



Internet Security: Browsing Safely & Securely

George A. Thompson
T3 Technologies



No Safety In These Numbers

- ◆ 10 million people have fallen prey to identity theft in the past 5 years. Over 50% of email is SPAM
- ◆ Phishing growing by about 50% monthly
- ◆ Fourfold increase in new Windows viruses in first half of 2004 compared with 2003



The Internet is Not Secure

Safest Options

- ◆ The Best
 - Turn off Your Computer
 - Buy a Macintosh





Safest Options

◆ Good

- Email Filters
- AntiSpam Software
- Antivirus Software

◆ Better

- Ad/Spyware Blockers
- Alternative Browsers
- Firewalls
 - Hardware
 - Software



Practice Safe Browsing

- ◆ Proceed with caution when
 - downloading files
 - “Viewers” and “helpers”
 - purchasing goods and services
 - `https://`
- ◆ Read the fine print
 - About this Site
 - Security and privacy policies



Spyware & Adware

- ◆ Attempts to steal your private information
- ◆ Records your online behavior and transmits it to others
- ◆ Turns your PC into advertising machine.
- ◆ Identity Theft
 - Worst Case



Common Forms of Ad/Spyware

◆ Browser Hijackers

- replaces browser home page with one of their own

◆ Search Hijackers

- intercept legitimate search requests and return phony results

◆ Pop-up Generators

- Produces a plethora of ads

◆ Key Loggers

- records keystrokes,
- sends information back
- used or sold to blast you with ads or spam, or to conduct identity theft.



Spy/Adware Solutions

- ◆ Ad-Aware SE Personal
 - www.lavasoftusa.com
- ◆ Spybot Search & Destroy
 - www.download.com (type in spybot)
- ◆ Spy Sweeper (\$)
 - www.webroot.com.
- ◆ Microsoft AntiSpyware
 - www.microsoft.com/spyware (Windows XP)



Gone Phishing

- ◆ E mails claim to be from legitimate businesses, such as banks and credit card companies, direct recipients to a replica of the actual company's Web site.
- ◆ Once they arrive at the site, victims are asked to 'update' their personal financial information, such as passwords, account numbers and Social Security numbers.
- ◆ The information is then used to steal the person's identity, along with their money, and defraud businesses.



From Phishing to Pharming

- ◆ Uses sophisticated worms and viruses attached to Web browsers to redirect users to spoofed Websites when they try to access valid sites.
- ◆ Once they arrive at the site, victims are asked to “update” their personal financial information, such as passwords, account numbers and Social Security numbers.



Don't Get Reeled In

- ◆ Antiphishing Tools
 - CoreStreet SpoofStick
 - EarthLink ScamBlocker
 - GeoTrust TrustWatch
 - WebRoot Phish Net



Secure Website

- ◆ Uses Secure Socket Layer (SSL) protocol
 - Encrypts the data before sending over ‘Net
 - https:// = secure site
 - Padlock Icon



Cookies

- ◆ A text-only string that gets entered into the memory of your browser.
- ◆ Not inherently dangerous
- ◆ The good
 - Stores some personal information
 - customizes experience
- ◆ The bad
 - Stores some personal information
 - can possibly invade your privacy/security



Privacy Policy Example

Cookies & Web Beacons

To enhance your experience with our sites, many of our web pages use "cookies." Cookies are text files we place in your computer's browser to store your preferences. Cookies, by themselves, do not tell us your e-mail address or other personally identifiable information unless you choose to provide this information to us by, for example, registering at one of our sites. However, once you choose to furnish the site with personally identifiable information, this information may be linked to the data stored in the cookie.

We use cookies to understand site usage and to improve the content and offerings on our sites. For example, we may use cookies to personalize your experience at our web pages (e.g., to recognize you by name when you return to our site), save your password in password-protected areas, and enable you to use shopping carts on our sites. We also may use cookies to offer you products, programs, or services.

"Web beacons" or clear .gifs are small pieces of code placed on a web page to monitor the behavior and collect data about the visitors viewing a web page. For example, web beacons can be used to count the users who visit a web page or to deliver a cookie to the browser of a visitor viewing that page. We may use web beacons on this site from time to time for this and other purposes.



Cookie Management 101

- In IE 6.0, go to the

Tools/Internet Options/Privacy menu.

This menu allows you to select how discriminating the browser will be when accepting cookies, based on two factors:

- (1) the source of the cookie, and
- (2) whether the source has a "privacy policy."

<http://www.cookiecentral.com>

<http://support.microsoft.com/default.aspx?scid=kb;EN-US;q283185>



Before Using MS Internet Explorer

1. Open up a session of Internet Explorer.
2. Click **Tools** —> **Internet Options** —>.
3. Click the **Security** tab.
4. Click the **Internet** icon —> Click the **Custom Level...** button.
5. Choose **Medium** from the drop down menu at the bottom —> click the **Reset** button.
6. Click **Yes**, if prompted. Then click **OK**.
7. Click **Custom Level** again.

At this point you will see several headings. Set the following options as indicated in parenthesis

Under the .NET Framework-reliant components heading

- Run components not signed with Authenticode (Disable)
- Run components signed with Authenticode (Prompt)

Under the ActiveX controls and plug-ins heading

- Download signed ActiveX controls (Prompt)
- Download unsigned ActiveX controls (Disable)
- Initialize and script ActiveX controls not marked as safe (Disable)
- Run ActiveX controls and plug-ins (Enable)
- Script ActiveX controls marked safe for scripting (Prompt)

Under the Miscellaneous heading

- Access data sources across domains (Disable)
- Drag and drop or copy and paste files (Prompt)
- Installation of desktop items (Prompt)
- Launching programs and files in an IFRAME (Prompt)
- Navigate sub-frames across different domains (Prompt)
- Software channel permissions (High safety)
- Userdata persistence (Disable)

Under the Scripting heading

- Allow paste operations via script (prompt)
- Scripting of Java applets (Prompt)

After you set these options, keep clicking **OK** until you are back to the normal view of Internet Explorer.



Alternative Browsers

- ◆ Better security and privacy than IE
- ◆ Better pop-up blocker
 - Netscape Navigator
 - Opera Opera
 - Mozilla Firefox



Firewalls

◆ Broadband Routers

- Belkin
- Linksys
- D-Link

◆ Software Apps

- Internet Firewall
 - Windows XP
- Zone Alarm
 - Zone Labs
- Micro-cillin
 - Trend Micro



Email

◆ SPAM

- *Unsolicited commercial e-mail.*
- *Firewalls, antivirus, or antispyware programs DO NOT STOP IT.*
- *Obtain and install an antispam program, or turn on the antispam feature in your e-mail program, or do both.*



Spam-Proofing Your InBox

- ◆ Use An Email Filter
 - Permission-based: block messages from anyone who isn't on you're A-list
 - Challenge-response: blocks email from an unknown source unless the sender of the email replies to a special message correctly
- ◆ SpamNet (Outlook)
 - Cloudmark
- ◆ SpamCatcher
 - Aladdin Systems
- ◆ McAffe SpamKiller
 - Network Associates
- ◆ PC-cillin
 - Trend Micro



7 Steps to Highly Effective Emails

1. Look for "calls to action" in an email.
Most phishing scams include prompts to do something immediately or the user will suffer a financial loss. Phishers want the person to react without thinking.
2. Always access financial and other Websites by typing in the Web address the organization provided you with, or via a bookmarked URL.
3. If you are unsure about the legitimacy of an email, call the organization or company that sent it to verify. Check the company's Website for disclaimers against sending out such emails.
4. Never click on a link supplied in an email that supposedly comes from any company or organization.
5. Make sure you have anti-spyware software on your PC and keep it updated.
6. Never respond to an unsolicited email.
7. Always think twice before opening any email. Think about where it is coming from, who sent it and why they sent it.



Virus Blocking

- ◆ Removes infections inadvertently released via email or file downloading
- ◆ 100,000 viruses
 - www.wildlist.org
- ◆ Internet Security
 - Trend Micro
- ◆ Norton Internet Security
 - Symantec
- ◆ McAfee Internet Security
 - Network Associates



Instant Messaging

- ◆ Real-time communication
 - teenage chat
 - business can also use effectively
- ◆ Send & Receive files
- ◆ Share folders
- ◆ Instant Messaging Clients
 - AOL Instant Messenger
 - Yahoo Messenger
 - MSN Messenger
 - Windows Messenger (XP)
 - ICQ



Instant Messaging

- ◆ Keep a low “profile
- ◆ Encryption
 - Digital signatures via digital certificates (Verisign)
- ◆ IMSecure
 - Zone Labs utility



Layers of Internet/Web Security Summary

		Prevents or Blocks
Firewall	Hardware	unsolicited incoming communications (masks ports/IP address)
	Software	Backdoor apps, Trojan horses, from sending FROM a PC Protects laptops on networks
AntiSpam	Software	email scams (phishing) Reduces email sorting
AntiVirus	Software	Worms, viruses, Trojan horses
AntiSpy	Software	Adware, spyware, cookies, malware



- ◆ **System Sector Viruses:** These infect control information on the disk itself.
- File Viruses:** These infect program (COM and EXE) files.
- Macro Viruses:** These infect files you might think of as data files. But, because they contain macro programs they can be infected.
- Companion Viruses:** A special type that adds files that run first to your disk.
- Cluster Viruses:** A special type that infects through the disk directory.
- Batch File Viruses:** These use text batch files to infect.
- Source Code Viruses:** These add code to actual



Virus

* appends itself to a file or program and then spreads itself from computer to computer.

Worms

A worm is similar to a virus. They replicate themselves like viruses, but do not alter files like viruses do. The main difference is that worms reside in memory and usually remain unnoticed until the rate of replication reduces system resources to the point that it becomes noticeable.

Trojans

A firewall is a protective barrier that prevents



www.fdic.gov

- ◆ www.securityfocus.com — information on freeware and inexpensive applications.
- ◆ The wild list



<http://www.firewallguide.com/newsletter.htm>