. This is
followed by a brief review some of the hazards associated with these types of mass mailings.

Section five assumes a slightly different tack. Instead of concentrating on network and computer-based vulnerabilities, the next to last section focuses on harmful behavior that is enabled by the Internet and Web. The topics in this section are broken down into two sub-sections. The first part deals with wireless, instant messaging and the dangers of chat rooms and the second part looks at newly emerging patterns of behavior (e.g., cyber-stalking, P2P file sharing, and the proliferation of offensive and illegal content).

Finally, given the current state of the art, section six provides a number of guidelines and makes recommendations on how “best” to secure your network, computer and assets. The topics covered are: (i) passwords, (ii) firewalls, (iii) maintenance, backups and patches. Finally, the last section wraps up with a brief summary of Secure Florida “best practices.”

References


Internet: A Tool for Empowering People in the Information Age, The

Secure Florida
Security

“Good programmers write good code, bad programmers write bad code, but all programmers seem to write insecure code.” – Marcus J. Ranum

“Trust is hard to build and easy to lose: a single violation of trust can destroy years of slowly accumulated credibility.” – Jacob Nielson

Definition

A typical computer-based system has objects i.e., hardware and software resources that are comprised of processors, memory, storage, network bandwidth, and so on. Subjects (users, entities or processes executing on behalf of users) access and use these objects usually through well-defined interfaces.

There is no agreed upon definition for security. For the purposes of this Manual, security is loosely defined as the protection and detection of “unauthorized” access or “illegal” actions directed towards computer-based systems. The main thing to remember: security is a process, not a product and while traditional preventive security products go a long way to securing computer networks, but they can never close the window of exposure. All existing systems are vulnerable to attack.

In the context of cybercrime, traditionally, most security efforts have been are directed towards:

- Computers—the protection of files from direct attacks that take advantage of vulnerabilities in the system architecture; and
• Communications—the protection of information against passive attacks that occur during transmission.

A security policy is a set of rules written in general terms that describes the security requirements of a system. It states what is permitted and what is not permitted and regulates how resources or digital objects are to be used and by whom.

A security violation is any action that violates the “rules” that have been written down in the security policy.

Protection mechanisms (“how”) allow for the enforcement of policies (“what”).

Computer-based systems are considered “incident-free” when they can be used as intended. In general, a secure system will enable anyone with authorized access to:

• Verify the identities of all entities (e.g., other users and system services) while operating the system.

• Safeguard sensitive information (e.g., personal data, cryptographic keys, passwords, etc.) during storage, transmission, and use.

Elements of Security

While it is difficult to come up with a precise definition, depending on the context, one or more of the following elements are used to establish trust:
Availability—Is the system functioning when you need it. Availability is concerned with the prevention of unauthorized withholding of information or resources.

Authorization—Who will be given access? The process of allowing only authorized users access to sensitive information. An authorization process uses the appropriate security authority to determine whether a user should have access to resources.

Authenticity—How do I know who sent this? For most online transactions, businesses will want to know that the person conducting the transaction is who they claim to be. For example, only authorized signatories should be able to access a business bank account.

Integrity—Has the data/information changed? Integrity deals with the issue of how to preserve digital objects to make them trustworthy, i.e. how to avoid the unauthorized modification of objects.

Non-repudiation—How do I know that the sender won’t deny sending this?” Users need certainty that a transaction conducted over the Internet is irrevocable, and that the person who conducted the transaction will not be able to deny (at a later date) that the transaction never took place.

Privacy and Confidentiality—How do we keep secrets secret? It involves the assurance that data are not disclosed to unauthorized persons, processes, or devices and sensitive information is not leaked as a result of physical, technical or electronic penetration and exploitation.
Verification Processes

Authentication is the process of verifying that someone is, who he or she claims to be. For most online systems, authentication is based on a user ID and password. Table 1 shows a breakdown of the different types of authentication techniques based on the level and type of security required.

Note that the process of authentication does not grant the user access rights to resources. This is accomplished through the authorization process.

Threats

Regardless of the type of system or platform you may be using, all computers are subject to misuse and vulnerable to attacks.

Vulnerabilities are loopholes that attackers can use to gain access to computer- or network-related resources and they represent a “potential for unintended use.”

Common types of system damage include the following:

- Leaking (reading, say) of sensitive data
- Modification of sensitive data
- Destruction of sensitive data
- Unauthorized use of a system service
- Denial of a system service, and
- Disruption or degradation of any system operation in general
Table 1
Authentication Procedures

<table>
<thead>
<tr>
<th>Based on</th>
<th>Criterion</th>
<th>Techniques</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name(s)</td>
<td>How someone or something is called.</td>
<td>Certificates/identification issued by an authorized source/entity; someone willing to vouch for one's identity.</td>
</tr>
<tr>
<td>Attribute(s)</td>
<td>Characteristics owned/ acquired.</td>
<td>Certificates/identification issued by an authorized source/entity; someone willing to vouch for one's identity.</td>
</tr>
<tr>
<td>Token(s)</td>
<td>Something possessed.</td>
<td>ID badge with a photograph on it; keys, cards, etc.</td>
</tr>
<tr>
<td>Knowledge</td>
<td>Something known.</td>
<td>Password/Passphrase, personal identification number (PIN).</td>
</tr>
<tr>
<td>Anatomy (internal)</td>
<td>DNA, skull typography, skeletal injuries, earlobe patterns, hand geometry, DNA.</td>
<td>Body scans (retina, ear, face); finger and hand prints.</td>
</tr>
<tr>
<td>Appearance (external)</td>
<td>Height, weight, skin/hair/eye color, physical markings, race, gender.</td>
<td>Verified by still images and measurements.</td>
</tr>
<tr>
<td>Social Behavior</td>
<td>Interactions with other people.</td>
<td>Film showing habituated body signals, voice characteristics, and keystroke patterns.</td>
</tr>
<tr>
<td>Bio-dynamics</td>
<td>How something is done.</td>
<td>How a signature is written; statistically-analyzed voice characteristics.</td>
</tr>
<tr>
<td>Tracking Devices</td>
<td>Where someone/thing is located in time and space.</td>
<td>Physical restraints, e.g., dog tags, collars, bar codes, bracelets/anklets, embedded microchips and transponders.</td>
</tr>
</tbody>
</table>
The key point to remember is that a vulnerability is NOT an attack, but rather a weak point that is exploitable. Hackers exploit vulnerabilities in order to achieve some goal—to gain control of, damage, or bring down a device or network.

Examples of system vulnerabilities that attackers take advantage of:

*Protocol design*—attackers can take advantage of weaknesses in communication protocols to gather information and eventually gain access to systems they are monitoring.

*Commands revealing sensitive information*—Unix commands such as “finger” can reveal account information that attackers can use to break into a system.

*Asynchronous transfer mode (ATM)*—using a technique called “manhole manipulation.” In order to compromise security, attackers obtain direct access to network cables and connections in underground parking garages and elevator shafts.

*Software bugs*—programmers can never track down, much less eliminate, all of the vulnerabilities that are located in code. To mount an attack, hackers need only find one vulnerability (e.g., buffer overflows).

In contrast to vulnerabilities, security threats can be likened to potential violations (malicious or otherwise) of security and they exist because of the weaknesses found in most systems.

There are two basic types of threats:

1) *Accidental Threats* are non-malicious and they result from: (i) the inadvertent exposure of confidential information (e.g.,
clients’ social security numbers are posted to a website), (ii) a system malfunction that causes an illegal state to occur (e.g., a disk full error that causes a harddrive to be overwritten); or (iii) a natural disaster (e.g., damage caused by hurricanes, floods and/or fire).

2) *Intentional Threats* are malicious and it is the result of (i) deliberate harm against a computer (e.g., the destruction, corruption, modification, fabrication, interruption or interception of data). or (ii) security violations (e.g., unauthorized access, electronic fraud, and/or hijacking accounts).

While there are many variations of specific attacks and attack techniques (these will be covered in detail in the remaining sections), it is useful to think about threats in terms of what the attacker is trying to achieve. This changes your focus from the identification of every specific attack—which is really just a means to an end—to focusing on the end results of possible attacks.

**Critical Success Factors**

In order to maintain a safe environment, security is function of three interrelated actions:

1) *Prevention*—involves polices that prevent resources or information from being damaged, altered or stolen. Preventative measures can range from locking disks in file cabinets to establishing high-level security policies that spell out actions to be take in the event of a security breach.
2) *Detection*—involves reporting mechanisms that allow authorized personnel to detect: a) when resources or information have been damaged, altered, or stolen, b) how they have been damaged, altered, or stolen, and c) who or what entities have caused the damage. Detection mechanisms can range from ad hoc inquiries to automated tools that monitor the system for any signs of intrusions, damage or alterations, and any evidence of malware.

3) *Response*—involves the recovery of resources or information, even if lost or damaged. Reaction time is based on how quickly someone can recover from an incident. In a system where dependability is mission critical, the system must be protected against both intentional and unintentional threats. Bear in mind that to the end user, there is not a huge difference between someone deliberately disconnecting the power to a system, someone doing it by mistake or a hardware failure that disconnects the system. All three situations amount to the same thing: a failure to operate. On the other hand, from a security perspective, there is a big difference and depending on the nature of the incident, a totally different reaction would be warranted.

In conclusion, good security is based on prevention, detection, and response. Preventive countermeasures provide defense in two ways: they provide a barrier to overcome, and they force the attacker to spend time overcoming the barrier. For the remainder of this Manual, we will be covering a number of countermeasures you can use to secure your computer, your assets and your person.
References


Home Network Security


Attacks

Definition

An *attack* is defined as an action (unfriendly or vengeful) that is taken with the express purpose of harming an asset or violating security. It represents an intentional threat. For example, an attack might produce the destruction, modification, fabrication, interruption or interception of data. Similarly, a system breach might result in the disclosure of confidential information, the defacement of a website or the disruption of service.

In contrast, actions that are taken to reduce the harm caused by an attack and/or to mitigate the effect of an attack is considered a countermeasure. One of the main objectives of the *Florida Cyber-Security Manual* is to encourage users to do whatever they can to neutralize the effect:

- **Attacks are destructive.**
- **Attacks cost money.**
- **Attacks result in a loss of confidence;**
  and
- **Attacks make it harder to do business.**

of cyberattacks.
Attackers generally have deliberate motives for doing what they do:

- Monetary
- Extortion
- Revenge
- Vandalism
- Political
- Terrorism
- Espionage
- War

For example, an attacker might install a keylogger so they can steal personal data for ID Theft; or, they want to disrupt the flow of traffic to bring down a website as part of a grudge match; and/or, they want to gain unauthorized access to a wireless network so they can send non-traceable e-mails). Based on a determination of the primary motivation for breaking/entering, an attacker can generally be classified as one of the following:

- Competitor
- Disgruntled Worker
- Enemy Country
- Explorer
- Hacker for Hire
- Hacktivist
- Script Kiddie
- Spy
- Terrorist
- Thief

Finally, to accomplish their goals, most attackers make use of a variety of tools and techniques (most of which can be downloaded from the ‘Net) to exploit vulnerabilities and circumvent security. For example, they may use scripts/automated programs to harvest personal data; launch distributed denial of service (DDoS) attacks to close down a website, and breach security using low-tech methods, e.g., dumpster diving or social engineering.

Finally, please note that more detail on attacker exploits and methods is covered in subsequent sections of the Florida Cyber-Security Manual.
Vectors vs. Payloads

The term “vector” is derived from biology. It refers to any agent that carries and transmits a disease—*Typhoid Mary* is generally cited as the classic example.

In the context of security, an attack vector is the specific method or route used to gain entry into a computer or network. To do this, attack vectors take advantage of vulnerabilities (e.g., exploiting system defects) and deception (e.g., commandeering the human element) to get past system defenses.

Strictly speaking, not all vectors are threats—an e-mail attachment only becomes a threat when it is carrying an executable that contains malicious code and a hoax only becomes a threat when someone acts on the information.

Secondly, be careful that you don’t confuse the term “payload” with “vector.” A payload is the malicious activity (code) that is carried or transmitted by the vector and some attacks are able to deliver multiple payloads (*aka* warheads).

For example, a virus is often the attack vector as well as carrying the payload. A worm is always the attack vector. However, it can carry a virus as the payload. Trojan horses are always payloads, as are spyware, dialers, hijackers, etc.

To help keep the two terms straight, consider the following analogy:

The attack vector is the “truck: (i.e., the mode of delivery) and the payload is the “stuff in the back of the truck” (i.e., the platform or the cargo bay).
A “trigger” is the condition that causes the payload to activate. Some payloads will trigger on a certain date whereas others will depend on the availability of an Internet connection or the execution of certain program. Sample payloads include:

**Violation of privacy**—passwords, credit card numbers etc. sent over Internet;

**Impersonation**—spoofing i.e., sending messages as if they are coming from you;

**Corruption**—deleting and/or trashing data and system files;

**Damage**—reprogramming the BIOS so a machine cannot boot; and

**Denial of service**—interference with website functionality.

### Types of Attacks

Attacks can be: (i) direct vs. indirect or (ii) active vs. passive (see Table 2 for a mapping of representative cybercrimes).

**Direct Attack**—is an assault aimed directly at the target, with little or no subterfuge involved. For example, an online intruder might break into a database and steal credit card numbers. In addition, several components of a system may be attacked before the intended (final) target can be breached. For example, prior to breaking into the database, the attacker might steal the password file.

**Indirect Attack**—in this type of covert/stealth operation, information is received from or about the target of the attack without actually attacking the target itself. For example, an attacker might use a sniffing device to derive
confidential information about a “competitor” or a “rival” without breaking into the target’s information systems.

Table 2
Attack Vectors

**Active**

<table>
<thead>
<tr>
<th>Active</th>
<th>Indirect</th>
<th>Direct</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trojan Horses</td>
<td>Viruses</td>
<td></td>
</tr>
<tr>
<td>Spyware</td>
<td>Worms</td>
<td></td>
</tr>
</tbody>
</table>

**Passive**

**Active Attack**—is a direct strike that is designed to change system behavior in some way. For example, an attacker might recode a piece of software or insert a piece of code into existing software in order to modify or delete existing data. Similarly an attacker might deliberately tamper with system software causing it to fail.

**Passive Attack**—in this type of online foray, no attempt is made to breach security. Instead the attacker monitors a system in order to steal information or snoop on the activities of the target. In general, this type of attack is very hard to detect.

Given the nature of the intrusion, the attacker does not need to interact with or disturb normal system functions. As a result, a
significant amount of time might elapse before the target of the attack realizes that his/her system has been compromised. Monitoring network traffic/CPU/disk usage is a classic example of a passive attack.

However, not so long ago, it was possible to differentiate between attack scenarios that are designed to: (i) steal or divert data, (ii) corrupt data or programs, (iii) bring down systems, or (iv) make network components inaccessible.

In today’s hostile environment, the newest attack vectors are being designed to do all of the above. What’s more, some of the newest attack vectors are “polymorphic” which means they can change characteristics as they propagate.

An attack that starts out as a nuisance might (with provocation) transform into a lethal threat. For example, the release of a worm that is capable of morphing into a Trojan Horse that will emerge as a stealth virus—should it be detected).

In our opinion, attackers, regardless of intent, are all one and the same. Anyone who breaches security is and should be treated as hostile. For the reminder of the Manual, no distinction is made between a “script kiddie” who seeks unauthorized access for fun vs. a “spacker” who does so for profit. They are ALL engaged in unethical and/or illegal behavior. Likewise it will soon become clear that several types of attacks that we cover have nothing to do with computers or technology. This is because most attackers depend on users to help facilitate the attack (ergo, social engineering).
Anatomy of an Attack

Individual circumstances notwithstanding, the recipe for most online attacks is based on:

\[ \text{Goal} + \text{Method} + \text{Vulnerabilities} = \text{Attack} \]

and an online attack follows a fairly predictable pattern. The standard methodology for an online attack is:

**Survey and assess**—attackers will monitor the activities of potential targets in order to identify and assess system vulnerabilities and expose possible points of entry. Once they have completed their reconnaissance (e.g., ping sweeps, DNS zone transfers, TCP or UDP port scans, and/or indexing of public web servers to find cgi holes), they will use the information gathered during this phase to plan an attack.

**Exploit and penetrate**—after having cased and selected a potential target, the next step is to capitalize on an exploit (if possible) and attempt to gain entry into the system. If the backgate is locked down (i.e., the network and host are fully secured), the attacker will try to get in through the front door. They will do this by using deception (e.g., social engineering) or else, they will use the same modes that legitimate users use. For example, they may gain entry through an application’s that does not require authentication or they might take advantage of a known loophole.

On the other hand, instead of grappling with the firewall, most attackers can take advantage of port 80, especially if proper security patches have not applied. Once an
attacker is in, they can then use commonly available hacker tools to quickly defeat the soft internal security. Once that happens, it’s game over. The target system has been hacked!

**Escalate privileges**—after a system has been compromised, the attacker will immediately seek out the highest level of permissions/rights in order to upgrade their privileges. In particular, they will look for user accounts (non-root) that have been given administration privileges and then attempt to parlay them into higher levels of access.

**Maintain access**—after having gained access, an attacker will take steps to make future access easier (e.g., by planting back-door programs or by using dormant accounts that lack strong password protections) and s/he will attempt to cover his/her tracks by hiding tools and cleaning log files.

Finally, in the event that would-be attackers do not or cannot gain access to a potential target, they will often retaliate by mounting a denial of service attack. While the point of this maneuver may be the goal of the attack, usually it is carried out as a kind of grudge-match to prevent other users from getting access to the target of the attack.

**References**


Academic Computing And Communications Center (2000) ”Spoofing and Sniffing,” The A3C Connection, posted January/February/March 2000, URL: http://www.uic.edu/depts/


Networks

“Network security is a complicated subject, historically only tackled by well-trained and experienced experts. However, as more and more people become ‘wired’, an increasing number of people need to understand the basics of security in a networked world.” – Matt Curtin

**Definition**

A network is defined as a group of two or more computer systems linked together. The most common networks are:

*Local-area networks (LANS)*—LANs are made up of computers (physically close together) that are connected (by cable) into a single network (for example, the computers might be located in a single building or department).

*Wide-area networks (WANs)*—WANs are made up of computers that are farther apart (geographically separated) that are connected by telephone lines or fiber optics (for example, the computers might be located in different regions of the country or in different parts of a city).

*Internet (‘Net)*—the ‘Net is a global network comprised of a series of nodes (access points) interconnected by communication paths. The Internet is considered to be the largest network whose ownership is shared amongst different entities (governments, public/private corporations, schools/colleges/universities) and is spread across myriad locations (international, national, regional, and local).

*Virtual Private Networks (VPNs)*—VPNs are private data networks built on top of the Internet. Hosts within a VPN use “encryption” to talk to other hosts; hosts outside the VPN
are excluded (even though they are using a public network). In this way, a VPN ensures that only authorized users can view or “tunnel” into the private network.

Other criteria used to characterize networks are:

- **Topology**—the geometric arrangement of devices on the network. Common topologies include a bus, star, and ring. For example, devices on a LAN can be arranged in a straight line.

- **Protocol**—the common set of rules and signals computers use to communicate on a network. For example, the web uses the HTTP protocol, file transfers use FTP and the Internet uses TCP/IP.

- **Architecture**—networks can be broadly classified as using either a client-server (many-to-one) or a peer-to-peer (one-to-one) architecture.

- **Media**—devices can be connected to a network using twisted-pair wire, coaxial cables, or fiber optic cables. Some networks communicate via radio waves.

In addition, networks can be classified in terms of who can use the network (open or closed), whether it carries voice, data, or both kinds of signals; the issue of ownership (public or private); and what type of connection (dial-up or switched, dedicated or non-switched, or virtual connections) is required for access. To learn the more about network variations and the types of equipment needed to set up a network, visit the Secure Florida website <www.secureflorida.org> and click on the “Networks” link.
Network Components

The main components that are necessary to run a network are:

- **Router**—this device hooks multiple computers to one Internet connection by sending data between the Internet and the correct computer.

- **Network Interface Card (NIC)**—a NIC is an expansion board (network adaptor) that is inserted into your computer so it can be connected to a network.

- **Ethernet Cable**—the most common Ethernet cable is Category 5 or CAT5 and it supports both traditional and fast Ethernet. The Ethernet connectors, look like a RJ-45 connector that is used with telephones, except that it is slightly wider.

In addition, before you can get connected to the Internet, you must set up an account with an Internet Service Provider (ISP). These days, there are a wide range of companies and organizations who operate as either stand-alone ISPS (e.g., cable companies, phone services, service providers such as AOL, MSN) or they may be schools, businesses or community networks who have online resources you can access. In the latter case, you may be required to set up a separate wireless or broadband connection in order to get online access.

For the audience of this Manual, it is assumed that you are connected to the Internet and have already set up an Internet account through an ISP. If you are new to the ‘Net and not sure how do this, visit the Secure Florida website <www.secureflorida.org> to learn
what steps you need to take in order to get online.

Internet Backbone

The Internet backbone is the equivalent of an interstate highway that spans the globe and moves large amounts of data that travel vast distances at high speeds. The Internet Backbone (aka the M-Bone) consists of three interacting components:

1) Phone lines and cables make up the channels along which information travels.

2) Network Service Providers provide high-speed Internet access and services for Internet Service Providers (ISPs), who then make these services available to individual Internet subscribers.

3) Network Access Points (NAPs) allow messages to 'hop' or transfer from one network to another. NAPs provide the connectivity that links privately and publicly owned networks.

The interoperation of these three components facilitate the seamless movement of digital goods and services.

Internet Addresses

A “typical” user is most likely to encounter the following types of Internet addresses:

E-mail Address—the e-mail address is easily recognizable and usually takes the form of:

userID@hostname.TLD /

or
info@secureflorida.org.

**IP Address**—IP stands for “Internet Protocol” and it is used to identify the location of a computer on the Internet. Every computer on the Internet is assigned an IP address that uniquely identifies each machine or device that is being used to access the Internet, regardless if it is through a dial-up modem or a high speed connection (e.g., ISDN, cable, DSL, ADSL, T1, etc.)

The IP address takes the form of a dotted-quad number and looks something like:

```
xxx.xxx.xxx.xxx
```

or

```
128.175.13.92.
```

**Web Address**—This is also referred to as a domain name or a Uniform Resource Locator (URL). In the USA, the most common top level domains (TLDs) are: .com, .org, .net, .gov, and .us. In recent years, the policy on setting up new TLDs have been relaxed and the number of registries have been expanded, so we are now seeing the emergence of new TLDs (e.g., .info, .biz, etc.)

A domain name usually takes the form of:

```
www.domain_name.TLD
```

or

```
www.secureflorida.org
```

However, other addressing information can be appended such information that indicates what object the address is referencing. For example, a URL might have one of the following extensions: .index (this usually indicates a
home page) or .htm / .html for an embedded webpage or it might end with .gif / .jpeg / .png to indicate that the object is a graphic and so forth.

Note that an assigned domain name maps directly to the IP address. Similarly, using a tool like nslookup (a DNS whois tool that performs forward/reverse DNS queries for a domain address and getting an IP address of a hostname and hostname of the IP address (for more details see below), the IP address that corresponds to a particular Domain Name and can be easily traced.

**Secure Sockets Layer (SSL)**

SSL creates a secure channel over which data can be exchanged. Because SSL is the most widely used standard, it is supported by Internet Explorer, Netscape, Mozilla and Opera, to name just a few of the mainstream browsers. To verify if a website is using SSL, look to see if there is a small padlock or key located in a top/bottom corner of the browser. If the padlock/key is closed/unbroken on the screen, the computer has successfully established a secure connection with the website. This means that the information you are sending across the Internet (e.g., personal details, order details, credit card details, delivery address and contact telephone numbers) has been encrypted any anyone who is attempting to intercept that information will not be able to read it.

Apart from the icons, using SSL is a fairly invisible process. The browser may display a warning message to let users know they are beginning or ending a secure connection. The only other clue that you can look for to see if the web page you are accessing is secure, is to
look for a web address that begins with https:// rather than http://.

To find out more about Internet addressing and naming conventions and how to secure online transactions, check out the Secure Florida website <www.secureflorida.org>.

**Network Tools**

A set of networks tools are readily available (either they come pre-installed with your software or you can download directly off the Internet). The most common tools available to homes users are:

- **ping**—Are you out there?

  Use ping to determine whether a particular host machine is “alive.” Note that ping does not tell you what the remote machine does, what kind of machine it is or who it belongs to.

  Type:

  ```
  ping [host-name or IP-address]
  ```

- **traceroute / tracert**—How do I reach you?

  Packets of data sent over the internet seldom go directly from originator to recipient. Instead they may pass over any number of intermediary stops (host machines). The route packets takem, can sometimes be of interest, particularly if other tools fail to provide complete information about a suspicious host.

  For Unix-based machines, type:

  ```
  traceroute [host-name or IP-address]
  ```
For Windows-based machines, type:

```bash
tracert [host-name or IP-address]
```

The traceroute/tracert command sends out a packet of information to each device (called a node or hop) individually.

Note: an * indicates that a "hop" has timed-out

To illustrate, in Windows, go to the Start menu, choose Run and then type:

```bash
tracert www.fsu.edu
```

and the following output will be returned:

```
Tracing route to www.fsu.edu
[128.186.6.14] over a maximum of 30 hops:

  1  <10 ms  <10 ms  <10 ms  192.168.0.1
  2  <10 ms   10 ms  <10 ms  10.119.68.1
  3  <10 ms   10 ms   10 ms  172.30.89.209
  4  <10 ms   10 ms   10 ms  172.30.89.250
     .     .       .       .
     .     .       .       .
     .     .       .       .
```

- `nslookup`—I know your name, but what's your IP address?

If you enter a domain name, nslookup will return the corresponding IP address (assuming it exists).

Alternatively, if you enter a numeric IP address, nslookup returns the principal host name by which the machine is known

Type:

```bash
nslookup [host-name or ip-address]
```
Note: nslookup does not tell us whether the host is available or what it does, only what DNS returns is the name or address that corresponds to the address or name you supplied.

For example, you can use nslookup to test whether a host name given (one found in the routing header of an e-mail) actually corresponds to the IP address that has been assigned to it.

- **whois**—Who owns this domain?

  This utility enables you to obtain information about who has registered a domain name. Note that for reasons of privacy, a lot of Domain Name registries no longer openly post this information.

  If you are using a Linux/Unix-based system, it is available from the command line

  ```bash
  whois [host-name or domain-name]
  ```

  or this can be accessed from a website that provides these types of tools.

- **telnet**—How do I access a site safely?

  You can use this utility to fetch a page, however note that a lot of ISPs, for security reasons, will not allow telneting into their sites.

  To use telnet, you need to:

  1) issue the telnet command, giving the port option:

  ```bash
  telnet [web-server-name-or-ip] [port-number]
  ```
2) after the connection is made, use the HTTP command "GET" (upper case). For example, type:

GET [/file-to-get]

- **curl**—How do I surf / retrieve files safely?

The utility command curl [URL] can fetch files using HTTP, FTP, and WAIS.

The curl command is usually included w/ most Linux distros, but you can also obtain it from http://curl.hazz.se/

With curl (as opposed to telnet) you can redirect standard output to a file.

- **Obfuscated URL Decoder**—How do I deconstruct this URL?

To perform this operation, you need to access tools that are resident on a website. “HayWyre” is an example of a javascript tool that spammers use to encode their pages in order to make them less human-readable and harder to track back to their source. You can use the “HayWyre Nullifyer” to decode an obfuscated webpage. Note that the URL for this script can be found at Secure Florida <www.secureflorida.org>.

**Network Toolkit**

Network tools are your first line of defense when trying to locate the origin of a suspicious e-mail (e.g., spam or phishing). Table 3 contains a listing of how you can find the information you need (e.g., to forward to an ISP in order to get an account closed or a website terminated) using freely available tools.
## Table 3
### Basic Network Tools

<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Use...</th>
</tr>
</thead>
<tbody>
<tr>
<td>...find out whether anyone is online and responding to IP communications</td>
<td>ping [IP or hostname]</td>
</tr>
<tr>
<td>...find out the IP address of a host (or the host name associated with an IP address)</td>
<td>nslookup [IP or hostname]</td>
</tr>
<tr>
<td>...trace the network route to a host</td>
<td>traceroute [IP or hostname]</td>
</tr>
<tr>
<td>...find out who controls a given IP address</td>
<td>whois -h [RIR] [IP]</td>
</tr>
<tr>
<td>...find out who has registered a given domain name</td>
<td>whois [domain] whois -h [registrar] [domain]</td>
</tr>
<tr>
<td>...find (maybe) abuse contacts registered at abuse.net</td>
<td>whois -h whois.abuse.net [host]</td>
</tr>
<tr>
<td>...download the raw contents of a web page safely without using a browser</td>
<td>curl [url] telnet [host] 80 [...] GET [page]</td>
</tr>
<tr>
<td>...decipher a hard-to-read URL</td>
<td>run [javascript]</td>
</tr>
</tbody>
</table>

To conclude, please be advised that network security is beyond the scope of this basic Manual and thus, won’t be discussed in any great detail, except in the sections on Denial of Service and Wireless networks. More “advanced” topics that deal with the issue of how to secure your home or small business network, can be found at the Secure Florida website <www.secureflorida.org>.
References


Networking 101
URL: http://compnetworking.about.com/od/basic_networking_concepts/ Last Visited: July 18, 2004.

networking

Networks

Part II

Network-related Threats
Denial of Service

“Today, online criminals use stolen credit card numbers as illicit currency. The information is traded for other commodities, such as Social Security numbers or access to networks of compromised PCs that can be used in distributed-denial-of-service (DDoS) attacks.”
- Dennis Fisher

Definition

Denial of service (DoS) attacks (originating from a single computer) and distributed denial of service (DDoS) attacks (originating simultaneously from several computers) take place over the Internet. DoS attacks can have a malicious intention, or they can occur accidentally through user/system administrator or even programming error.

While there many different types of attacks or exploits that can be mounted against public/private organizations (more on that later), DoS attacks are usually designed with a single purpose: to disable the legitimate use of a service in order to cause disruption and inconvenience. Success is usually measured by how long the chaos lasts.

Examples of DoS attacks include:

- Saturating network resources to prevent users from accessing network.
- Crashing connections between two computers to disable communications.

Basically, most DoS/DDoS attacks can be divided into three categories:
1) *Consumption of scarce resources*—these attacks work by opening many connections simultaneously.

2) *Destruction or alteration of configuration information*—these attacks work by altering routing table contents, and redirecting network traffic.

3) *Physical destruction or alteration of network components*—these attacks work by deleting/changing information or by creating power interruptions.

**DoS Structure**

The critical components that are necessary to for a DoS/DDoS attack to take place are as follows (see Figure 1 for a graphical depiction of the hardware setup):

- The **client** is the machine from which the hacker coordinates the attack.

- The **handler** is a compromised host with a special program running on it. These machines (between three and four) are under the attacker's direct control. They act like “generals on a battlefield” to carry out the attacker's orders and each handler is capable of controlling multiple agents.

- The **agent** represents a compromised host that also runs a DoS program. On cue, agents (*aka* broadcasters or zombies) unleash the denial of service attack. Numbering in the thousands, these machines act like the “foot soldiers in the infantry,” since they are responsible for running the code that figures in the attack.
DoS Configuration

In order to mount a successful DDoS attack, the attack needs to compromise several hundred to several thousand hosts. Using automated tools, a DoS attacker will:

- **Initiate a scan phase**—a large number of hosts (100,000 or more) are probed for weaknesses. Using port scanning software, the attacker will try to appropriate root privileges.

- **Exploit known vulnerabilities**—e.g., hackers will use dictionary and brute force attacks or download a Trojan to gain a foothold on the user’s machine.

- **Install DoS tools**—these tools will remain dormant until the time of the attack.

- **Iterate and redeploy**—the attacker will use the “hostages” to scan and compromise additional hosts.

Because the process is automated, it takes less than 5 seconds for an attacker to disable an unsuspecting host and install the attack tools. This means that: (i) thousands of poorly secured machines can be commandeered in less than an hour and (ii) even unskilled
individuals (programming-wise) can launch fairly sophisticated attacks.

Once the attack vectors are in place, a DoS attack presents an almost unstoppable threat. Because the attack originates from many different machines, would-be victims must completely disconnect from the Internet or deny access to all clients (both legitimate and non-legitimate) in order fully protect themselves.

**Implications**

As a rule, most DoS attacks do not result in the theft of information or the destruction of hardware/software. Nor do they affect the confidentiality and/or the integrity of the data. Nevertheless, these attacks tend to be quite devastating. A DoS attack can negatively impact the target (person or company) in terms of opportunity costs (i.e., lack of availability—customers go elsewhere; a tarnished reputation—rivals gain a competitive advantage, system outages—productivity suffers, and/or lost revenues—profit margins are squeezed). In most situations, the shut down is temporary, but in other cases, depending on how hard or how concentrated the hit, the website owner may be forced to cease operations.

Reasons behind DoS attacks are as varied as the perpetrators who mount them. In general, the main excuses for launching a DOS attack are: political, revenge, and economic. All too often, most DoS attacks have no motivation other than to wreak havoc (virtual vandalism). Plus, they generally don’t result in any gain for the hacker other than the inexplicable “joy” of rendering the network, or parts of it, inoperable.
**Zombies**

Zombies are the primary attack vector in DDoS attacks. These are user machines—usually sitting on insecure “home” networks—that are taken over by a hacker who plans to turn them into agents. For example, an attacker will upload commands to the zombie via an open port. Once an attack is launched, the zombie is instructed to send out packets of useless information in order to clog the routers of the targeted website. Because the traffic being sent is garbled, the computer on the receiving end spends an inordinate amount of time and resources trying to understand the influx of data.

One of the main lessons to be derived from the C-SAFE program (covered in greater detail in Section Six) is to NEVER allow your machine to function as a zombie. In the event of an attack, your machine, not the hacker’s, will be implicated.

**Counter-Measures**

Once a deliberate DoS/DDoS attack has been unleashed, short of pulling the plug, it is next to impossible to get it stopped. While the biggest attacks make the headlines and are fully investigated, the reality is, small attacks, the ones that occur much more frequently, are able to slip through the cracks. While there are lots of products on the market for countering DoS/DDoS attacks, most of them are not practical for individual users or small networks.

Currently, your best defense lies in anticipating rather than responding to an attack. Both administrators and home users need to make sure their machines are secure and this can be done by: (i) using strong passwords, (ii) keeping up-to-date with patches, (iii) closing open ports, and (iv) installing firewalls. These techniques (covered in Section Six) can help...
prevent your computer from being turned into zombie. To learn more about DoS/DDoS attacks and what you can do, visit Secure Florida <www.secureflorida.org>.

References


E-Mail

Definition

E-mail is primarily a text-based communication system that transmits messages over a computer network. The types of information that can be sent using e-mail range from word documents, HTML, to graphics, and audio/video files. An e-mail client (consisting of a text editor, address book, file folders, and a communications module) is used to read, write and send messages.

To be a valid e-mail address, three key elements are required:

- A user ID or handle—this is used to associate a user with an online account
- A domain name—this represents a unique name that a company, organization, school or Internet service provider (for example, amazon.com, secureflorida.org, fsu.edu or aol.com) registers for use on the Internet.
- An "@" symbol—this symbol must be included in the address in order to work.

Thus, a typical e-mail address would look something like:

your.userid@companyname.net
E-Mail Security

No e-mail is a 100% secure.

An e-mail address or the information contained in an e-mail header can be easily spoofed (faked or tampered with). While some e-mail systems may allow the sender to secure the contents (using encryption), the other parts of an e-mail message may or may not be correct. Thus, the recipient of the e-mail message is responsible for verifying authenticity. Recall the following factors that—if taken as a whole—either increase/decrease our confidence that an e-mail message has not been tampered with and/or compromised:

Confidentiality—protects data from being exposed to the “wrong” person.

Integrity—confirms that data received is the same as data sent.

Authentication—verifies the identity of the organization and/or the user.

To minimize the threat of an attack, e-mail filters can be used to intercept incoming or outgoing e-mails or to block unwanted messages. Most software programs offer a quarantine option. A “suspect” message is placed in a separate directory where the user (depending on what rules have been set up) or the network administrator (depending on what policies have been established) can decide whether or not the message is allowed.

On the other hand, e-mail monitoring systems do not intercept e-mail to prevent harmful messages from being sent or received. Instead, these programs are used analyze stored messages for attributes such as
offensive words, attachment names, and file sizes. In this way, these programs can be used to detect e-mail abuse patterns or function as a policy enforcer. When using this kind of software, it is necessary to have a proper e-mail policy in place before installing the software.

“Suspicious” Messages

Because almost anything in the “headers” of an e-mail message can be “spoofed”, including the “From” and “Reply To” addresses (for more information, see Spoofing), it is necessary to double-check before responding to a suspicious e-mail. A bogus message may appear to be coming from someone you know or from a trusted source. You need to be a more than “a little suspicious” about any message you wouldn’t have expected to receive.

Furthermore, a legitimate business will never ask you to reply to an e-mail that directs you to provide personal information such as date of birth, credit card data, password, or other critical data such as your password or PIN number. NEVER reply to an e-mail that asks you to submit this kind of information.

If an e-mail instructs you click on a link in order to supply personal data or up-date your account profile, make sure that you don’t end up at a spoofed website, that is, one that appears to be a real, but it’s not. For example, the link might look like:

www.my-bank.com
or
www.mybank.bus
when it SHOULD be:
Common sense is your best defense against spoofed e-mail and websites. Delete any messages that look suspicious—even those that appear to be from someone you know.

E-mail Threats

Common e-mail threats include:

**Spam**: Unsolicited Commercial E-mail (UCE), bulk e-mail.

**Intrusions**: Denial of Service (DoS) attacks, unauthorized access.

While it is beyond the scope of this manual to cover all the e-mail vulnerabilities that have are prevalent, the main ones pertain to:

- *Weak passwords*—using recognizable words that can be found in a dictionary, names of family members or a family pet, or any information (for anyone who knows you) can be readily deduced and/or is easy to guess.

- *Open file shares*—using e-mail clients that do not allow for encryption. Sending an unencrypted e-mail is like sending a message that has been written on the back of a postcard.

- *Missing security patches*—system weaknesses that have not been closed or repaired can be exploited by attackers.
E-mail Attack Vectors

While e-mail attachments are still the biggest hazard, spam is quickly becoming a serious attack vector. Malicious code “technology” has been moving from attachments into the message itself. Just reading the message can launch an attack.

Combined attacks are also being used. If reading the message doesn’t get you, opening the attachment will. The payload of hostile e-mail can be completely hidden. For example, an e-mail in HTML format can contain computer code that accomplishes the same thing that a malicious attachment would. Reading the message, or simply viewing it in a preview screen can immediately activate any hidden malicious content. You can defeat this kind of e-mail by setting up your e-mail client (program) properly.

Attachments

When dealing with e-mail attachments there are three file types to be aware of in a security context:

1) Executable files

2) Exploitable files

3) Inactive files

The first two categories involve “active” content that may, or may not, contain hostile code. This means that Windows will enable whatever action they have been programmed to do—good or bad.
Until recently, inactive files (for example, graphics, music and video files) were generally considered safe. With the advent of powerful media software (for example, Windows Media Player) that is embedded in the operating system, this is no longer the case. For example, hostile content in MP3 files can enter through a flaw in older versions of WinAmp.

**Handling Attachments**

When dealing with attachments:

- Be careful with any attachment you were not expecting—*even though it’s from someone you know.*

- Be suspicious of an attachment that has been forwarded to you—*even by someone you know.*

- Be paranoid about attachments—*especially from anyone you don’t know.*

Even if you know where an e-mail is coming from, you need to stop and ask yourself: “Was this message sent by a real person or was it generated by a virus?” Unless you have evidence to the contrary, you need to assume that any attachment you receive may be carrying a malicious payload.

If you don’t have up-to-date AV software installed on your machine, the malicious code might not be detected.

In addition, you need to examine messages and attachments as a whole, not separately. For example, attachment details—size, name, or file extension—combined with the information contained in the subject line or the content of the message will alert you to the fact that the message is bogus.
Look for inconsistencies:

- Did the sender of the message struggle with grammar, spelling, or punctuation?

- Is there anything about the message that doesn’t add up—who it’s from, address it’s from, the subject, the kind of attachment, file name, why you would get such a message?

- Can I live without what this attachment offers, even though I’m curious?

- Does the message appear to come from someone I know? If yes, then verify (by phone or a separate e-mail) that the person sent you an attachment.

- Is the message well written, convincing, and reasonable, and do you feel that the attachment is safe enough to risk opening?

- Have you received messages exactly like this one before? From the same address, the same person, the same or related subject, the same kind of message, the same kind of attachment?

When you are sure the attachment is safe, go ahead and open it. If not, then proceed with caution. Never “double click” or “right click > open” an attachment you’re not sure of—it might contain malicious code that would be activated.

**Precautions**

Because e-mail is often used as a delivery vector, hostile code can be delivered directly through HTML formatted e-mail. To further reduce your risk:
- Try using a text-based e-mail client instead of client that uses HTML.

- Disable the options allow you to automatically open an attachment.

- If you are still unsure, try installing a program or software utility that will let you open an e-mail without activating an executable file.

**FYI**

The widespread use of e-mail raises many legal and practical concerns for users, including the extent to which e-mail is private, the potential impact of e-mail in harassment, and the impact of e-mail in litigation generally.

Because of these concerns, prudent employers should develop e-mail policies tailored for their organizations with respect to:

- Sending personal messages to friends
- Employee monitoring
- Misuse of company resources

**Liability**

With respect to liability, the potential areas of concern for individual users are:

- Careless “speech” that may subsequently be determined to have harassed, defamed, or discriminated against someone;

- Inadvertent disclosure of trade secrets or confidential information;

- Infringement of copyright;
- Unintentional modification of contracts; and

- Violation of civil or criminal laws (for example, the proliferation of material that is deemed to be child pornography or obscene). In addition, an employer is also subject to potential liability in the following areas:

  - An employee’s casual e-mail statements may be deemed as additional warranties for its products or services.

  - If notice has not been provided, monitoring or searching an employee’s e-mails may subject it to liability; and

  - Archived e-mail will be subject to discovery procedures in any lawsuit or criminal investigation.

**E-Mail At-Work**

In short, how e-mail is used at work will depend on the policies that have been established by the employer. If there are no written policies and you are using e-mail for both work-related and personal use, then err on the side of caution. There is no expectation of privacy when it comes to e-mail.

Lastly, e-mail is permanent. Deleting an e-mail message doesn’t necessarily mean it has been permanently deleted. Your best defense is to:

**THINK BEFORE YOU TYPE.**
The KRESV Test

Since following safe e-mail practices can not be emphasized enough and the risks of opening a contaminated e-mail attachment are so high, we conclude by recalling advice that has encapsulated in the KRESV test:

- **Know:** Is the email from someone that you know?
- **Received:** Have you received e-mail from this person or sender before?
- **Expect:** Were you expecting an attachment from this person/sender?
- **Sense:** Does the contents (as described in the Subject line) and the name of the attachment(s) make sense?
- **Virus:** Does this e-mail contain a virus?

Even if a suspect e-mail passes all tests, you still need to exercise caution when opening an attachment and/or clicking on a link.

References


Spam

“Spam will end when it is no longer profitable. Spammers will see their profits tumble if nobody buys from them... This is the easiest way to fight spam, and certainly one of the best.” – Heinz Tschabitscher

“There is a genuine concern that too much spam will kill off e-mail.”
- Eric Allman

Definition

You may think you know spam when you see it, but there is no consensus on just what it is. Spam has proven surprisingly difficult to define. Is it “unsolicited commercial e-mail” (UCE)? Would “unsolicited bulk e-mail” (UBE) work better or should spam be referred to as “unsolicited electronic mail solicitations” (UEMS)—bearing in mind that the latter term includes single unsolicited e-mails as well.

Many e-mail marketers would prefer a definition that requires “only misleading unsolicited e-mail be considered spam;” that is, e-mail where the true sender is intentionally obscured or the sender is making fraudulent claims/offers. Unfortunately, the difficulty in coming up with an ironclad (read: “unambiguous”) definition makes the problem of eliminating spam that much harder.

Most users consider any e-mail they don’t want or didn’t expect to be spam, regardless of origin or intent. But there are plenty of legitimate companies and organizations that would vehemently object. In their opinion, contacting customers and clients with relevant information is a targeted service and therefore, should NOT be considered spam. In fact, they would argue that legitimate concerns should be
given at least one chance to send out an ad-based message—the so-called “one bite” approach and if e-mail recipients don’t want to be contacted again, the onus is on them to opt-out. Secure Florida calls this type of e-mail NOT-spam. Other examples include:

- E-mails sent by viruses, though not generally considered spam, can have a similar effect;
- Notifications sent to you by an ISP to inform you about network status, delivery failures, and viruses; and
- Bounced e-mail (as a result of spam sent out in your name) that did not reach their destinations or were bounced back by users.

Commercial spam has been likened to “telemarketing on steroids.” Instead of contacting one person at a time and at great expense, companies can send bulk e-mail to literally millions of people. Apart from the fixed costs (for example connection/bandwidth) bulk emailing is virtually free. The real costs—in terms of lost productivity—are born by the recipients, not the senders.

Finally, the term “SPAM” (uppercase) is used to designate the meat-in-a-can product prepared by Hormel Foods and “spam” (lower-case) is reserved for the junk e-mail that fills your inbox.

**Who are the Spammers**

They are members of a relatively small, shadowy group of pros who are capable of generating hundreds of millions of e-mails each day. In an effort to ensure a maximum response rate, spammers use evasive tactics to
avoid being caught. They are becoming more innovative in the way they create and distribute their messages—hoping to dupe the more cautious recipient and at the same time skirt the restrictions being imposed by corporate and legal regulators.

The second most common source of spam is being generated by *malware*. Once a computer becomes infected by a worm or a virus, it will commandeer your user ID and e-mail copies of itself to everyone listed in your address book. Assuming that these e-mails (or attachments) are opened, the worm/virus will continue to reproduce at a faster rate, creating even more junk e-mail that fills up inboxes.

A third source of spam is referred to as the *family-and-friends assault*. According to Gartner, a new form of spam, described as “friendly fire” is starting to clog up the networks. Here, they are referring to the increasing amount of e-mail being exchanged between family and friends on a daily basis. They expect this to become an even greater problem as users become more familiar with creating and sending e-mails that include bandwidth-hogging files (for example, MPEGs, GIFs, BMPs and MP3s).

**Components**

In order to work, the sending of spam requires three main parts:

- The initial e-mail
- A companion web page, and
- Bullet-proof hosts

The spam perpetrator (*aka* the spammer) obtains a list of e-mail addresses from one of several sources:
- buying/selling mailing lists to third parties or on the black market;

- using robots to scrape (i.e., harvest) names off the Internet;

- generating random addresses in the hope that some will be genuine;

- guessing e-mail addresses by adding common names and letter combinations to corporate domains for example, “bob5@aol.com;”

- requiring users to fill out a form with a checked-off ‘opt-in’ box in order to get access to a website.

With a “list of addresses” compiled from various sources, the spammer then uses a bulk e-mail client (this allows them to fake the name listed in the “from” line) to send out millions of e-mail messages. This in turn, drives traffic to a companion web page where innocent victims are asked to fill out a form (including personal information) and/or are encouraged to buy a product or subscribe to a service.

While both of these components have to operate in unison for the spammer to get paid, equally important is the existence of bullet proof hosts (“bulk e-mail friendly Web hosting services”) which are provided by Internet service providers. For a price, they ensure that the spammer’s site won’t be shut down once the deluge of complaints starts to pour in.

This practice is bolstered by “plausible deniability.” Spam complaints are often met with the response that the consumer must have volunteered for e-mail offers at some point in time and in this way, they are able to shift blame to an (unidentifiable) affiliate or marketing partner.
The reasons spammers appear to have the upper hand are many. First of all, spammers are highly motivated. Why? Because, like it or not, spam works. Since it costs next to nothing to send out millions of e-mails, even with a poor response rate, they can make huge profits.

Secondly, spammers are not stupid. They are extremely adept at circumventing spam controls and disguising questionable pitches as legitimate e-mail.

Thirdly, if pressured by legislation, most spammers will not close down. Instead they will move offshore and/or they will start hijacking home computers to use as a base for their clandestine operations.

Finally, most spammers enjoy a “first-strike” advantage. It’s impossible to predict, much less to respond, when the next spam wave will take place and what tactics will be used to thwart detection.

For example, in response to the development of more advanced filters, spammers have begun using tricks like spelling words slightly wrong, replacing letters with numbers, and adding spaces in the middle of words in order to fool filters. Random strings of text are being included in the subject lines or at the bottom of the message in order to foil the routines that are used to detect spam. Because most users automatically delete messages that contain gibberish, spammers have started formatting this as white text on a white background—this way, users don’t see them but the filters still do.
Recognizing Spam

Spam e-mails might also be attempting to generate traffic for a (usually adult) website by containing a hyperlink to it. In most cases, these unsolicited e-mails are easily spotted.

Typically they will be from an unfamiliar or nonsensical e-mail address, have poorly worded content with minimal information of the company or person who sent it, and in most cases be completely generic to those who receive them. Those who look at the header of these e-mails will also find they contain incorrect ID names, e-mail addresses, and other forged information. Hundreds of thousands of these messages flow through the Internet each day.

Most spammers go great lengths to: (i) hide their identities; (ii) obscure the origin of their messages/websites, and (iii) disguise the fact that they are collecting personal information and surfing and buying habits—all without permission.

Tips for Fighting Spam

Besides using filters and other technical means to combat the deluge of spam, the best way to deal with spam is through avoidance and redirection. Here are some tips that have been compiled by Secure Florida (www.secureflorida.org) that you can use to help reduce the amount of junk mail you receive:

- Don’t reply to spam or use the “remove from list” option and never, never, never click on a link—any or all of these actions will verify to the spammer that your e-mail address is active. (The one
exception is commercial e-mail from a well-known company or a bona fide list-server. Most of their “remove me” features are for real.)

- If you want to complain, contact your ISP or else use the e-mail headers to locate the origin of the e-mail. (Note: you can find information at the Secure Florida website <www.secureflorida.org> on how to read an e-mail header or else you can read the information contained in the section on Spamming.)

Once you’ve identified the culprit, visit:

www.spam.abuse.net

for the appropriate contacts, and send a message requesting that they help stop spam coming from the offending domains.

References


CAN-SPAM Act of 2003


fight spam


Mike Fuhr’s Spam-Fighting Page


Spoofing

“Spoofing generally isn't illegal because no hacking is required, FBI officials say, leaving prosecutors with little recourse unless there's a threat of death or violence involved. And finding culprits is tough—after all, they are using someone else's identity. The purported senders then get angry replies—along with e-mails returned as undeliverable because they went to bad addresses or full mailboxes. These returns are how individuals and groups learn they've been spoofed.” – Leapfrog

Definition

“Spoofing” in the context of the Internet occurs when someone assumes an identity without permission. Variations on spoofing involve: masking, mimicking, impersonating, masquerading, and social engineering—i.e., the hacker term for “tricking” users into revealing passwords and other personal information that can be used to gain access to a user's private accounts and assets (e.g., SSNs, PINs, mother’s maiden name, etc.).

Strictly speaking, the simple act of spoofing an identity is not “illegal” (i.e., no hacking is involved in the commission of the act). It only becomes illegal when a threat of death or violence is involved or personal data are stolen in order to commit fraud or identity theft.

Types of Spoofing

Most users, at one time or another, will encounter a minimum of three types of spoofing:

- **IP spoofing**—it is beyond the scope of the Florida Cyber-Security Manual to discuss IP spoofing in any detail. Suffice it to say that
masking IP packets is one of the ways that malicious hackers use to breach the security of small business or home networks.

Most systems are configured to allow network traffic coming from a trusted source to pass through the firewall. All other traffic is denied. To put it simply, before accepting any packets, the firewall examines the source IP addresses to determine whether they are legitimate or not. A malicious hacker will try to get past this form of security by "spoofing" the source IP address of packets sent to the firewall.

- **Web spoofing**—tricks the browser into serving up a different web address than the one it appears to be resolving i.e., the URL that you think you clicked on is different from the one that is eventually displayed. This form of deception is accomplished by (i) attacking the DNS (domain name system) that maps the web address (e.g., www.website.com) in the URL to a network location (IP address), (ii) modifying a webpage (i.e., the source code) so it returns a misconfigured URL, (iii) confusing the browser when it tries to interpret a form (e.g, cgi data) or read a script (e.g., Perl, JavaScript, etc.) and/or (iv) creating a ‘fake’ website that sits between the user and his or her intended destination (note: this type of spoofing is covered in more detail in the section on Phishing. Once the browser has been tricked into the serving up the wrong webpage, the hacker can send bogus information or prompt the user to provide personal information (e.g, passwords, credit card numbers and so forth). Depending on how good the “con” is, the user may not even notice that s/he has been duped.
E-mail spoofing—is the act of forging the “header” information in an e-mail so that it appears to have originated from a bona fide source (e.g., the network administrator) when in fact, the dubious e-mail has been sent from a suspicious source (e.g., a hacker, a con artist or a spammer). The main motivation behind a spoofed e-mail is to trick the user into: (i) making a damaging statement, (ii) releasing sensitive information or (iii) clicking on a link that will take that the user to a forged webpage. In addition, e-mail spoofing is a favorite ploy used by malicious hackers. They rely on forged e-mail to make it more difficult for investigators (of a malware attack) to track down the offender(s).

Because SMTP (Simple Mail Transfer Protocol) lacks authentication, it is fairly easy to spoof—particularly if a network administrator has configured the mail server to allow connections to the SMTP port. This enables any hacker/attacker to connect to the SMTP port and issue commands that will send e-mail that appears to be from the address of the would-be con/scam artist’s choice (either a valid e-mail address or a fictitious address that has been correctly formatted).

Or else, all the user has to be is reconfigure the settings on any standard e-mail client or if they are using web-based e-mail, all they have to do is modify the web browser interface. Plus, many unscrupulous websites offer services that automate the creation and distribution of spoofed e-mails.

Joe Job

A “Joe job,” named after the first victim, is one of the simplest exploits to carry out. All the attacker has to do is change the "Reply To"
address in their e-mail program. This type of attack involves the sending of huge volumes of unsolicited bulk e-mail that appear to be from someone (usually a reputable person or organization) other than the actual source (usually a spammer). In addition, a Joe job may also be used as a act of revenge. For example, anyone who report spammers to ISPs or who advocate on behalf of legislation might find themselves victimized in this manner. In this case, the attacker is said to be “Joeing” the legitimate owner of the e-mail address they have appropriated.

**Social Engineering**

Internet lore notwithstanding, social engineering is not mind control. Nor is it a new form of social experiment. Rather social engineering is a term that has been coined by hackers to refer to the “art and science” of getting users to comply with their wishes. In this case, the level of deception is aimed at the user/operator as the vulnerable entry point and it is based on an accepted article of faith that states: “in any system, people are the weakest link.”

Relying on social engineering techniques, hackers are able to get people reveal information that should be kept secret or perform tasks outside their norm or behave ways that are contrary to their own self-interest.

For example virus writers use social engineering techniques to compel e-mail recipients to open attachments that carry viruses and worms. Would-be hackers use the phone to get users to reveal passwords or other sensitive information. Lastly, it's not just malware that you need to be on the look out
for. Internet cons (scams, fraud and hoaxes) and to some extent spam, all require the unwitting cooperation of the user in order to succeed.

Not all social engineering takes place via the Internet. Dumpster-diving for pieces of paper that contain sensitive information (e.g., credit card numbers) is a common ploy. Another favorite trick is to call up low-level employees and get them to reveal information that hackers will later use will to compromise a system/network.

**Spotting Spoofed Webpages**

Some forms of webpage spoofing are fairly easy to pick out if you know what you are looking for. Keep the following tips in mind the next time you are looking at an unfamiliar website or you are typing in a URL from a unreliable source. The place to start is the browser's location line. It is key to determining if there's anything unusual about a site's URL. For example, another way to be on the look out is to pay attention to where a link is taking you—is it going to a place you expected or is it taking you someplace else. The next time you surf the web, consider the following:

- Each time you hover (with your mouse) over a link, the status line displays the corresponding URL. Check to see if there are any discrepancies between the information displayed on the status line and the information displayed in the URL locator.

- As a webpage is downloading to the browser, the status line will show the name of the server. Be suspicious if the
server name is different from the one you were expecting.

Unfortunately, spotting bogus websites is not always so easy or straightforward. Clever hackers can mask a web spoofing attack through programming tricks. For example, if the hacker is using JavaScript, she can write to the status line and rewrite the location line URLs or she can make all requests for a particular URL go to the attacker’s system. Plus, once the attacker obtains the desired information, she might code the spoofed webpage to reroute you back to the intended site.

Whenever you are accessing a website with which you are familiar and it asks you, out of the blue, to fill in a form or supply private information that you have previously input and/or provided in the past, stop and take a minute to evaluate the situation. If at all possible, pick up the phone or send a quick e-mail to verify the request. At all times, when in doubt, check before you type.

**Spotting Spoofed E-mails**

Being able to spot spoofed e-mails takes a little more time and effort. To begin with, you need to examine the routing information contained in the e-mail headers. However, before we examine the headers, we need to deconstruct the e-mail message. Most e-mails are comprised of two distinct parts:

1) *The Header*—i.e., the envelope. It is a section of code that contains information about where the e-mail came from and how it reached its destination. It also contains the e-mail address of the originator and/or the computer that the perpetrator was
using. As such, the header contains mainly technical information:

- Origin (the machine that sent the e-mail)
- Relay (the machine that passes the e-mail from one serve to the next)
- Destination (the machine that finally receives the e-mail)
- IP address, and
- Domain name.

2) *The Body*—i.e., the message. The body contains the actual text and any attachments that might accompany the e-mail.

The “full” header is visible—only if the recipient chooses to view it and most people do not. The address used during the delivery process (the envelope address) does not necessarily correspond to the addresses listed in the message header.

To check for any discrepancies, you need to view the full headers. This is especially important when viewing Spam—where the “To:” and “From:” headers are usually spoofed which means they are meaningless.

The key to spotting spoofed e-mail is to realize that:

- The address in the header of the message can be spoofed but the envelope address can NOT be spoofed.

- Addresses that appear in the “To:” and “From:” lines are NOT the addresses used to deliver a message. The addresses found in the header are the ones that are used to deliver the e-mail.
**Cloaking Techniques**

Hackers and spammers go to great lengths in order to hide their identities. Some of the “artful” dodges commonly used to transmit or cloak suspicious e-mail, notably spam, are listed below:

**The transfer of e-mail via open relay, onshore and offshore (spam-friendly) ISPs, and/or insecure mailback scripts.** Spammers use these techniques to release their messages on the Internet. Many spam-fighting groups have developed 'block lists' that a network administrator can use to detect and reject mailings that originate from questionable sources.

**Transfer of mail via open proxies.** First, a spammer breaks in and secretly plants software on the computers of unsuspecting home or small business users. Then, they use these compromised systems to broadcast unsolicited e-mail *via* remote control. So far, open proxies have provided excellent cover. As a result, they have become the preferred “spam” vector.

**Forged header information.** To hide the origins of suspicious e-mails, hackers and spammers “prepend” bogus routing information in the headers. This is done in order to avoid punitive action from ISPs or law enforcement. Forging header information is considered highly unethical and can be grounds for a user’s privileges being terminated or charges being laid.

**Obfuscated URLs.** To mask their underhanded activities, hackers and spammers use bizarre encodings to render website addresses in a form that, while legible to browsers, cannot easily be interpreted by humans. This technique only has mixed
success. If a URL is valid, it can usually be decoded. To make their websites look legitimate, spammers will use the infrequently-used user-ID field in the URL (e.g., “http://www.iamnotspam.com@10.11.12.13/.” where the part of the string to the left of the @ sign is a bogus “user id” that most web servers will ignore. On the other hand, the 10.10.10.10 part of the string points to the “actual” location that the web browser will resolve. To a casual observer, the URL may look like “www.iamnotspam.com” when in fact, the true IP address is 10.11.12.13.

**Encoding of message bodies and other data.** To get past less sophisticated spam filters, hackers and spammers will encode their messages (or portions thereof) using standard Internet encoding techniques like MIME, URL encoding, and HTML character entities.

**Javascript-generated message bodies.** This is another ruse that hackers and spammers use to hide message details. While the use of cryptic data, in conjunction with scripts provide a temporary cover, note that the e-mail header remains unaffected which means you can use any URL or mailto links for tracking purposes.

**Disabled right mouse button.** In e-mails that have been formatted for HTML, a JavaScript is used to intercept right mouse clicks. This prevents the reader from displaying the usual pop-up menu with its “view source” command. Hackers and spammers employ this technique to prevent someone from examining the HTML source code—though it only takes a few seconds and a couple more keystrokes to located that information. This ploy does not work, provided you know how to access the source code in your browser.

**Hashbusters.** To circumvent server-side spam prevention programs, hackers and spammers
put random character strings in the subject line or body of spam e-mails. While this trick is able to deflect spam filters, it can’t fool a real person since the gobbledygook in the subject line immediately identifies the message as spam.

**Embedding a recipient’s e-mail address in hyperlinks or ‘web bugs’ (beacon URLs).** To order to get a message back that indicates you have opened and possibly read an e-mail message, hackers and spammers will plant a web bug into a URL within the body of a message. Not only is this technique effective, it works whether you click on any links or not. The very fact that e-mail is opened will prompt the beacon to send back a message indicating that a “live” e-mail address has been identified. This information can then be acted on by the hacker/spammer or else sold to other unscrupulous operators.

**“Personalized” messages and provocative subject lines.** Personalization is another technique that is used to induce an e-mail reader to open or respond to a message. Every trick in the book has been used to compel readers to open and read spam. Examples of “socially engineered” subject lines are:

- Haven’t heard from you lately?
- Regarding your account
- Payment past due
- You are being monitored.

**“Creative” misspelling.** Hackers and spammers will deliberately misspell certain “key” words by substituting letters with look alike numbers or other symbols. For example, if a message contains the word “Viagra,” the spammers will spell it as “v1agra” or “bagai.” The next time you see a lot of misspellings in an e-mail and conclude that the sender is clueless. Think again. The apparent mistakes
not due to ignorance or negligence; rather they are clever work-arounds that are designed to circumvent the spam filters.

**Invisible bogus text.** A similar ploy that is used to defeat the spam filters is to introduce nonsensical or unrelated text into the body of the messages. This is accomplished by using sophisticated spam mailers with “random insert” capabilities. This trick is only partially successful since Bayesian spam filters look at the content of a message and “weigh” the presence of spam-related words against the message as a whole. To bypass this barrier, hackers and spammers will include lots of unrelated words or phrases and then they will mask this verbiage by making the font the same color as the page background so it looks like “white space” to the naked eye.

**Obfuscation of HTML message bodies.** Most browsers are designed to be tolerant of invalid HTML tags. Taking advantage of this fact, hackers and spammers conspire to make the HTML message body unscannable by less sophisticated content-based filters. To do this, they use bogus, empty, or malformed HTML tags into the middle of key words in the message. For example, they utilize empty tag pairs (e.g., “mort<b></b>gage”) and tags outside their intended context (e.g., table cell tags “<td></td>”) in the middle of a plain text message.

**Viewing Headers**

Most e-mail clients have an option that will display the header information. Check the documentation for the program you are using to read mail in order to see how to view the source code. As part of the default settings, most e-mail programs only display the standard *To:*, *From:*, *Subject:*, and *Date:*
headers. However, the most important information (for tracking purposes) is usually hidden is the Received: line—it tells you what the route the message took before it reached your destination. Plus, it is harder to fake (though some of the lines can be) because it records the path taken and the mail servers used to process the message.

For your convenience, we have listed some tips on how to view a “full” header for some of the more popular e-mail clients:

- **America Online**—under “My AOL,” go to “Preferences” and select “Mail” in the preferences box.

- **Elm, Pine, & Mutt**—press "h" from the message selection menu. For this to work, make sure that the “enable-full-header-cmd” feature has been selected in the configuration settings.

- **Eudora**—open a message. Under the title bar are four options. Select “Blah, Blah, Blah” to display the full headers.

- **Hotmail**—go to “Options” on the navigation bar and select “Preferences. Scroll down to “Message headers: and select “Full” to display the Received: headers.

- **MS Outlook**—double click on an e-mail and then click on “View,” then select “Options.”

- **Netscape/Mozilla Mail**—click “OPTIONS” from the menu bar and then select "Show Headers". Choose full headers.

- **WebMail**—click the “Options” button and select “Show message headers in body of message.” Then, click OK.
If you have trouble displaying the full header, another solution you can use is to open your e-mail using a standard text editor (e.g., use WordPad or NotePad). The information contained in the full header will be automatically displayed.

**E-mail Protocols**

This section provides a line-by-line description of some of the more common e-mail protocols. For a complete listing and interpretation, visit the Secure Florida website <www.secureflorida.org> and check out the links/references that will guide you, step by step through the process of reading an e-mail header.

**Comments:** This is a nonstandard, free-form header field.

**Content-Transfer-Encoding:** This line has no direct relevance to the delivery of mail, but it affects how MIME-compliant mail programs interpret the content of the message.

**Content-Type:** This line tells MIME-compliant mail programs what type of content to expect in the message.

**Date:** This line specifies the date that the message was composed and sent. Due to discrepancies in clock settings, this information cannot be completely relied upon. Also, it might be forged.

**Errors-To:** This line specifies an address for mailer-generated errors, (e.g., where bounced messages are to be sent instead of the sender’s address.) This header information is not all that common since most senders usually want to have any bounced messages returned to the sender.
**From** (without colon) This line is not actually part of the e-mail header. The e-mail transfer software inserts it when the mail is received. This line will always be the first line in the headers. This line can also be spoofed, but not always.

**From:** (with colon) This line indicates whom the message is from. It is the easiest to forge, so it’s the least reliable.

**Message-ID:** Not always, but for the most part, the “Message-ID:” can be treated as a unique identifier that is assigned to each e-mail message by the first mail server the message encounters. The information contained in the “Message-ID:” tells you where the message originated; its value, followed by "@", followed by a machine name.

The format of a “Message-ID:” field is <unique string>@<sitename>For example:

```
Message-ID: <3A2EDAFA.F4735272@myisp.com>
```

If the “Message-ID:” is malformed (e.g., an empty string or no @ sign), or if the website listed in the message ID isn’t real, then that should be your first clue that the e-mail might be a forgery. However, be aware that to spoof a “Message-ID:” requires a lot more specialized knowledge than forging the “From:” line, so in the majority of cases, the “Message-ID:” is most likely genuine.

Finally, note that the “Message-ID:” only identifies the system that the sender used to log in, rather than the actual system where the message originated. Since each e-mail program has its own unique style of string, a forgery can often be detected by comparing the “Message-ID:” with a legitimate message that has been sent from the same ISP/location.
**Received:** The received lines are the most important components of an e-mail message in terms of forgery detection. They indicate where the message originated and what route the message took to get to you. This is the type of information you will need to supply if you want to make a complaint about spam.

**Reply-To:** Specifies an address where replies are sent. While this line can be easily forged, it is useful for tracking purposes, Forged spam often has a legitimate “Reply-To:” field so spammers can receive mail orders.

**Return-Path:** This is the e-mail address for return mail, so it is essentially the same as the “Reply-To:” field.

**Subject:** The subject is a free-form field, specified by the sender, that is intended to describe the subject of the message.

**To:** This line identifies who the message is being sent to. However note that “To:” field need not contain the recipient’s address.

**X-Headers...** This is a generic term that is used to identify header lines that start with a capital X and a hyphen. X-headers follow a nonstandard format and are to be used for information purposes only. However, this rule is frequently violated.

### Decoding E-mail Headers

To track down the origin of spoofed e-mail, you need to be able to read and decipher the e-mail header information. To facilitate this process, there are a number of questions you need to keep in mind as you pursue your inquiry:
- Who sent me the mail?
- When was it sent?
- Where did it go (i.e., what path did it take)?
- What is it about?

To interpret the e-mail header information, you begin by working from the bottom up. First, begin by discounting the obvious. Eliminate your own e-mail address and incoming mailbox details. Next, pay attention to:

*The Embedded Information*—you can extract several useful pieces of information from the “Received:” lines to help identify the message’s true origins: the name the sender used, the IP address of the incoming SMTP connection, and the name of each host that has been added as the e-mail is passed from one mail server to the next. As part of your examination, compare “who a server claims to be” with “what the server (one level up) claims it is” and if the two don’t match, you can conclude that the earlier “Received:” line has been forged.

The important thing to remember when parsing the received lines is that they operate like “registered mail.” Each received line functions like routing information that indicates: (i) when the letter was received, (ii) who sent it and (iii) where or how it was forwarded to by the post office.

*The Sender’s Address*—to extract the real name associated with the IP address, you will need to use the Network Toolkit (e.g., nslookup and traceroute/tracert are outlined in the section on Networks). For example, you may need to do a reverse DNS look-up on the IP number. Secondly, if the “Message-ID:” ends with an IP address instead of a domain name, be sure to look that up too. Next, you can use the whois command (also part of the
Network Toolkit) to find out who owns the IP address.

As you inspect the received lines, read from the bottom up because that is the order they pass through the e-mail system. Beyond the system address contained (in parentheses) in the first “Received:” line, each domain name, username and IP address should be considered suspect. Secondly, as you analyze the information be on the look out for:

- **A wrong Eastern Timezone, e.g., -0600 (EST).** EST is normally -0500, while EDT is -0400.

- **Forged addresses in the “Received:” lines.** A genuine “Received:” line has the address of the recipient as the address listed. If the address indicated isn't yours, this line has probably been forged. Also, try to determine if all all machines that the e-mail passed through are legitimate or not.

- **A spoofed SMTP ID.** A real one generally matches its first letter to the hour of the time that the hand-off occurred; e.g., if the time listed in the e-mail being scrutinized is between midnight and 1:00 a.m., then its SMTP ID should start with "A..."; between 1:00 a.m. and 2:00 a.m. should indicate "B..." and so on.

- **IP numbers that start with 0 or are greater than 254.** IP addresses only range from 1 to 254. (0 indicates a network address and 255 is for broadcasting).

- **A reverse DNS lookup that returns a different host name for the IP number that appears next to it in the header.** It may represent the true domain name of the hacker or spammer who sent the message.
After you finish your review, make a list of all the information that you can determine to be factual (be sure to include any additional information—for authentication purposes) that may be used to establish an evidentiary trail. Secondly, if the information is unavailable, make a note of what types of information you need to look up or make a request for and from whom (i.e., what source).

Lastly, don’t forget to check if there are any suspicious e-mail addresses or websites that have been included in the body of the message or hidden in the source code.

Finally, be sure to pay a visit to the Secure Florida website <www.secureflorida.org> where you can find more in-depth information on how to read an e-mail header.

In closing, please note that many of the attacks and exploits that are presented in Parts III – V are based on deception and they employ many of the spoofing techniques that have been covered in this section. By increasing your awareness of the dangers that lurk online, we hope that it is less likely that you will ever become a victim of cybercrime.

References


Email Spoofing

e-mail spoofing


How to Interpret Email Headers
Joe job


Viewing Headers on Various Popular Email Software Packages

Part III

Computer-related Threats
Definition

Malware - “malicious software” - is defined as any type of program that is introduced into a computer to cause damage, steal information and/or act in an unexpected or undesirable manner. It is important to note that this kind of code executes \textit{without} the express consent of the user. Malware covers the entire gamut of “hostile” code - viruses, worms, and Trojan Horses to commercial software (unauthorized registration, undisclosed adware, spyware, stealth installation of bundled apps), device drivers, \textit{Hacker tools and network sniffers}.

The 4 E’s

Most malware behavior involves the four E’s: (i) Enter, (ii) Escalate, (iii) Extend, and (iv) Execute.

1) \textit{Enter}—this represents the primary entrance points where malware can enter a system.

Such entrance points are: files incoming via users, removable disks, downloads or email attachments, data files (Office and HTML) where scripts are auto-executed, and

“The Internet has caused an evolutionary change on many levels, from the speed at which malware can proliferate to how wide spread the damage can be. Releasing a virus in the pre-Internet era was like releasing a polio victim on a steam ship. The person carried a disease that was only new to some, with most either already being vaccinated against it or capable of being so before the ship reached its next port days later. Today, however, the release of hostile [mobile] code into the wild is more like releasing Ebola into Times Square at rush hour. The transmission and effectiveness of the virus is far more immediate and disastrous.” – Robert J. Bagnall
hacking in through the network (LANs or the Internet). In addition, entrance may be gained where a limited range of behavior is possible, for example, a script embedded in an HTML e-mail message, or a scripting language that places limits on what can be done.

2) *Escalate*—extends the range of possible behaviors from whatever initial beachhead the attacker may have established. Escalation may exploit secondary entrance points such as backdoors or startup routines.

3) *Extend*—during this phase, the malware propagates itself and it is similar to the escalate phase except that here, the malware spreads from machine to machine. Not all malware self-propagates.

4) *Execute*—this represents the payload, the nature of which may terminate all of the other E’s with the functional death of the host.

Before downloading or installing any program, the onus is on the user to ensure that the program or script doesn’t contain any malicious code. When using commercial applications, the vendor should certify that any code used in the development of the product is malware-free.

Understanding how each piece of malware works is the first step in hardening a system against these types of attacks. The following section takes a look at each of the major types of malicious code and some of their less notable variations.
References

About Malware


google free tools


Malware
Malware


Viruses

Definition

A virus is a code fragment (not an independent program) that spreads by attaching itself to a host, often damaging the host in the process. The host is another computer program, often a computer operating system, which then infects the applications that are transferred to other computers. It may damage data directly, or it may degrade system performance by taking over system resources, which are then not available to authorized users. Upon execution, the virus replicates. The key issue here is the fact that the user does NOT give his or her permission for the code to run. Viruses are hard to detect as well as hard to deactivate. They spread widely and have the potential to keep infecting the environment over and over again.

Most viruses have a two-pronged objective: (i) propagation, that is, to spread themselves from system to system and (ii) destruction that is, to perform some action (the virus payload) on each system they infect. The payload varies from virus to virus. Benevolent viruses might be programmed to display an annoying message or alter the appearance of your desktop whereas a malicious virus might be programmed to destroy data stored on your hard drive or crash your system.

“In 1996 74% of viruses were transmitted on disks, but by 2000 this number had dropped to 7%.” – Mike Chapple

“Many researchers have concluded that 30 percent or more of small businesses are vulnerable to viruses either because they don’t keep their virus-scanning software updated or because they don’t install it correctly.” – Virus Threat Analysed
Most computer viruses are malicious — they can erase your files or lock up whole computer systems. Other computer viruses are more benign — they don’t do any direct damage other than by spreading themselves locally or throughout the Internet. Some viruses wreak their effect as soon as their code is executed; other viruses lie dormant until circumstances cause their code to be executed by the computer. Regardless of intent, computer viruses should always be treated.

**Virus Types**

In the early days, most viruses started out as someone’s “research project” and these viruses were tightly contained. The viruses that you are most likely to come in contact are “in the wild” and were mostly likely written by amateurs and pranksters. According to virus expert Paul Ducklin, in order for a virus to be considered in the wild, it must spread “as a result of normal day-to-day operations on and between the computers of unsuspecting users.” For a description of the different types of viruses, see Table 4.

Some viruses masquerade as a fun program (like an electronic greeting card) that secretly infects your system. If you pass the program along, not realizing that it contains a virus, you will enable the virus to propagate manually.

Viruses can be transmitted as e-mail attachments, as downloads, or be present on a diskette or CD.
# Table 4

## Virus Types

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Boot Sector</strong></td>
<td>A boot sector virus replaces or implants itself in the DOS boot sector on diskettes or the Master Boot Record on hard disks. Boot-sector viruses hide in executable programs (attached to e-mail or shared documents).</td>
</tr>
<tr>
<td><strong>File Infector</strong></td>
<td>File infector viruses are hidden in program or application files (.exe, .dll, .pif or .com). These viruses can be spread through floppy diskettes, downloads or scripts sent as an attachment to an e-mail note.</td>
</tr>
<tr>
<td><strong>Macro</strong></td>
<td>A macro programming language (e.g., Visual Basic) is used to modify commonly used commands such as the ‘Save’ command to trigger a payload. These viruses activated by opening a shared document file or spreadsheet and they are transmitted in documents, the most prevalent being Microsoft Word and Excel. These viruses account for about 75 percent of viruses found in the wild.</td>
</tr>
<tr>
<td><strong>Multipartite</strong></td>
<td>A multipartite virus infects both files and the boot sector of a computer system and this type of virus can reinfect a system several times before it’s finally eliminated.</td>
</tr>
<tr>
<td><strong>Polymorphic</strong></td>
<td>Polymorphic viruses are comprised of two parts: (i) the encryption/decryption engine and (ii) the infector. The crypto engine encrypts/decrypts the infector and each time the virus is activated, it uses a different crypto-key. Because the crypto engine cannot encrypt itself -- if it did, there would be no code to decrypt the engine next time the virus ran – it relies on a form of self modifying code that changes whenever it is transmitted.</td>
</tr>
<tr>
<td><strong>Stealth</strong></td>
<td>A stealth virus hides its presence by making an infected file appear non-infected. SPAM (Stealth, Polymorphic, Armoured, Multipartite) represent the most dangerous and sophisticated form of this type of virus. These viruses are equipped to disguise themselves from AV software by employing stealth tactics. The virus itself is encrypted and the structure of it armoured making the task of writing AV software much harder.</td>
</tr>
</tbody>
</table>
How Does a Virus Spread

Strictly speaking, viruses are not the attack vector. They usually function as the payload. The main attack vector for viruses used to be infected floppy disks; these days, the primary vectors for viruses are e-mail attachments, downloaded files, and worms.

Most viruses are designed to spread from computer to computer. To successfully duplicate itself, a virus must be permitted to execute code and write to memory. For this reason, many viruses attach themselves to executable programs.

Below is a list of some of the most common ways viruses are transmitted:

Once a virus has infected your system, it may automatically send out e-mails containing more copies of the virus using the address book in your e-mail program.

A macro virus may attach itself to any document you create or modify. If you send another document to someone by e-mail, the virus goes along with it.

What Kind of Damage Can a Virus Do

How much damage a computer virus can inflict on your system depends on a number of factors, including how sophisticated the virus is. Some viruses can delete or change files. They can slow down your system, impairing performance or they reformat your hard drive making your computer unusable. Viruses can take advantage of your address book release confidential information or they can e-mail
personal data back to the virus developer. Other viruses might plant monitoring software or change security settings - allowing hackers to enter your computer, take control and steal information.

**Hiding Strategies**

Viruses employ different kinds of obfuscation. In the old days, viruses (especially in MS DOS) alter the information attached to the files it infected, for example, last updated and the file size. Another hiding technique was to infect the hard disk drive instead of the files saved on it. The stealth viruses try to exploit the failings of how modern antivirus software tries to detect viral infections. Modern state-of-the-art viruses encrypt themselves to avoid detection. This is often done with a combination of encryption and self-modifying code.

**Virus Information Centers**

More detailed information about viruses and how they propagate can be found at the following websites:

Compinfo

Computer Associates Virus Information Center

Computer Security Resource Center

NAI (McAfee) Virus Information Center
Anti-Virus Software (AV)

AV software is one of the most important defense mechanisms for the home user. To safeguard your computer, you need to install an AV software program and run it on a regular basis. To be effective, the virus signatures (the fingerprints or DNA of the viral agents) must be kept up-to-date and the program must be configured properly or the AV program will soon become relatively useless.

Most AV software comes with a year’s worth of updates and you can configure the software to either automatically download the updates, or display a reminder for you to do so. While the vast majority of viruses are written to infect Windows-based systems, Macintosh and Linux users should still install virus protection too.

In order to avoid a false sense of security, you should be aware that AV software has a number of limitations:

- AV tools only defend against known virus patterns.

- AV vendors cannot always update their signatures in time against the deadly viruses that are distributed worldwide via e-mail in a matter of hours (such as the LoveLetter virus and its variants). Oftentimes AV software is only effective against secondary infections.
Most AV solutions have a narrow scope and are slow to respond. It is often ineffective against many of the new worm-based attacks.

Lastly, don’t feel a false sense of security just because you are running an AV program. These software suites do NOT fully protect against many worms and Trojans, even when they are fully updated. While such countermeasures are important, AV programs should not be your front line of security - the user is always on the front line! Instead AV programs serve as a backup in the event that some kind of malware ends up on your computer.

**How Does AV Software Work**

AV software looks for a virus in one of two ways:

1) If it’s a known virus that is, one that has already been detected in the wild and has an antidote - the software will look for the virus’s signature - a unique string of bytes that identifies the virus like a fingerprint - and will just wipe it from your computer. Because the signature code is fairly stable, most AV programs will catch both the initial virus and any of its variants. Depending on the software package, you may also be protected against:

- Incoming e-mails and e-mail attachments with viruses.

- Viruses received through Instant Messaging, such as ICQ.

- Infected downloaded files, before you open the file.
- Attacks against your computer from outside (aka firewall software).

2) With respect to new viruses where no antidote has been created, the AV software uses “heuristics” that is, rules that look for unusual virus-like activity on your machine.

If the AV software detects any suspicious patterns, it will quarantine the questionable code and broadcast a warning to you about what the code may be trying to do (such as modify your Windows Registry).

If you think the unknown code may be a virus, you can send the quarantined file to the AV vendor, where their researchers will examine it and if appropriate, they will determine its signature, name and catalog it, and release and antidote. In this fashion it will become recognized as a “known” entity.

The DURCH Tests

When purchasing an AV program, use the DURCH Test to help you make an informed decisions:

Demand—Can the AV program check a file on demand? For example, when you want to forward an email attachment that you received from a friend and you want to make sure that the attachment does not have a virus?

Update—Can virus signatures update automatically to add the latest known viruses? If this feature is not available, then perform signature manually, preferably on a daily basis.
Respond—How does the AV software inform you about an infected file and then, how does it respond? Is the AV program able to clean a file, eliminate the virus, and repair the damage.

Check—Can the AV program check every file that is loaded into your computer? Are these checks automated? Note: some vendors turn off the auto-checking feature to make installation easier. Therefore you need to make sure that this feature is enabled.

Heuristics—Does your AV program perform heuristics tests? If so, how are they defined and how does it handles code that appears to be virus-like in its behavior?

Sample AV Tools

The following is a list of some of the more popular AV programs:

avast! Antivirus
URL: http://www.avast.com/.

BitDefender

Command Antivirus

Computer Associates / eTrust EZ Armor
URL: http://www.my-etrust.com/microsoft/index.cfm?CFID=1279212&CFTOKEN=ee00d18311c3116a-C08C9FF8-EE76-6E89-4EDE7221104E1DA0.

Dr.Web
URL: http://www.dials.ru/english/download/.
F-Secure  
URL: http://www.f-secure.com/download-purchase/.

G Data AntiVirusKit  
URL: http://www.gdata.de/filemanager/download/650.

Kaspersky Antivirus Pro (aka AVP)  

McAfee  

McAfee FreeScan  
URL: http://us.mcafee.com/root/mfs/default.asp?.

NOD32  

Norton AntiVirus  
URL: http://www.symantec.com/nav/..

Panda Software  
URL: http://www.pandasoftware.com/download/.

PC-cillin Internet Security  

Process Guard  

RAV Anti-Virus (Linux)  
URL: http://www.ravantivirus.com/.

Trend Micro's Free Online Virus Scan
URL: http://housecall.antivirus.com/housecall/start_corp.asp.

Virex for Macintosh (free with a .Mac subscription)

Additional Countermeasures

While it is important to install an AV program on your computer, your most effective defense against viruses can be your own wits and common sense. The best protection against becoming infected by a virus is to know the origin of each program or file you load into your computer or open from your e-mail program.

That’s why you need a complete, multi-layer defense for online security. Viruses can cause significant damage and recovering from an attack can be expensive. Using preventive measures can significantly reduce your exposure at a fraction of the cost it would take to recover from them.

Firstly, a lot of viruses exploit loopholes in your software. It is good practice to keep your software up to date. For example ‘Code Red’ exploited a loophole that Microsoft had already produced a patch to fix before the virus broke out. Users who had kept their software up to date were not affected by it.

- Always scan a removable disk (for example, thumb drives, CDs, diskettes) for viruses before using it.
- Back-up critical data and system configurations on a regular basis and store the data in a safe place.

- If you receive an e-mail attachment from someone you know, and your AV program does not automatically scan incoming e-mails, save the attachment to your hard drive and scan it with the antivirus program. Your friend or colleague’s computer may be infected with a virus.

- If you download software from the Internet, be sure to download it from the company’s site or a recognized download site. Download the file to your hard drive and scan it using your AV program before you run or decompress it.

- If someone sends you a ‘joke’ file or electronic greeting card that you must launch to view, be very wary.

- If at all possible, don’t use Outlook or Outlook Express as your primary e-mail program. More viruses are spread as a result of the security holes in Outlook than any other e-mail program.

- If you’re running Windows ME or XP and remove a virus, do not subsequently use a system restore point that might have included the virus, or you may need to remove it again.

**References**


Virus Threat Analysed

Viruses

Viruses
Worms

“The term worm come was coined by researchers at Xerox Parc who used benign worms to do system maintenance tasks. They were apparently inspired by a John Brunner novel "The Shockwave Rider" which featured a “tapeworm” program... The term 'worm' should not be confused with WORM (ALL CAPS), Write Once, Read Many, a property of some computer storage media.” – The Worm FAQ.

“Warhol worm is a term for a worm that can spread in less than 15 minutes (thus recalling Andy Warhol's quote about how everyone could have 15 minutes of fame).” – Clive Thompson.

Definition

Worms are similar to viruses. They share the same goals of propagation and payload delivery but they differ in terms of modus operandi. A virus attaches itself to, and becomes part of, another executable program, whereas a worm is self-contained. It does not need to be part of another program to propagate. Nor do they alter any files.

Instead, worms reside in active memory and they use the facilities of an operating system that are meant to be automatic and invisible to the user. It is not uncommon for worms to be noticed only when their uncontrolled replication consumes system resources, slowing or halting other tasks.

Because of their ability to spread independently, worms are able to cause a great amount of destruction in record time. Millions of computers can be attacked in minutes, spreading exponentially like an epidemic of human disease, or a nuclear chain reaction amongst fissionable atoms.
**Disruption**

Worms cause disruption in several ways. First, they use a newly compromised computer to look for more vulnerable computers. Second, they use up network and system resources as they spread. The more systems they infect, the greater the amount of traffic they generate.

Like viruses, worms may damage data directly, or they may degrade system performance by consuming system resources and even shutting down a network. Other ways that worms can cause indirect damage include:

- Degrading service levels (worms can generate a phenomenal amount of network traffic);
- Sending junk e-mails that may include information from/about the victim;
- Moving/deleting information on the victim system;
- Installing backdoors for subsequent misuse; and
- Permitting spammers to use victims' machines for sending spam while hiding their own tracks.

**Worms vs. Viruses**

While both worms and viruses can be classified as malicious code that spread through a network, the boundary between the two is muddy. There is no consensus as to “what is a worm?” and “what is a virus?” Stuart Staniford of *The Worm Information Center* differentiates between them as follows:
If the malicious code *can break into another computer and start running without any human intervention, then it’s a worm.*

If the malicious code piggybacks on some other content and it depends on explicit human intervention in order to get started, then it is a virus.

The confusion arises in the case of e-mail worms that depend on users to open an attachment in order to set them free. This type of malware has been dubbed “worm-like viruses.” Thus to distinguish between the two comes down to whether or not the malicious code is self-activating. Using this rule, Code Red, Slammer, and Blaster would be classified as worms; I Love You and SoBig would be viruses and Nimda would be indeterminate because it has the capability of both viral and worm spreading algorithms.

Operation-wise, the biggest difference between worms and viruses has to do with the time it takes for an infection to spread. Due to their self-replicating features, worms spread at lightening speed compared to viruses. On the other hand, viruses are much more common. This is due to the fact that they have been around longer. Existing antiviral defenses are adequate against most virus attacks, provided that the software has been installed on your computer and kept up to date.

Unfortunately, most AV defenses are fairly useless in stopping or slowing down the initial spread of a worm. Their value lies in preventing your computer from becoming re-infected—assuming of course, your signature files are kept up-to-date.
Sample Worms

It seems that every week, the news is reporting the emergence of a new worm. Some of the more (in)famous worms that have exploited Microsoft vulnerabilities include:

**Bugbear**
URL: http://securityresponse.symantec.com/avcenter/venc/data/w32.bugbear@mm.html.

**Code Red**

**Nimda**
URL: http://securityresponse.symantec.com/avcenter/venc/data/w32.nimda.a@mm.html.

**SQL Slammer**

**MSBlast**

In addition, we would be remiss if we didn’t point out that both the Apple and the Linux operating systems (OSs) are also vulnerable to worm attacks. Though infrequent, some of the more notable worms for Linux include:

**Linux/Adore**
URL: http://www.sophos.com/virusinfo/analyses/linuxadore.html.

**Linux/Cheese**
How Worms Work

Regardless of the OS, all worms need several interdependent components to cooperate in order to work. They need: (i) a spread algorithm for finding other hosts, (ii) one or more exploits allowing them to break into other computers remotely, and (iii) a payload, which is what it does to your computer after it’s broken into it, other than just using it to spread.

Oftentimes, a user may be unaware that his/her computer has been infected by a worm until it is too late. In part because a worm can infect a single machine and then propagate to another machine while removing itself as it moves along. On the other hand, a worm can remain silent and invisible, idling in the background, until certain conditions are met.

However, once a worm is activated, it can send back information, trigger alarms, create status messages, or take any other actions for which it has been programmed. They can carry any kind of payload (from viruses to Trojan Horses).

In fact, the newer class of worms has evolved into a highly efficient multi-headed attack vector that can carry several executables as their payload.
Payloads: Past and Future

According to the *Worm FAQ* website, the types of relatively “benign” payloads that worms have been known to carry, include:

- Installing backdoors to later allow control of the computer.
- Defacing websites.
- Installing patches (so-called good worms).
- Conducting distributed denial of service (DDOS) attacks against other sites.

In terms of lethal payloads, it is feared (and some of these fears have already being realized) that worms will soon be able to:

- Damage hardware for example, by reflashing the BIOS of the computer.
- Mount large scale (retargetable) distributed denial of service (dDoS) attacks against many important targets simultaneously.
- Search for commercially or militarily significant information on infected computers.
- Steal personal information (for example, credit card numbers) from infected systems.
- Sale access to personal computers.

Finally, a type of malicious payload that has yet to materialize in the wild but is expected with the newer version of worms has been called “cryptographically signed updates” (CSUs). With CSUs, each worm can keep track of the computers it has infected and the ones
that is it is trying to re-infect. When the author of the worm is ready to upgrade (that is, release a new piece of malicious code), a worm embedded with a CSU would be able to perform the following functions:

- Verify that the code was signed by the appropriate private key
- Spread a copy to every other worm it has come in contact with
- Then execute the new (updated) code.

CSU-enabled worms would be able to spread like wildfire, allowing the author of the worm to modify or experiment with the levels of maliciousness, perform debugging one-the-fly and/or seek out new targets from an existing installed base of worms.

In conclusion, any one of these payloads would create a particularly destructive attack but used in combination, they could be truly devastating. For that reason, it is imperative, that you employ a range of countermeasures to avoid falling victim to a worm attack in the first place.

**Preventing Worm Attacks**

The best way to defend against a worm attack is to prevent one from happening in the first place! There are several precautions you can take to avoid becoming infected.

Many of the same lessons that were covered under the section on viruses still apply, but they are worth repeating...
Subscribe to the Secure Florida Alerts and Highlights <http://www.secureflorida.org> services to learn about the emergence of different types of malware and what action(s) you need to take in order to minimize your risk of exposure.

- Install AV Software (if you haven’t already) and make sure you regularly download the latest signature files.

- Regularly visit the Microsoft website to keep your OS up-to-date with the latest security fixes (patches).

- NEVER open an e-mail attachment unless you are completely sure what it is and whom it is from... and even if the e-mail appears to come from a friend or colleague, it could be carrying a lethal payload.

Please note: Microsoft and AV software vendors DO NOT send out updates as e-mail attachments. Updates are delivered as downloads from their website or they are included in the software. Any e-mail that informs you otherwise may be a trick to make you open an infected file. Unless you know you are receiving information from a reliable source, delete these types of e-mail immediately.

- Beware of hidden file extensions (see the section on Spam for more details).

- Disable features in your programs that automatically get or preview files. Those features may seem convenient, but they let anybody send you anything, including dangerous worms. Typically these are previewing files in Outlook or other e-mail programs.
- Don’t download an executable program just to “check it out.” If it is a worm, the first time you run it, you are infected and it can then spread independently of your actions.

- If you don’t need File and Print Sharing services for Windows then turn them off and/or uninstall them.

- When chatting online, never blindly type commands that others tell you to type, or run pre-fabricated programs or scripts (not even popular ones). If you do so, you are basically handing the control over your computer over to a complete stranger, which can lead to worm infection or other serious harm.

- If you engage in at-risk behavior (e.g., peer-to-peer (P2P) file sharing, playing interactive games and/or chatting online), consider running a sandbox in addition to your AV software. To find more details on setting up a sandbox, visit the Secure Florida website <http://www.secureflorida.org>.

References


Computer worm


Microsoft Update Service


Worm FAQ, The

Worms Threat Analysed
Underware

Definition

Underware (aka sneakerware, foistware, and snoopware) can be differentiated from malware in the sense that it is quasi-legal software the surreptitiously adds hidden components to your system—foisting them on naive users.

The term underware can be differentiated from malware in the sense that “bait” (e.g., free stuff, games, nifty apps, etc.) is dangled before unsuspecting users as an inducement to perform an “impulse install.” The bait element of the software bundle is the attack vector.

During the installation of the “bait,” the underware will be installed too, usually without the express knowledge of the user. Sneaker software is designed to spy and/or hijack the browser in order to divert users to other websites.

Secondly, to further differentiate underware from malware, the user’s consent—express or implied—is needed before underware products can be installed. Not surprisingly, the standard operating procedure is to make this request as obscure as possible, to ensure as large an installed base of users as possible.

Besides taking advantage of social engineering techniques, the main vectors that underware utilizes are:

“Targeting, profiling, and tracking individuals across the Internet is UNETHICAL unless the individual has given these companies explicit permission to do so. Absent explicit permission, surveillance represents spying which should be prevented, banned, and outlawed.” - Steve Gibson
• Clicking the “ok” button

• Low or nonexistent security

• Incorrect / default settings.

Plus, most underware developers count on the fact that most users won’t read the licensing agreement. Instead, they will blindly click “I agree” in order to get access to the bait.

For the most part, underware is able to mislead users in one of two ways:

*Misrepresentation of source*—this happens when a product claims to be from a single vendor when in fact it includes code that has been developed/packaged by an “undisclosed” third party. The classic example of this type of misrepresentation is adware that is bundled with P2P filing sharing applications.

*Misrepresentation of intention*—this occurs when there is a mismatch between what a product claims to do and what it actually does. For example, a product that promises to block advertisements shouldn’t come bundled with ads.

Underware can be classified as:

<table>
<thead>
<tr>
<th>Benign</th>
<th>Malignant</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adware</td>
<td>Backdoor Santas</td>
</tr>
<tr>
<td>BHO’s</td>
<td>Trojan Horses</td>
</tr>
<tr>
<td>Cookies</td>
<td>Spyware</td>
</tr>
<tr>
<td>Web Bugs</td>
<td>Stalkers</td>
</tr>
</tbody>
</table>

Note that the line between these two categories is fuzzy—they are not mutually exclusive. Whether they are considered benign or malignant is very much in the eyes of the beholder.
Common types of (benign) underwear are:

**Adware** allows targeted ads to appear on your screen. It is used to track your browsing habits and, unbeknownst to most users, it will report this information back to a central ad server. Shareware or freeware authors often use it to generate revenue from their software.

Permission to install adware is outlined in the fine print of the End User Licensing Agreement (EULA) and by clicking the “I accept” button; you have entered into a contract (a clickwrap agreement) that gives the adware company free rein over your machine. Unless you read the entire EULA, you might not be aware that you also are installing ad-serving software.

Even more disturbing is the fact that the EULA for the adware can be buried under a EULA for another product or service. While adware is the least offensive in terms of underwear, it is still quite intrusive, annoying, and sometimes disruptive. They can reset your home page, add links to your Favorites / Bookmarks and point you to a site of their choice even when you are trying to go elsewhere.

**Browser Helper Objects (BHOs)** enable developers to customize and control Internet Explorer (IE). As a result, applications which install BHOs have become popular and because BHOs don’t require a user interface (some of them create toolbars, but most of them don’t) that means it’s possible for BHOs to be installed without the user’s knowledge. While there are some valid uses for BHOs, the potential exists for them to be used for malicious purposes like gathering information on surfing habits.

Not surprisingly, some developers go out of their way to hide the presence of covert BHOs. In a constant game of one-upmanship,
companies that employ BHOs find ways around the most popular detection tools by changing their product regularly—just enough to avoid detection until the next version of anti-spyware software is released.

Cookies are a well-known mechanism for storing information about user behavior. These files are stored on the hard drive and their existence and use is not concealed from the user. In fact, at any time, you are free to modify your preferences and disallow access to cookie information. But be aware that if you decide to delete your cookies, the next time you revisit a website you may be restricted in your movements and be required to re-register. Because websites use cookies to keep track of your browsing behavior, cookies can be considered a benign form of spyware.

Drive-by Downloads (DBDs) are software-based auto-installers you inadvertently pickup whenever you visit a website that makes use of these types of application. Adult websites and game sites are famous for forcing self-installing DBDs on hapless users. These downloads can contain either benign or malicious underwater.

A web bug is a one pixel high by one pixel wide (1x1) transparent .gif image. Being transparent the user can’t see them, but an HTML-enabled viewer (which includes your browser and more importantly, your e-mail client) can. The browser will go out and fetch the tiny .gif from a foreign server whenever the image is displayed.

Since e-mail messages can be easily “bugged,” spammers are using these devices not only for confirmation purposes but as tracking devices too. Even if you never click on a link or you end up deleting the message, they can still tell whether or not you actually viewed their spam.
If cookies are enabled then you’re in for a double whammy—a full “cookie exchange” will transpire as well. For this reason, despite their size and simplicity, web bugs are considered to be a fairly intrusive and a major threat to one’s privacy.

If cookies and web bugs don’t get you, a new innovation called *fake dates*, can still be used to track your movements. By uniquely and individually “faking” the last modified date of a web bug, your online actions can be tracked just as deliberately and uniquely as if cookies were being deposited on your machine. How so? If your browser contains a web bug in its cache, it will query the server to find out if the image has been modified since the last “fake date” listed. Since everyone is given a “different fake date,” this process serves as a unique identifier and it can later be used to monitor your actions.

**Gimmicks**

Sites or applications that use techniques that can be classified as underware make use of or spring upon unsuspecting users, the following types of gimmicks:

- Porn without permission
- Missing or disappearing uninstallers or uninstallers that leave working code behind
- Hijacking searches
- Modifying web pages you visit
- Silent download and execution of arbitrary code
- Programs that fight back when you try to remove them
- Lost network and Internet connections
- Imperfect removal / removal refusal
- Gratituitous pop-ups and pop-unders
- Lousy Code causes errors and crashes
- Opening security holes
- Disabling security software, and
- Tampering with changes to settings.

Finally, should you come in contact with a site or application that relies on underware to keep track your movements, *caveat 'netor*— let the surfer beware. For more information on underware and how to eradicate it, visit the Secure Florida website <www.secureflorida.org>. In the next section, we focus on two pernicious forms of malicious code: Trojan horses and spyware.

**References**

BHO's- Browser Helper Objects


What is Adware?
Trojan Horses

“Beware geeks bearing code” – Unknown

“Trojan defenses have been getting better, but computer scientists have known for some time that future Trojans would be much harder to detect and eradicate. These "third-generation" Trojans ... are like cockroaches—they're very secretive, spread rapidly, and are almost impossible to stamp out.” – T. Bradley.

Definition

A Trojan horse is an independent program that appears to perform a useful function (such as gaming) but in reality, it hides an unauthorized program that allows the collection, exploitation, falsification, or destruction of data, without the user’s permission.

Trojan horses are similar in function to remote administrative tools (RATs) that are used by system administrators to install programs or update files on multiple computers from a central location. However, most Trojan horses found “in the wild” are illicit RATs.

A Logic Bomb is a special type of Trojan horse. It includes a feature (such as a timer) that causes it to perform some destructive or security-compromising activity. A logic bomb will lie dormant until certain threshold conditions/criteria are met. Crossing the threshold will activate the logic bomb code. The threat posed by logic bombs tends to come from insiders (for example, disgruntled or former employees).

A Hijacker is a Trojan horse that resets your browser’s home page and/or search settings to
point to another site (for example, one containing porn) loaded with advertising.

A new breed of malware, called *uber-Trojans*, is capable of completely hiding itself. These process-injecting Trojan horses attach themselves to a key process in Windows and then they proceed to deactivate any firewalls, antivirus programs, or anti-Trojan horse programs that might be installed on the machine. Once that mission is accomplished, the user is no longer in control of the computer, much less its assets.

**Trojans vs. Worms vs. Viruses**

A Trojan horse differs from a virus in that it is a stand-alone program. Usually a virus is a portion of code that targets specific applications such as Microsoft Word or Excel. Nor does a Trojan horse require a host program in which to embed itself. A Trojan horse differs from a worm in that it does not move from one computer to another on its own. A person must transfer it intentionally, using some type of container that is, an e-mail/attachment, script, program, and so on. Worms generally act as the attack vector and a Trojan horse or virus functions as the payload. In addition, the newer Trojans horses are being used to lay the groundwork for Distributed Denial of Service (DDoS) attacks.

While Trojans horses are not much different from the vectors that deliver viruses or worms, there is a key difference and that has to do with purpose. Viruses and worm are explicitly designed to cause disruption and they make themselves known by the damage they produce. For Trojan horses, just the opposite is true. They try to stay hidden for as long as
they can so that the attacker can take control of the machine.

**How Trojans Work**

A Trojan horse has two parts: a server and a client. Contrary to expectation, the *server* is installed on the victim’s machine and it contains a program or file that masks the Trojan horse. The *client* remains on the attacker’s system. Once the server is resident on the machine, the Internet is used to establish a connection between the victim’s machine and the attacker. Using remote access, the attacker can perform almost the same actions as if he was right there - copy/view/delete information from the hard drive, run applications, change settings, and control the infected computer’s hardware. All of this can be done without the user of the infected machine being aware that the computer has been taken over by a hostile party. In fact, a user may never realize that a Trojan horse has been mounted on their machine, or they discover it only by accident.

In theory, there is no limit to what a Trojan horse can do. In reality, most are used as a backdoor, or trapdoor—the classic example is Back Orifice.

Hackers also use Trojan horses to turn personal computers (PCs) into “zombies.” It is not uncommon for an unwitting user to get “a knock on the door” because the FBI has traced a denial of service attack back to their IP address. Or worse still, the user is served a subpoena because a stash of pirated “warez” (hacker tools), put there by somebody else, is discovered on his or her PC.
How Trojans Get In

Most Trojans horses are spread by infiltrating small utility programs (for example, screen savers, wall paper for desktops, games, pirated warez) or applications (for example, spread sheets, web pages, greeting cards). They can be sent via e-mail. Or, they can hide in a worm. Trojan horses can be installed on your machine by another user. Or, they may come bundled with decoy software (that is, when opened, the program does what it’s supposed to do, plus it secretly installs a Trojan horse in the background). Nor is it unusual to find that one or more have been secretly installed on one machine, just waiting for someone to sniff them out. There are thousands of hackers scanning the Internet at any one time, looking for Trojan horses that can be used for mischief making.

Worms aren’t the only means for spreading Trojan horses. Peer to Peer (P2P) file sharing programs have become another popular attack vector. Grokster and Limewire were used to spread W32.DIDer, a Trojan horse that was designed to copy user ID names and Internet addresses. To eliminate the vulnerability, these companies were forced to rewrite their software. Likewise, attackers are also taking advantage of the vulnerabilities in Instant Messaging to hide Trojan horses.

The key point to remember when dealing with this type of attack vector: Trojan horses do not need to infect a network, system, disk, or file in order to spread. They rely on someone (users, hackers) or something (programs, files, other malware) to be executed.
Sample Trojans

Because of their covert nature, it is difficult to Pinpoint how many Trojans may be in existence. Some of the more infamous ones are:

**Back Orifice**

**SubSeven**

**Sysbug**

Do I Have a Trojan

To determine if a Trojan horse has been placed on your machine, perform the following check:

- Scan your computer with an anti-Trojan horse program to see if it is infected - bear in mind that the toughest ones will be too well hidden and too well disguised to easily locate.

- Is your hard drive constantly active when you’re online—despite the fact that no auto-update processes are running; no files are being downloaded; and no websites are being accessed.

- Is your AV program or firewall working properly—if this happens to be the case, this type of Trojan horse may be impossible
to eradicate, short of wiping your machine and starting over.

**Anti-Trojan Software**

The following programs are listed in the order of their robustness:

**TrojanHunter**
URL: http://www.misec.net/.

**PestPatrol**
URL: http://www.pestpatrol.com/.

**TheCleaner**

**Trojan Defense Suite**

**BOClean**

**Online Scanning Tests**

If you don’t have anti-Trojan software, you can run scans/tests online to see if your computer is infected. The following sites have been identified by Secure Florida <http://www.secureflorida.org>:

**PCFlank.com**

**Trojanscan.com**
URL: http://www.trojanscan.com/.
Don’t be Duped

Trojan horses, like their historical counterpart, prey upon the trust of unsuspecting users. To avoid being infected with a Trojan horse, do the following:

- Follow the same precautions recommended for viruses and worms that were outlined previously

- Consider having anti-Trojan horse software installed on your machine or else visit a reputable online site that scans for Trojans.

- Add a firewall: ZoneAlarm, Black Ice, McAfee, Norton, and Tiny Personal Firewall are some recognized vendors.

In addition, there are many other products on the market that will warn you if data tries to leave your computer without your knowledge.

- Be careful when visiting dubious websites and be very suspicious if any strange or unexpected popup windows appear on your screen.

Last but not least, because Trojan horses are designed to be cunning and opportunistic. It is next to impossible to get rid of them. Most all-purpose AV programs are completely ineffective when dealing with the 3rd generation Trojans—in part because this new crop of nasties are programmed to turn off and disable your defenses.

To avoid becoming infected in the first place and to learn state-of-the-art best practices, visit the Secure Florida website <www.secureflorida.org> and be sure to sign up for the Alerts and Highlights services.
References

AntiTrojan Tools


Extensive links to anti-Trojan resources


Kerner, Sean Michael (2004) “Fake Microsoft Service Pack is Xombe Trojan,” Internet News,

Trojan Defenses

Trojan Horse

Trojan Horse

Trojan Horse Attacks

What is a Trojan Horse's Trapdoor?
Spyware

"When you get the urge to download and install that great new piece of software, take a moment to find out if it is a known spyware program. This will save you the headache of trying to get rid of it later. You can lookup the programs at spywareguide." – Russell James

“Consumers can avoid spyware by taking the time to closely read software privacy policies and descriptions before they download the programs.” – Brian Krebs

Definition

Spyware is defined as any product that employs a user’s Internet connection in the background to send information to another destination on the Internet. Most commercial spyware programs are fairly innocuous—these companies gather information to build user profiles for statistical data, or to repackage and sell consumer information to third parties to do targeted advertising. For this reason, they collect referrer information (log data that reveals what URL you linked from), IP address (identifies location on the Internet), and system information (time of visit, type of browser used, operating system/platform, and CPU speed).

Other types of spyware programs, bundled with freebies, may contain spyware that scans for proprietary data and communicates with unauthorized remote hosts. This latter type of malicious code has recently come to public attention and is now raising the alarm bells. Many of these spyware programs that are being installed without users’ express permission pose significant security and privacy risks.
Spyware differs from adware in that it involves a two-way flow of information, whereas most adware involves only a one-way flow. In this respect, spyware has the ability to act like a Trojan horse, allowing your machine to be controlled by a third party and unless you’ve installed a host-based firewall that reports network activity, you may not be aware that many common personal productivity programs (for example, Microsoft Money) and some hardware (for example, a wireless mouse and keyboard) communicate with the vendor at regular intervals. This form of spyware is often referred to as “nagware.”

**Earmarks of Spyware**

Most spyware is considered “anti-consumer” because it is primarily designed to:

- Collect information (personal, financial and behavioral)
- Transmit a unique code (for tracking purposes)
- Log keystrokes/make screen captures/record conversations
- Monitor computer use and habits
- Reinstall itself, even if it has been removed
- Perform any other actions for which is has been programmed

*ALL without the user’s knowledge or consent!*

Even when consent is obtained, it has probably been secured by using some form of subterfuge or obfuscation which means the user has not been properly informed as to its existence and intent. This capability, often
referred to as the “auto-update” feature, is particularly bad for users in the sense that they threaten the security of computers and undermine the integrity of online communications.

Programs to watch out for:

- Aureate/Radiate
- Bonzi Buddy
- ContextPro
- Cydoor
- Download Demon
- Ezula
- Gator
- KaZaA/Grokster
- IMesh
- RealDownload
- SmartDownload
- TOPText/HOTText
- TSADBOT
- Xupiter

Lover Spy is another deceptive program that should be avoided. Heavily advertised through spam, this spyware app poses as a (fake) greeting card. It tricks the would-be victim into performing an install—by claiming to be a plug-in—needed to view the card. Once it is loaded, Lover Spy records e-mails, chats, web site visits, keystrokes; steals passwords, and takes screen shots of opened windows. Then, this information is secretly e-mailed back to the person who sent the card.

Ethical Conduct

According to the Center for Democracy and Technology, a better label for spyware would be “trespassware” and a number of sources, most notably Steve Gibson have begun advocating for a Code of Back Channel Conduct (CBC). As a start, he recommends:

- No unnecessary information gathering
- No insecure capabilities
- Formal online privacy statement
- Preemptive request for consent
- Removable with Windows Add/Remove Programs, and
- No Fine Print “Funny Business.”

In addition, Gibson argues that the silent background use of an Internet “backchannel” connection must be: (i) preceded by a complete and truthful disclosure of proposed backchannel usage and (ii) followed by the receipt of explicit, informed consent for such use.

**Detection and Removal**

Because spyware installs an executable file along with other files in various locations throughout an operating system (spyware traces), trying to remove the spyware without the use of a dedicated anti-spyware tool will leave behind the traces. This means that some of the symptoms might be alleviated but it won’t get rid of the problem. In fact, some types of spyware can retaliate when any attempt is made to remove them.

In other cases, the spyware changes names and jump from one location to another when it realizes it has been detected and is about to be destroyed. As a result, anti-spyware strategies that work in one context might not work in another. The rapid metamorphosis of spyware points to the need for an automated update system, as well as a dedicated antispyware program that has the ability to adapt as it encounters new spyware patterns.
Even though the use of spyware on home computers is a relatively new phenomenon, a number of very good anti-spyware tools have been developed and are available for a small fee (donation) or can be downloaded from your ISP (for example AOL, Earthlink, and MSN have announced that they will soon begin providing automated anti-spyware).

To get rid of spyware, a three-prong approach is recommended:

1) Obtain and run a well-known and trusted spyware detection and removal program.

2) Obtain and run a popup blocker that has been developed/provided by a reputable company.

3) Obtain and run a decent firewall program (i.e., one that can be configured to monitor and block outgoing traffic).

Finally, we would be remiss if we didn’t point out that there is a downside. If you remove any adware or spyware that comes bundled with hardware/software, you may disable the host program. Secondly, you should be aware that some scanning tools produce false alarms.

For this reason, you need to proceed with caution before removing any program otherwise you may end up destroying or corrupting the wrong app! Read all the documentation (Help or FAQ files) before attempting to remove any pests and last but not least, when installing any new programs, be sure to make backups—and that includes your data too!
Anti-Spyware Tools

If you suspect that your computer has been infested with one or more varieties of spyware, the best thing to do first is to install and run one of the freely available spyware detection and removal tools:

- **Ad-Aware**
  URL: http://www.lavasoftusa.com/software/adaware/.

- **BHODemon**

- **Spy Sweeper**
  URL: http://www.spysweeper.com/.

- **SpyBot - Search and Destroy**

Spyware Removal Tips

Because these programs are running in the background and are sending and receiving data, they will eat up system resources and slow your computer down. To remove these programs, do the following:

1) Run a virus scan with an up to date Anti-Virus software package to make sure that the spyware is the only problem slowing your computer down.

2) Use an anti-spyware removal tool to identify/eliminate any underware resident on your machine.
3) Download a popup stopper/blocker.

4) Delete temp files and (non-essential) cookies and temporary internet files.

5) Defrag your hard drive on a regular basis (see the section on Maintenance for more information on how to optimize system performance).

Spyware Prevention

To protect against underware, some countermeasures you can add to your security arsenal include the following:

Install an Outbound Blocking Firewall

ZoneAlarm (free for personal use), for example, is a firewall product that has been specifically designed for outbound traffic detection and blocking. It can be used to detect if any spyware has been installed on your machine.

Set Activex Controls

The most common vector for unwanted installation of spyware programs (besides clicking the ‘ok’ button without looking) is using low security or incorrect settings of these Active-X control buttons. If you are using Windows XP and Internet Explorer, there are some browser settings that can be configured to deal with how Active-X controls are handled by your browser.

Be forewarned: never "blindly accept” Active-X" software installations.

Activex controls are programs that can be run by Windows operating systems straight from a
web page and many developers use Active-X controls to enable the installation of their software. To avoid this, visit the Secure Florida website <www.secureflorida.org> and download a set of instructions that will walk you through the process of disabling these types of controls.

**Do not download any files or software, including browser plug ins, updates, etc.**

Unless you are not 100% sure of that you are dealing with a trusted source, and even then, you still need to exercise caution.

To safeguard against unwanted software—first and foremost—read the fine print. The majority of spyware applications attempt to install themselves either from security permission windows or as an “opt-out” feature software.

To opt-out means that the program will be installed by default and you must specifically request—during the install—that it NOT be added.

**Read the End User Licensing Agreement**

Almost all legitimate software installations will include an End User Licensing Agreement (EULA) that includes a lot of information. You should make a habit of reading these EULAs. Ideally, they should tell you exactly what they intend to install on your machine and the limitations to your use of the software. If the EULA is hard to find, or if the documentation is unreasonably difficult to read and understand, then maybe you should think twice before agreeing to install the software. Secondly, if you take the time to read the EULA before you click “ok,” you are less likely to have any spyware being installed on your machine without your knowledge or consent.
Pay Attention to Security Warnings

"Security Warning" screens that flash on the screen need to be heeded. This bit of advice is self explanatory!

Finally, to keep abreast of all the changes in the area known as underware, be sure to visit the Secure Florida website <www.secureflorida.org> on a regular basis and sign up for the Alerts and Highlights services so you are informed when a new kind of threat emerges that places you and/or your assets at risk.

References


spyware

SpyWare, AdWare and MalWare

Spyware, begone!

Spyware Guide

Spyware Protection and Removal


Blended Threats

“This blending of worms and spam indicate that spam—usually seen as a nuisance or legal risk—poses security risks, too.” — Gartner

“Security experts are tracking a new piece of malware that appears to be compromising large numbers of Windows PCs and may be laying the groundwork for the creation of a large spamming network or a major attack in the future... Analysts at NetSec Inc., a managed security services provider, began seeing indications of the compromises early Thursday morning and have since seen a large number of identical attacks on their customers' networks. The attack uses a novel vector: embedded code hidden in graphics on Web pages.” — Dennis Fisher

Definition

Spacking, a new type of blended threat, represents the combination of spammers and malicious code writers who are joining forces to create a new generation of attack tools called “combo malware.” Until recently, spammers, hackers and malware writers were three distinct entities. This isolation has ended, with potentially serious consequences.

Combo malware is a hybrid menace that combine several species of malicious code (viruses, worms and Trojan horses) into a single attack vector, making it much harder to detect, much less eradicate. In fact, most modern viruses include worm characteristics for propagation. An important feature of blended threats is their ability to circumvent firewalls and AV software and exploit vulnerabilities to launch a cyber attack. For these types of attack vectors, the deeper the level of penetration, the more likely the attacker will be able to disguise the breach.
Recent Trends

Symantec reports that in the first half of 2003, the number of blended threats increased by 20 percent. The speed of propagation is also increasing. Blaster, a slow worm by today’s standard was able to infect as many as 2,500 computers per hour. Given the speed with which worms can now be spread, Symantec expects to see more overloads to network hardware—crippling network traffic and seriously preventing both individuals and businesses from using the Internet. (For a progression of these types of threats over time, see Figure 2).

Another trend to emerge is one driven by greed. Gone are the days when malware writers created viruses and worms in order to boast about their achievements or to get their 15 minutes of fame in the media (like with the Warhol viruses). Nowadays, most worms are carefully engineered attack vectors that steal financial and personal data from victims.

Examples of recent Internet worms that were developed for ‘money’ as opposed to ‘ego’ are Mimail, Tanatos, and SoBig. Mimail tricked users into believing it was a PayPal membership update in order to steal credit card information. The Sobig worm revealed its connection to the spam community by first installing a spam-routing program on infected systems and then removing itself so as to evade detection. It has since been speculated that one of the reasons why no new variants of the Sobig series has appeared since August 2003 is the $250,000 bounty that has been placed on the head of its author - a worm writer seeking recognition might be tempted to take on Microsoft, but a worm writer looking to profit from their exploits will duck out of sight.
Malware Trends

Figure 2

G = generation
What makes Sobig.F different? First of all, this is the first worm to blur the line between malware and spam. It uses techniques common to both. Secondly, it spread quickly and widely. The AV antidotes were only effective against secondary infections. Finally, it represents a new generation of e-mail threat. In fact, the new crop of worms, of which Sobig.F is a harbinger, are much better at evading detection and maintaining self-control.

Worst-Case Scenario

To get an idea of what a future attack might look like, consider the following:

An individual or group hacks into a website of a reputable software vendor and, instead of defacing the home page; they replace downloadable copies of the vendor’s software with modified versions of their own software and then cover all of their tracks.

The modified software still performs as expected, but it also has been programmed to gather intelligence, which reports back, using a service such as email or HTTP, which easily gets past any firewalls that might be in place.

The infiltrated program also contains a logic bomb that has been programmed to launch a denial of service attack against either the host network once the Trojan horse has been detected.

While this scenario might sound like science fiction, in fact, the know-how currently exists to mount these types of attacks.
Taking Precautions

Here are some of the precautions you can take to avoid falling victim to blended threats:

- *Never install or run “untrusted” software*—sounds easy, but it’s not. Although you may have used a vendor’s software in the past and you trust them, you need to be aware that their site might have been hacked. To be absolutely certain, rely on digital certificates/ signatures or hashes (a cryptographically signed checksum) to guarantee that that the package you install is the same as the one the author or vendor originally released.

- *Monitor system activity and network connections to ensure that all the processes running on your computer are both authorized and accounted for*—again, easier said than done, given that most networks and operating systems run a large number of processes that are unknown to the average user.

- *System hardening and patching is essential*—no doubt, you’ve heard this a hundred times already, yet many computer-based services continue to be deployed with minimal security. With combo malware on the way, it’s time to get serious about locking down your system.

- *Don’t be tricked by social engineering*—think twice before you click, and never give out any passwords or personal information without verifying who is making the request and why. Better to be safe than sorry.

- *Use up-to-date anti-malware software*—some AV programs can stop malware in its tracks, other programs only detect and
remove malware. To keep up to date with the latest trends, subscribe to the Secure Florida Alerts and Highlights services <www.secureflorida.org>.

Just securing the perimeter is no longer sufficient. With combo-malware a holistic defense strategy is needed and the next generation of tools must be able to identify any suspicious or unusual activity. Most malware needs cooperation on the part of user before it can penetrate your system. By addressing multiple vulnerability points, hardening your overall system and preparing for the worst, you should be ready for the next onslaught.

**References**


Part IV

Asset-related Threats
Internet Cons

“It’s a dark night in a foreign town. You’re a tourist. Do you a) wander around unlit back alleys flashing your Rolex, speaking English loudly and constantly referring to your Lonely Planet guide or b) stay in well-lit good neighbourhoods and get advice from your hotel where they are? It’s obvious really... But when it comes to the Internet, a depressing number of people (and businesses) lack the street smarts to avoid becoming a victim of online crime. You might think it won’t happen to you—and by following a few simple rules, it won’t—but cyber-fraud is on the rise.”

- Matthew Stibbe

Definition

To qualify as cybercrime, the intended fraud or scam must involve the use of a computer (for execution and transmission purposes) and the solicitation or transaction must take place in a virtual venue (for example, in a chat room, through e-mail, on a message board, or through a website).

Trends

Once the Internet and the World Wide Web “opened” for business, they became a haven for fraudsters and scam artists, looking to make a fast buck.

Each technical innovation spawns a new wave of swindles that are even more insidious, more deceptive, and more harmful than the previous generation of cons. Add to the mix the risks posed by spam, malware, and underware and a very disturbing pattern emerges ... the risk that YOU will become a victim of cybercrime has never been greater.

During the past ten years, just about every type of scheme imaginable has been tried online. Table 5 shows a breakdown of the
## Table 5
### Internet Cons

<table>
<thead>
<tr>
<th>Ages of Victims</th>
<th>Under 20</th>
<th>3 %</th>
</tr>
</thead>
<tbody>
<tr>
<td>20-29</td>
<td>25 %</td>
<td></td>
</tr>
<tr>
<td>30-39</td>
<td>28 %</td>
<td></td>
</tr>
<tr>
<td>40-49</td>
<td>25 %</td>
<td></td>
</tr>
<tr>
<td>50-59</td>
<td>14 %</td>
<td></td>
</tr>
<tr>
<td>60-69</td>
<td>4 %</td>
<td></td>
</tr>
<tr>
<td>70+</td>
<td>1 %</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Type of Scam</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Online Auctions</td>
<td>90.0 %</td>
</tr>
<tr>
<td>General Merchandise</td>
<td>5.0 %</td>
</tr>
<tr>
<td>Nigerian Money Offers</td>
<td>4.0 %</td>
</tr>
<tr>
<td>Computer Equip/Software</td>
<td>.5 %</td>
</tr>
<tr>
<td>Internet Access Services</td>
<td>.4 %</td>
</tr>
<tr>
<td>Work-at-Home Plans</td>
<td>&lt; .1 %</td>
</tr>
<tr>
<td>Information/Adult Services</td>
<td>&lt; .1 %</td>
</tr>
<tr>
<td>Travel/Vacations</td>
<td>&lt; .1 %</td>
</tr>
<tr>
<td>Advance Fee Loans</td>
<td>&lt; .1 %</td>
</tr>
<tr>
<td>Prizes/Sweepstakes</td>
<td>&lt; .1 %</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Initial Contact</th>
<th>WWW</th>
<th>94 %</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Email</td>
<td>6 %</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Payment Methods</th>
<th>Credit Card</th>
<th>34 %</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Money Order</td>
<td>30 %</td>
</tr>
<tr>
<td></td>
<td>Check</td>
<td>14 %</td>
</tr>
<tr>
<td></td>
<td>Debit Card</td>
<td>7 %</td>
</tr>
<tr>
<td></td>
<td>Bank Debit</td>
<td>6 %</td>
</tr>
<tr>
<td></td>
<td>Cashiers Check</td>
<td>3 %</td>
</tr>
<tr>
<td></td>
<td>Cash</td>
<td>2 %</td>
</tr>
<tr>
<td></td>
<td>Wire</td>
<td>1 %</td>
</tr>
<tr>
<td></td>
<td>Other</td>
<td>3 %</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Company Location</th>
<th>California</th>
<th>16 %</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>New York</td>
<td>9 %</td>
</tr>
<tr>
<td><strong>Florida</strong></td>
<td>8 %</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Texas</td>
<td>6 %</td>
</tr>
<tr>
<td></td>
<td>Outside U.S. or Canada</td>
<td>5 %</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Victim Location</th>
<th>California</th>
<th>13 %</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>New York</td>
<td>7 %</td>
</tr>
<tr>
<td></td>
<td>Texas</td>
<td>6 %</td>
</tr>
<tr>
<td><strong>Florida</strong></td>
<td>5 %</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Pennsylvania</td>
<td>4 %</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Losses</th>
<th>Total</th>
<th>$14,647,933</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Average</td>
<td>$468</td>
</tr>
</tbody>
</table>

types of scams that have been foisted upon an unsuspecting public.

On the surface, the type of fraud associated with each of these schemes appears to be quite different; in reality, they are all variations on the same theme, that is, exploitation and human frailty that involve a predator and prey (victim) type situation.

Scam Artists

The reasons the Internet has become so attractive to scammers are many, but main factors driving the increase in cybercrime result from the combination of anonymity, low cost, rapid growth, and the adaptability of the medium. The purveyors of greed can hide by spoofing, they can avoid detection by commandeering zombie machines, and they can evade jurisdiction by running offshore operations.

Technically-savvy con artists are doing all three. The ease with which con artists and cyber thieves can use technology to practice deception is unprecedented. We, as law-abiding citizens, have yet to grapple fully with the implications of cybercrime, much less its impact on average users.

It is beyond the scope of the Florida Cyber-Security Manual to review individually each of the scams listed in Table 5. To get an inkling of how some of these schemes work, the section will focus on a longstanding con that uses e-mail as the primary attack vector—the Nigerian Money Offer and Phishing, a relatively new scam that uses a combo approach. In this scam, both e-mail and a companion website are used as the primary attack vector.
Then, we will focus on Auction Fraud—a cybercrime that represents the highest number of reported incidents by the Internet Crime Complaint Center (IC3); and finally, we will wrap up with a brief consideration of Urban Legends, Rumors, and Hoaxes—why they continue to thrive on the 'Net and what implications that has for security and productivity.

**Reporting A Scam**

If you are victim of cybercrime or you know someone who is a victim, you can visit the following website and fill out a form detailing the nature of the violation.

- How to Report an Email or Web Scam
  URL: http://www.fightidentitytheft.com/how-to-report-scams.html

**References**


Crimes of Persuasion: Schemes, Scams, Fraud

Fraud Victim Assistance and Education
URL: http://www.fraudaid.com/.

Internet Schemes, Scams, Frauds (ISSF)
NetScams
URL: http://www.netscams.com/.

ScamBusters
URL: http://www.scambusters.org/.

Nigerian Scam

“Nigerian advance-fee fraud has been around for decades, but now seems to have reached epidemic proportions... If you're tempted to respond to an offer, the FTC suggests you stop and ask yourself two important questions: Why would a perfect stranger pick you—also a perfect stranger—to share a fortune with, and why would you share your personal or business information, including your bank account numbers or your company letterhead, with someone you don't know?” – Federal Trade Commission

Definition

The Nigerian scam aka the 419 Fraud (named after the relevant section of the Nigerian Criminal Code) is a variation on the “advance fee fraud.” As one of the oldest scams on the Internet, running since the 1980s, it has evolved from snail mail to fax machines to email.

The Nigerian scam operates worldwide and has bilked millions of dollars out of victims who were taken in by the promise of a get rich quick scheme.

The Nigerian scam (see Figure 3 for a sample letter) can be recognized by the following features:

The message is marked “urgent” or “confidential” and is usually poorly written using all uppercase.

There is an appeal for “up-front” money to secure your involvement in their transaction. In return, they promise you millions of dollars for your help, once the transaction is completed.
Sample Nigerian Scam Letter

Date: Wed, 30 Jan 2003 05:11:48 -0700
From: DR.MARTIN ZINGAWA <martex@netster.net>
Reply-To: martex1@caramail.com
To: [user Id removed]
Subject: URGENT BUSINESS PROPOSAL

PRIVATE AND CONFIDENTIAL

ATTN: sir/madam,

I am a member of the contract award committee, federal ministry of petroleum and resources, Nigeria. I am in search of an agent to assist us in transfer of (USD35m) and subsequent investment in properties in your country, you will be required to

(1) ASSIST IN THE TRANSFER OF THE SAID SUM

(2) ADVISE ON LUCRATIVE AREA FOR INVESTMENT

(3) ASSIST US IN PURCHASE OF PROPERTIES.

(4) SEND ME YOUR BANKING DETAILS, HOME ADDRESS AND PRIVATE TELEPHONE/FAX NUMBER.

If you decide to render your service to us in this regard, 15% of the total sum of the above will be for you, and 10% for any expenses incurred during the process.

Please if you are interested kindly sent an email to me so that i can give you the modalities.

Alternative Email: (martzing3@caramail.com)

Yours faithfully,

MARTIN ZINGAWA

Fax: 234 1 7599389.

Figure 3
The pitch includes a scheme or reason for contacting you—like an inheritance that is tied up, money frozen by government or there has been a calamity of some sort.

Most Nigerian-schemers present themselves as important people like doctors, lawyers, or sons of ex-generals.

In return for helping extricate them out of an embarrassment or a legal problem, you will be entitled to a percentage of the booty.

They direct you to provide them with detailed information about yourself—personal data, letterheads, banking information.

Typically, the letter concludes with a statement that claims they are working with the Central Bank of Nigeria or some other official sounding bank.

**Gist of a Nigerian Scam**

To guarantee participation in the “opportunity,” the targeted victim is asked to pay some “minor” up-front costs (for example, bank fees, COD charges, and the like) on behalf of the sender. If the victim goes ahead and hands over the cash, he soon discovers that there are “complications” which requires him to make additional (advance) payments in order to secure the funds (sunk costs) that have already been paid out. Something always goes wrong: paperwork is delayed, officials need to be bribed or an unforeseen event takes place.

These “requests” continue until the victim runs out of money or pulls out of the deal.
This con works because it blindsides victims with the promise that they will receive huge sums on money in exchange for a willingness, on their part, to launder the money or help cover incidental costs.

Please note: to date, any funds stolen using the Nigerian scam have never been recovered. Secondly, the Bank of Nigerian disavows any association with the persons involved in this scam. Finally, there are hundreds of versions of this letter in existence, each one names different people, describes different situations, and comes from far-flung countries located all over the globe. The original ones came from Spain, the latest ones are coming from Afghanistan and Iraq.

The “best” way to avoid becoming victimized by this type of scam:

NEVER REPLY TO A NIGERIAN SCAM!!!!

References


Phishing

“Email users are being bombarded with authentic-looking messages that instruct them to provide sensitive personal information. It's called 'phising.' Individuals who 'bite' are exposed to identity theft.” – Privacy Rights Clearinghouse

“Phishing isn't really new—it's a type of scam that has been around for years and in fact predates computers. Malicious crackers did it over the phone for years and called social engineering. What is new is its contemporary delivery vehicle—spam and faked Web pages.” – Kay Russell

Definition

Phishing is a graphic term, coined by hackers to indicate how easily an innocent victim can be “hooked” online. This type of scam relies on e-mail to drive users to a spoofed website where they are tricked into sharing their passwords or credit card numbers. Phishing combines the use of e-mail and the web to create a deceptive attack vector.

For example, spam is used to lure users to websites that look like those of reputable companies, and social engineering techniques are used to pressure users into divulging critical information such as passwords or financial data. Major corporations who have been hit by this scam include: Best Buy, eBay, and Citibank. Information obtained in this matter is later used to commit identity theft.

The main elements involved in phishing (also called “carding”) are:

- The source code of a major website (an ISP, major retailer, a financial services company) is copied.
A fake e-mail (usually HTML-based) is sent out with a link to the spoofed page.

The e-mail informs the user that there has been a problem with their account, e.g., the social security number is missing.

The recipient is instructed to fix the problem by entering their credit card numbers or other sensitive personal information at the site or else they risk having their account terminated or access will be denied.

The phishing messages being spammed to users will contain legitimate “From:” e-mail addresses, logos, and links that have been appropriated from reputable businesses such as AOL, PayPal, Best Buy, Earthlink and eBay. These elements are used deliberately to confer a feeling of legitimacy and authenticity.

Such sites will ask you to input your name, address, phone number, date of birth, Social Security number, and bank or credit card account number. Providing this kind of information will leave the person who responds to the query at great risk for identity theft.

How Phishing Works

The key thing to remember—phishing is a two-part scam that works as follows: the “look and feel” of a well-known company is spoofed. This can be done by simply downloading the source code with the images and saving it on another server.

To the casual observer, the forged website appears to be an exact replica of the original site. Don’t be fooled. There are some subtle differences and you need to look for these. On first blush, the URL (address) will look real but
if you look closely you’ll notice some hard to detect elements (for example, spaces or underscores or hyphens) that have been added to give the appearance that the URL is bona fide.

Another popular modification, called “link alteration” involves the alteration of the return address in a web page to make it go to the hacker’s site rather than the legitimate site.

This is accomplished by adding the hacker’s address before the actual address in any email, or page that has a request going back to the original site. To check whether the URL has been modified in this fashion, you need to look at the source code. Either of these tricks will ensure that anyone who clicks on the link is routed to the spoofed site and not the real one.

Next, the hackers will spam millions of users with a barrage of e-mails falsely claiming to be from the “real” company. This e-mail will inform the recipient that if he doesn’t update his account information ASAP, his account will be closed. To prevent this from happening, the e-mail urges the person to click on the link provided. This link then takes the soon-to-be victim to a website that contains a form that can be used to input the information.

In addition to personal information, the person may be asked to enter their password or to include their credit card number. Once the form is submitted, it sends the data to the scammer and it returns the victim back to the “real” company’s website so he or she won’t suspect a thing.

What makes the phishing scam really underhanded is how very convincing it can be. If the victim happens to have an account with the company named in the e-mail and they are unaware that this type of fraud is being
perpetrated, then it is very likely the victim will do as instructed. Because it appears to be “legit,” it is not hard to understand why or how someone might be tricked into believing that they are dealing with a trusted source.

Ironically, phishing scams have begun appearing that play into our worse fears. The latest batch of spam crosses the line on the meanness scale. The latest scam advises users to sign up for a “new” service to protect their credit cards from fraud. They ask for updated credit card account information or other pieces of personal financial information and state that the consumer’s account will be immediately terminated if the information being requested is not provided.

**Rising Number of Attacks**

In recent months, the number of phishing attacks has increased dramatically (see Figure 4). According to the Anti-Phishing Working Group (APWG), Phishing scams surged to 1,100 in April, a 178 percent increase from the month of March. During the month of May, the number of unique phishing attacks reported increased 6 percent in May to 1,197, with an average of 38.6 reports each day, slightly higher than in April.

The APWG said that 95 per cent of these bogus emails employ so-called 'domain spoofing', which uses a forged 'from' address to hide the sender's identity. Gartner reports that close to one million people (roughly one in five Americans) at a cost of $1.2 billion were the target of a "phishing" scam in the past year.
Phishing Attack Trends

You May be a Victim If...

You have provided any personal information in response to a dubious e-mail.

*If you did, assume the worse.*

In all likelihood, there is an 80% chance that you will become a victim of identity theft.

*If you provided your social security number or your credit card number, the odds are even higher.*

Depending on how much time has elapsed (it might be too late) contact the major credit reporting agencies and have a fraud alert added to your profile. Depending on what
information you might have leaked, cancel your credit cards and/or set up new accounts.

When you get your bank/credit card statements, review them carefully to make sure there aren’t any unauthorized charges.

Finally, for more information on how to protect yourself and your assets, visit the Secure Florida website <www.secureflorida.org> and be sure to consult the sections on Scams and Identity Theft.

On the other hand, if not much time has elapsed and you move fast, there is a good chance that you can prevent the use of some of your personal information. Begin by following the prevention measures listed below.

**Prevention Tactics**

Do not “Reply to” or “Click on” a link in an e-mail that warns you (without prior notice) that your account will be shut down unless you confirm your billing information. Instead, contact the company cited in the e-mail using an authenticated telephone number or other form of communication that you are sure is genuine.

If you are submitting financial information through a website, be sure to check that there is a locked padlock / unbroken key on the browser’s status bar or look for “https://” at the beginning of the web address in your browser’s address window. While the presence of either one of these security indicators does not necessarily mean that the site is secure, their absence should cause you to proceed with caution.
Apply the latest patches for your web browser and/or operating system (see the section on Patches for more information or else visit the Secure Florida website <www.secureflorida.org>) and make sure that you are downloading patches from a reputable and trusted source. Do NOT click on any links for patches that have been sent in unsolicited e-mails. Any e-mail that instructs you to so is likely to be some kind of trick.

**Unearthing a Phishing Scheme**

If you have filled out a bogus form that asked you to provide password information for any of your accounts, then you need to change them ASAP.

After you have changed your password (read the section on Passwords or visit the Secure Florida website <www.secureflorida.org> to find out how to set up a strong (hard to break) password).

To determine if you might be a victim, check your transaction history to see if any fraudulent entries have been made. If not, you may be okay. If so, then you need to report this incident to the appropriate authorities IMMEDIATELY.

Next, review your credit card and bank account statements as soon as you receive them to determine whether there are any unauthorized charges, erroneous or atypical transactions. If your statement is late by two or more days, call the credit card company / bank to find out whether they mailed your statement. Also, take the time to confirm your billing address...
and account balances to make sure no changes have been made without your approval.

Because many phishing scams originate from outside the U.S, domestic phone number are not likely to work. If you receive a suspicious e-mail, verify the phone number and area code, mailing address, and any other information that can be used to authenticate the company and confirm the legitimacy of the website.

Finally, report suspicious activity to the FTC. Send a copy of the actual phishing e-mail (including header information—note the section on Spoofing explains how you can do this) to:

   URL: uce@ftc.gov .

You can also forward any suspicious e-mail to the Better Business Bureau at:

   URL: nophishing@cbbb.bbb.org .

Notify other companies that are being victimized as well.

If you believe you have been defrauded, file your complaint at:

   URL: http://www.ftc.gov

or else visit the Secure Florida website <www.secureflorida.org> to get up-to-date links for websites that provide self-help information on Identity Theft for residents of Florida.
Inspecting URLs

Before clicking on any link that is contained in an e-mail message, verify the following:

Is the URL (web address) familiar? If not, it may not be real. For most legitimate websites, the URL will contain the organization’s name or trademark followed by a “.com, .org, .edu, .net, .gov, .us, .info,” and so on.

Does the URL (i.e., web address) string start with “https://”? This will be your first clue that the site is protected by data encryption. As a general rule, most scam artists don’t go to the trouble of encrypting their websites.

Does the URL contain a lot of characters, with the legitimate business embedded in the string? Note: NOT all excessively long URL’s are bogus. But to be on the safe side, before clicking on any link, verify that the e-mail is coming from a reliable source.

Is the URL taking advantage of browser display bugs? For example, is it using a floating address bars that mask the true web address. For more information on cloaking techniques, consult the section on Spoofing or else visit the Secure Florida website <www.secureflorida.org> to discover more “defensive” tactics.

Are there any spaces or gratuitous characters or words in the URL? Some fraudsters spoof legitimate websites by embedding spaces or hyphens in the names. For example,

www.e-bay.com

www.master card.com

or they hide the information in plain sight. Using clever syntax, scammers create legitimate sounding web addresses:
www.visa-security.com

that look the real deal but are NOT!

Lastly, pay attention to the fonts. A common trick is to replace lowercase “l’s” with uppercase “I’s”. Even if the e-mail client draws these characters in a slightly different way, there is no discrepancy in the way they are written in the URL, so the visual cue is lost. For example, a recent phishing scam used a combination of serif and sans serif fonts to obfuscate:

www.personal.barclays.co.uk/goto/pfso1b_login

To anyone using a sans-serif font, that URL might look completely genuine—even if you carefully read the source code.

Checking Source Code

To verify the HTML source code of a suspicious e-mail message or web form, do the following:

1. Depending on your browser, hit the appropriate button to view the source code.

2. Once the source code is viewable, perform a search to find the <form> tag to determine where the form results are being sent. The tag will probably look something like this:

<form action="/cgi-bin/FormMail.cgii">

Note that if the <form> action starts with the string “http://…” then the results are being processed on a separate server.
3. Next, look for a hidden field below the `<form>` tag that will look something like this:

```
<input type=hidden name="email" value="phisherID@BEaCon.com">
```

This is the e-mail address that will receive the results of the form. So, if the e-mail looks like it is coming from a reputable company but any information provided in the form is being sent to BEaCON.com, you should immediately suspect something phishy!

4. Next, try to determine who is responsible for the servers referenced in the form and who owns the e-mail account (see the sections on Networks and Spoofing to learn more about what tools you can use to find out this type of information).

## Tracking Down Rogue Servers

The best way to track down parties who might be responsible for a server that has been used by a phishing scam is to use of the various WHOIS services located on the web. However, for privacy reasons, please note that some of the information you need (for tracing purposes) might not be publicly available.

First, take the domain name or IP address you found in the e-mail or web page and then do a “whois” search. For example, these search tools can be found at:

- Network Solutions WHOIS Server
Avoid Getting Hooked

By following the suggestions listed below, you minimize your chances of becoming hooked by a phishing scam:

Any e-mail request for financial information or other personal data should be viewed with caution. If you receive such an request, do not reply to the e-mail and never respond by clicking on a link contained in the message. Instead, use legitimate phone numbers or web addresses (provided in your bills / monthly statements) to verify if the e-mail is genuine.

NEVER send personal information (credit or debit card number, Social Security number or PIN) in response to an e-mail request from anyone or any entity. Legitimate businesses and/or government agencies will never ask you to provide any kind of confidential or financial details via an e-mail request. However, if you complete an online transaction form (i.e., order a product, activate an account, subscribe to a mailing list or enroll in a program), you should expect to receive a confirmation e-mail from the company/entity that notifies you of the transaction.
Keep a record of your online transactions by saving or printing a copy of the transactions details or the order confirmation number.

Stay clear of e-mails from businesses that alert you to customer account problems and asks you to divulge personal information such as account numbers, PIN numbers, passwords, user names, Social Security Numbers, mother’s maiden name and other sensitive data.

On the other hand, if you happen to receive an e-mail from a company or agency that routinely does business with you, be suspicious if the e-mail:

- Fails to confirm that the sender does business with you by referencing a partial account number.
- Informs you that you have been the victim of fraud.
- Has spelling or grammatical errors.
-Warns you that your account will be shut down unless you reconfirm your financial information.

Be extremely cautious when providing personal and account information online. Make sure to verify a business's legitimacy by visiting their website, calling a phone number obtained from a trusted source, and/or checking with a reliable resource such as the Better Business Bureau's BBBOnLine Reliability Program.

Never use regular e-mail to send payment information because it is insecure. Most reputable merchant sites use encryption technologies that protect data from being accessed by others when conducting an online transaction.
When filling out a form, always answer the minimum number of questions.

- If the information being requested is optional, leave it blank.

- If asked to provide information concerning your age, income, or any other personal stats in order for the form to be accepted, type in obviously “false” information.

- If the form has a “comments” section, let the vendor know that because of the risk of identity theft, you should not be compelled to provide this type of information.

- Lastly, before clicking on the send button, read the website’s privacy policies. Find out what types of information the website gathers and how it will be used. If the company doesn’t have a privacy policy: (i) use the “comments” section to complain and (ii) be extra careful about what kinds of information you provide. The absence of a privacy policy could mean that your information is being sold to a third party.

**Business Counter-Measures**

There are a number of actions large and small businesses can take to minimize the risk to your customers:

- Personalize e-mails so customers are assured of their legitimacy. Also, be sure that any e-mails you send are strictly professional (i.e., no typos, no sloppy grammar, no spam-like mass mailings).

- Keep digital certificates up-to-date so customers are assured of your website’s
legitimacy, timeliness, and continued viability.

- Begin signing your e-mails and then educate your customers on how to discern between an e-mail that’s been digitally signed and one that’s not.

- Provide location-based contact information and domestic phone number(s) that customers can use to verify your company’s *bona fides* and follow up on any e-mail requests for information.

- If your turn-around time to respond to e-mails is more than a day, customers need to be apprised of this fact so they can use other means to contact your company in the event of a problem.

- Instruct call center employees to identify and notify management if there any reports of suspicious e-mails.

- Register similar domain names. Then, if your customers misspell or type the wrong web address, they won’t end up a website that has been set up to scam your customers.

- Monitor the Internet for: (i) the use of key content by unauthorized users (i.e., content that has been produced and copyrighted by your company) and (ii) fraudulent variations of your firm’s name, trademarks, seals, icons, or website address.

- If your company has been victimized by a phishing scheme:

  IMMEDIATELY post a prominent alert describing the incident on the company’s website.
Contact consumers by phone or through the US postal service warning them not to respond to suspicious e-mails.

At every opportunity, remind your customers that it is not your company’s policy to solicit sensitive information through e-mail.

Inform staff and third-party vendors about the attack and ask them to be on the lookout for unusual or suspicious activity.

Advise customers who may have been victimized by a phishing scheme to change their passwords and to report the incident to the relevant authorities (e.g., Florida Attorney General’s office, credit reporting agencies, the FTC and so forth).

Contact the Internet Service Provider (ISP) hosting the spoofed website and request that it be shut down immediately. In the meantime, if you can, find out who owns the website. If that fails, contact law enforcement—local, state or federal—to pursue a subpoena or other appropriate remedies to mitigate the problem.

Finally, last but not least, join the Secure Florida website <www.secureflorida.org> so you can find out what strategies you can follow to avoid victimization.

References

Anti-Phishing Working Group


Morgan, Gareth (2004) “Sevenfold increase in phishing attacks,” *VNUNET*, posted June 29,


Auction Fraud

"You make your bid, you lie in it—Know what you’re bidding on.”
- Scambusters

“It’s been said that 10% of everyone you’ll ever meet will try to cheat you, 10% would never think of it, and the other 80% is someplace in between. Fraud is a lousy reality of life... but luckily it’s not the norm. Do take steps to protect yourself.” – Auction Fraud Resources

Definition

Online auctions are virtual trading communities (i.e., virtual bazaars) where individuals / businesses can buy and sell hundreds of categories of products (e.g., cameras, computers, artwork, jewelry, collectibles, and so on). Popular auction sites are: Amazon, eBay, Yahoo Auctions, and Ubid.com.

Most auction services feature five basic activities:

1. Initial buyer/seller registration—this step deals with authentication issues. Both buyers and sellers establish a “user account name” before they can participate. Sellers also must agree to pay a fee for each item that is auctioned.

2. Auction events—this step establishes the rules of the auction (e.g., price, delivery, dates, terms of payment, starting / closing dates, contact information, and provides tools for sellers to set up virtual stores and provide customized item descriptions.

3. Bidding procedures—this step implements bidding controls (e.g., minimum bid,
reserve prices, bid increments, bid status and updates, and auto-bidding).

4. Bid Termination—this step enforces the auction closing rules and notifies the winners and losers of the auction.

5. Trade settlement—this step transfers payment to the seller and handles the rating of buyer and seller. Once an auction has been completed, buyers and sellers are expected to rate the transaction. However, this process is not full proof. For example, positive comments might be “planted” by the seller and “negative” comments might come from a competitor. Bottom line: caveat emptor.

Auction site operators do not physically control the merchandise for sale, but they do accept payment. These sites facilitate trading by allowing buyers and sellers to search by product type, name, description, etc.

Buyers offer a specific amount of money and compete with other bidders until the auction closes. Registered users can make bids and keep track of the bidding process. Many sellers set a time limit on bidding and, in some cases, a “reserve price” which represents the lowest price they are willing to accept. If no one bids at or above the reserve price, the auction closes without a winner.

At the close of an auction, the buyer and seller agree to the terms of the transaction, including the shipping costs. The buyer sends payment. If the cost of an item is high, most buyers will use an escrow service that holds payment until the buyer receives the goods and has a chance to inspect the item(s). Once accepted, the escrow service releases the funds to the seller.
Online vs. Offline

Though online and live auctions have lots in common, they differ in a number of significant ways:

- Online buyers usually rely on descriptions and/or images rather than direct observation to determine an item's value before bidding.

- Unlike live auctions, online participants usually do not know each other and never meet face-to-face. For the most part, contact between buyers and sellers is limited to e-mail, regular mail and telephone conversations.

- At the end of an online bidding process, goods and payment are not exchanged immediately so there is no instant gratification. Instead, the buyer and seller communicate—usually by e-mail—to arrange for payment and delivery. Once the seller receives confirmation, the goods are released. The buyer can wait anywhere from a week to 10 days before receiving the items.

Types of Auction Fraud

As a general rule, fraud is most likely to occur during two distinct phases of the online auction process:

1) During the bidding process:

*Bid shilling*—this occurs when sellers create false identities called “shills” or arranges for false bids to be placed on the items they are selling. Shills then make bids designed to
jack up the price of the goods. The overall impact of this practice is to encourage legitimate bidders to continually increase their bids in an effort to win the auction.

Bid shielding—in this type of fraud, a buyer and a partner artificially inflate the bids in order to discourage other buyers from participating in the auction. Then, just before the auction ends, the shielder (high bidder) cancels his/her bid so that the shielded partner can win the auction with a low-ball bid.

Bid siphoning—Here, bidders are lured off legitimate auction sites. Con artists offer to sell the “same” item at a lower price and their intent is to trick the buyer into forwarding a payment, without first forwarding the item. Note: by going off-site, consumers lose any protections the original site may provide, such as insurance, feedback forms or guarantees.

Account Hijacking—another common trick is to steal a legitimate user’s account by password hacking and account hijacking which underscores the importance of choosing hard to guess passwords, changing them frequently, and never giving your password to anybody else (see the section on Passwords).

2) At the close of the auction, there are numerous opportunities for fraud to occur on both the part of the seller and the buyer:

a) Seller-related fraud

Fee stacking—fees, usually "related" to shipping costs, are added to the cost after the sale has been made. Instead of offering a flat rate for shipping and handling, the seller adds separate charges for postage,
handling, and the shipping container, causing the buyer to pay more than anticipated. This means more profit for the seller since auction fees are not paid on shipping and handling costs.

Merchandise Switching—once the winning bidder has paid for an item, the seller will either ship different merchandise (i.e., different from the item(s) stated in the description) or the seller will provide items of lower value or lesser quality.

Tardiness—the seller fails to deliver in a timely manner but in the meantime has the use of the buyer’s funds.

Non-delivery—the winning bidder sends payment to the seller but the merchandise is never delivered. Consumers who pay by certified check or money order have little or no recourse when it comes to getting their money back when this happens.

Misrepresentation—the seller may misrepresent the rarity, authenticity, or condition of the items being sold. Or, the may overstate the true value of an item. Or, they may fail to disclose all relevant information about a product or terms of the sale. Because bidders must rely on online images or read online descriptions provided by the seller, they can easily be deceived.

Identity theft—during the course of the transaction, the seller asks the buyer to provide personal data, such as a social security number or driver's license number, with the intention of using it to commit fraud or theft. When bidding on an item, there is no reason to provide personal information for a seller.
Shell Auctions—in this type of scam, no merchandise exists. The sole purpose of the auction is to get money or credit card numbers from unwary buyers.

Bogus Escrow Services—another type of fraud occurs when sellers pose as escrow services to improperly obtain money or goods. The so-called seller puts goods up for sale on an Internet auction and insists that prospective buyers use a particular escrow service. Once buyers provide the escrow service with their payment information, the escrow service doesn't hold the payment. Instead, it goes directly to the so-called seller. The buyer never receives the promised goods, can't locate the seller, and, because the escrow service was part of the scheme, can't get any money back. Or, the escrow service pockets the money and disappears rather than transmitting it to the seller.

Internet Fencing—this occurs when black market goods are offered for sale online. Black market goods are either stolen or copied illegally (e.g., pirated software, music CDs, and videos) and they arrive with no warranty, instructions, or original packaging.

Triangulation—in his case, the seller offers to send the would-be buyer an item (usually new, brand name goods) on approval. They then use stolen credit cards to order the item that is shipped to the buyer. Once the buyer pays for the goods (usually in cash), the seller disappears and the buyer ends up losing his money and may inadvertently be in possession of stolen goods.
b) **Buyer-related fraud**

*Failure to pay*—using fake money orders, bounced checks, stolen credit cards, or a number of other techniques, the buyer gets the goods and leaves the merchant with nothing in return.

*Refund scams*—unscrupulous buyers attempt to get a refund on an allegedly defective item before returning it. Once the refund is obtained, the item is never returned.

*Buy and Switch*—the buyer receives the merchandise from the seller and returns a similar item that has been damaged, or substitutes a fake item, with the claim, "It isn't what I expected." The seller must then refund their money, and is left with a broken and defective product that they can’t sell. Note: not all loss or damage claims are fraudulent. Items do get damaged in transit.

*Non-payment*—in some instances, a successful bidder refuses to complete a transaction and/or fails to send any payment to the seller. While the non-payment of items does not incur direct costs for the seller, it does incur several indirect costs relating to time, delays and opportunity costs. For example, there is no guarantee that the item will sell again, much less receive the same (or better) price.
Auction Fraud Victims

If you have been duped, here are some recommendations. First of all, let the auction site know what happened. The seller (or buyer) may be conning other buyers (or sellers) and that person can’t be stopped if no one files a complaint. If you don’t get any satisfaction or redress from the auction site, you can file a complaint with a number of private and public agencies:

- Florida Attorney General: URL: myfloridalegal.com/.
- Better Business Bureau (in the seller's area): URL: www.bbb.org ;
- FTC Bureau of Consumer Protection: URL: www.consumer.gov/sentinel
- Internet Fraud Complaint Center (IFCC), www.ic3.gov/ .

You can find an up-to-date listing of these agencies at the Secure Florida website <www.secureflorida.org>.

Finally, depending on the nature of the fraud, notify either local/state/federal law enforcement officials (either in your home location or in the town/state of the seller). More information on who you should contact and how can be found at the Secure Florida website <www.secureflorida.org>.
Cautionary Note

According to the Federal Trade Commission (FTC), auction fraud is the single largest category of Internet-related complaints in its Consumer Sentinel database (www.consumer.gov/sentinel), which logged more than 51,000 auction complaints in 2002. While this figure seems daunting, it is worth noting that the likelihood of becoming a victim is relatively rare. According to eBay, on average, only 0.0025% of the transactions taking place are fraudulent in nature.

Safe Bidding

If you are new to online auctions, here are some precautions you can take:

Make sure that the website you are dealing with is a reliable auction site. You can start by visiting the website at Secure Florida <www.secureflorida.org>.

Become familiar with the main terms and conditions—find out: (i) how the auction works, (ii) what the rules are (including shipping and handling costs, insurance options, warranty, returns/refund policies and arbitration), and (iii) who to contact in the case of a problem. Print out and keep item descriptions and photos to consult, if needed. Make sure you understand what your obligations are. Misunderstandings can result in getting stuck with items you don’t want.

Do your homework and research any items you wish to buy. By shopping around, you may discover that the item you want to bid on is available for a cheaper price at another website or you may learn that the item that is being auctioned as “rare” is available for a
discount at a “bricks and mortar” establishment.

To determine if a seller is trustworthy, check out the ratings. If the feedback is negative, think twice before making a bid. However, be aware that a “clean slate” does not mean that the transaction will go smoothly. Positive feedback can be spoofed by setting up tons of fake transactions and glowing endorsements can be planted by friends. Therefore, check the feedback carefully. If all the feedback is from users who have became members at the same time or they are coming from the same Internet Service Provider, beware. Also, be wary of sellers who use free e-mail accounts or PO boxes. Before bidding on anything, ask the seller for a phone number and take advantage of the “reverse lookup” telephone directories on the Internet to check out the seller. If the phone number provided by the seller does not match up with the location listed for the seller, you need to be extra careful with dealing with this seller.

When making a purchase, use a credit card. By the way, paying with credit cards protects all parties to a transaction— the buyer, the seller and the auction site.

Be wary of shills. If a number of bids appear to be coming from “throw-away” e-mail accounts (e.g., Hotmail and Yahoo!), shills may be participating in the auction. If this appears to be the case, notify the auction website so they can investigate. To minimize the effects of shilling, use a technique called “snipping” i.e., wait until the last minute before placing a bid. Also this will give you a good chance to determine if there are any irregularities in the bidding process.

Question unique or one-of-a-kind items. If it is a collectable, it might not be genuine. Because
you are unable to inspect the merchandise prior to bidding, you need to be extra careful when entering into this type of transaction.

Lastly, be a discerning seller. Verify the physical address of the buyer before shipping any items. Techniques like triangulation enable phony buyers to use stolen credit cards to pay for a purchase and then they arrange to have the merchandise sent to a different location. When drafting the description that accompanies an item offered for auction, make it clear that you won’t accept credit card transactions if the physical addresses don’t match.

References

Are Online Auctions Safe?

Auction Fraud Resources

Auction Watch


Online Auctions URL: http://www.ag.state.mn.us/consumer/fraud/Fraud_OnlineAuctions.htm.


ID Theft

“Officials estimate that ID theft victims spend an average of 175 to 200 hours to repair the damage done by ID thieves.” – H. A. Valetk

“Identity theft often goes undetected. Within a month of being committed, half of the crimes still remain unnoticed. One in ten stays hidden for two or more years.” – Federal Reserve Bank of Boston

Definition

Identity theft is a crime where an impersonator willfully obtains, and illegally uses, your personal information without your consent in order to:

- Open new lines of credit (credit cards, utilities, phone service);
- Drain money out of your bank account(s);
- Purchase goods and services (automobiles, luxury goods, trips);
- File for government benefits (unemployment insurance, tax refunds);
- Rent an apartment or buy a home;
- Receive medical services;
- Obtain employment; and
- Commit crimes ranging from traffic infractions to felonies.

Nearly every Internet-based crime—from auction fraud to child pornography to cyberstalking—originates with the theft of someone else’s identity.
Personal information includes:

- Name
- Date of birth
- Address
- Telephone number
- Driver’s license number
- Social security number
- Mother’s maiden name
- Bank account numbers
- PIN (personal identification number)
- Password
- Unique biometric data, and
- Credit card numbers

Because identity thieves buy and sell names on the black market, a stolen identity may be used more than once and in different parts of the country. It may be months or years before the victim even becomes aware that his or her identity has been stolen and it can take even longer—at great expense both financially and emotionally to the victim—to get it all straightened out.

**Looting Information**

These days, identity thieves are using a combination of low tech and high tech methods to get access to personal information.

In the bricks-and-mortar world, a thief can get your personal information by:

- Stealing your purse or wallet or credit card;
- Pilfering information from your mail box or filling out a change of address form that diverts your mail to another location;
- Posing as an employer, loan officer or landlord to get your credit report;
• Shoulder surfing—peeking over a person’s shoulder while they type in their password or PIN number; and

• Dumpster diving—going through the trash looking for credit card receipts.

Using electronic readers, identity thieves “skim” or “swipe” customer credit cards at restaurants or cash stations and transmit the data to another location, most likely overseas, where it is re-encoded onto fraudulently-made credit cards.

Once a key piece of information has been obtained, an identity thief can access public records to find out your place of employment, date of birth, mother’s maiden name, et cetera. By posing as a trusted source (representative of a financial institution, an internet service provider, medical establishment, and so forth), the identity thief can use the phone to “con” a would-be victim into telling them what they want to know (aka pretexting).

In the online world, authenticating your identity depends on:

• **Who you are** (level of privileges)

• **What you know** (password or PIN), and

• **What you have** (token, card, biometrics)

Anyone who engages in identity theft knows that if they can get hold of this information, they can spoof (fake) your identity (for more information on authentication procedures, see the section on Security).

Alternatively, data containing personal information can be purchased off the Internet from fee-based electronic reference services
such as Informus, Infotel, Knowx, and LEXISNEXIS.

As a last resort, techniques based on social engineering may be used to trick you into revealing your password or opening an e-mail attachment containing a Trojan horse with a keystroke logger.

In the hacker underground, digital dossiers sell on average, for $30 a pop.

**Victimization**

For most victims, the discovery that they have been violated can be a rude awakening. They may only learn about the problem after they apply for a loan and find out they have been turned down—due to a negative credit report.

In other cases, a creditor or collection agency calls them to demand payment for a loan they never took out. Worse still, they may be pulled over and arrested because a criminal act has been committed, using their “good name.” Besides harming their reputation, most victims are left with unpaid bills, delinquent payments, bounced checks, and overdrawn bank accounts.

Businesses are victims too. In addition to bearing direct monetary loses, they may experience other negative effects including: loss of brand equity, customer defections, missed business opportunities, and costly litigation. If an incident involving a customer results from an internal breakdown, they also bear the cost of implementing more robust security measures to avoid being ripped off again.
Remedies

If you think you might be victim of identity theft:

- Immediately report the crime to the police. Provide as much evidence as you can.

  Get a copy of the police report so you can send a copy to all of the financial institutions that may be implicated.

- After filing a police report, contact the credit bureaus and any credit card companies or banks where you have accounts that may be at risk. Then, contact any other creditors who know who may be involved.

When dealing with each of these parties, be sure to keep a copy of your correspondence, a record of your phone calls and any other documents that will demonstrate the action you took and the efforts you made to correct the problem.

Dealing w/ Credit Agencies

First of all, you need to contact each of the three major credit bureaus to get a copy of your credit report:

**Equifax**
P. O. Box 740241
Atlanta, GA 30374-0241
www.equifax.com

  To report fraud: 1-800-525-6285
  
  To order a credit report: 1-800-685-1111

**Experian**
P. O. Box 2104
Allen, TX 75013-0949
www.experian.com

To report fraud: 1-888-397-3742

To order a credit report: 1-888-EXPERIAN (397-3742)

**Trans Union**
P. O. Box 1000
Chester, PA 19022
www.transunion.com (New browser)

To report fraud: 1-800-680-7289

To order a credit report: 1-800-916-8800

If you are unemployed, on welfare, were recently denied credit, or if your report is inaccurate because of fraud, you are entitled to a free copy. Otherwise, you will be charged a small fee ($8/report). Before any information can be released, the credit bureau will ask you to provide them with your Social Security number, date of birth, phone number, current address, any previous addresses over the past two years, and the name of your current employer.

Next, ask each credit bureau to send you a copy of your credit report. You can use this information to guide you in tracing any fraudulent transactions that were made using your identity.

Secondly, instruct the credit bureaus to flag your account. Find out how long the “fraud alert” will remain in effect and how it can be extended, if needed.

Thirdly, arrange to have a victim’s statement appended to your report. At a minimum, this statement should include your full name, the specifics of the problem and how you can be reached. Insist that all creditors be required to
contact you in order to verify the legitimacy of any future applications.

Finally, if you do reach the credit bureau by phone, be sure to follow up with a detailed letter that can be included in your file. In the long run, the protection you receive will be stronger if you report the problem immediately and in writing.

When reviewing your credit report, check to see if:

- Your social security number is correct;

- The accounts listed are ones that you are aware of and the associated balances are what you expect them to be;

- Any unauthorized person or business has received a copy of your credit history (some identity thieves use “pretexting” to pose as a landlord or employer);

- Any inquiries have been made about loans or leases you didn’t apply for; and

- Any addresses are listed where you have never lived or worked.

Should you discover that there is incorrect information listed on your report, you need to contact all the relevant parties (credit bureau, creditor(s), employer, or government agency) immediately and get them to rectify any discrepancies.

After a few months have elapsed, order new copies of your credit report to confirm that no new fraudulent activity has occurred. Even with a “fraud alert” in place, identity thieves will find ways to open new accounts. If you find any additional errors or incorrect entries, ask the credit bureau to supply you with free
reports every few months until the matter is resolved and/or your record is cleaned up.

**Situation in Florida**

According on figures from 2002, Florida was sixth in the nation when it comes to identity theft. The top five locations were Miami, Orlando, Tampa, Jacksonville and Fort Lauderdale. Table 6 shows a ranking for each of the types of crimes committed and how many victims were involved.

In response to growing threat, the Florida Attorney General’s Office, together with the Florida Department of Law Enforcement, joined forces to develop a step-by-step guide that outlines what victims should do, and who they should contact. They also provide an ID Theft Affidavit form that victims can use to help clear up their records. This guide can be found at:

**Florida’s Identity Theft Victim Kit**

**Preventative Measures**

No matter how careful you are you can still become a victim of identity theft. When it comes to online transactions, you need to take a proactive role in protecting your personal information. To minimize your risk of exposure:

- Always be wary of giving out any of the following information that can be used to establish your identity: social security number, current and previous address, financial institution or investment account numbers, credit card numbers, date of birth, driver’s license number, mother’s
Table 6
Florida ID Theft Victims

<table>
<thead>
<tr>
<th>Rank</th>
<th>Type</th>
<th>#</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Credit Card Fraud</td>
<td>5,188</td>
<td>48</td>
</tr>
<tr>
<td>2</td>
<td>Phone / Utilities Fraud</td>
<td>2,167</td>
<td>20</td>
</tr>
<tr>
<td>3</td>
<td>Bank Fraud</td>
<td>1,854</td>
<td>17</td>
</tr>
<tr>
<td>4</td>
<td>Loan Fraud</td>
<td>768</td>
<td>7</td>
</tr>
<tr>
<td>5</td>
<td>Government Docs / Benefits Fraud</td>
<td>744</td>
<td>7</td>
</tr>
<tr>
<td>6</td>
<td>Employment-Related Fraud</td>
<td>630</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>- Other</td>
<td>1,650</td>
<td>15</td>
</tr>
<tr>
<td></td>
<td>- Attempted IDTheft</td>
<td>993</td>
<td>9</td>
</tr>
</tbody>
</table>

[Source: URL: www.consumer.gov/sentinel/states03/florida.pdf .]

maiden name, passwords/PINs and phone numbers, both daytime and home.

- Don’t give out personal information on the phone or over the Internet unless you’ve initiated the contact and/or you know who you’re dealing with (for example, you have a prior/contractual relationship).

- Never e-mail personal information unless you are sure that the e-mail client uses encryption.

- If you are asked to provide personal information in order to complete an online transaction, verify that the site is secure. Look for: (i) a closed lock/unbroken key at the bottom of the browser window and (ii) “https” in the web address (URL).

- To shield your primary ID, consider setting up a disposable online identity with an incorrect address and phone number. Use a “free” e-mail account to register for web sites, participate in chat rooms and
subscribe to online services you are unfamiliar with.

- Ask your financial institutions for their policies about sharing your personal information. Ask them specifically about pretexting. Then alert family members to the dangers of social engineering and explain that only you, or someone you authorize, can provide any personal information over the phone or online.

When setting up online accounts, do not associate your password any easy-to-guess information (for example, mother’s maiden name, birth date, the last four digits of your SSN or your phone number) that can be used to retrieve forgotten passwords.

Finally, you need to be aware that (i) identity theft is the foundation for a number of fraudulent crimes and (ii) it is a crime that is growing exponentially (e.g. Figure 5 shows a projection of national trends). To learn more about identity theft and what countermeasures you need to implement in order to avoid becoming a victim, check out the online resources that have been compiled by Secure Florida <www.secureflorida.org>.

**ID Theft (National) Trends**

References


Urban Legends…

“When a man tells another, 'I've got a dragon in my attic!', he is probably at best regarded as 'wildly imaginative'. But when he tells of a woman who found a dead mouse floating in her Coke bottle, he almost unfailingly receives the attention of an eager listener who is willing to believe every word. How is this possible? He is telling an urban legend, a legend suitable for the taste of a modern city dweller, who is too educated and well-informed to take seriously a princess-stealing dragon or a witch flying on a broom. Thus, a new set of legends have emerged to satisfy our constant hunger for a juicy story.” – Seppo Raudaskoski

“A rumor goes in one ear and out many mouths.” – Chinese proverb

Definition

Urban legends, rumors and hoaxes are defined as sensational stories wrapped in plausible sounding narratives that contain tiny slivers of truth about routine events that run amuck.

The “what if” element is the driving force behind every legend.

One way to differentiate between an urban legend and other types of popular fiction is to compare where they come from and how they are disseminated.

Why do people create urban legends, rumors, hoaxes and myths? Only the “author” knows for sure, but it seems that most legends get started as a prank or as a form of pay-back. Some of the reasons given are:

- **Scope and scale** (e.g., the desire might be to see how far and how long a chain letter will continue to circulate);
- **Harassment** (e.g., the aim here is to deliberately or intentionally hurt someone or some entity);

- **Revenge** (e.g., the motive is driven by a desire to damage the reputation of a company, organization, or person);

- **Prestige** (e.g., the hope on the part of the author is to gain bragging rights amongst his or her peers); and

- **Monetary Gains** (e.g., a pyramid scheme might be set up that bilks money out of unsuspecting victims).

### Chain Letters

On the Internet, chain letters are the main vector for propagating urban legends, rumors, and hoaxes.

There are two main types of chain letters:

1) *Urban legends* are designed to be forwarded. They usually warn users about a impending threat or else they claim to be notifying the recipient of important or urgent information. Another common format are e-mails that promise monetary rewards (if the message gets forwarded) or e-mails that suggest by adding your name to the list, this message will be submitted to a particular group or cause. Most urban legends are more interested in pushing someone’s buttons that causing any real harm.

2) On the other hand, *hoaxes* are malicious attempts to damage or defraud users. By mimicking journalistic style, by attributing the text to ‘legitimate’ sources, and/or by implying that powerful interests (corporate/
government) are trying to keep the information from you, hoaxsters will use every trick in the book to make their “untruths” sound believable.

Urban Legends

The following elements are typical of most urban legends:

- They tend to be narrative-based stories that appear to be spontaneous. They are rarely traceable to a single author or point of origin.

- To be considered an urban legend, the story must be patently untrue. However, the most compelling feature of such a story is the fact that the events depicted in it are perfectly plausible.

- Because an urban legend passes from one person to another, over and over again, details of the story tend to change over time. Thus, no two versions of an urban legend are ever exactly alike.

- The main character of an urban legend usually ends up getting killed, hurt or embarrassed due to his or her own stupidity, crookedness, or negligence.

- To boost credibility, the teller of the urban legend will attribute the story to an purportedly trustworthy secondhand source (e.g., “a friend of a friend who swears it’s true” or “the husband of my brother’s best friend told him...”).

- An urban legend passes from individual to individual either orally or in written form (e.g., via fax, photocopy or e-mail). Most e-mail versions circulate in the form of
warnings or alerts instead of personal anecdotes.

To recap, indications that a story may be an urban legend are: (i) the incident happened to a friend of a friend and not to the storyteller; (ii) there are many variations of the story; (iii) the topic of the story is either a news-worthy item or it is the likely subject of gossip (e.g., death, sex, crime, contamination, technology, ethnic stereotypes, celebrities, and so on; (iv) the story contains a warning or moral lesson; and (v) the story is just too weird, too horrible or too good to be true. Not all urban legends are false, however, they are always told AS IF they are true, despite the fact that there is no supporting evidence to support the underlying basis/claim.

Rumors

Rumors (aka gossip and hearsay) have long been regarded as a form of idle and potentially destructive chatter. A rumor may be either spontaneous or premeditated in origin and it usually consists of opinion represented as fact or a nugget of truth misrepresented to the point of falsehood. Because most rumors are unconfirmed by facts or evidence, they are subject to challenge.

Rumors are similar to urban legends and in many respects it is impossible to tell the two apart. However, rumors differ from legends in the sense that that they're shorter-lived. Nor are they passed along in narrative form. Three types of rumors have been identified:

- **Pipe dream rumors** (i.e., wish-fulfillment) convey the wishes and hopes of those who circulate them.
- *Bogie rumors* (i.e., anxiety-based) project the fears and anxieties of those who circulate them.

- *Wedge-driving rumors* (i.e., divisive) are motivated by aggression or hatred on the part of those who circulate them.

### Hoaxes

First of all, most hoaxes are comprised of three distinct elements and they follow a fairly standard pattern. The main components are: (i) a hook, (ii) a threat and (iii) a request.

**The Hook**—the main purpose of the hook is to tap into our worse fears. Most hooks are designed to catch readers’ attention so they will continue reading until the end of the letter. Examples of common hooks are: “Danger!” and “Virus Alert!!” or “A Little Girl Is Dying.”

**The Threat**—once hooked, you read the threat. What makes this type of threat compelling is the fact that hoaxes contain official or technical sounding language that convince anyone reader the letter that it’s real. The element of doom and gloom is compounded by the fact that most hoaxes warn of terrible calamities should the reader break the chain and they prey upon a person’s greed/sympathy to get them to forward the letter.

**The Request**—with snail-mail hoaxes, readers are asked to edit (e.g., add/remove names) the letter and then pass it on. Whereas, with e-mail hoaxes, readers are urged to “Distribute this letter to as many people as possible.” In the case of a malicious hoax, readers may be instructed to delete critical system files or reformat their hard drive.

Secondly, there are two known factors that increase the likelihood that a hoax will be
widely disseminated. They are: (i) technical sounding language and (ii) credibility by association.

*Language*—if the message in the hoax uses industry- or discipline-specific terms and references, most readers, on first blush, will be inclined to believe that the warning being issued is real. For example, a health-related hoax might use medical jargon to convince readers that a medical emergency is looming. Or, a technical sounding virus alert might convince users to download a Trojan that masks as a patch.

*Credibility*—this refers to “who” is sending the warning. For example, if it seems that an insider (e.g., a file clerk) sent the e-mail, people on the outside will tend to believe what they read because they’ll assume that someone on the inside should know what is going on behind-the-scenes. In this type of situation, it is the prestige of the company or organization with whom the sender is affiliated that lends credibility to the warning and makes it appear plausible. Classic examples of credibility by association include hoaxes that drop names like IBM, Dell, the FBI and/or FDLE. With the advent of the web, some hoaxes will even include generic links to respected websites. In this way, the hoaxster wants you to assume the website has important information about the alert that has been issued.

Finally, regardless of the specific form a hoax may take, what distinguishes it from mere error or folklore is the fact that it is “deliberately” deceptive.
Security Issues

Once an urban legend or a hoax is released in the wild, well-intentioned users, due to ignorance or credulity, forward these messages to family, friends, and co-workers. By doing so, they are co-opted into becoming the attack vector. Proving once again, social engineering works. While these messages are not fraudulent in the strictest sense, they represent a significant risk.

Strictly speaking, it is difficult to classify where and how legends, rumors, and hoaxes fit into the overall security mix. For example, when alerts of this sort are released on the Internet, they tend to be more of a nuisance than a real threat. However, there are instances when messages cause users to take actions that are contrary to their own self-interest (e.g., by persuading them to download fixes that contain spyware). Therefore, this type of threat, though relatively benign, should not be ignored or treated lightly.

Bogus E-mails

Like other types of suspicious e-mail, these messages contain:

- Overly emphatic language, e.g., titles/words written in ALL CAPS.
- Gratuitous use of punctuation, e.g., lots of exclamation marks!!!!!!!
- Poor grammar and frequent misspellings.
- An emotional appeal that urges the reader to alert everyone they know, otherwise there will be tragic consequences.
- The message has been forwarded multiple times (evident from the trail of e-mail headers in the body of the message).

- A reference to an authoritative source that is cited as having issued the warning.

- Statements that claim the opposite of what they mean, e.g., "This is NOT a hoax" or "This is NOT an urban legend."

**Sample Letters**

Archetypal examples of urban legends and hoaxes include:

*Bad Luck Tales*—these are traditional chain letters that threaten bad luck if you do NOT forward them (e.g., the recipient of a chain letter is asked to forward the letter to the top n people on the list and if they break the chain, something bad will happen to you or someone you love/respect).

*Urban Myths*—these include warnings and stories about bad things happening to people and animals that never really happened (e.g., the cat in the microwave or the surreptitious removal of body parts).

*Sympathy Letters and Requests for Help*—someone has a problem and they need your help (e.g., an underprivileged child has been in a car accident and the family needs money to pay medical bills).

*Malicious Code Warnings*—these include warnings about Trojans, viruses, and other type of malware that no basis in fact (e.g. the “Good Times” virus warnings).
Fear Factor

Like spam, chain letters are considered “bad” because (i) they consume a lot of bandwidth, (ii) they waste precious resources and (iii) they ramp up a level of fear and paranoia that may lead to unintended consequences. Even harmless chain letters can have negative repercussions if they are forwarded back and forth by millions of users.

Unfortunately, the past few years has witnessed the emergence of a more serious problem. It concerns the use of chain letters to spread lethal payloads (most notably viruses, worms and Trojans). To learn more on this evolving threat, see the section on Malware or visit the Secure Florida website <www.secureflorida.org>. Examples of the most recent exploits include:

- A virus/worm is disguised as a well-known and previously debunked hoax that has been reactivated, only now it contains a malicious payload, usually in the form of an attachment. Because the hoax is not new, it is not taken seriously. However, users with their guard down, may open the attachment and fall prey to the hoax.

- Another variation is to propagate the payload with a message that claims to be protection against a known virus/worm attack. However, once the user opens the attachment, they release the virus/ worm or else, they end up installing a Trojan.

- Finally, an especially dirty trick is to send a message that urges the recipient to delete an “infected” file. Then, they are instructed to forward the message to everyone they know so they can purge their systems too. Not only do victims of this type of hoax unwittingly assist in the propagation of
malware but they also take actions that render their system(s) inoperable.

**Fact Checking**

The next time you find an “unsolicited” alarming or sensational message in your inbox, check it out before you click the “forward” button,

Besides Secure Florida <www.secureflorida.org>, there are a number of first class websites that have as their mission the tracking and debunking of urban legends and hoaxes. These websites can be found at:

**Hoaxbusters**
URL: http://hoaxbusters.ciac.org/ .

**Snopes**

**Symantec Security Response Hoaxes**

**Hidden Costs**

On first blush, the up-front costs of dealing with a hoax don’t seem that high. After all, how long does it take to read and discard an e-mail? When you take into consideration, one hoax per machine, it does not appear that onerous. However, if you consider the number of users with e-mail accounts—just in the US—what appears to be trivial, quickly translates into some pretty significant “hidden” costs.

Take the following scenario: if 50,000,000 Internet users were to receive one hoax per day and they spend, on average, one minute
to read and discard the message and their time is worth, on average, $50 per hour, then the costs of dealing with just one hoax would work out to:

\[50,000,000 \times \frac{1}{60} \text{ hr} \times \$50/\text{hr} = \$41.7 \text{ million}\]

For many individuals and businesses, when you factor in benefits and overhead, actual time lost, together with opportunity costs, the burden is even greater. Plus, most users receive more than one hoax per day!

Not surprisingly, the biggest risk associated with chain letters is their ability to multiply. For example, if someone takes a hoax seriously, they are likely to send it to everyone in their address book. However, imagine if each person in the chain, only sent it to 10 people.

In other words, consider: the initial person to receive a copy of the hoax (i.e., the first generation) sends it to 10 friends. The second generation forwards the message to 10 of his or her friends and colleagues (= 100 e-mails) and so on. After 6 generations, the original recipient of the hoax will be responsible for spawning a million copies:

\[
\begin{array}{cccccc}
1 & 2 & 3 & 4 & 5 & 6 \\
10 & 100 & 1,000 & 10,000 & 100,000 & 1,000,000 \\
\end{array}
\]

What is even more amazing is the fact that this viral-like (read: bandwidth-hogging) behavior can take place in less than a day!
References

CIAC Hoax Categories


Hoaxbusters

HoaxKill

How to Recognize a Hoax
URL: http://hoaxbusters.ciac.org/HBHoaxInfo.html#identify .

How to spot a hoax computer virus alert

Information About Hoaxes
URL: http://hoaxbusters.ciac.org/HBHoaxInfo.html#identify .


Myth

Snopes / Urban Legends Reference Page

Truth or Fiction

Urban legend
Urban Legend Combat Kit, The

Urban Legends & Superstitions

Urban Legends: An Electronic Art Exhibit

Urban Legends Archive, The
Part V

Behavior-related Threats
Wireless

“Wireless security is not much different from wired security. You want several things from security, wired or not: authenticate whom you are talking to, secure the data as it travels from the handheld device to the destination host, and ensure that the traffic hasn't been altered en route.” – Mike Fratto

Definition

In a wireless local area network (WLAN), a user can connect to a network using radio frequencies. In terms of functionality, a WLAN corresponds to regular local area network, with one key exception: no physical interconnecting wires are required. The term “Wi-Fi” (wireless fidelity) is used to designate a high-frequency WLAN.

There are two communication modes: ad hoc and infrastructure. In the ad-hoc mode, mobile devices, using a NIC, communicate directly with each other in a peer to peer fashion. In the infrastructure mode, a central AP acts like an Ethernet bridge (See Figure 6 for a graphic depiction.)

Communications between mobile devices are mediated through the central AP.

802.11 Standard

Wireless devices require the use of an underlying technology that can handle both radio frequencies and data transmission. The most widely used standard is 802.11 (a family of specifications), produced by the Institute of
Wireless Communication Modes

**Ad Hoc**

**Infrastructure**

![Diagram of Ad Hoc and Infrastructure Modes](image)

*Figure 6*
Electrical and Electronic Engineers (IEEE). This standard defines all aspects of wireless networking.

While several emerging standards exist, the main ones are:

- 802.11b has been around the longest. It is the most widely used and is adequate for basic WLAN deployment.

- 802.11a, is faster, but you can’t mix and match 802.11a and 802.11b hardware and software on the same WLAN.

- 802.11g has better throughput than 802.11b, but it is more expensive to deploy. However this particular standard is gaining popularity in the consumer and SoHo (Small office/Home office) market.

- 802.11i is being developed as a secure WLAN specification. Wi-Fi Protected Access (WPA), a subset of 802.11i, is being designed to replace the existing Wireless Equivalent Privacy (WEP).

- 802.1x is a new vendor-independent post-based authentication standard for 802.11 that will work for wired as well as wireless networks. This specification acts as overlay for the existing 802.11b and 802.11a WLANs. One major drawback, 802.1x requires additional hardware and software for its implementation.

Wireless Set Up

Sounding like alphabet soup, a basic WLAN configuration includes the following components:
Access Point (AP)—this is a type of router that enables wireless devices to access the WLAN. Access points are usually placed outside the firewall to facilitate convenient access, but this also makes them vulnerable to attacks. Wireless APs are also called hotspots.

Media Access Control Layer (MAC)—a WLAN can be set up so that the router will only recognize MAC addresses that are “trusted.” A MAC address is essential to prevent unauthorized access.

Wireless Network Interface Cards (NICs)—NICs are analogous to Ethernet cards. Using radio frequency transmissions, wireless NICs enable mobile devices to communicate with compatible APs. For example, to use an 802.11b AP, an 802.11b NIC is required. In addition, each NIC has a unique MAC address which is fixed. This means it can be used for authentication purposes.

Wireless Equivalent Privacy (WEP)—WEP, a form of encryption, is the original security standard for WLANs. It is used to protect wireless communications from eavesdropping and modification. To prevent unauthorized access, WEP relies on a secret key that is shared between the wireless device/station and the AP. To keep protect privacy, WEP should be enabled. Note: 802.11b and 802.11g provide up to 128-bit WEP, while 802.11a provides up to 152-bit WEP encryption.

Wi-Fi Protected Access (WPA)—WPA, a subset of the future 802.11i security standard, is designed to replace WEP. WPA uses the Temporal Key Integrity Protocol (TKIP) to generate new keys for every 10K of data transmitted over the network making it more difficult to access. WPA is available as firmware for most Wi-Fi-compliant hardware. WPA also uses 802.1x to provide additional authentic-
cation features. The use of WPA to augment existing security measures (available for 802.11 WLANs) is not widespread yet.

*Wireless Application Protocol (WAP)*— WAP is a specification for a set of communication protocols that standardize the way wireless devices obtain Internet access.

Service Set Identifier (SSID)—the SSID is a sequence of characters that is used as an access control mechanism. It uniquely names a WLAN and it is this “name” that allows individual devices to connect to the AP when multiple independent networks operate in the same physical area.

*Mobile Devices*—these include laptops, Personal Digital Assistants (PDAs), Tablet PCs and other similar devices that mobile users can carry with them to do their work or communicate with family/friends. Unless the mobile device is equipped with wireless network capability, it cannot access the WLAN.

### Security Risks

Wireless technologies are still in their infancy. As a result, a host of new security issues have been identified. For example, security, for most 802.11 WLANs, means device authentication, not user authentication – just the reverse of how it’s done in traditional wired networks. Not surprisingly, the establishment of a WLAN is still an anathema to most security professionals who have adopted a “wait and see” attitude.

There is no question that the benefits to be derived from wireless are appealing (i.e., flexibility, convenience, ease of use, mobility, and popularity with users). However, it is up to the user to decide if the costs outweigh the
benefits. For example, the encryption and authentication methods specified in the 802.11 standard contain some serious flaws that render WLANs vulnerable to attack. Some of the more notable vulnerabilities are:

**Default Settings.** If the default settings are changed during installation, attackers can exploit this vulnerability and use it to gain access to the network. For example, the SSID setting should be changed. If not, an intruder can easily find out what names are associated with the different routers and then use that knowledge to find and break into vulnerable WLANs.

**Rogue Access Points.** Because APs are relatively inexpensive and easy to install, individual employees/departments set up unauthorized WLANs. Rogue APs, if undetected, not only leak sensitive information, they are a fairly easy target attackers to exploit. In addition, a single rogue AP connected to a WLAN can be used as a backdoor. Many data raiders have taken advantage of rogue APs, not only to get free Internet access, but to use it as an anonymous platform for launching DoS attacks, sending spam and releasing malware.

**Crackable Keys.** The data encryption standard for wireless networks. WEP has been found to have major flaws. Most WLANS can be “cracked” wide open in as little as two hours.

**Mobile Devices.** Because mobile devices are untethered, they are more susceptible to abuse. They can be either lost or stolen and because authentication is tied to the device and not the user, anyone who can get their hands on one, can gain unauthorized access to the WLAN and if the WLAN.
Errant Broadcast Signals. WLANs send out signals that enable wireless clients (devices) to find the AP so they can configure the appropriate communications settings. This beacon announces what SSID and channel the AP is using. While this type of broadcasting system makes “finding and connecting to WLANs” convenient for the user, it represents a major security vulnerability.

Spillover Effects. Because the range of most WLANs exceeds the physical boundaries of the intended network, attackers can manipulate or eavesdrop from uncontrolled locations or geographic areas to steal service and gain unauthorized access.

This particular vulnerability, unique to wireless, has given rise to new subculture activities called wardriving, the act of driving around in a vehicle looking for unprotected WLANs; warchalking, the practice of using chalk marks to show the location of WLANs (see Figure 7 for sample symbols—by the way, if you have a WLAN and you notice these symbols near your building, you can assume that the following: not only has your wireless network been compromised but the breach has been publicly identified) and warspamming, the use of unprotected WLANs (by unauthorized users) to send millions of spam anonymously by breaking into insecure WLANS.

Because of these vulnerabilities, WLANs are currently less secure than traditional networks.

Wireless Attacks

In the case of WLANs, there are four types of attack that deserve special attention:

- **Spoofing**—to mount this type of attack, the attacker first sniffs the wireless traffic to
capture a valid MAC address. The attacker then uses the captured MAC address to trick the AP into accepting him/her as authorized user.

- **Jamming**—the objective behind this type of attack is to intentionally interfere with the radio signals being emitted in order to render the AP incapable of transmitting any information over the WLAN. Hence, any activity that requires the use of the WLAN will be disrupted.

- **Session Hijacking**—during this type of attack, a hacker tricks the user into believing that the connection has been dropped, then once the user is removed, the hacker takes over the “still” active WLAN connection.
- **Man in the Middle (MITN)**—to pull off a MITM attack, the attacker first reconfigures his/her wireless device so it behaves like an AP. Then, all the traffic (from an authorized user) is forced to travel through this rogue device, which acts like a pseudo-router. This type of attack is made possible because WLAN specifications only provide client-side authentication. By default, AP authentication is not available so there is no way to confirm if you are connected to an authorized AP or not.

### Securing WLANs

If you are planning to set up a WLAN, at home, here are some recommendations you can use to minimize your risk:

- Change the default settings set by the manufacturer. If you don’t change the passwords, SSIDs or the IP addresses, you are making it easier for an attacker to take over your system.

- Avoid using a descriptive name for the SSID.

- Don’t broadcast the SSID. Anyone who needs to connect to a WLAN should know the SSID or have it preconfigured in their clients.

  - Change the SSID on a regular basis.

- Enable the highest level of WEP that ships with the AP.

  - In spite of its shortcomings, WEP does provide some protection.

  - Avoid products that use weak WEP keys.

  - For most manufacturers, the default setting for WEP is “OFF,” and many WLAN
configurations are set to this default mode when they are shipped.

- If you can avoid it, do not enable the dynamic host configuration protocol (DHCP) on the AP. Disabling the DHCP will prevent rogue users from getting an IP address.

- By turning off DHCP, you will not completely eliminate your risk (e.g., an attacker could breach your security using a sniffer) but this security measure may be enough to discourage a less experienced attacker.

Limit the scope of the WLAN to the number of devices that need to be supported.

Reserve addresses for specific systems. This way, you are not providing extra addresses for would-be attackers to use.

Require a MAC address for access.

- Even through MAC addresses can be easily spoofed, the attacker still has to determine which MAC addresses are legal. While this action may not be a foolproof, it deter a less experienced/determined attacker.

Set the AP to operate in infrastructure mode. If the ad-hoc mode is not disabled, an attacker (in your wireless range) will be able to gain access your WLAN by posing as a legitimate wireless user.

- Place the AP as close to the center of your house or building as possible. Placing an AP near an exterior wall can cause wireless signals to “bleed” excessively, providing attackers with a strong enough signal to hack into your network. On the other hand, if you are setting up a WLAN for a small business, place the AP on a separate subnet.
and put a firewall between that subnet and the main network.

Disable the “broadcast” signal in which APs periodically transmit their SSIDs. Attackers can easily discover the default names of many APs, and then they can use freeware, or even Windows XP, to located nearby WLANs.

Finally, instead of turning on encryption and hoping for the best, register with Secure Florida <www.secureflorida.org> and keep up-to-date with the latest advances in wireless technology and learn how to set up a WLAN that doesn’t become a magnet for rogue APs.

References


Instant Messaging

“The rapid consumer adoption of IM networks makes IM the fastest growing communication channel in history.” - Face Time

“Instant messaging might be one of the hottest new channels of communications to hit the enterprise, but if it’s not properly regulated, it could easily bring with it a myriad of security headaches.”
- Christopher Saunders

Definition

Instant Messaging (IM) is a text-based communication service that enables two parties to create a private chat room. IM differs from e-mail in the sense that it is instantaneous.

It is no longer an exaggeration to suggest that IM is revolutionizing the way we communicate with friends, acquaintances, and business colleagues. Once limited to desktops, popular IM systems are being included with handheld devices, personal digital assistants (PDAs), and cell phones. This allows users to communicate from virtually anywhere and anytime, provided there aren’t any constraints.

To function properly, most IM systems require that the users be subscribed to the same network and be located within reach of a cell tower.

“Presence awareness” is another distinguishing feature of IM. It lets you know who is willing to accept messages. If this feature is enabled, the IM system will notify you when a “buddy” is online and let you know if their mobile is turned on and likewise, they can find out the
same information about you. The more advanced systems are being designed to keep track of one’s whereabouts based on login and location information derived from the coordinates taken from the wireless network.

There is a downside to “wide-open” presence awareness. To prevent privacy and security breaches, this aspect of presence awareness needs to be carefully controlled. To avoid letting the world know when you leave home, only certain degrees of presence information should ever be broadcast over the network. That way, depending on your circumstances, you can remain “totally invisible” to complete strangers, you can set up “away from the office” messages for business colleagues and, if you want, you can offer “full presence” information to family and friends.

Most IM systems also feature a “buddy list” (also called a contact list or a UIN for unique identifier). This list is used to determine if someone on the list is logged in or not. The “list” can be used to keep track if someone is offline, online, online but away from the computer, or talking on the phone.

How IM Works

Virtually all IM systems use the basic client-server architecture that became the norm with the World Wide Web. These servers are managed centrally using proprietary (non-standard) protocols. Besides controlling the flow of messages back and forth between two or more users, the IM servers perform authentication and manage the online presence status of the users.

Users install IM clients on their own equipment—desktop computers, wireless devices, or PDAs, for example—and these
clients communicate with the IM server to locate other users and exchange messages. In most cases, messages are first sent to an IM server, and then the IM server reroutes them to the intended recipient. In contrast, with peer-to-peer IM systems, the messages pass directly from user to user, bypassing a centralized authority.

**IM Services**

Even though it seems like IM is brand new, the technical know-how has been in existence for a couple of decades. Internet Relay Chat (IRC) was the first full-scale IM. Since then, several subscription-based systems have been developed—AOL Instant Messenger (AIM) and ICQ (pronounced I Seek You) from America Online, MSN and Windows Messenger from Microsoft, and Yahoo! Messenger from Yahoo! In addition, most cell phone companies have developed their own brand of IM. While each vendor may offer different bells and whistles, they all provide the same basic service: real-time chatting and file transfer capabilities.

**IM Threats**

IM may be a solid communication application, but when it comes to security, it is full of holes. Without adequate countermeasures, anyone who uses IM is vulnerable to attack.

The principle vectors for home computer users are: viruses, worms, and Trojans.

- _Break and Entry_—IM is now the “carrier of choice” for most malware. While there is no question that stand-alone viruses, worms, and Trojan horses continue to be a serious problem, blended threats are quickly
becoming the biggest risk. There is ample evidence that worms (with viral payloads) are trans-generating, that is, crossing the species (from e-mail to IM and vice versa).

Trojan horses are being used to steal information and export data. Some IM Trojan horses can modify configuration settings so the entire system is unrestricted. In this way, an attacker can circumvent security and gain access to all the data stored on the hard drive.

Another reason IM has become so attractive to attackers has to do with the very features that make IM attractive to users. To find victims the attacker doesn’t need to scan for unknown IP addresses, rather he selects from an updated directory of “buddy lists” and with IM in “start up” mode, the attacker is notified each time a PC is fired up. This makes it easier for the attacker to keep track of infected computers. Because no new ports have been opened, any suspicious activity is not stopped by the firewall.

- **Impersonation**—without going into details, most IM accounts are hijacked in order to steal assets (financial accounts, passwords, personal data, et cetera). With IM enabled, a compromised password doesn’t just harm the victim; it endangers everyone on his/her buddy list.

Since most IM protocols don’t encrypt network traffic, an attacker can also hijack the connection using a man-in-the-middle (MITM) attack. A MITM attack can insert messages into an ongoing chat-session, thereby impersonating one of the chatting parties. Somewhat more challenging, a MITM attack can be used to hijack the entire connection.
First, the attacker might use a DoS exploit to make the user's client disconnect and since the server keeps the connection open (that is, the server doesn’t know that the client has disconnected), the attacker can take over the connection and impersonate the user.

- **Eavesdropping**—Most IM systems send traffic across the network unencrypted (that is, the transmitted data are plainly visible). A script kiddie can easily download a packet sniffer or similar technology to eavesdrop on each and every transaction. Using a Trojan, a more persistent attacker might install spyware to monitor communications and file transfers on an ongoing basis.

- **Scamming**—[Wired](http://www.wired.com) recently reported that crooks have begun exploiting the Windows pop-up feature to launch “phishing” attacks. Taking advantage of the unsolicited e-mails that were being used to pitch software that blocks Windows Messenger spam, a scammer took advantage of the opportunity and used IM to send “phishing” notices to AOL members. Using a pop-up window and purporting to be from “AOL Billing” the message instructed users to visit a website - updatedp.com - to correct problems with their credit card numbers. Not surprisingly, quite a few people were taken in by the ploy.

At present there are few tools that can effectively block a determined IM attack.

Nor are they any firewalls that are able to differentiate between authorized and unauthorized IM traffic.
On the other hand, if a hacker uses a blended threat as the attack vector, and you have AV software and firewalls installed, the malware should be eradicated assuming that you have kept up-to-date with your patches and signatures. Recognizing the danger inherent in IM, AV vendors are beginning to develop plug-ins for each IM client.

The Future

Not surprisingly, it is expected that the security problems associated with IM will be exacerbated by the proliferation of broadband. Currently, most attacks are aimed at individuals and not the IM network. However it is expected that this will change as more people start using IM—more users, more exploits.

The future looks grim. If you haven’t done so already, visit the Secure Florida website <www.secureflorida.org> and take the time to learn how to safeguard your person, your assets, and your computer. If you or your family use IM, sign up for the Secure Florida Alerts and Highlights sections so can keep informed about the latest exploits and what you need to do to avoid becoming a victim.

References

chats and messaging


Chat Rooms

"Keeping your kids away from the computer is not the answer. But careful planning can make the Internet useful and safe." - Wade F. Horn and Carol Keough

“If you have never been in a chat room and wonder what they are all about, let me explain that not all chat rooms are created equal.” – Mike Sullivan

Definition

In cyberspace, a chat room is a virtual place or “channel” where two or more people gather to discuss topics of mutual interest. Chatters can participate in an open forum (public chat room) or they can set up a closed session (private chat room). Anyone can create a channel by being the first to join a non-existent channel (new group). In this way, the user becomes the channel operator which entitles him/her special privileges (for example, access denial) not extended to ordinary channel members.

Basically, there are two types of chat services: IRC-based and web-based. The similarities and differences are:

1. IRC represents a vast conglomerate of unmoderated chat rooms set up on the Internet to discuss a wide range of topics. Because some of these forums have been around for so long, they can be more dangerous than the regular chat rooms (for example sex, drugs, hacking, and piracy are common topics for discussion). A number of community networks (for example, Tallahassee Freenet) offer IRC. The software used, mIRC, can be downloaded from the Internet.
2. Web-based chat rooms (for example, MSN, Yahoo!, and a multitude of sponsored chat sites) are popular because they are more family-friendly (restricted in terms of content) and don't require the use of specialized software. Their sites are easier to use but they have fewer features than IRC.

Within each type of setting, there are various rooms, which can be divided by age range (for example, kids’ chat rooms, teen chat rooms, and adult chat rooms) or topics (for example, movies, sports, school). As was mentioned in the previous section, IM also offers chat services.

**Chat Room Basics**

Using IRC as an example, to initiate a chat session the use of specialized chat software (for example, mIRC) is required. During registration, the user chooses a screenname, or nickname (“handle”). The type of “nick” you choose will determine what kinds of treatment you can expect, outside of anything you say or do. For example, a handle like “seXysuZy” or “BIGbertha” will tend to incite more notice than a handle like “webid123” or “jjones.” A word of advice: don’t make the mistake of choosing a handle that acts like a “red flag,” inadvertently drawing all sorts of unsavory come-ons that cause a lot of grief. You can save yourself a lot of trouble in the long run if you go with the “nick” that is non-inflamatory.

Secondly, until you are familiar with the setting and you have a fair idea of what “types” of chatters populate the forum, don’t set up a profile. But if you feel you must, under no
circumstances should you include any information that could be used to track you down in real life. That means NO address, NO phone number, NO pictures, and NO reference to any information that can be pieced together (using social engineering) to infer who you are (for example, my father is the CEO of XYZ, I was the valedictorian of Florida High in 2003, or my boyfriend is the quarterback for the Gators). Depending on the type of group you join, be ready ahead of time for how you are going to respond to the infamous “asl” question (age/sex/location).

Thirdly, while you’re getting set up, look for a button that says “Personal Messages,” “Private Messages,” or “Whispers.” If there is no direct link, you might look under an options tab. Find it and turn it off! This is the most popular way for those who prey on newcomers to initiate a contact. Once you are identified as a “newbie,” and you haven’t disabled private messaging, you will probably see a pop-up window that only contains a screen name and the dreaded “asl” question. Whatever you do, don’t respond and instead, quit the session so you can reset your preferences. If and when you meet someone you want to talk with privately, you can always turn it back on to have a conversation and then turn it back off, once you are through chatting.

Fourthly, chat room etiquette depends on the kind of courtesy you would show anyone that you deal with face to face. In fact, just by being considerate, you will lessen the likelihood of a personal attack. Here are a few guidelines that should be observed by a beginner:

- Learn the ropes—if there are rules specific to the room you are in, follow them, otherwise use common sense.
- *If you’re not interested in the topic*—don’t complain. Find another chat room.

- *Ask questions*—even chatters like to be helpful but be careful about revealing that you are new to chatting.

- **DON’T TYPE IN ALL UPPERCASE LETTERS (CAPS)**—that’s equivalent to shouting, and will evoke a negative response. Plus, this type of gaffe will single you out as a newcomer.

- *Don’t pretend to be someone you’re not*—that can come back to haunt you.

- *Never use come-ons or outright sexual comments*—that type of behavior is completely inappropriate in a public place. Again, you’ll find that you may be subjected to all kinds of unwanted (read rude and inflammatory) behavior.

- *Never ever pose as another chatter*—this kind of act would be considered a serious violation of privacy. Such behavior can get you banished for life from that particular chat room.

Before entering a chat room (for the first time), you need to consult the public directory to find out the name of the chat room that you would like to visit. The directory will list how many people are currently logged on (during that session). Conversely, the names of private chat sessions are not posted in the directory since these sessions are “by invitation only.”

The main thing to remember: **not all chat rooms are created equal.** Some rooms will be very friendly and inviting and others will be clannish and openly hostile to newcomers.
Over the years, IRC has developed its own set of rules and if you want to figure out what is going on, you will need to learn the lingo. It’s best to “lurk” until you get a feel for the room or else carefully read any documentation provided (FAQ, README files, the chat room rules). By the same token, you should not jump into the fray without doing your homework. There are some excellent guides on how IRC works, they can be found using a search engine like Google or you can visit the Secure Florida website <www.secureflorida.org> and start with the link for “Chat Rooms.”

Other types of chat rooms may be “moderated” which means “nonconforming” or unacceptable messages will be blocked. In unmoderated chat rooms, abuses and conflicts can quickly give rise to “channel wars.” (When obnoxious or rogue members are kicked off, they sometimes retaliate by using another address with a new screenname to rejoin the group, or else they flood the “banned” channel with unsolicited network traffic, called “syn/ack or ping flooding.”) The majority of chat rooms are “open,” which means messages get posted without any human intervention. Pretty much anything goes in these types of settings. If you choose to participate in an unmoderated chat room, you need to be on guard at all times. These types of chat sessions are more likely to attract users with hidden agendas.

Online chatting involves real-time interaction where participants sit at keyboard and carry on a conversation using text messages. If two people are chatting privately, say in a “Talk” session, one half of the screen will be reserved for inputting text and the other half will be used for displaying the other party’s response. If more than two people are involved (a multi-session) the software will display the user handle to the left of the screen and all the
responses will be displayed to the right of the screen.

Finally, given the risks associated with "stranger danger," anyone who decides to participate in a chat room should exercise extreme caution. Always be on the lookout for anyone who is trying to take advantage of you.

Online Predators

It is a well-known fact that most predators are either looking for weaknesses to exploit or they’re interested in making a personal conquest. For this reason, they look for behavior that singles out the newbie, a term used to designate a newcomer. A predator looking for individuals who are new to the ‘Net, don’t have far to look. Most “newbies” are easy to pinpoint:

- They don’t know the lingo.
- They ask a lot of naïve questions.
- They need (technical) help getting set up.

Online predators will patiently wait for someone to openly discuss their personal problems and when the time is right, they will jump in and offer comfort or compassion. Invariably, online predators will appear to share similarities in likes and dislikes and not surprisingly, they will agree with you (on the issues being discussed). Once they have gain your confidence, they may insert themselves into a conversation by mentioning they have been to the area where you live or they have experienced the same things you have or attended the same school.

This is not to suggest that everyone who empathizes is, by definition, a predator. On the
contrary, it is meant to heighten your awareness. If you notice someone is pushing you to reveal all kinds of personal information or they are moving too fast, then it’s up to you to put on the breaks. But this is easier said than done. Most predators are masters of manipulation. They are going to tell you what you want to hear and they will know better than you do, where your “hot buttons” are.

Bottom line, you need to understand that “stranger danger” is not an idle threat. Predators use chat rooms as a hunting ground to locate would-be victims. Once they are able to infer a certain amount of information about you (like where you work or what’s your IP address) they will use that information to either track you down (see the section on Cyberstalking) or rip you off (see the section on ID Theft).

**Danger Online**

Anyone who chats online is at risk. But allowing children or teenagers to participate in unsupervised chat rooms is even riskier. Chat rooms are the primary attack vector for predators seeking their prey. They spend hours looking for vulnerable children. Once a mark is found, they use trickery to establish trust and subterfuge to create a false sense of security. Children who are “groomed by adults” for illegal or illicit activity, end up being harmed one way or another—physically, emotionally, or psychologically.

**Warning Signs**

Here are some of the warning signs that someone you care about (yourself, your spouse, your child, your sibling, your parent,...) is spending too much time online:
• Still logged on late at night.

• Online activity is excessive.

• Spends hours alone in front of a screen.

• Evasive in describing online experiences.

• Minimizes the screen when you walk by.

• Programs listed in the task bar, nothing on the screen.

Most browsers come with a “browser history” feature that you can use to check online activity.

**For Internet Explorer:**

To view the history: there is a history button on the top of the browser, or you can click on “View” then select “Explorer Bar” then “History.” Or you can hit the “Ctrl” key and the “H” key together.

To adjust the number of days kept in the history: click on “View” then select “Internet Options” and then use the up or down arrow to adjust the number of days.

To clear the history: click on “View” then select “Internet Options” then “Clear History” button in the history section.

**For Netscape/Mozilla:**

To view the history: click on “Communicator? Then select “History” (on some versions, you need to follow the following path: Communicator then select Tools then History) or you can just enter “Ctrl + H.”

To adjust the number of days kept in the history: use the above procedure and once you
are in the history window, click “Edit” then select “Preferences” and enter the how many
days you want the information kept.

To clear the history: Follow the “adjust the
number of days kept” procedure then click on
the “Clear History” button.

Be aware that anyone can clear the history of
the sites they have been visited. If you
discover a family member is constantly
clearing out their cache (especially if they
never did till now), you might consider
installing monitoring software on your machine
to find out why.

Safe Chatting

First and foremost when communicating with
someone online, you need to be aware that the
person you are chatting with may NOT be who
they say they are. He could be a 40-year-old
sexual predator posing as a 19-year old guy or
a pedophile pretending to be a 13-year old.
With this in mind, there are a few safety rules
you need to abide by in order to safeguard
your person. Plus, you need to make sure that
family and friends are following them too:

- Include as little personal information as
  possible in your member profile. Better still
  leave your profile blank.

- Never mention your last name, street
  address, home phone number, employer’s
  name, or the names of any family
  members.

- Never use your primary e-mail address (use
  a throw away address instead) when
  participating online.
Never give out any passwords, SSN, driver’s license, credit card numbers, and the like.

If, after entering a chat room and you feel uncomfortable, someone is hitting on you, or they are being obscene, leave that room and do something else. If the attention is directed at you personally, try to diffuse the situation. Whatever you do, don’t allow yourself to be drawn into a flame war. If you are using IRC, you can type “/ignore {Nickname}” to make them disappear off your screen.

Finally, for the sake of your safety and that of your family and friends, do not ignore these rules, and if you DO decide to meet someone face to face (a risky practice Secure Florida <www.secureflorida.org> does NOT recommend) then only agree to meet if you are certain that you know who they are.

Secondly, never agree to meet a fellow chatter on your own. Take a trusted parent/sibling/friend with you and make sure you agree ahead of time that they won’t leave you alone and they won’t let you leave with the new person you are meeting.

Lastly, be sure to meet in a public place. If you decide to go with a friend rather than a family member, be sure to tell your parents or siblings where you are going and when you expect to be back. Also, take a mobile phone with you and make sure ahead of time that it is fully charged and turned on.

To learn more about chat rooms and the risks that pose, visit the Secure Florida website <www.secureflorida.org> and read more information has been provided in the section on Chat Rooms.
The CHAT Test

**Careful**—Be aware that people online may NOT be who they claim to be.

**Hording**—Hang on to your personal information. DO NOT give out your primary e-mail or home address, phone number, age, place of work/school, etc.

**Arrangement**—Never arrange to a meeting with someone offline unless (i) you are sure who they are, and then, (ii) only agree to meet in a public place and (iii) take someone (you can count on and trust) with you.

**Tell**—Be sure to tell friends/family/teachers (or other authority figures that you trust) if you come across anyone who makes you feel uncomfortable online.

**References**


Chat Rooms and The Predators


Sending Your Kids Out in Cyberspace To Chat URL: http://familyinternet.about.com/library/weekly/aa031299.htm. Last Visited: October 29, 2003,

Cyberstalking

“People, when they think of stalking, they think of somebody that's constantly calling, they think of someone that's following people. They don't realize the extent that you can cyberstalk in today's society. This is really widespread . . . Katrina [a woman whose name and address was posted online as a supporter of terrorists, prompting a barrage of e-mails, letters and phone calls] is one of many people who have contacted us.” – Sen. Steven Geller (D-Hallandale Beach, FL)

Definition

Under the new Florida Cyberstalking law that went into effect on October 1, 2003, cyberstalking is defined as follows:

“To cyberstalk is to engage in a course of conduct to communicate, or to cause to be communicated, words, images, or language by or through the use of electronic mail or electronic communication, directed at a specific person, causing substantial emotional distress to that person and serving no legitimate purpose.”

Besides e-mail, the Florida statue also includes cell phones, pagers, and any electronic device (already invented or not) that can be directed at a person.

This new law also revises the crime of aggravated stalking to include not only placing a person in fear of their own death or bodily injury, but it also “fear for the victim’s child, sibling, spouse, parent or dependent.”
Online vs. Offline Stalking

To avoid becoming a victim of cyberstalking, you first need to understand (theoretically) what it means to be stalked.

To be considered stalking, the behavior must be:

- A course of conduct that is unwanted,
- Repeatedly directed at a specific individual. and
- Threatening to the victim.

In concrete terms, stalking behavior constitutes an implied threat. As a rule, it involves harassing or threatening behavior that an individual engages in repeatedly—such as following a person, appearing at a person’s home or place of business, making harassing phone calls, leaving written messages or menacing objects, or vandalizing a person’s property.

In other circumstances, the solicitation of minors for illicit purposes would be considered stalking.

While some conduct may be annoying, it might not be considered stalking because it falls short of the legal definition. Nevertheless, upsetting or unacceptable behavior should never be ignored.

For this reason, strategies and techniques that have been developed to combat stalking can be adapted for cyberstalking. In most instances, cyberstalking can be considered regular stalking using high-tech tools.
For example, cyberstalking might entail:

- The transmission of threatening, obscene, or hateful e-mail;
- The spreading vicious rumors about you online;
- The theft of the victim’s identity;
- Electronic sabotage (for example, sending e-mail bombs that overwhelm your inbox with hundreds of e-mails);
- Damage to data or equipment; and
- Computer monitoring and surveillance.

What makes cyberstalking even more threatening (for the victim) than regular face-to-face stalking has to do with an artifact of point-to-point asynchronous communications, viz., concealment. The veil of anonymity afforded by the Internet tends to embolden stalkers.

A cyberstalker’s identity can be masked by using different ISPs, adopting different screen names (i.e., handles), or by using automatic remailers.

Should the cyberstalker deliberately use subterfuge to cover his/her tracks, it is practically impossible to determine his/her true identity, short of catching the would-be offender in the act.

As for the victim, the prospect of dealing with the unknown can be truly unnerving. A cyberstalkers could be in another city, around the corner, or in the next cubicle at work. Or, s/he could be former friends or lovers, total strangers met in a chat room, or simply bored teenagers playing a practical joke. The inability
to identify the source of a threat can be extremely unsettling and adds to the hysteria that accompanies these types of cases.

On the other hand, a cyberstalker might exercise control over the victim by using an indirect approach. The stalker might post controversial information (“Looking for a good time...”) in a sex-related chat room under the name, phone number/e-mail address of the victim. This in turn may result in a flood of “lewd and lascivious” e-mail, or the victim might get a number of callers who are looking to “party.”

Current trends suggest that cyberstalking is a serious problem that will grow in scope and complexity as more people take advantage of broadband and other telecommunications technologies.

Nature and Extent

Online harassment and threats can take many forms. Many stalkers—online or off—are motivated by a desire to exert control over their victims. Both stalkers and cyberstalkers engage in similar types of behavior to accomplish this end.

As with offline stalking, the available evidence (which is largely anecdotal) suggests that the majority of cyberstalkers are men and the majority of their victims are women, although the number of reported cases of women cyberstalking men and of same-sex cyberstalking is on the rise.

In most cases, the stalker and the victim have had a prior relationship, and the stalking begins when the victim attempts to break off
the relationship. However, there also have been many instances of cyberstalking by strangers.

Given the enormous amount of personal information available through the Internet, a cyberstalker can easily locate private information about a potential victim with a few mouse clicks or keystrokes.

The fact that cyberstalking does not involve physical contact may create the misperception that it is more benign than physical stalking. This is not necessarily true.

As the Internet becomes an ever more integral part of our personal and professional lives, stalkers can take advantage of the ease of communications. Whereas a potential stalker may be unwilling or unable to confront a victim in person or on the telephone, he or she may have little hesitation about sending harassing or threatening electronic communications to a victim.

Finally, as with physical stalking, online harassment and threats may be a prelude to more serious behavior, including physical violence.

**Stalker Motivation**

Stalkers come in all shapes and sizes. What sets stalkers apart is the fact that they are not easily deterred and they tend to be obsessive. Many stalkers continue to harass the victim, even after they have been convicted. While it is impossible to come up with a definitive profile that explains the motivation and why stalkers behave as they do, a number of stalker types have been identified:
- *Jilted lovers* have most likely had an intimate relationship with their victim and their behavior is a mixture of the need for revenge and a desire for reconciliation.

- *Intimacy seekers* want to start a relationship with someone they find attractive. They also mistakenly assume that the object of their affection will reciprocate.

- *Incompetent suitors* want to develop a relationship with someone but because they are socially inept and don’t abide by the rules governing courtship, they are usually spurned.

- *Resentful stalkers* harass their victims with the specific intention of causing fear or bodily harm. They are driven by the desire for retribution in order to rectify (an actual or supposed) injury or humiliation.

- *Predators* engage in information-seeking behavior in order to locate a potential victim. Once they have found a prospect, they begin grooming them (all part of the fantasy) in preparation for an attack.

### Cyber-stalking Toll

According to the National Center for Victims of Crime, lack of physical contact with an online perpetrator does not mean that that this type of crime is not terrifying or frightening.

Based on their findings, cyberstalking victims often experience physical and emotional trauma as a result of their victimization. Some of the effects they cite include anxiety, feelings of helplessness, hyper-vigilance; fear for their
Avoid Becoming a Victim

To prevent becoming an online victim, it is recommended that YOU:

- Use a gender-neutral online name.
- Don’t provide personal information online.
- Don’t believe everything you read on the Internet.
- Avoid using your middle initial. Middle initials can be used to locate people with common names.
- Use a “public” e-mail account (i.e., one that is a disposable throw-away) when posting to newsgroups.
- Make sure that the online services you use have an acceptable use policy that prohibits cyberstalking.

Anti-Cyber-Stalking Tips

To avoid online harassment that might escalate into cyberstalking, here are some tips that have been compiled by the research team at Secure Florida <www.secureflorida.org>:

- If you are receiving unwanted attention, make it clear that you want the harassment to stop. For evidentiary purposes, save a
copy of all communications and do not edit or alter them in any way.

- Keep a log of every stalking incident, plus names, dates, and times of any contacts with ISPs and law enforcement officials.

- If the harassment continues, contact the person’s ISP. Most ISPs have clear policies prohibiting the use of their services to abuse another person.

  If the ISP has a website, check to see if they have any information on how to file a complaint.

  If no contact information is listed, use the “whois” command (see the sections on Networks and Spoofing for more information on how to use Internet tracking tools) to find out who owns the site and how to reach them.

- In addition, install blocking software to filter messages from the harasser. Chat room contact can be blocked as well. However in some cases (threats of violence), it may be more appropriate to save the information and contact law enforcement authorities instead. You may be dealing with a clear-cut case of cyberstalking.

- Let family, friends, employer, co-workers, and neighbors know that information about you should be held in confidence.

  Alert them to be suspicious of anyone inquiring about your whereabouts or schedule.

- If you find the situation overwhelming, get professional counseling or seek help from a victim support group. They can help you
deal with fear, anxiety, and depression associated with being harassed/stalked.

Finally, last but not least, you can visit the Secure Florida website <www.secureflorida.org> to get an up-to-date list of self-help groups and to find out how to file a police report (should you become the unfortunate victim of cyberstalking).

**References**

Cyberstalking


Getting Help When You Are Threatened Online


Stalking Assistance Site


Working to Halt Online Abuse (WHOA)
P2P File Sharing

“‘It's time to face the fact that in today's world, copyright law is broken. Our current copyright regime makes criminals out of music lovers. Worse, it makes suspected criminals out of all Internet users.’
– EFF, Let the Music Play

Definition

Peer-to-Peer (P2P) file sharing differs from the traditional client/server model—where one computer is dedicated to serving the other computers (one-to-many relationship). With P2P, each node (individual computer) has equivalent capabilities and responsibilities (one-to-one relationship). With this type of setup, member nodes are able to search for and share content in real-time.

How P2P Works

Very briefly, to participate in P2P file sharing session, the user (client) engages in the following routine:

1. A connection (using a P2P client) is established.

2. The user searches for a file using keywords, titles, artists, and so forth. For example, if the user is searching for a particular band, they would enter this name into the search box and hit enter.

3. Once the sought-after file is located, the user downloads the file (or correspondingly, if the sought-after file is stored on a user’s hard drive, it would be uploaded,
once it is located). Downloading and uploading are carried out directly by the participating peers.

4. After the file has been acquired (and no more searches are conducted), the connection is closed and the peer vanishes (that is, disappears off the network). Another popular application for P2P file sharing networks is distributed computing.

Distributed P2P is based on the premise that during normal operation, 90 percent of the processing cycle (on a typical PC) remains unused. One estimate suggests that idle computers (aka “the black matter of the Net”) represent an aggregate 10 billion MHz of processing power and 1000 TB of storage. By using P2P networking, organizations would be able to exploit these globally distributed “spare” computing resources. (An example of a distributed project that has been in existence for some time and includes the involvement of hundreds of users is called “SETI@home.” This P2P network uses thousands of online PC nodes to help in the search for extraterrestrial intelligence.) Finally, it is important to recall that the Internet was originally designed as a P2P network.

To get a more in-depth view of the various types of P2P networks (hybrid vs. pure) and the legal battles being fought, please consult the resources and links that are listed at the Secure Florida website <www.secureflorida.org>.

**Exemplars**

For the remainder of this section, we will be focusing on P2P file sharing networks that have been, or are being, used (inappropriately) to
share unauthorized copyrighted materials. The main players are:

- **Napster**—was the first widespread P2P file-sharing program that was used to acquire “free” digital music (MP3s). It was not strictly P2P in the sense that Napster had a centralized database that facilitated file sharing and downloading. The Napster service took off like wildfire and it was very popular with teenagers and college students. It was only online for a few months before the Recording Industry Association of America (RIAA) sued Napster for copyright infringement. Napster lost its appeal and finally shut its doors in July of 2001.

The Court ruled that even though Napster may not have committed the infringement itself it was guilty because it facilitated the illegal acquisition of music files. In addition, the Court found that Napster was liable because it was able to stop its users from downloading music files, and it did not do so.

Update: Napster reopened in 2003 as a (legal) subscription-based service.

- **The Napster Clones**—in the wake of Napster’s demise, a whole new crop of P2P file sharing services emerged. Some of them, like Napster, were sued out of existence (for example, Aimster, Scour); others went on to take Napster’s place. The most notorious ones are: Grokster, Morpheus and KaZaA (FasTrack).

In addition to music, these P2P file sharing services offered video games, TV shows, software, text, pictures and pretty much anything else that can be digitized. To the dismay of the entertainment industry, the
newer services did not make use of a centralized database. Unlike Napster, the P2P file sharing protocol, developed by FasTrack, used a layered architecture and supernodes to speed up searches and help locate peers with higher bandwidth for more efficient downloads.

Grokster, Morpheus and KaZaA were sued by the RIAA, together with the Motion Picture Association of America (MPAA) too. This time, the Courts ruled against the RIAA/MPAA. It found that companies providing P2P file sharing software couldn’t be held liable for copyright infringement on the part of its users.

As a consequence, the RIAA/MPAA have begun targeting individual P2P file sharers who upload/share “substantial” amounts of copyrighted music. Anyone found to be in violation would be sued for copyright infringement.

Under the Digital Millennium Copyright Act (DMCA), the RIAA also has the power to subpoena ISPs for user names, addresses, and any other personal information that can be used in a lawsuit involving those individuals.

- **Gnutella**—is an open source P2P network. It does not require a centralized server for indexing files. It enables a host computer to function as both a client and server. To use the protocol, a software application called a “Servent” (Server + Client) is running on each machine. A member node can search for other online member nodes. Usually, each member node keeps track of four or five other member nodes. Thus, there is a web of virtual interlinked member nodes.
So far, there has been no litigation filed against Gnutella (or its participants) and that probably has to do with the fact that Gnutella is not a proprietary service so there really is no one, apart from the individual users, to sue.

**Why P2P is Dangerous**

P2P file sharing is not inherently bad. What makes P2P potentially dangerous has more to do with “what” is being traded as opposed to “how.” In retrospect, the P2P file sharing activity that took place in the heady days of Napster seems relatively benign. In those days, all you could get were MP3 files—no warez (i.e., pirated software), no Napster bombs and no pornography. Today, P2P file sharing is some of the riskiest online behavior that a user can “directly” engage in.

Without getting embroiled in a debate over the legal or ethical issues (we leave that for you to sort out), the following list presents some of the reasons WHY (from a security perspective), P2P file sharing is bad:

- **Malware**

  P2P file sharing has become one of the primary attack vectors for the distribution of malware. For example, viruses and worms targeted for KaZaA users include: Benjamin, Duload, and Kowbot. They all masquerade as MP3 or video files. In addition, a number of worms have been written for Gnutella.

- **Underware**

  Many of the most popular P2P file-sharing programs (for example, KaZaA, BearShare, LimeWire, Morpheus, Grokster and iMesh) install adware/ spyware that is used to track
online activity. Some spyware will even connect to the Internet and send information about users’ online purchases and viewing habits back to the sponsor. In addition, a lot of spyware continues to reside on the hard drive even after the original P2P program is uninstalled.

- **Pornography**

To understand how someone can unwittingly be exposed to pornography, you need to recall how P2P file sharing programs work.

To find a file, the user types in a word or phrase and depending on what keywords are used, harmful and/or illegal content may be included as part of the search results. This can happen because anyone who makes a file available through P2P file sharing is “free” to call it anything they want, even if it turns out to be incorrect or misleading.

In a recent study, the Government Accounting Office, using innocuous keywords, found that 42% of the files returned using KaZaA, contained child pornography. Another 34% were riddled with adult pornography.

**Computer Check**

Finally, some clues to look for if you think your computer is being used for P2P file sharing without your knowledge:

- Is the Internet connection constantly busy? Look for flashing or blinking lights.
Are there P2P icons sitting on the desktop? Look for file folders or corporate logos. If not, check the sub-directories.

Are there any P2P programs listed in the add/remove programs menu? Look for the names of popular file sharing programs (Note: if you do not know the names of some of these programs, Secure Florida <www.secureflorida.org> has links to up-to-date lists.

Are there lots of CDs sitting around the computer? Look for blank CDs and check the names of any copied CDs for the names of copyrighted works.

How NOT to Get Sued...

If you didn’t find any evidence of P2P file sharing, you can safely ignore this section.

On the hand, if you did, that is, you or one of your kids is swapping files, then you need to carefully read this section. Depending on your particular situation, there are a number of strategies you can use to reduce your risk of becoming implicated in a lawsuit:

**Strategy # 1: Stop uploading/downloading copy protected files**

—Unless you have permission from the copyright holder. Meaning? You have paid for the use of the material or you are using the content in a way that qualifies as fair use. Otherwise, you have no right to copy or share copyrighted materials online.

—Unless material is clearly marked as “public domain.” Under the law, only the copyright owner holder has the exclusive right to
reproduce and distribute copyrighted materials.

**Strategy # 2: If you are going to engage in P2P file sharing, take the following precautions:**

—Remove any copyrighted files from your shared folder. As a general rule of thumb, you can share a file if: (1) the copyright holder has given you (written) permission to redistribute the material, (2) the content contained in the file(s) has been placed in the public domain, or (3) a license has been issued that entitles you to share the material (for example, open source, Creative Commons).

—Change potentially misleading file names. The RIAA/MPAA use “bots” that scour the ‘Net looking for copyright violations. If you happen to choose names for files (in your shared folder) that might be confused with the names of artists (Madonna, Sting) or the titles of movies (Matrix, Titanic, Spiderman) there is a chance that you might be (incorrectly) identified as having pirated material on your machine.

—Disable the “sharing” or “uploading” features on your P2P application. If you do this, other P2P file sharers will be prevented from scanning your directories and/or downloading any files from your machine. To find more information on how to disable this feature, visit the P2P file sharing section at Secure Florida <www.secureflorida.org> and click on the link called “How to Disable File Sharing.”

—Don’t be a hub. It appears that the RIAA/MPAA are targeting users who allow their computers to be classified as supernodes. To learn more about supernodes/servents and how to make sure your computer is not one, visit the Secure Florida website <www.secure
Florida.org> and click on the link called “Supernodes.”

Legal Implications

Ignorance of the law will not protect you from prosecution.

Under the law, anyone who obtains or distributes copyrighted material without the permission of the copyright holder, can found liable for copyright infringement. In a civil lawsuit, if you are found liable for copyright infringement, you might be ordered to pay between $30,000 - $150,000 per copyrighted work in damages. In cases where the amount and the willfulness of the infringing activity is particularly flagrant, criminal prosecution may be possible.

To combat the problem of P2P file sharing, a new bill has been introduced into Congress called the Author, Consumer, and Computer Owner Protection and Security Act (ACCOPS, HR 2752). ACCOPS will make it a felony to transfer music over the Internet without prior authorization. Should ACCOPS become law, a person could spend up to five years in prison, pay a $250,000 fine and lose their right to vote – just for trading a “single” copyrighted song.

Down-/Uploading

From the point of view of the Internet, to download is to transfer of a file from one computer system (e.g., a server, a webpage or a single machine that is functioning as a peer) to another (e.g., the local machine or a mobile device). On the other hand, uploading a file is to transmit a file in the opposite direction—say, from the locate machine to the remote.
The transfer of a file can take place through a separate program that utilizes the file transfer protocol (FTP) or else it can happen by virtue of saving a file (e.g., right-clicking on a link, an image, a document, etc.).

Technically speaking, once you call up a webpage, you are effecting a file transfer, however, most of these files are cached in a “temp” file and should be periodically should be purged. On the other hand, when you send a file with an e-mail, this is an attachment, not a download per se. (For more information on attachments, see the section on E-mail).

The LOCATE Test

Extreme caution must be exercised when exchanging files or installing programs from an untrusted source. Before running a program or opening a file that you have downloaded from the Internet, perform the LOCATE test in order to verify the authenticity of the program/file. In this way, you can minimize any threat posed by inadvertently downloading an harmful content or installing a program that contains malicious code.

Learn—Before initiating a file transfer, particularly from a source you don’t know very well, make sure you learn as much as you can about the site? Is it a reputable website? Do they post how many downloads that have been made? Do the provide any direct links to the programmer/creator? Is there a feedback section so downloaders can leave comments? Does the company have a privacy policy? Lastly, once you have completed a download, be sure that you read the EULA so you don’t end up waiving any rights and above all, make sure you’re NOT (i) giving permission for any
third parties to monitor your online activities and (ii) renting out processing capability or space on your hard drive (unless of course, you want to).

**Operate**—what does the program do? Does it include documentation and technical support? If the file is a non-executable, what format has it been written in? Do you recognize it? Are there any hidden file extensions?

**Change**—Prior to activating any installers or opening any files, you need to consider what types of changes might be made to your system as a result of the action. To be on the safe side, make sure that you have backed up your computer so that if something goes wrong, you will be able to recover (see the section on Maintenance for information on how to backup your system or else visit the Secure Florida website <www.secureflorida.org> and click on the Backup link.)

**Author**—Do you know who created the program, developed the project (if it is open source) and/or produced the media? Depending on the purpose or the type of material you are dealing with, you may want to check out the author (through product/media reviews) to make sure that they are on the up and up. If at all possible, buy/acquire your online products and services from a developer/creator that has been recommended by a trusted source or has an established reputation.

**Test**—After you have installed/opened the downloaded files, run some diagnostics (AV software, anti-Trojan software, anti-spyware, etc.) to make sure that the new programs/files do not contain any surprises.

**Evaluate**—If you do encounter any problems after installing/opening a new program or file,
find out if anyone else has experienced similar problems? If so, find out what they did to remediate the problem. If not, then check your system to see if any of the problems may be due to misconfiguration, software/hardware conflicts, lack of compatibility and the like. If not, be forewarned that you may have a problem that first should be reported to the vendor/distributor (assuming the source of the problem is legal and/or inadvertent). If that is not the case, you may want to report the problem to your ISP/law enforcement (assuming the source of the problem is unauthorized (contrary to policy) or possibly illegal).

References


File Swapping: Dangers You May Not Know About


How Not to Get Sued by the RIAA for File Sharing


Let the Music Play


peer-to-peer architecture


Using Peer To Peer File Sharing Programs

Harmful Content

“...The World Wide Web is an exciting place for inquisitive young minds and it does not take long for children to pick up the skills needed to go online. However, without proper precautionary measures, cyberspace can be a potentially threatening environment in which children and young people can be exposed to hate messages, sexually explicit material, graphic violence and even predators who roam chat rooms in search of innocent prey.” – UNICEF

Definition

When dealing with inappropriate content, we first need to determine whether the material in question (e.g., text, images, audio/video) is offensive, illegal, or just plain annoying (e.g., the content in question may be protected by the First Amendment). Unfortunately, making such a determination—even for the courts—is not cut-and-dried. What may be acceptable in one jurisdiction might be considered offensive in another. Communities have different moral standards.

Legal and ethical quagmires notwithstanding, the next section offers some guidelines to shield you and your family against harmful and illegal content found on the Internet.

Offensive Content

Offensive content refers to material that may offend the values and feelings of other persons. Offensive content may also be classified as inappropriate material that is sexual, hateful or violent in nature. It might be used to express political opinions, religious beliefs or views on racial matters. In some cases, even though, strictly speaking, the content may be legal, it still can be harmful to
children. For this reason, parents need to take care that their children are not being exposed to inappropriate content.

Alternatively, the designation of whether something is offensive or not will depend on cultural norms. It is often left up to each locality to decide what is permissible and not permissible. This becomes real challenge for politicians who must find a balance between passing laws that protect people against offensive material whilst ensuring freedom of expression.

**Illegal Content**

Many federal, state, and local laws have been passed that limit the use and distribution of offensive content. For example, the possession and distribution of child pornography is clearly illegal. Using copyrighted materials without permission (for example, peer-to-peer file sharing) may or may not be illegal—that will depend on several factors:

- Are you uploading or downloading?
- Are you time/space shifting content?
- Does “fair use” apply?

Other types of material may be illegal if they become implicated in a crime, for example, the dissemination of racist material, terrorism, and types of forms of fraudulent activity. Note that the posting of “adult material” may be objectionable but it is not necessarily illegal.

Adult material includes: pornographic or erotic text/pictures, pictures showing nudity, and any other material that is forbidden to minors.
To be on the safe side, assume that any material that violates U.S. or international laws (for example, pirated software, certain kinds of pornography, and death threats) is illegal.

Other materials might be considered quasi-illegal in the sense that they infringe on the rights of individuals (protection of privacy) or the rights of corporations (confidentiality, reputation, and return on investment).

Content that involves a breach of copyright, libel, invasion of privacy, or unlawful business practices is usually be litigated at the initiative of the person/entity whose rights have been infringed. The injured party will file a civil action for damages or an injunction. With respect to the infringement of intellectual property, remedies may also be sought under criminal law.

Avoiding Inappropriate Content

In all likelihood, if you surf the Web, you are bound to come across websites that post illegal/offensive materials. If you’re lucky, you’ll be able to tell when something is illegal, just by the URL (for example, “www.madonna-bootlegs.com,” www.stolengoods_r_us.net).

Never download anything from one of these sites. Why? Apart from being illegal—which could land you in trouble for copyright infringement or some other type of infraction—a lot of pirated goods contain Trojan horses or spyware. If you aren’t careful, you could end up a victim of identity theft.

Other times, you may come across an offensive/illicit website when you are looking for something else. For example, you are
looking for information on the President and you make a typo. You enter “www.whitehouse.com” instead of “www.whitehouse.gov.” Or else your child is looking for “Bambi” and instead of getting information about the Disney movie; he or she ends up at a website with explicit pictures of what appear to be underage girls.

Tips for Safe Viewing

By taking responsibility for your family’s online computer use, you can minimize some of the potential risks. First of all, if someone sends you any messages or images that are obscene, lewd, filthy, or indecent with the intent to harass, abuse, or threaten, contact your local law enforcement. If you become aware of the transmission, use, or viewing of child pornography—again, immediately report this information to your local law enforcement. Likewise, encourage your children to tell you if they encounter such messages.

On the other hand, if you encounter material that is harmful, but not illegal, forward a copy of the message to your ISP, and ask for assistance. Most ISPs will make a reasonable effort to investigate legitimate complaints about harmful content or network abuse, and if necessary, they will take appropriate action. Please note that ISPs do not have the legal power to decide whether material in question, is illegal or not. Only the courts can make that determination. If an ISP discovers that harmful or illegal content is being posted on one of their servers, they will take the necessary actions to see that the content is removed. Finally, to minimize your risk of exposure, consider installing/using content filters.
The Basics of Content Filtering

Most filters are software programs that block the transmission of data over the Internet to prevent at-risk users (for example, children) from viewing objectionable content. Most filters use two primary methods for blocking data: word blocking and site blocking. Word Blocking, or “keyword blocking,” matches web pages against a list of keywords. This method is the easiest form of filtering to implement, because it relies on software, rather than human intervention.

In a nutshell, here’s how it works: If the software file discovers content that contains words that match the keywords, the web pages will be blocked. Most filters require two components in order to work:

- **The Rating Component**—value judgments are used to categorize websites based on their content. Access is granted or denied based on:
  - **Blacklisting**: access to listed sites is blocked based on criteria set by the software vendor
  - **Whitelisting**: access is only possible to expressly authorized sites
  - **Neutral labeling**: sites are labeled or rated by the author/publisher. The onus is on the user to use the label or rating, otherwise no sites are blocked. In addition, the must set their browser up so that only content that they deem permissible is allowed to be displayed.

- **The Blocking Component**—each request is examined to see if the resource is on a
“not allowed” list, or if it has the proper labeling. If either condition applies, the filtering software informs the user that access has been denied, that is, the browser does not display the contents of the web page. Depending on the product and how a user configures it, someone trying to access an “off-limits” site may receive a warning message, a browser error message, or a partial view of the blocked site. Sometimes, the browser itself will shut down.

Site blocking rules match web pages against a list of predetermined sites (stoplist). When a user attempts to access an objectionable site, the filter’s stoplist prevents this action by displaying a “denial page.” The denial page informs the user that the site in question has been blocked. Stoplists are created, in part or entirely, by the employees of the filtering companies who decide which sites should be included/excluded.

Content labeling is another method for blocking objectionable content. One such method, developed by the World Wide Web Consortium (W3C), is called the Platform for Internet Content Selection (PICS).

PICS uses “metadata” tags to filter of all types of websites that use an Internet “address” (URL) (Web pages, FTP, and Usenet newsgroups). It is based on the principle of “neutral labeling” which means that PICS can provide Internet access control without censorship. It works by separating the two functions for evaluating content into: (a) the rating of sites and (b) the filtering of sites. Computers can process the labels in the background and automatically shield users from undesirable material.

There are two main approaches for rating of sites: self-rating and third-party rating. Self-
rating means that the website publishers can evaluate their own content and put the PICS rating information directly into their web pages. For example, ratings can be established by entertainment companies with family-oriented websites. Third-party rating means that interested third parties can use PICS ratings systems to evaluate websites and publish their own ratings. Examples of third party raters include: educational groups, religious groups, and so forth.

For a website to be viewable, it must carry a PICS label, and be within the parameters set by parents on the home computer. It is up to the home user to decide, using the PICS parameters, what is acceptable and what is not. This means that users must examine each of the categories to decide how much they are willing to allow. Once these choices have been made, the browser software uses them to filter sites. When the users click on a website, the browser compares the site’s rating with the user’s selection. If the ratings for the site fit within the parameters chosen by the user, it is displayed as usual. If the ratings fall outside of those parameters, access to the site is prohibited and the user is shown a message indicating that the site is blocked.

PICS labels can support different types of information, both ratings (for example, for evaluating language, nudity, sexual content, violence), and pointers (identifying content according to its relevance or interest for various constituencies of users).

Separating the two functions of rating of sites and filtering of sites, and allowing a high degree of flexibility and security, PICS is undoubtedly the most comprehensive and innovative solution yet to tackle Internet contents issues. Rather than censoring what is
distributed, PICS enables users to control what they want to receive.

Internet Filtering Programs

A number of filtering programs have been developed and are available for home users. Below is a partial list of some of the more popular ones:

**CyberPatrol**  
URL: http://www.cyberpatrol.com/.

**CyberSitter**  
URL: http://www.cybersitter.com/.

**Cyber Snoop**  

**NetNanny**  

**Surf Watch**  
URL: http://www.surfcontrol.com/.

**We Blocker**  
URL: http://www.we-blocker.com/.

No Tool is Perfect

When filtering content, one needs to be aware that no tool is perfect. All filters have pros and cons. Some of the problems that have been identified are:

*Underblocking*—even with the best filters, a certain percentage of objectionable content gets through. To effectively control all of the objectionable content would essentially mean blocking most, if not all, the materials on the
Internet. It's not just a matter of improving the blocking technology or coming up with more comprehensive stoplists, rather, it has more to do with the complexity of human language and thought.

For example, some sites with harmless content are blocked because of an offensive word or phrase (for example, "breast") the software is not able to take into consideration the context (chicken breast or breast cancer).

Overblocking—similarly, because of the crudeness of some filters, over-zealous content raters tend to block more than is necessary. This action ends having a negative impact on free speech rights and the civil liberties of anyone who is accessing, publishing, or broadcasting on the Internet. While this type of over-correction may not be problematic for home users, it does present a major dilemma for public facilities, such as schools and libraries, where First Amendment issues are always a primary concern.

"Expert control"—even the simplest blocking technology is difficult to operate, so most people who rely on blocking technology, depend on the "experts" to decide what they should and should not see. Because this type of information is proprietary, the companies keep their stoplists secret, even from those using the blocking technology. This means that users have no way of determining whether they are being denied access to wrongfully excluded websites. Secondly, because the stops are secret, there is a great temptation for abuse e.g., there is nothing preventing unscrupulous operators from unfairly blocking a site for reasons, other than objectionable content. For example, a company could pay "a fee" under the table to have their competitors' websites blocked.
Subjectivity—the criteria used to block content are vaguely defined and subjectively applied, rather than designed and customized to meet the needs of particular communities.

Error prone—lots of mistakes are made when assigning websites to the lists used for blocking. Most software vendors rely on automated systems for making content decisions. This leads to lots of false positives. Nor are there any “open” or systematic ways: (i) to check if a site has been wrongly blocked, (ii) to correct a problem in the event that a site is wrongly blocked, (iii) to override the blocking, or (iv) to appeal an incorrect decision made by a blocking company or service.

At best, filters and labeling are tools that provide users with the cyberspace equivalent of separation, like the ones used by stores to limit access to “adult materials.” Given the far reaching claims of some filtering products, you must be careful not to be misled by the hoopla. Nor should you develop a false sense of security. Finally, be aware that filters are useless in preventing adults from preying on children. Lest we forget, it is important to recall that filters can NEVER substitute for parental involvement.

References


Internet Blocking & Censorware


Plain Facts About Internet Filtering Software

Protecting children from harmful material on the Internet


Part VI

Additional Safeguards
Passwords

"With all of our advances in security technology, one aspect remains constant: passwords still play a central role in system security. The difficulty with passwords is that all too often they are the easiest security mechanism to defeat. Although we can use technology and policy to make passwords stronger, we are still fighting the weakest point in any system: the human element." – Mark Burnett

Definition

When you first turn on a computer or log into a network, the system will respond by asking for a password. The password is a “string of characters” used for authentication.

At a minimum, a password should contain some combination of:

- Upper and lower case letters (Aa, Bb, ... Zz)
- Base 10 digits (0 - 9)
- Nonalphnumeric characters (@, #, $, ^ ...+)
- Punctuation (, . : ; ... ?).
When creating a password, you should never use your full name or your user ID (the name that is assigned to you when you set up an account). Reserve these names for use at the login prompt.

A good password is not easily guessed, yet it is easy to remember. It consists of letters, number, and symbols, yet it can be typed quickly and without error. It appears to be random, yet it’s based on a term or expression familiar to the user.

Note: it takes only ONE weak password to compromise a system!!!

Password Security

Passwords play a central role in system security. Because they rely on humans, they are considered the weakest links in the security chain. Some of the problematic aspects are: (i) hard to remember, (ii) too many of them; and (iii) different rules regarding their construction. Furthermore, the difficulty with passwords arises from the fact that they are one of the easiest security mechanisms to defeat. Gone are the days when you could use your goldfish’s name as your password. The increase in the number of cyberattacks in recent years makes the user of strong passwords a must.

Not surprisingly, there are people, who will try to crack (find out) your password. Once attackers get your password, they can gain unauthorized access to your account; compromise the accounts of other users on the system; or use your account as a jumping off point to break into other networks or machines on the Internet. For this reason, the excuse that “I don’t need a good password because...” doesn’t work anymore.
System security is everyone’s responsibility and passwords are the first line of defense. Don’t be the “weak link” that compromises everyone else’s security. Each user can help strengthen password security by doing the following:

DON’T tell anyone your password.

DON’T write your password down.

DON’T choose a password that can be easily guessed.

DON’T hesitate to change your password if someone else knows it.

DON’T type in your password if anyone is watching you or looking over your shoulder. Wait for them to leave or ask them to step away.

Password Vulnerability

Passwords are vulnerable to cracking tools that are available on the Web. These tools can scan for any word as well as letter-numeral combinations. Weak passwords are easy to guess. Examples of weak passwords include: the name of popular movie characters, default passwords, family names, birthdates, names of pets, etc. Users should never include any part of the user ID as part of the password. Also, using common facts about you or your family is a no-no too.

You should avoid the obvious when selecting a password. For example, you need to pick a password that has no easily discerned significance to you. First of all, never choose a common word that can be found in a dictionary.
There are several ways an unauthorized person (that is, hacker/cracker) might try to gain knowledge of another person’s password. Often, people use personal information such as their own or a family member’s name as a password. This is one of the first things a hacker or cracker might try. A more sophisticated method is password-cracking software.

Most of these programs can ‘crack’ a password within seconds by using large dictionary files and lists of common names or passwords. Another type, known as a ‘brute force’ attack, attempts every possible combination of letters, numbers or special characters.

However, a brute force attack can take up to days or months or years, depending on the strength of your password.

Password Attacks

Your password is stored in an encrypted form. After you set your password, not even the network administrator knows what your password is, unless you tell him. What that means is, attackers can’t discover your password by simply querying the system. Instead they must use cracking tools. There are basically two type of attack: a dictionary attack and a brute force attack.

Dictionary Attack—An attacker will use a program called a “password cracker” to breach security. This program works as follows: it takes a string of characters, encrypts them and then it compares the encrypted text against the password (in encrypted form). The software continues searching until it finds an exact match.
To find an exact match, the cracker program runs through all the words in the dictionary. If your password happens to be a recognizable word, it will be fairly easy to crack. In addition, the cracker will tack characters at the beginning or end of words. So if your password happens to be “your nickname + birth date,” that too will be fairly easy to crack.

Similarly, other password crackers are designed to go through every number-letter combination. Generating combinations of 0-though-9 across six or eight decimal places is a function of processor speed and time. The more speed and time available, the more likely an attacker will uncover your “secret” number.

Because it takes too long to try every combination of letters, the password cracker only tries the most likely combinations. It starts with everything it can find out about you (login name, full name, address, social security number) and then it will search of these combinations. This is accomplished in a matter of seconds.

To perform this type of attack, an attacker uses a “meta dictionary” containing words from all languages, place names, people names, names of characters in books, jargon, slang, and acronyms. It tries all of them as your password. This takes several minutes. After the password cracker is done with that, it tries variations on those words, such as any word that is written:

- Backwards
- Capitalized
- With a punctuation character at the end
- With a punctuation character at the beginning

- With a punctuation character in the 3rd character place

- By replacing all “l’s” with 1’s, “t’s” with 3’s or “o’s” with 0’s

- As any two words, put together with a number between them. And so on. A password cracker can try millions of word variants per second and every combination imaginable.

*Brute Force Attack*—If a dictionary attack doesn’t work, a determined attacker will try a brute force attack. A random password composed of eight letters can be cracked in 24 hours; add numbers to the mix and it may take up to five days or more.

**Password Rules**

Over the years, a number of policies have been established pertaining to passwords. As with any rule, in order for “it” to work, there needs to be some flexibility:

- **Change passwords early and often**

  First of all, if you have been given a default password, you should change it as soon as you log on (or install) for the first time. Passwords on a network account should be changed every 60 to 90 days. Passwords on a home computer should be changed approximately every 6 months.

  Changing your password often is one way to thwart a brute force attack. On the other hand, if you are forced to change passwords too often, you are more likely to write them
down (so you don’t forget) which in turn further undermines security.

Frequent password changes causes users to develop predictable patterns. Unless there is an extreme risk involved, passwords should be changed on a regular basis but not too often that it becomes counterproductive.

- **Never write down your password**

Although this is good advice, it may be necessary to keep your password in a safe place (for example, wallet, safety deposit box, locked filing cabinet) especially if you have accounts that other people might need to get into should something happen to you. If you do write your password down, be sure to disguise it by either omitting the last character, adding some extra characters or by interchanging letters (changing a “b” to a “2”). What ever you do, never write your password on a Post-it note and stick it close to your machine.

- **The Use of Random Password Generators**

There is a common misperception among IT professionals that the most secure passwords are random passwords, created by a password generator. In fact, just the opposite is true. On first glance, a randomly generated password might appear to be strong, but unless you can turn it into a mnemonic or meaningful phrase, it will be hard to remember, slow to type, and vulnerable to attack. If an attacker can get his hands the password generating algorithm, he can recreate a set of randomly generated passwords and then use them to gain unauthorized access to someone’s account.
How to Make Strong Passwords

The following are some suggestions on how to create a strong password:

Use the first letter of each word in a sentence or an expression that is easy to remember.

- Invent a sentence, with numbers and proper nouns in it, that is appropriate to your own life and then take the first letter of each word, and convert the numbers to digits.

- Replace letters (or entire words) with numbers and symbols such as “0” for “o” or “$” for “s.”

Another way to create a strong password is to run several short words together with underlines, hyphens or other characters to separate the words. In addition, there are other elements (patterns, repetition, rhymes, humor) and data structures (phone numbers, file paths, URLs) that are easy to remember and qualify as unbreakable passwords. Other techniques for creating strong passwords are listed below (see Table 7 for sample passwords created using these strategies):

- **Vanity Plate Passwords**—the idea for this type of password is based on license plates (vanity plates) that are customized with initials, names or personal messages. To create this type of password, use a combination of letters and numbers to create a phrase without using complete works.

- **Compound Word Passwords**—passwords using compound words are relatively easy to remember and you can use numbers,
special characters or misspellings to make them harder to break.

- **Phrase Password**—using the first letter of each word in a phrase can also help construct a good password. The object is to pick a phrase that is at least eight words long and then use the first letter of each word.

- **Keyboard Pattern Passwords**—for a password that is visually distinct, you can create a pattern using the keyboard (for example, geometric patterns, series of lines, or zigzags). When constructing an easy to remember pattern, be sure to include numbers and special characters. Never use a single line like QWERTY. One drawback to pattern passwords pertains to shoulder surfing. If you are not careful, someone from across the room might be able to figure out your password from the way your hands move across the keyboard. To minimize this risk, make sure that you use a password that requires the use of both hands.

- **Address Passwords**—any password using the structure of a street address can be easily recalled at a later date without having to write it down as long as you are consistent in the type of structure you choose. For example, you might always begin with a capital letter, then alternate case and alphanumeric / punctuation / symbol thereafter.
<table>
<thead>
<tr>
<th>Table 7</th>
<th>Strong Passwords</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Vanity Plate</strong></td>
<td></td>
</tr>
<tr>
<td>Music is for me</td>
<td>MusikS4me</td>
</tr>
<tr>
<td>Day after today</td>
<td>dayFter2day</td>
</tr>
<tr>
<td><strong>Compound Word</strong></td>
<td></td>
</tr>
<tr>
<td>Rocketship</td>
<td>rokiT7shiP</td>
</tr>
<tr>
<td>Doghouse</td>
<td>DAWG#howz8</td>
</tr>
<tr>
<td><strong>Phrase</strong></td>
<td></td>
</tr>
<tr>
<td>Jack and Jill went up the hill</td>
<td>J&amp;Jwuth2fap0w</td>
</tr>
<tr>
<td>to fetch a pail of water</td>
<td></td>
</tr>
<tr>
<td>I spent too much at the fair</td>
<td>s2matf1n</td>
</tr>
<tr>
<td>last night</td>
<td></td>
</tr>
<tr>
<td><strong>Pattern</strong></td>
<td></td>
</tr>
<tr>
<td>Horizontal zigzag starting</td>
<td>r5t6y&amp;u8</td>
</tr>
<tr>
<td>with ‘r’</td>
<td></td>
</tr>
<tr>
<td>Series of lines starting</td>
<td>asdrtty&amp;789</td>
</tr>
<tr>
<td>‘a’, ‘t’, and ‘7’</td>
<td></td>
</tr>
<tr>
<td><strong>Address</strong></td>
<td></td>
</tr>
<tr>
<td>2000 E 2nd Ave</td>
<td>S2e0C0n0D</td>
</tr>
<tr>
<td>Tampa FL 33605</td>
<td>Tz+3Fl36o5</td>
</tr>
<tr>
<td>3000 Cleveland Ave</td>
<td>F3m3(0)f1</td>
</tr>
<tr>
<td>Fort Myers FL 33901</td>
<td>C3@2x3f9M()l</td>
</tr>
<tr>
<td><strong>SACs</strong></td>
<td></td>
</tr>
<tr>
<td>Yahoo 814</td>
<td>67hJ^$6493fuh5y05edha</td>
</tr>
<tr>
<td>Mail certificate 537</td>
<td>BbdnItbAA$</td>
</tr>
<tr>
<td></td>
<td>Gggrw422a~I;jg588bas3DR</td>
</tr>
<tr>
<td></td>
<td>Bdghbwtrb53</td>
</tr>
</tbody>
</table>
By using a “seemingly” random combination of letters and numbers, you should be able to come up with a password that you don’t need to write it down, especially if you associate your password with a string of text that is easy to remember. For example, you might use a phrase password based on a couple of lines from a poem you learned in 8th grade.

Then, to keep track of your password, all you need to write is something like “grade 8 poem” and that should be sufficient to trigger your memory.

Finally, the following strategy can be used when you are required to keep track of several passwords:

1) Memorize eight different sequences of alpha-numerical sequences (SACs). Each SAC should be different in size and made up of a combination of numbers, symbols and uppercase letters.

2) Assign a number to each sequence, e.g, SAC1, SAC2, SAC3 and so forth and when you are done, you might come up with a scheme that looks like the following list:

<table>
<thead>
<tr>
<th>SAC#</th>
<th>Sequence</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAC1</td>
<td>fuh5y05edh</td>
</tr>
<tr>
<td>SAC2</td>
<td>g8bs=hb56hRRT</td>
</tr>
<tr>
<td>SAC3</td>
<td>!;g588bas3DR</td>
</tr>
<tr>
<td>SAC4</td>
<td>aBbdnltbAA$</td>
</tr>
<tr>
<td>SAC5</td>
<td>Gggrw422a~</td>
</tr>
<tr>
<td>SAC6</td>
<td>&gt;&gt;GAEB53th8g3e</td>
</tr>
<tr>
<td>SAC7</td>
<td>Bdghbwtrb53</td>
</tr>
<tr>
<td>SAC8</td>
<td>67hJ^$6493</td>
</tr>
</tbody>
</table>

3) For each account, select three SACs and then put them in a specific order. This arrangement can be used as your password.
4) To keep track of each password, write down the order of each SAC in a password protected database (here, be sure to use a simple, easy to remember password). If you need to write down your passwords in a less secure location, create a reminder a list of all of your SAC's but only with the first two characters being correct. The rest of the letters are put there as disinformation. Then based on the first two characters you should be able to remember what the SAC is. You (insecure) list might look like:

<table>
<thead>
<tr>
<th>SAC#</th>
<th>Written Down</th>
<th>Real Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAC1</td>
<td>fuh355y9wtga9</td>
<td>fuh5y05edh</td>
</tr>
<tr>
<td>SAC2</td>
<td>g8betb8g</td>
<td>g8bs=hb56hRRT</td>
</tr>
<tr>
<td>SAC3</td>
<td>l;kyh35h9</td>
<td>l;g588bas3DR</td>
</tr>
<tr>
<td>SAC4</td>
<td>aBfbvsh4</td>
<td>aBbdnitbAA$</td>
</tr>
<tr>
<td>SAC5</td>
<td>GgfasdG</td>
<td>Gggrw422a~</td>
</tr>
<tr>
<td>SAC6</td>
<td>&gt;&gt;GSDFGWRw44</td>
<td>&gt;&gt;GAEB83Ew4</td>
</tr>
<tr>
<td>SAC7</td>
<td>BbgRhgw52354</td>
<td>Bdghbwtrb53</td>
</tr>
<tr>
<td>SAC8</td>
<td>6775u3ed5us</td>
<td>67hJ^$6493</td>
</tr>
</tbody>
</table>

So the password for the Hotmail452 would end up as:

“aBbdnitbAA$Gggrw422a~g8bs=hb56hRRT”

(Note: typed as a single string, no spaces and no quotes).

Lastly, please bear in mind that even the strongest password can be discovered through some other means (using a keylogger or through social engineering). Therefore, it is important that you follow the recommendations for securing your computer, assets, and person, listed in other sections of the *Florida Cyber-Security Manual*. Additional tips can be found at the Secure Florida website <www.secureflorida.org>.
For your protection, do NOT use any of the passwords that have been listed in the Manual (or are used during the presentation). Because these passwords have been publicly revealed, they are less robust. Meaning? There is a good chance that they will added, if they haven’t been already, to a meta dictionary.

For Added Protection

Both complexity and length affect the strength of the password:

A password that contains a mixture of letters, symbols, numbers, and spaces is more complex than one that doesn’t. The use of complex passwords will greatly reduce the chances of having your account hacked by a dictionary attack.

The longer the password is, the more time it takes and more processing power will be needed to crack the password. Using a complex password with five or less characters can be found in seconds using a brute force attack. Passwords with seven or more characters take longer. It follows that the longer the password, the more combinations a password cracker must try before guessing the correct one. Due to the way that passwords are created and stored, the optimal length for a password is between 8-14 characters long.

Managing Passwords

Not all passwords are created equal. The need to safeguard your New York Times password is much less than the need to protect the password you use for online banking or the one you use to access your Hotmail account.
For the former, reusing the password for similar sites is acceptable whereas in the latter two cases, you need to make sure you come up with passwords that are harder to crack. It is easier to manage several passwords if you segregate them into separate categories. For example:

- **Nuisance**—anything will do for websites that require a password to access their content. For example, your password for the New York Times might be: my_nytnews!.

- **Sensitive**—something stronger is needed here. With these accounts, you need to use a password generating formula. For example, your password for online chatting might be: first letter of the IM client you are using (AOL Instant Messaging) + the numbers in your street address (2342) + the number sign which would give something like: A#2o3l42.

- **Critical**—unique passwords need to be created for online banking or mutual fund accounts. For these types of accounts, you need to create strong passwords that are easy to remember. For example, for your online accounts, you might decide to use a combination of web address and your personal identifier to generate a password. If you do online banking with the Capital City Bank and their URL is www.ccbg.com/, the password you create might be the URL + your PIN number (1357): 2C1_be3.G5-7.

---

**Password Protected Screensavers**

Password protected screensavers can be used as an additional line of defense for deterring
intruders and snoops. The use of password protected screensavers is necessary if you are using a machine, say at work, and you need to leave your machine unattended and unprotected. As well, screensavers are handy, if you are working at home and you don’t want your kids to modify your files.

A password protected screensaver will lock your machine after a few minutes of inactivity.

Once you return to what you were doing, you will be required to type in a password to reactivate your machine. According to TruSecure, the use of a screensaver password provides more protection from unauthorized access than the use of, say, randomly generated passwords that need to be written down to be remembered. Similarly, it is usually easier to tell if your hardware has been tampered with than it is to find out if your password has been stolen.

To wrap up, please visit the Secure Florida website <http://www.secureflorida.org> and check out the additional resources that have been compiled on Passwords. Plus, you will find step-by-step instructions that will show you how to set up a password protected screensaver. Lastly, to keep up with the latest security trends, subscribe to the Secure Florida Alerts and Highlights news service.

References


START

Firewalls

“People often think that having a firewall between your internal network and the “Big Bad Internet!” will solve all your security problems. It may help, but a poorly set up firewall system is more of a security risk than not having one at all. A firewall can add another layer of security to your systems, but it cannot stop a really determined cracker from penetrating your internal network. If you let internal security lapse because you believe your firewall to be impenetrable, you have just made the crackers job that much easier.” – Gary Palmer and Alex Nash

Definition

A firewall is the first line of defense for "always-on" connections. Set up as either a program or hardware device, a firewall’s main responsibility is to enforce an access control policy, monitoring what gets into a network and what gets out. Figure 8 (see below) shows a diagrammatic depiction of how firewalls perform the gatekeeper function.

A firewall sits at the junction point, or gateway, between the two networks, usually a private network, such as a local area network, home network, or personal computer (relatively safe) and a public network, such as the Internet (relatively unsafe). Firewalls are used to keep a computer or network secure from attack. For example, a Demilitarized Zone (DMZ) is formed by installing firewalls between the Internet and the DMZ and the DMZ and the computer network—forming a type of “oreo” (as in cookie). With a DMZ set up, an attacker needs to pass both firewalls before they can get to resources that are located behind the firewall; whereas e-mail and web services which are subject to constant attack are located in the DMZ.
Of all security mechanisms in use today, firewalls are the most widespread and yet the least well understood.

At its most basic level, a firewall are designed to fulfill a number of interrelated objectives: (i) to block any incoming data that might contain a hacker attack; (ii) to hide information about the network so an intruder will only be able see traffic originating from the firewall rather than the network itself, and (iii) to screen network traffic in order to prevent abuse (unauthorized use of the Internet) and/or control access (to remote sites). Because incoming traffic poses a greater danger than outgoing traffic, it is usually screened more closely.

A Generic Firewall Set Up

![Diagram of a generic firewall setup]

Figure 8
Types of Firewalls

Firewalls come in three main flavors: software-based, appliance-based, and hardware-based.

*Software firewalls* can be extremely flexible and they have been developed for a full range of architectures. In spite of their widespread use, software firewalls have certain drawbacks. They require continuous operating system upgrades/patches and they exhibit poor throughput performance. In contrast, *application firewalls* offer the best bandwidth throughput. However, as more rules are added and more demands are placed on what is to be inspected, the throughput rate falls correspondingly. Finally, most *hardware firewalls* are routers that come with firewall protection.

Firewalls also work in conjunction with most AV software. While AV software scans in-coming communications and files looking for malicious code. A firewall not only makes your machine/network invisible on the outside world, it also blocks communications from unauthorized sources.

While a firewall is absolutely essential if you are using high-speed Internet access through a cable modem or a DSL (digital subscriber line) connection, you should be aware that it won’t detect malware if it comes in through authorized channels (open ports) such as e-mail, Instant Messaging or P2P file sharing. Therefore the combination of up-to-date AV software and a firewall is a must if you are to minimize your risk of an attack.

Ports

A “port” like the name suggests, can be likened to an opening or an end point of a connection. With respect to the Internet, it refers to the critical portion of the (logical) connection point
## Table 8
TCP/IP Services and Ports

<table>
<thead>
<tr>
<th>Service</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ping</td>
<td>7</td>
</tr>
<tr>
<td>FTP</td>
<td>20 &amp; 21</td>
</tr>
<tr>
<td>SSH</td>
<td>22</td>
</tr>
<tr>
<td>Telnet</td>
<td>23</td>
</tr>
<tr>
<td>SMTP</td>
<td>25</td>
</tr>
<tr>
<td>HTTP (WWW)</td>
<td>80</td>
</tr>
<tr>
<td>MS file &amp; print sharing</td>
<td>137-139</td>
</tr>
</tbody>
</table>

### TCP/IP Port Reservations

<table>
<thead>
<tr>
<th>Type</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Well-known ports</td>
<td>0 - 1023</td>
</tr>
<tr>
<td>Registered ports</td>
<td>1024 - 49151*</td>
</tr>
</tbody>
</table>

* In practice most systems start assigning dynamic ports at 1024

between two computers using TCP/IP and common services (e.g., Simple Mail Transfer Protocol (SMTP), Hypertext Transfer Protocol (HTTP), or File Transfer Protocol (FTP)). A sample of common ports and the corresponding service is listed in Table 8).

Because ports are commonly probed and attacked, it is important to block all unused ports and only allow specific protocols (those for which you have a business/personal requirement) to enter your network perimeter. Please note that even blocked ports you must constantly monitor and be on the look out for any intrusions. For this reason it is important to turn on your firewall logs or if warranted, install an intrusion detection system (IDS).
How Firewalls Work

A firewall functions as more than a locked door; it doubles as a security guard, too. Depending on the type functionality required, firewalls can be segregated into the following categories: packet filtering firewalls, proxy servers (application level and circuit level gateways), and stateful packet inspection firewalls.

Packet Filtering Firewalls—this type of firewall works at the network level and it can be likened to a type of router. The simple ones are “static” that is, stationary which means data are only allowed to leave the system if the firewall “rules” aka the Access Control List (ACL) allow it. For example, applications such as FTP (file transfer protocol) and HTTP have static TCP ports. For example, setting a packet-filtering firewall to block data traveling out of port 80 (the standard port used for HTTP) will have the effect of disabling web browsing for all computers inside the firewall.

As packets arrive, they are filtered by: (i) their type (application or protocol), (ii) source address (SA), (iii) destination address (DA), and (iv) the port information contained in each packet (source port number and destination port number). Every packet is inspected for compliance with predetermined rules. These rules are examined in order, until one of the rules fits.

For example, most packet filters have “deny all” as the last rule. Not surprisingly, the more rules there are, the longer it takes for a packet to be cleared.

Once the status of the packet is determined, the firewall can drop the packet, forward it or
send a message back to the originator. The more complicated type of packet filter firewalls are “dynamic” that is, during each the session, the two end points determine what ports will be used based on their position relative to the other (static) connections.

For example, most web-based databases use dynamically assigned ports which can number in the thousands. Dynamic packet filters offer two primary benefits over static packet filters: (a) they can support all applications with more granularity (levels) and (b) throughput rates are higher since they don’t need to compare every packet against the ACL.

The main advantages of packet filtering firewalls have to do with their low cost and low impact on network performance. Their disadvantages have to do with the fact that they only filter ports and IP addresses. They don’t verify, much less examine, the content of the data.

To set them up, also requires some technical knowledge especially if you wish to customize them. Most cable/DSL routing devices use packet filtering as a part of their firewall protection.

**Proxy Servers**—proxies intercept inbound and outbound traffic. They also mediate communications so that both “hosts” talk only to the firewall itself, and not directly to each other. There are two types:

(a) *Circuit level gateways*: these act like a switchboard. They check sequence bits to ensure that the TCP handshake between two hosts is legitimate (this helps to prevent “IP spoofing”) and they allow data in based on requests coming from computers inside the network. If there is no match, then the data
are blocked. In other words, all ports remain closed until the firewall opens them.

Another advantage is that anyone scanning the network from outside will only see the address of the firewall and not the rest of the network. The main disadvantage lies in the fact that unless this type of firewall is combined with some other form of filtering, any type of data requested from inside the firewall will be allowed though. In addition, they don’t filter individual packets.

(b) Application level gateways: examine each individual IP packet to verify authenticity. They are similar to circuit level gateways in how they operate but they differ in the way they handle traffic. The circuit level gateway only examines the address and port information, not the content.

An application level gateway is more discriminating. It runs proxy applications to view common types of data (HTTP for webpages, FTP for file transfers, and SMTP or POP3 for e-mail) before allowing them to enter through the firewall. Because of the control they offer, application level gateways are considered very secure. Because of the proxy applications they use, they are slow at passing data. Because client applications need to be configured, they are harder to set up. As a result, application servers are better suited to large networks and are not for home use.

**Stateful Packet Inspection Firewalls**—represents a combination of packet filtering with some of the elements of the gateway methods. It includes all the advantages of packet filtering and proxy servers without the throughput problems. In addition, they offer a high level of security, good performance and transparency to end users. The downside: they are more expensive and due to their
complexity they can end up being less secure if they are not configured properly.

Each type of firewall has its pros and cons. To learn more about firewalls, go to the Secure Florida website <www.secureflorida.org> and click on the Firewalls link. This section will provide you with state-of-the-art advice on: firewall vendors, the types of firewall products best suited for small business/home users, and firewall selection criteria. In addition, Secure Florida has links that will provide you with how-tos on properly configuring a firewall, test sites and the best way to set up a DMZ.

Limitations of Firewalls

It would be remiss on our part if we didn’t point out some of the limitations. Most firewalls are incapable of defending against today’s advanced threats. Firewalls only operate at the boundaries, which means they are poor at intercepting an attack that is able to slip past the firewall and get in via authorized channels for example, e-mail, instant messaging and the like.

With the widespread proliferation of DSL and cable modems aka “always on” connections, the risks have never been higher. Despite the limitation, firewalls have an important role to play in your overall security. They are important because they provide a single “choke point.” If you are constantly vigilant and you install a firewall that monitors both incoming and outgoing traffic, it is less likely that your system will be compromised.

The point we want to leave you with is this... there is no single technical solution available that will cover all situations. However, if you follow a “defense in depth” strategy, your odds
of withstanding a cyber attack increase significantly.

Last but not least, be sure to register with the Secure Florida website <www.secureflorida.org> so you can continue to be informed about the latest trends in firewall technologies and what countermeasures you need to adopt to minimize your overall exposure.

The PORT Test

The following set of tests have been developed to help users practice “due diligence” when installing a firewall. When programming a firewall, you can follow a *laissez-faire* firewall strategy where you allow anything in or else you can follow a *deny-all* firewall strategy where you let nothing in and nothing out.

Either of these two extremes are impractical at best since what you end up with will be a compromise that depends on your particular situation and work/play habits. The PLAT test is designed to help you set up a firewall so that minimizes your risks and maximizes your productivity/enjoyment:

- **Program.** Based on the applications and program(s) you use, make a list of what destinations you visit and what types of connections you need to access. Similarly, make a list of what programs you run that require the ability to upload/download/synch with an outside source. Avoid setting up general rules that allow unfettered connections—since this contributes to unwanted and unchecked behavior.
- **Outside.** Determine the address and port number you need to configure in order to connect to an outside source. Again, try to restrict the applications/programs so they are only connecting to locations you want and can account for.

- **Required.** When assessing a particular connection, decide whether it is allowed or denied? Note that your firewall rules will contain some of each.

- **Temporary.** Is the connection you are considering, temporary or permanent? For example, if you’re going to connect to a particular Internet destination five or more times each time you use the computer, then you should make the connection permanent. If not, define it as temporary and adjust your firewall rules accordingly.

### References


Firewalls FAQ


Maintenance

“Computers are at their best—and their most secure—when well-maintained. Without regular cleaning and organization, your hard drive gets cluttered with data, your file system becomes messy, and overall performance slips. Without frequent backups and weeding, your data is less secure and more difficult to restore. And, unless you occasionally update your software and renew your subscriptions, your programs will not perform optimally.” – Home Computer Maintenance 101

Definition

Preventative maintenance includes all the activities involved in keeping your system in top working order. While it is beyond the scope of the Florida Cyber-Security Handbook to address each and every activity involved in following a proper schedule (only security-related topics will be covered), you can find more maintenance-related information at the Secure Florida website <www.secureflorida.org>.

Weekly Tasks

To maintain your computer for better security, there are a number of routine tasks that need to be performed on a daily or weekly basis (depending on your needs):

- **Get information about what’s new.** Sign up for:
  - Secure Florida Alerts and Highlights <www.secureflorida.org> website to receive notifications about the latest security threats and attacks.
- If you buy/install new software or hardware, take a minute to register the product/service to keep informed about patches, upgrades, updates and security bulletins.

- If you are using Windows XP, Windows ME, or the Windows 2000 SP3 operating system (OS), you can receive automatic alerts about security updates.

If you are using Windows 98, you can sign up to receive Critical Update Notifications—to subscribe to either of these services, go to the Microsoft website < www.microsoft.com >.

- **Automate maintenance tasks.** If you have a Windows OS, you can use the Windows Task Scheduler to schedule routine file maintenance such as automatic disk cleanup, disk fragmenter, and virus scans. If you have an Apple OS, you can use the Auto Update feature that is included in the software.

- **Set your AV software up to automatically scan your files.** Schedule your AV software to: conduct weekly scans of all system files, and check files or executables on an *ad hoc* basis (i.e., whenever new files are downloaded onto your machine or copied from removable media).

If you are not receiving automatic updates or notifications from the AV software vendor, then it is your responsibility to keep up-to-date with any changes to the software or the AV signatures. This advice also applies to any other software programs you are running that are in need of frequent updates in order for their “preventative capabilities” to remain current (e.g., anti-
spyware software and patches for vulnerabilities).

Semi-annual Tasks

Twice a year, it is necessary to perform the following tasks:

- **Change your passwords.** Don’t run the risk that someone will discover your password and compromise your personal computer or a network for which you have been given certain privileges. Visit Secure Florida <www.secureflorida.org> to keep abreast of the latest tactics on “strong” password creation.

- **Make sure that your anti-virus (AV) subscriptions are up-to-date.** Whatever you do, don’t ever let them lapse. Why? The minute you let your guard down is the time something “bad” happens. Think of your anti-malware software as insurance. To find out about the latest trends in AV tools and techniques, visit Secure Florida <www.secureflorida.org> on a regular basis.

- **Reassess your situation.** Take a moment to consider whether your security and privacy needs have changed over the past 6 months. Is there anyone new who is using your machine or has been added to the network? What types of applications are you using that you didn’t use before? Are you engaging in risky behavior, e.g., P2P file sharing, chatting online? To get information on the latest attacks and countermeasures, register at the Secure Florida <www.secureflorida.org> website and get on the mailing list for the *Alerts and Highlights* services.
LEST YOU FORGET: security is a process. Make securing your network, your computer, and your assets part of your routine and the chances are, you will never become a victim of cybercrime.

**Hard Drive Disposal**

Whenever you are getting rid of your computer, you need to be aware that “erased” disk drives, may harbor confidential information such as credit card numbers and medical records.

Whenever a hard drive changes hands (say, you sell it on eBay), there’s absolutely nothing (except for the basic honesty and ethics of others) to prevent the new owner from gaining access to data that has not be purged. It could be your old e-mail, tax/medical records, passwords, and so forth.

Even if you go to the trouble of emptying the recycle bin or reformatting the hard drive, all you have done is release hard drive space for future use. You haven’t deleted any data.

The potential financial and legal ramifications of old data stored on unused areas or “blocks” of the disk drive could be huge.

Following is a list of tools you can use to sanitize your hard drive before you sell or donate machine:

- Autoclave

- Darik’s Boot and Nuke
  URL: http://dban.sourceforge.net/.
• KillDisk
  URL: http://www.killdisk.com/.

• NecroFile
  URL: http://www.necrocosm.com/.

For a more complete/up-to-date list of tools that can be used to purge your computer, visit the Secure Florida.org <www.secureflorida.org> website.

**Backups**

A backup refers to a second (spare) copy of a file, file system or other digital asset that can be used in case the primary file/system/asset fails, becomes corrupted or is destroyed. Equally important is the ability to recover the file(s) after they have been backed up.

As a rule of thumb, if you are saving work that is critical, two backups (stored on different media/locations are advisable). Saving work that can be easily retrieved/replicated, gives you a lot more flexibility in choosing a backup schedule that fits your needs.

Backups are essential. Unfortunately, it usually takes a melt down of your hard drive or the accidental deletion of anything you would hate to lose or can’t replace (for example, digital pictures, music collection, letters, recipes or tax returns, or whatever) for this truism to sink in.

While most users would contend that any backup is better than no backup at all—that is not necessarily the case. The only backup worth anything at all—is the one you can use.

Backups that take too long; are too expensive; or give you any reason to avoid doing them, are practically worthless.
Some golden rules for backups:

- Back it up or give it up, and
- What has NOT been backed up, cannot be recovered.

It goes without saying, backups stored locally do not survive a disaster. Please note that ordinary backup programs CANNOT backup your “system.” To backup Windows files and other critical sectors on your hard drive, you need to perform a full system backup using a program designed for the purpose.

Having a full backup means that should something catastrophic happen—a motherboard fails, there is a malware-related scourge that is raging across the Internet or lightening strikes—not only will you be able to recover your data but you’ll be backup and running in a fraction of the time it might otherwise take.

On the other hand, in case you’re thinking: “I don’t have to worry about backups because my system is new.” Think again! A brand-new computer (or hard drive) is more likely to fail (that is, lose your data) than one that has been operating for a while. See Figure 9 for a graphic depiction of the Bathtub Curve.

Notice the shape of the curve—instead of resembling a straight line that declines gradually with age, the failure rate for hard drives looks like a flattened “U.”. This type of failure rate indicates that hard drives are most likely to fail either when they are new or when they are old. In between, they are fairly stable.

New hard drives will most likely fail as a result of manufacturing defects; whereas, old hard drives will most likely fail as a result of wear-and-tear due to age. This pattern of decline fits
The Bathtub Curve

![The Bathtub Curve Diagram]

most products, but it is even more pronounced in the case of electronics.

**Backup Principles**

Because it is always “too late” to make a backup after you need one, the following backup principles are designed to help you prepare for a worse case scenario:

- Adhere to a regular backup schedule and be sure to backup your system “before and after” any critical operations have been performed (e.g., installing or uninstalling programs).

- The number of times you perform a backup is a matter of personal preference. But bear in mind the following tradeoff: the more backups you make, the more space you need to store backups and the harder it will be to find any particular backup copy when you need it; the fewer backups you make, it is less likely that you will be able restore the exact version of a file/document when you most need it.
Organize your file system so you only need to backup the files that have recently been changed.

Likewise, you need to keep your backups organized too or you’ll have a hard time finding them when you need them. Use at least a couple of storage disks, to reduce the risk (e.g., one of the disks might be damaged or infected).

Note that not all of your files need to follow the same backup regime. For example, there are some files that don’t require backing up at all—either you don’t care about them (they have low intrinsic value) or else, you have master copies that you can re-install. The point is, when making up a schedule, bear in mind that different files have different backup requirements. In this case, one size fits all is a waste of time and resources.

After you make a backup, don’t forget to do the obvious, viz., write the backup date on the label!

Be sure to store your backups somewhere other than your primary hard drive or place them on a second drive/removable media. In fact, you may want to store critical backups in a different location altogether (e.g., in a safe deposit box, at a family member or a friend’s house or any place where a fire, flood or other natural/man-made calamity won’t destroy both your computer and your backup at the same time).

Test your backups to see if they work in the event you need to recover your files. If file restoration doesn’t work during a test, chances are, it won’t work when you most need it.
Finally, to avoid overwriting perfectly good files in a haphazard fashion, consult the Secure Florida website <www.secureflorida.org> for tips to how to restore backup files in a reliable and safe manner.

**Storing Assets**

There are no hard and fast rules on *how best to* store your digital assets, other than it is recommended that this decision should be approached in a prudent and thoughtful manner. The same safeguards you use to evaluate your tangible assets should be used for your intangible ones. First, take time to critically review all your assets and then, when choosing what technologies you would like to invest in, to secure those assets, use the following formula to help you determine your tradeoffs:

- It should cost *less* to secure the asset than the value of the asset.
- It should cost *more* to steal the asset than the asset is worth.

**The FORMS TEST**

To help safeguard your digital assets, use the FORMS test to walk you through the process:

**Files**—Performing a backup is a time consuming process. Therefore you need to “triage” what files you are going backup. A high priority should be assigned to those files and data that cannot be easily duplication, *viz.*, irreplaceable content (e.g., stuff you have created yourself or got from a family member
or friend). Don’t waste your time backing up programs that can be easily copied from websites/masters.

**Often**—How often you back your files and data up depends on your own unique circumstances. The operative rule is to perform frequent backups for information that is dynamic and constantly changing and intermittent backup for information that is relatively static.

**Recover and Replace**—As technology continues to evolve, you need to consider how you are going to keep your data up-to-date as you continue to upgrade your OS. Choose a migration strategy that will enable you to recover files that have been written in formats that may become obsolete in the not-to-distant future. Otherwise, continue to rewrite and replace files each time you undertake a major upgrade.

**Media**—Here, the issue concerns what media you will use to backup your data. Again, bear in mind that storage technologies are evolving. If you have a DVD or CD burner, backup to a DVD/CD, otherwise use a floppy, tape or a removable disk (e.g., a thumb drive). This decision will be driven by cost and convenience.

**Store**—Now that you have made your backups, where should you store them? Obviously, it is not wise to save your backups in same location as the originals. For those of us who live in Florida, make sure that you store your backups in a location that is hurricane proof and if that is not practical, then make sure you keep them in containers that will survive wind, water and fire damage. There is no point in taking the time to perform backups if you end up losing them as a result of negligence.
Patches

A patch is a piece of “benign” code that is inserted into a program as a temporary fix for a flaw or a bug in the software. Note that the terms “update” and “patch” mean pretty much the same thing, i.e., the replacement of old system files with new system files or the addition of new ones to correct existing problems. Note the following:

- Patches are released, by the software developer, to resolve weaknesses, repair security holes and improve functionality.
- Once vulnerability is detected, attackers/hackers will post this information (on websites or IRC channels) to other members of their community.
- Until a patch is developed and deployed, security may be severely compromised.
- Patches are necessary for all platform types and systems.

The Attack-and-Patch Cycle

Patch management is not easy, even at the best of times. In an environment that includes blended threats, keeping up-to-date with patches is a time consuming and thankless task. To simplify the process, vendors have begun releasing patch “rollups” i.e., collections of patches that you can install all in one session. These service packs simplify the patch management process because the patches are (i) cumulative, (ii) product specific, and (iii) bundled together for easy downloading. When you are in the middle of a transfer, make sure that you are installing the latest service packs, otherwise, you could end up with a false sense
of security. How? Because you performed the download, you think you are up-to-date, when in fact, you’re not! Also, make sure that you are NOT downloading from a spoofed website (see the section on Spoofing).

Before downloading any kind of patch, you will need consider:

- What systems and programs you are using?
- What versions you have?
- What are the known threats and vulnerabilities?
- What countermeasures have been employed?

This information must be kept current! If you are not sure how to obtain this information, click on the Patch Management button at the Secure Florida website <www.secureflorida.org>.

Secondly, before installing any kind of patch or service pack, your system must be completely backed up. Sometimes updates or upgrades don’t work out, and you may be left with problems you can’t remedy or even a computer you can’t even restart. Note that if you are running Windows XP, a backup may be unnecessary since you can make use of a recent System Restore Point.

Install updates in chronological order, with the oldest first. Otherwise, you might end up undoing the “newer” fix.

One of the downsides with patch management has to do with the fact that sometimes a patch that is intended to fix one problem may end up creating a new one and attackers/hackers love to exploit these idiosyncrasies. When this
happens, you may find yourself in an endless loop, called attack-and-patch cycle. Unfortunately, there seems to be no end in sight—at least for the foreseeable future—for this constant game of one-upmanship!

Patch Management

If you are a Microsoft user, you will soon discover, if you haven’t already, that patch management is a MUST if you are to keep your system safe and secure. Because patching is a painstaking process that requires diligence and patience, you need to be careful when you are installing new patches. Like most things involving computers, patch management implies an element of risk.

It is no secret. Microsoft products are renown for their vulnerabilities. Without going into all the whys and wherefores, the fact that their products are tightly integrated means that if and when an exploit occurs in one area of the system, by definition, all areas are equally impacted. Not to mention, the fact that Microsoft enjoys a monopoly in the home computer market, makes them the target for most attackers.

Finally, be careful that you don’t confuse patches (updates) with settings (preferences). Settings are the options you choose to make your OS (e.g., Windows), your browser (e.g., Netscape/Mozilla or Internet Explorer) and your e-mail client (e.g., Eudora or Pine) as efficient as possible. While patches are used to plug security holes; settings are used to configure your system so it will be more functional and user friendly.
The BUT Test

To avoid getting caught off guard, try relying on the BUT test. This test will enable you to determine, in a proactive manner, whether you should go ahead and install a patch or wait until a “patch to the patch” is released or you bite the bullet and change operating systems / programs altogether.

**Break**—Does the vendor’s website indicate whether or not the installation of the patch will affect another program/service? Should that be the case, you need to proceed very carefully. In addition, try contacting the vendor to find out what is the likely impact is and what recommendations they have so you can avoid crashing your system.

Otherwise, try “googling” the problem. You may discover that another user has encountered the same problem and devised a reasonable work-around.

Better yet, visit the Secure Florida website <www.secureflorida.org> to find out what news items have been posted and whether there are any security alerts that place you at risk.

Last but not least, you can decide NOT to install the patch. But if you choose this option, be aware that there an element of risk, i.e., without the patch, your system may be extremely vulnerable to an attack.

**Undo**—Assuming “all systems go,” then the next issue you need to resolve is:

*If you install the patch, can you undo it?*
In other words, can you restore your system to the way it was before you attempted the upgrade? Currently, most reputable vendors are releasing patches that include an “uninstall” feature that allows you to remove a patch that does not perform as expected.

In the event of crisis (read: lock-up), some OSs will allow you to go back to a “previously known and working state.” Bottom line: know what the vendor provides before you go ahead with the install so you can undo the operation, if necessary. Otherwise, make sure you perform a backup before proceeding.

**Timeliness**—Like most things in life, timing is everything. Be sure to make the time to keep your system and programs patched and up-to-date. If not, then make the time to know what your risks of exposure are. Finally, be an informed consumer and make an effort to visit the Secure Florida website <www.secureflorida.org>. If there is a problem or a new exploit that has been released in the wild, you’ll be one of the first people to know about it and based on that knowledge, you can take whatever actions are necessary to safeguard your assets.

**Policies**

In light the range of issues covered in the *Florida Cyber-Security Manual* (note: the topics included in the Manual only represent a mere sampling of the types of exploits and threats that can be found on the Internet/Web and new ones appear everyday), it should be clear that securing your network/computer/assets is no longer the sole preserve of network administrators and law enforcement. Security is everyone’s responsibility particularly if you are in a situation where you are share a computer and/or are connected to the Internet. If this applies to you and your family,
then you need to establish some policies that will ensure that “you all” subscribe to the same objectives (viz., to be safe and secure) and that anyone who has permission to access your computer is fully aware of what the dangers are and what countermeasures can be taken to mitigate the risks. Secondly, by establishing some written policies you can sure that no one is working at cross-purposes. Meaning? You set up a firewall to monitor incoming and outgoing traffic but meanwhile unbeknownst to you, your teenager is engaged in P2P file sharing and instant messaging.

It is beyond the scope of Florida Cyber-Security Manual to stipulate what policies you ought to put in place, i.e., these are context specific. At a minimum, it is our opinion that you should address the following issues:

- **Establish the ground rules.** Particularly if any children in your house are using the Internet, you need to be absolutely clear and make sure they understand (and why): what sites they can visit, what types of activities they can engage in, what types of files they can download, and whether they can visit chat rooms, gaming sites, and so forth. Don’t forget to make them aware of the safety tips and advice that has been compiled by Secure Florida so they are equipped to deal with unanticipated situations.

- **Enforcement.** Rules are only effective if they are enforceable. In fact, setting up rules that are unenforceable does more harm than good. Rather than trying to impose a top-down approach, invite your “family and friends” to help you establish policies that minimize your exposure. As well, get them to agree in advance what the penalties should be in the event that a rule is broken. That way, you are more likely to
get a higher compliance rate. However, don’t make the mistake of being over zealous or too onerous. The goal is to create a set of rules that everyone can live by.

- **Remediation.** Murphy’s Law notwithstanding, if you are active on the web, you increase the likelihood of an incident. Therefore, make a plan of what you are going to do, should a mishap occur. That way, you will not be taken by surprise and your family will know what to do and in the event of an emergency. Be sure to include the contact information for your ISP and local law enforcement.

In the meantime, safe surfing!

**Best Practices**

To wrap up and conclude the *Florida Cyber-Security Manual*, we want to leave you with a restatement of Secure Florida’s best practices:

1. **Use anti-virus software.**

   Your anti-virus software should be set to constantly monitor your system using “real-time monitoring,” and you should be sure your virus definitions are kept up to date.

2. **Install hardware and software firewalls.**

   Your network should be behind a hardware firewall, particularly with a high-speed connection. Install a personal firewall to block any content that the hardware may miss.
3. **Create strong passwords.**

   A strong password is one that has at least 8 characters including letters, numbers, and other non-alphanumeric characters.

4. **Establish a back-up schedule for important data.**

   Creating and maintaining a set schedule for backing up your data can prepare you for any unfortunate breach that could occur despite your best efforts to remain secure.

5. **Maintain up-to-date security patches.**

   Carefully review and install software patches as soon as they become available. This will help to reduce the amount of time that you are vulnerable to an attack.

6. **Use password-protected screen savers.**

   Reduce the chance that others are able to access your data by using a screen saver that activates after a short time and requires a password to return to the desktop.

7. **Check the settings in your e-mail client and web browser.**

   In your e-mail client you should use content filter settings to block unwanted e-mail. You can also set your Web
browser to block cookies and unwanted JavaScript.

8. Use safe e-mail and download practices.

Most computer viruses spread through e-mail or direct downloading to your computer. With this in mind, you should think carefully about everything that you download.

9. Increase your awareness of Internet security.

Become aware of the dangers surrounding you on the Internet. You can do this through formal training, or simply keeping up with the latest Internet news and alerts.

10. Establish policies and rules for information security.

Policies or rules should be established in your business or agency, and even in your home, providing guidelines for secure computer use.

Lastly, if you haven’t done so yet, visit the Secure Florida website <www.secureflorida.org> and register for the security Alerts and Highlights.
References

All About Windows Backups.
URL: http://www.backupcritic.com/main.html


Backups and Disaster Recovery


Computer Maintenance for Beginners

connect computers

Fast guide to backup/recovery
URL: http://searchstorage.techtarget.com/originalContent/0,289142,sid5_gci886601,00.html . Last Visited: November 23, 2003.

Fast, Easy Backups For Win98 / ME / NT / 2K / XP


Home Computer Maintenance 101

How to maintain your computer for better security


Patch Management

Practical Maintenance Tips


Protect Your PC


Updates and Patches
update your computer

Glossary

802.11x—is the industry standard specification for wireless design.

Adware—is a separate program that is installed at the same time as shareware. It’s purpose is to generate pop-ups and advertising.

Attack (or Exploit)—an action taken to harm a computer or data. This refers to an intentional threat rather than an accidental one.

Attachment—is a file that accompanies an e-mail and it can be a risk because it might contain malicious code.

Attacker—in the context of computing, an attacker is someone tries to breach security in order to cause damage to a system or to steal assets.

Asset—is a valued resource (usually money) but it could also be data.

Authentication—is the process of verifying that someone is, who he or she claims to be. For most online systems, authentication is based on a user ID and password.

Buddy List—also called a contact list, it allows a user to monitor the presence of their friends online. It can also be configured to allow only those whom you know to contact you.

Client—See server.

Communications Security—the protection of information against exposures and passive attacks during transmission.

Computer Security—the protection of files stored on computers against exposures and direct attacks.

Countermeasure—a safeguard that addresses a threat and reduces risk.

Cybercrime—is a broad term that refers to criminal activity (e.g., fraud, Identity theft, hacking, etc.) that is committed using the Internet.

Cyberstalking—according to Florida statute, (Florida State Statute 784.048 (d), to cyberstalk” means to engage in a course of conduct to communicate, or to cause to be communicated, words, images, or language by or through the use of electronic mail or electronic communication, directed at a specific person, causing substantial emotional distress to that person and serving no legitimate purpose.

Default—is a value or setting that a program or device automatically select if you do not specify a substitute setting. Computer default setting are often not secure for all applications (see “Due Diligence”).
**Denial of Service (DoS) / Distributed Denial of Service (DDoS)**—flooding a system to prevent it from servicing normal and legitimate requests; actions that prevent any part of a system from functioning due to excessive traffic.

**Downloading**—is the transmission of a file from one computer system (i.e., the remote/host machine) to another (the local machine/device). See Uploading.

**Due Diligence**—is the process of checking and verifying information. This refers to the research and homework a computer user must do to ensure that the settings on their computer and software give them the appropriate degree of security.

**Ethernet**—this is the cable that is used to connect the computers to the router, that is used to access the Internet using high-speed connections (e.g., cable and DSL). It is slightly thicker than a phone cord but transfers data at a much higher speed.

**File Extensions**—the file extension displays a file’s format as part of its name so that users can quickly understand the type of file it is without having to open it. Examples of file extensions are: MyHomework.doc, MyMusic.mp3, and MyBudget.xls

**File Transfer Protocol (FTP)**—allows users to connect to remote systems and transfer files back and forth. Anonymous FTP allows users who do not have an account on a computer to transfer files to and from a specific directory.

**Firewall**—is a combination of hardware and software, used to protect a network from unwelcome traffic. It also prevents unauthorized outgoing traffic.

**Flame War**—occurs when an online discussion (on a mailing list or in a chat room) degenerates into a series of personal attacks.

**Gnutella**—is an example of a decentralized P2P file sharing program. Examples of clients include: Limewire, and Bearshare.

**Hacker**—literally, the term “hacker” refers to an amateur or a programmer who lacks formal training. It has since become a pejorative term that refers to individuals who gain unauthorised access to computer systems for the purpose of stealing and corrupting data. Hackers, themselves, maintain that the proper term for such individuals is cracker, however for the purposes of this Manual, no distinction has been made. In the opinion of Secure Florida, any unauthorized access to a computer system is probably illegal.

**Handle**—in online communications, a handle is the name that users adopt in order to identify themselves. It can be a the person’s real name, a nickname or it can be completely fictitious name.

**Header**—in the context of an e-mail, a header refers to the addressing and routing information that is used to transmit an e-mail from its source to its destination.

**Identity Theft (ID Theft)**—occurs when an unauthorized party pretends to be you in order to get access to your personal information or your assets.
Instant Messaging (IM)—a type of text-based communication service that enables you to create a private chat room with another person on the Internet.

Intentional Threats—refers to deliberate harm against a computer, a person, or electronic information.

Internet Service Provider (ISP)—is a company or organization that access to the Internet. Before you can connect to the Internet you must first establish an account with an Internet Service provider. America Online is an example of an ISP.

Keylogger—is a program (hidden in spyware or Trojan horses) that secretly captures a user’s keystrokes and reports the information back to the program controller.

Local Area Network (LAN)—is a small network of interconnected computers in a home or business.

Malware (aka malicious software)—is any type of malicious software that is introduced into a computer to cause damage or steal information and/or act in an unexpected or undesirable manner. The term is a shortened form of "malicious software."

Metadata—the terms is translated as “data about data” and it refers to the attributes that been be used to identify an information bearing object (e.g., document, database, image, etc.).

Napster—is a centralized P2P file sharing company that was litigated out of existence as a free service.

Network—is a collection of two or more computers connected to share almost any kind of digital information.

Network Interface Card (NIC)—this device allows your computer to accept the information from your router when connected through an Ethernet cable.

Newbie—is a colloquial term used to describe someone who is new to the Internet.

Nickname—see Handle.

Nigerian Scam—also called an "Advanced Fee Scam" or a “419 Scam.” This is one of the oldest scams with all sorts of variants from e-mail, to snail mail, and even fax machines.

Payload—This refers to the malicious activity that a virus performs. Not all viruses have a harmful payload, but all of them have the potential for it.

Password—is a string of characters that a user must type to gain access to a file, program, computer, or computer system.
**Patch**—is a piece of code that is inserted into a program to fix a vulnerability or to increase the functionality of the product. Malware often attacks unpatched software.

**Phishing**—(pronounced “fishing”) is the act of sending a message to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft.

**Ping**—is a utility that is used to determine whether a specific IP Address is accessible.

**Predator**—an online predator is someone who uses the mechanisms of cyberspace to hunt human beings with the intent to exploit, rob, plunder and pillage their assets or their person.

**Router**—this device hooks multiple computers to one Internet connection by sending data between the Internet and the correct computer.

**Sandbox**—aka a “safe zone,” a sandbox is a protected, limited environment where applications (e.g. Java programs downloaded from the Internet) are allowed to “play” without risking damage to the rest of the system.

**Script**—is a type of computer code than can be directly executed by a program that understands the language that the script is written in (e.g., Javascript, Perl scripts, etc.).

**Security**—for the purpose of this Manual, security is loosely defined as the protection of the information and physical assets that are associated with a computer system.

**Server**—this term refers to a centralized computer that is located on a network and it purpose is to provide access to other computers in the network to programs, web pages, data, or other files and services, such as printer access or communications access.

**Service Set Identifier (SSID)**—the technical designation that is used for the name that you choose for your wireless network.

**Social Engineering**—refers to the controlling and shaping people’s attitudes and behavior by using knowledge of who they are and where they are from; term used among hackers for exploiting weaknesses in people, rather than software.

**Spam**—is unsolicited “junk” e-mail that is sent to large numbers of e-mail accounts.

**Spoofing**—is the act of assuming someone or some entity’s identity without permission.

**Spyware**—a general term for a program that secretly monitors your actions. Software companies have been known to use spyware to gather data about customers.
**Trojan Horse**—what appears to be (on first blush) a useful and and innocent program contains hidden code that allows the unauthorized collection, exploitation, falsification, or destruction of data.

**Uniform Resource Locator (URL)**—is the address of a file or Web page accessible on the Internet (e.g., http://www.secureflorida.org).

**Uploading**—is the transmission of a file from one computer system (i.e., the local machine/device) to another (the remote/host machine). See Downloading.

**Vectors**—are the routes or methods used by attackers/hackers to get into a computer, usually for illegal or malicious purposes.

**Virus**—is a program or piece of code that is loaded onto your computer without your knowledge and runs against your wishes.

**Vulnerability**—is a weak point that is “exploitable,” meaning it can be taken advantage of by a hacker/attacker.

**Warchalking**—is the popular practice of using chalk marks to show the location of wireless networks.

**Wardriving**—involves someone with a laptop computer equipped with a wireless network card who drives around the neighborhood looking for unsecured wireless networks.

**Warspamming**—by logging into an unprotected wireless network, spammers can send their messages to millions of names while remaining completely anonymous.

**Wireless Equivalent Privacy (WEP)**—WEP is used to promote confidentiality by preventing eavesdropping and modification through unauthorized access.

**Wireless Access Point (AP)**—is the base unit used in a wireless LAN and it provides access wireless devices to get connected to the Internet.

**Worm**—is a self-contained program that is able to spread copies of themselves to other computers.

**Zombie**—is a computer (usually belonging to a home user) that has been implanted with code that puts it under the control of a malicious hacker—done without the knowledge or permission of the user. Zombies are used by malicious hackers to mount DoS attacks.
Index

Anti-Virus (AV), 97-101, 329
AV Tools, 100-101
DURCH Tests, 99-100
Software, 97-99, 235, 304, 314-315
Attacks, 15-24
Active, 21
Anatomy, 23-24
Brute-force, 288, 290
Chat Rooms, 239
Definition, 17-18
Dictionary, 288-290
Direct, 20
Indirect, 20-21
Instant Messaging, 232
Passive, 21-22
References, 24-26
Auction Fraud, 4, 153, 177-187
Definition (Auction), 177-178
Offline, 179
Online, 179
References, 187-199
Reserve Price, 178
Safe Bidding, 185-187
Types, 179-183
Victims, 184-185
Backups, 317-320, 330
Forms Test, 321-322
Principles, 319-320
References, 332-335
Storing Asssets, 321
Best Practices, 329-331
Blended Threats, 4, 142-146, 232. 235
Combo-Malware, 142, 146
Definition, 142
Precautions, 145-146
Recent Trends, 142-143
References, 147-148
Sobig, 143, 145
Worse-Case Scenario, 145
Chat Rooms, 237-247
Chat Room, 237
CHAT Test, 247
Definition, 237-238
Internet Relay Chat (IRC), 232, 237-240
Moderated/Unmoderated, 241
Online Predators, 242-243
Profile, 238-239
References, 247-248
Safe Chatting, 245-246
 Stranger Danger, 241, 243
Warning Signs, 243-245
Critical Success Factors, 12-13
Prevention, 12
Detection, 13
Response, 13
Curl, 37, 38
Cyber-security, 2-3,
Cybercrime, 2, 4, 6, 150, 153
Cyberstalking, 243, 249-257
Anti-Cyberstalking, 255-257
Definition, 249
Harassment, 252-253
Motivation, 253-254
Offline, 250
Online, 250-252
References, 257-258
Stalkers, 253-254
Victims, 255
Denial of Service, 4, 40-44, 123, 124, 234
Agent, 41-42
Client, 41
Definition, 40-41
Distributed, 40-44
Handler, 41
Implications, 43
References, 45
Zombies, 43-44, 124
Downloading, 268, 324
E-mail, 4, 45-54, 304, 331
Address, 45
At Work, 53
Attachments, 49-51
Bogus, 209-210
Definition, 46
KRESV Test, 54
Liability, 52-53
Precautions, 51-52
References, 55-56
Suspicious, 47
Firewalls, 302-311, 329
Access Control List, 306-307
Florida Cyber-Security Manual • Index • www.secureflorida.org
Definition, 302-303
DMZ, 302
Limitations, 309
Packet-Filtering, 306-307
PLAT Test, 310
Proxy Servers, 307-308
Rules, 306
Stateful Packet Inspection, 308-309
Types, 303-304
Fraud, 150, 152-153
See Auction
Harmful Content, 273-282
  Definition, 273
  Errors, 281
  Expert Control, 281
  Filtering, 277-280
  Filters, 276, 330
  Illegal Content, 274-275
  Keyword Blocking, 277
  Labeling, 277
  Offensive Content, 273-274
  Overblocking, 281
  PICS, 278-279
  References, 282-283
  Self-Rating, 279
  Site Blocking, 277
  Subjectivity, 281
  Stoplist, 278
  Third-Party Labeling, 279
  Underblocking, 280-281
Header(s), 4, 47
  Decoding, 81-84
  E-mail Protocols, 79-81
  Viewing, 77-78
Hidden Costs, 212-213
Hoaxes, 4, 203, 207-208
  Chain Letters, 204
  Definition, 203-204
  References, 214-216
  Identity Theft, 4, 159-160, 163, 190-199, 243, 275
  Credit Agencies, 194-197
  Definition, 190-191
  Florida, 197, 198
  Fraud Alert, 196
  Looting, 191-192
  Personal Information, 191
  Pretexting, 192, 196
  Preventative Measures, 197-199
  References, 200-202
  Remedies, 194
  Victimization, 193
Instant Messaging (IM), 230-235, 304
  Buddy, 230
  Buddy List, 231
  Definition, 230-231
  IM Services, 232
  Presence Awareness, 230, 231
Internet, 28
  Addresses, 31-32
  Backbone, 31
  Internet Cons 150-153
    Definition, 150
    References, 153-154
Legends
  see Urban Legends
Maintenance, 313-331
  Definition, 313
  Hard Drive Disposal, 316-317
  References, 332-335
  Tasks, 313-315
Malware, 4, 88-89, 116, 232, 263, 304, 318
  Definition, 88
  Enter, 88
  Escalate, 89
  Execute, 89
  Extend, 89
  References, 90-91
  Trends, 144
Networks, 4, 28-38
  Components, 30
  Criteria, 29
  Definition, 28-29
  Local Area Networks, 28
  References, 39
  Secure Socket Layer, 33-34
  Tools, 34-37
  Toolkit, 37-38
  Virtual Private Networks, 28-29
  Wide Area Networks, 28
Nigerian Scam, 4, 155-158
  Definition, 155, 157
  Gist, 157
  References, 158
Nslookup, 35-36, 38
Obfuscated URL Decoder, 37, 38
Objectives, 1
P2P File Sharing, 125, 259-267, 304
  Client/Server, 259
  Computer Check, 265
  Definition, 259
  Exemplars, 260-263
  Gnutella, 262-263
  Legal Implications, 267
LOCATE Test, 268-269
Napster, 261
Napster Clones, 261-262
References, 270-272
Sued, 265-267
Passwords, 159, 285-299, 315, 330
Cracking, 287-288
Definition, 285
Managing, 297-298
Rules, 290-292
Screen-Savers, 298-299, 330
Strong, 292-296
Patches, 235, 323, 330
Attack-and-Patch Cycle, 323-325
BUT Test, 326
Patch Management, 325
References, 332-335
Payload, 19, 233
Trigger, 20
Trojans Horses, 123
Viruses, 93, 94
Worms, 106, 110-112
Phishing, 4, 152, 159-174, 234
Attacks, 162-163
Business Countermeasures, 172-174
Definition, 159-160
How Phishing Works, 160-162
Link Alteration, 161
Prevention Measures, 164-165, 170-172
References, 174-176
Rogue Servers, 169
Source Code, 168-169
URLs, 167-168
Victims, 163-164
Ping, 34, 38
Policies, 327-329, 331
Pornography, 264
Ports, 304-305
Rumors, 4, 203, 206-207
Definition, 203-204
References, 214-216
Scams,
Scam Artists, 152
Security, 2-3, 6-8, 13, 15, 209, 315, 331
Authentication, 9, 10
Critical Success Factors, 12-13
Definition, 2-3
Due Diligence, 310
Elements, 7-8
E-mail, 46-47
Firewalls, 309
Passwords, 286-287
Verification, 9
Wireless, 222-224
References, 14-16
Social Engineering, 70-71, 116, 159, 239, 296
Spam, 4, 56-62, 159-160, 162
Components, 58-60
Definition, 57-58
Spammers, 57-58
Tips, 61-62
References, 63-66
Unsolicited Commercial E-mail, 56-57
Spoofing, 4, 67-84
Cloaking Techniques, 73-77
Definition, 67
E-mail, 47, 69, 72-73
IP, 67-66
Joe Job, 69-70
References, 84-86
Types, 67-69
Webpages, 71-72
Website, 47, 68, 159-161, 167
Spyware, 4, 131-139, 275
Anti-Spyware Tools, 136
Definition, 131-132
Detecton and Removal, 134-135
Earmarks, 132-133
Ethical Conduct, 133
Prevention, 137-139
Programs, 133
References, 139-141
Removal Tips, 136-137
Telnet, 36, 38
Threats, 9
Accidental, 11-12
Cyberstalking, 252-253
E-mail, 48
Instant Messaging, 232
Intentional, 12
Traceroute / Tracert, 34-35, 36
Trojan Horses 4, 88, 122-128, 142, 232, 275
Anti-Trojan, 127
Definition, 122-123
Hijacker, 122-123
How Trojans Get In, 125
How Trojans Work, 124
Logic Bomb, 122
Online Scanning Tests, 127
References, 129
Remote Administrative Tools, 122
Uber-Trojans, 123
Underware, 116-121, 264
Adware, 117-118, 132, 135
Browser Helper Objects, 118
Cookies, 119
Definition, 116-121
Drive-by Downloads, 119
Fake Dates, 120
Gimmicks, 120-121
Misrepresentation, 117
References, 121
Web Bug, 119
Uploading, 268
Urban Legends, 203,
  Chain Letters, 204, 205-206, 210
  Definition, 203-204
  References, 214-216
Vector, 19, 49, 116, 123, 125, 142-143, 152, 159, 204, 243
  Counter-Measures, 102-103
  Damage, 95-96
  Definition, 92-93
  Hiding Strategies, 96
  Information Centers, 96-97
  References, 103-105
  Spread, 95
  Types, 93-94
Vulnerabilities, 9, 11
  E-mail, 48
  Passwords, 287-288
Whois, 36, 38
Wireless, 218-228
  801.11, 218, 220
  Ad Hoc, 218-219
  Definition, 218
  Attacks, 224-225
  Infrastructure, 218-219
  References, 228-229
  Wireless LANS (WLANS), 218, 226-228
  Wireless Set Up, 220-222
Worms, 4, 88, 106-114, 123, 143, 211, 232
  Definition, 106
  Disruption, 107
  How Worms Work, 110
  Preventing Attacks, 112-113
  References, 114-115
  Sample Worms, 109-110