CYBERSECURITY: AWARENESS, PREVENTION, ACTION

Therese DonGiovanni. O'Neil
Indiana University of Pennsylvania

With the onset of Information Technology, your personal data has never been more vulnerable to electronic prying eyes than it is today. Anyone with a little patience, a few dollars, and a little time can find out where you shop, what files you download, the things you buy, and a lot more. This article delves into the insecurity of the Internet in terms of who is watching you and what information is being gathered about you without your knowledge. Topics covered are identity theft, cookie files, web bugs, Trojan horses, Internet spying, and much more. It begins with a general awareness of how your privacy is being invaded. Prevention measures are discussed on how to be more secure while web surfing. Finally, the actions taken by the government and universities to work toward Information Assurance are listed.

AWARENESS

Networks

The continued use of networks has increased the amount of security leaks. Information transmitted over a network has a higher degree of security risk than information kept on a stationary personal computer (PC).

Information Privacy

As more dotcoms go bankrupt, databases of consumer information become a 'hot' commodity for companies like Amazon.com. Although many companies have privacy policies, not many will agree to *not* sell your information to another site if their company becomes defunct.

Many companies are tracking your moves on the Internet. We need to be careful when filling out simple magazine subscriptions, a Department of Motor Vehicle (DMV) form, or a product warranty registration card. When completing these forms, one should not give out unnecessary information for the transaction. There would be no need, for example, to supply your social security number to complete a contest entry form. Once your social security number is obtained, a person can find out almost anything about you. One such site, http://www.docusearch.com, allows you, for a fee, to search such things as 20 of your closest neighbors, your insurance information from the DMV or searching for birth dates. Even the television market has gotten involved, collecting information from the newest technology in TV, TiVo.

Privacy Invaders

The three most common privacy invaders are *Cookies, Web Bugs* and *Trojan Horses*.

Cookies

Cookies are the most commonly known privacy invader.. Web sites begin to store cookie files (up to 4K) on your PC when you first visit so they will recognize you, along with your web browsing preferences and maybe your buying history, when you return. Sometimes cookies can be quite helpful if you are shopping online. Some third-party companies like DoubleClick Inc, use cookies to track your online travels without telling you. Taking cookies one step further is the use of bits of code being implanted into e-mail messages. The cookie is planted on the hard drive at various stages in the process of delivering and reading an e-mail message. In some instances, the cookie is set whenever the e-mail message is opened. This is a marketing tool used to detect whether the consumer visits the site days later. These cookies can also determine how much revenue was generated on a web site as a result of an e-mail campaign by following the recipient throughout a visit.

Web Bugs

Cookies are not the only devices that are worrying the Net user. Today, many companies use *Web Bugs* (sometimes called Web Beacons) to track your movements online. Also known as clear GIFs, *Web bugs* are tiny, (about 1 pixel in size) invisible graphic images that Internet marketers and advertisers implant on their web pages to track which pages are being viewed and by whom.

Web Bugs are placed on web pages by third parties interested in collecting data about visitors to those pages. Once the data is gathered, a personal profile can be created. This profile will determine what banner ad one will be shown on the next visit to that site. They collect information such as Internet Protocol (IP) addresses of the computer that fetched the *Web Bug*, the Uniform Resource Locater (URL) of the page on which the Web Bug is located, and the URL of the *Web Bug* image. Also viewed is the time the *Web Bug* was viewed, the type of browser used, any previously set cookie, and the *Web Bug* image. Undetected bits of code can also be planted in e-mail messages, mostly by spammers who send lots of mail simply to verify that e-mail addresses in their possession are valid. Once you view or open a piece of booby-trapped e-mail, a hidden receipt immediately wings its way back to the senders.

Not all *Web Bugs* are malicious, however. Some web sites use *Web Bugs* simply to monitor site traffic without identifying individual users or IP addresses. Some sites just want to count the number of times a particular site is viewed, or count the number of times a banner ad has appeared; or to simply measure the effectiveness of the banner.

Exterminating Web Bugs

There are various ways to exterminate these *bugs*. Since they are graphic files, you can disable image loading in your browser. This option is not popular as you will not see any images on the web site. Software can be purchased that will block your IP address by loading the web page first to their servers and then to your computer. That method, however, slows down your computer. You can also use 'Bugnosis', a *Web Bug* Detector. As you surf the web, it analyzes every page you visit and alerts you when it finds any web bugs. It

places a Bugnosis icon on your toolbar. Clicking this button either shows or hides the "analysis window" at the bottom of the screen. This window is where Bugnosis will tell you about Web bugs that it finds. It also makes visible the W*eb bugs* hidden on the page, so you can see their placement within the page. Bugnosis can be downloaded at http://www.bugnosis.org. Some common Web bug 'plants' are: http://www.pcworld.com, http://www.computerworld.com, both containing several bugs from DoubleClick.net, and http://www.cnn.com, has bugs hidden in highlighted images.

Trojan Horses

These files will hide inside your computer. They are designed to look like legitimate programs. *Trojans* allow access into your computer system by anyone who knows how to activate the Trojan. Once inside your computer, they can monitor, from their computer screen, your every move as you use your computer. A hacker who activates a Trojan in your system, turns their computer monitor into a 'picture/picture' screen, with your desktop picture in the corner of their screen. As you move, they see what you are doing, where you are going, what you are typing. For example, if you enter your bank's web site, type in your username and password, the intruder can keep a record of your keystrokes. Even though your password is changed to asterisks as you type, the intruder can check the cache log of keystrokes and obtain your password along with your bank account information. Some hackers just sift through your files, or they can disable virus-checking software. For the latest Trojan horses, consult http://www.antivirus.com/vinfo.

Trojan Horse files are easily available to hackers from the Internet. They can be downloaded from web sites, chat rooms, or bulletin boards.

Most Trojans will enter a computer via email attachments. Consequently, do not download attachments without a proper virus protection program monitoring the files as they enter your computer. Be especially wary of files with the extension .vbs, .exe. These two most common file types will carry viruses. A hacker who has gained access to your computer while you were online may plant a Trojan. This provides the portal through which another hacker can enter your system. Securing a proper firewall product will prevent intruders from entering into your system. Another way a Trojan may enter your machine would be downloading files from the Internet. Watch out for music sites that allow you to download MP3 files 'for free'. Very often, those files may be laced with a Trojan horse.

Wireless Technology Sparks Privacy Concerns

With consumers purchasing more and more cell phones, privacy concerns have escalated because of the GPS (Global Positioning Systems) units used in all cell phones starting in October, 2002.

Spyware

Another growing concern to our privacy is the use of Spyware, or Ad-Ware. These are programs that track your surfing activity, without your knowledge, sending the information, again without the user's knowledge, to a server designated by the developer of the Spyware

software. This allows for detailed user-profiles to be collected. They are not watching 'you' per say, they are watching and recording your mouseclicks.

The Nine Greatest Threats to your Privacy

1) Identify Theft

Identify Theft is one of the fastest growing crimes in America and has become a national crisis, according to the Social Security Administration. On the average, stolen identity is not discovered for 14 months. Avoiding identity theft can be as simple as being aware of what you carry in your wallet or purse. Identity thieves have various ways to steal your identity. They steal your credit card numbers by looking through your trash. Then they complete a 'change of address' form and the next bill goes to them, not to you. They steal wallets or purses. Someone may call on the telephone and say they work for your bank and they are updating their records, and then ask for your social security number, your checking account number, and so forth. To circumvent identity theft, only carry the information with you that you absolutely need for day-to-day dealings. Another good practice is to keep an eye on your mail; know your payment cycles on your credit cards. Ask 'why' people need to know your personal information. Never give personal information to people who contact you out of the blue and remember; no Internet Service Provider (ISP) or bank will ask you to send credit card information in an open email or on the telephone.

For more information on Identify Theft, consult the Identify Theft Resource Center (ITRC). The ITRC helps people prevent and recover from Identify Theft. They can be reached at PO Box 26833, San Diego CA 92196
San Diego, California
858-693-7935
http://www.idtheftcenter.org

2) Websites Do Look Back at You

Companies like DoubleClick sell cookies to third parties. DoubleClick is an ad network company that matches up its cookies with data from off-line marketing companies, thereby creating profiles of individuals and their web-surfing habits. They are currently involved in state and federal class action lawsuits from California, Texas and New York for privacy invasion on the Internet. At the writing of this paper, there has been a preliminary settlement set to be finalized May 21, 2002. Under the settlement DoubleClick has agreed to give consumers clear notice and choice of any data collecting practices stated within their privacy policy. In addition, DoubleClick must obtain permission from consumers before they can combine any personally identifiable data with their Web surfing history.

3) Theft of Personal Data from Websites you have visited

A few years ago, Amazon.com had approximately 100,000 customer databases stolen. These files contained customer's names, addresses and credit-card numbers. Amazon paid for their return.

4) Fake Websites

Trojan horses exists that appear like a legitimate website, but actually are traps that capture your username and password as you enter the site.

5) Government giving out your Information online

Many counties in the US have online information of homeowners in that county. Through property tax information online, anyone can find your home and your address.

6) Data Brokers

Data brokers are those that buy personal information and sell it. They sell this information to clearinghouse companies. Such companies buy and sell personal information.

7) Internet Spying

"Two-thirds of major American firms now do some type of in-house electronic surveillance" Your employer has every right to track your every move on the Internet from your desktop in your office. Companies even purchase software, called 'snoopware', to monitor desktop activity. Workplace surveillance leads the list of the Top 10 Privacy stories of the year 2000, according to the Privacy Foundation analysis.

Workplace Surveillance leads the list of the Top 10 Privacy stories of the year 2000, according to a Privacy Foundation analysis. Spectorsoft sells Internet Monitoring software that is used by businesses and homes. Many home users are using the product to track the surf habits of their children, or their spouse.

Project Echelon is used by the Government to scan all Internet traffic, cell phone conversations, faxes and long-distance telephone calls. Biometrics is another technique used to scan for potential security risks. Biometrics technology scans the faces of individuals, matching their faces with a database of criminals. An October 2001 Harris poll found 86 percent of respondents favor using facial recognition technology to scan for terrorists, in the wake of the September 11 attacks. But this technique has its privacy concerns.

8) A stranger may be using your computer to spy on you

Hackers can enter your computer while you are online, without your knowledge. A Trojan is set in your computer. This allows the next hacker to sift through your computer.

One of the latest techniques for gathering data about your surfing habits is the 'Mouseover Downloads'. If your browser is set to a low security level, advertisers can send files directly to your hard drive merely by you rolling your mouse pointer across an advertisement. Some of these downloads may contain a virus when downloaded. Freeware and shareware downloads may include more than you bargained for. Two companies, 'Gator' sold ads last year that appeared over the top of ads that already existed on major sites such as Yahoo. 'Bonzi' creates a directory on your hard drive and downloads the company's marketing mascot, a purple gorilla, which pitches to you whether you are online or off.

9) You may have a Cyberstalker

Stalkers meet their victims mainly via e-mail chat groups, newsgroups and instant messaging. Stalkers use the name of others and post personal ads, usually sexual in nature.

PREVENTION

As a famous Pennsylvania Statesman once said: "An ounce of prevention is worth a pound of cure". Benjamin Franklin was not talking about computers, of course, yet his words ring true today.

Secure your Web Browser

The first place to begin securing your computer is the web browser. Always download the latest version of a web browser. This will insure that the latest virus-protection code is protecting you while you browse a web site. Whether in Netscape or Internet Explorer, look for the secure label (a lock) on the status bar of the page. The lock will appear unlatched, or closed. When closed, the data you enter will be encrypted to its destination.

Use a Firewall

Another act of prevention is to download a firewall. –A firewall watches traffic coming into your PC and blocks suspicious activity. Go to http://www.symantec.com/securitycheck. This site has an online scanner that lets you test the security of your Internet connection. Another site used to test the vulnerability of your computer is http://www.grc.com. This site lets you take a 'Leaktest'. This site will purposely try to penetrate your computer. If your firewall is working, access will be denied. If you have no firewall, or your firewall is not working properly, the Leaktest will penetrate your computer indicating that your computer is vulnerable to a hacker attack. To download a free firewall, go to http://www.zonelabs.com. ZoneAlarm is the name of the product.

Beyond Firewalls

Use an Anonymizer. An anonymizer acts as a shield between you and all of the most prevalent online privacy/security threats. Among the tasks of the anonymizer is rewriting the web pages you want to view on protected servers. It will also remove privacy and security threats from web pages before serving them to you. In addition, it will hide your computer's unique IP address from web sites and other outside parties, preventing them from seeing you. It will also prevent outside parties from putting malicious files or codes on your hard drive. It will neutralize cookies, Java, JavaScript, ActiveX, Web Bugs and other threats.

Buy an Antivirus Software Package

In addition to buying an antivirus protection software package, you should update the virus signature weekly. There are approximately 73,000 known viruses. If you are going to get a virus, chances are it will be one of the most current ones. Some popular antivirus companies include Symantec, (Norton Antivirus), Network Associates (McAfee) and Trend Micro, (PC-Cillin). For a complete list of Antivirus vendors, visit http://antivirus.about.com/cs/antivirusvendors/index.htm

Look for the Seal of Approval

Secure sites will have a seal displayed on the web page. This is similar to the "Goodhousing Seal of Approval" for products. When you see a seal, you know the site is secure. Some common seals are from the Better Business Bureau, or Verisign.

ACTION

Government

The government is taking action in the field of Internet Security. In 1991, the Department of Justice established a Computer Crime Unit. It is called the Computer Crime and Intellectual Property Section of the Department of Justice, the CCIPS. This department is in charge of combating computer crime and intellectual property, including copyright and trademark crimes. It also develops enforcement policies, trains agents and prosecutors, promotes international cooperation, proposes and comments on federal legislation.

In October of 2001 the "USA Patriot Act' was passed by federal legislation. This Act gives investigators more tools for apprehending terrorists. Investigators can now use more powerful tools to monitor phone calls, e-mail messages, and even Web surfing. The changes also mean we now have even less guarantee of privacy on the Net.

Universities

Universities are also taking action toward the problem of securing the Internet. Carnegie Mellon University is a center of Internet security. Their program is called CERT: Computer Emergency Response Team. They study Internet security vulnerabilities, handle computer security incidents, publish security alerts, research long-term changes in networked systems, and develop information and training to help you improve security at your site. They can be found at http://www.cert.org.

Indiana University of Pennsylvania has an Information Assurance program. This program represents a major initiative to increase the number of skilled security professionals able and willing to protect the U.S. information infrastructure from attacks from both insiders and terrorists. As of March 5, 2002, Indiana University of Pennsylvania has been designated a Center of Academic Excellence in Information Assurance Education, a designation awarded by the National Security Agency of the United States. Coordinating these efforts are Indiana University faculty members Dr. Mary Micco and Dr. William Oblitey, of the Computer Science Department, and Dr. Dennis Giever, of the Criminology Department. For more information on this program, go to http://www.iup.edu/infosecurity. In summary, the security of the Internet depends upon your awareness of the problems you may encounter; knowing what preventative steps you can take to protect yourself, and knowledge of the plan of action that is already been implemented toward Information Assurance.

REFERENCES

Bass, S, (2001, February 12) Your Second Line of PC Defense, p 61.,*znet reviews.*

Brandt, Andrew, , (2002, September) Klez: The Virus that Won't Die *PC World Magazine, p* 32.

Cohen, Adam, (2001, July 2), Internet Insecurity, *Time Magazine.* "©2001 Time Inc. Reprinted by permission"

Grimes, B, (2001, May) Privacy Matters, Fumbling the Data, Future Threat, the No-Privacy Workplace, Taking Back Your Data, *PC World Magazine.*

Kandra, Anne, (2002, October) Consumer Watch: Don't Let Them Steal Your Good Name, *PC World Magazine.*

Kaiser, Fisther, Laura, (2002, March), 20 Net Scams, *Yahoo Internet Life.*

McKean, K, (Ed.), (2002, January) Changing Views of Online Surveillance, *PCWorld Magazine*, p 15.

Olsen, S., (2002, April 4) Is your e-mail watching you?, *CNET news.com*.

Olsen, S., (2002, March 29), DoubleClick nearing privacy settlements, *CNET news.com*.

Roy, Saumya, Medill News Service, (2002, January 25), Biometrics: Security Boon or Busting Privacy?, *PC World Magazine*

Spanbauer, Scott, (2002, February), Browsing & Beyond, *PC World Magazine*, p 83.

Spring, Tom, (2002, September), Web Ad Explosion, *PC World Magazine,* p 24.

Sweeney, Mark, (2002, January 29), CookieCop 2.2, Download It Here, *PC World Magazine.*

Zetter, Kim, (2001, November), PC Security: Holey Software!, *PC World Magazine.*

WEB SITES REFERENCED

(In order of appearance in the presentation)

http://www.docusearch.com
http://www.cookiecentral.com
http://www.privacy.net
http://www.antivirus.com/vinfo
http://www.tom-cat.com/spybase/spylist.html
http://virgolamobile.50megs.com/spyware/spyware.htm
http://stolen-identity.com
http://www.consumer.gov/idtheft/
http://www.idtheftcenter.org
http://www.privacyfoundation.org
http://www.spectorsoft.com
http://www.ZoneAlarm.com
http://www.ZoneAlarm.com
http://www.symantec.com/securitycheck
http://www.grc.com
http://www.anonymizer.com
http://housecall.antivirus.com
http://antivirus.about.com/cs/antivirusvendors/index.htm
http://www.bugnosis.org
http://www.simplysup.com
http://www.bbbonline.org
http://www.truste.org
http://www.webassured.com
http://www.pwcbetterweb.com
http://www.privacybot.com
http://www.verisign.com
http://www.usdoj.gov/criminal/cybercrime/searchmanual.htm
http://www.cert.org/
http://www.nsa.gov
http://www.iup.edu/infosecurity