Spyware: Friend or Foe?

Spyware is a software program installed on your personal computer (most of the time without your knowledge and/or permission) that collects information on your computing habits, Internet use, and other software use information. At a predetermined time, the software connects back to a server and reports your activity. Spyware maybe as innocent as tracking your Web activity to capturing key strokes for criminal activities (ex. ID Theft).

People are often lured into voluntarily installing the software as a Web procurement monitoring utility. For instance, Gator, a popular spyware program, monitors your Web surfing and tells you when someone else has the same item or competing item available for less money. Many people use Gator as a convenient utility for populating online information forms and saving passwords. While the online bargain locator and information completion feature is attractive, behind the scenes Gator is collecting and reporting your Web activity to its main marketing server. Gator is one of the least attractive, behind the scenes Gator is collecting and reporting your favorite Web procument monitoring utility. For instance, Gator, a popular spyware program, monitors your Web surfing and tells you when someone else has the same item or competing item available for less money. Many people use Gator as a convenient utility for populating online information forms and saving passwords. While the online bargain locator and information completion feature is attractive, behind the scenes Gator is collecting and reporting your Web activity to its main marketing server. Gator is one of the least attractive, behind the scenes Gator is collecting and reporting your browser habits for marketing efforts to capture key strokes for criminal activities (ex. ID Theft).

Congress has decided to tackle the spyware issue with new anti-spyware legislation known as the Software Principles Yielding Better Levels of Consumer Knowledge Act (SPY BLOCK). This act, along with a similar act in the Senate, passed unanimously through committee and will now go to the Senate and the House for final consideration.

Legislation overview:

- Prohibits installing software that automatically collects and then transmits information about users or their habits without the user’s permission.
- Prohibits the prevention of reasonable efforts to uninstall, remove, or disable the software.
- Prohibits vendors from using false or misleading means to entice consumers to install the software.

In the meantime, here are a few tips to protect yourself from spyware:

1. Turn off scripting in Internet Explorer. For further assistance, please contact IT Help Central at 742-HELP (4357).
2. Verify your Windows start-up programs. Most spyware starts automatically with the operating system.
3. Use a system firewall like the one that comes already enabled and running with Windows XP SP2. If you do not have XP, other software firewall solutions are available.

For assistance with these tips or any other related questions, please contact IT Help Central at 742-HELP (4357).

Safe Computing Practices Campaign Overview

As the Internet and information technology become an integrated part of daily American life, the importance of safe computing practices is paramount to our society. While the technology has become widespread, risks and threats continue to escalate. In fact, Cisco Systems reports a dramatic increase in hacker tool sophistication coupled with a decrease in hacker sophistication! As the malevolent tools become more sophisticated, they are easier to use and can be deployed by many more hackers.

In an effort to raise awareness and promote education, we are implementing a two-year Safe Computing Practices campaign for Texas Tech University and the surrounding community. Our goal is to empower people with knowledge and tools to reduce area Internet-based security threats. We will be offering training sessions, workshops, roundtables, bulletin articles, and special group presentations. Each event will offer a detailed account of certain security threats, accompanied by practical recommendations that promote security and prevention.

We will launch the campaign with the Chamber of Commerce Technology Luncheon on November 3, 2004. I invite the university community to participate in this strategic and important campaign! We welcome all ideas and suggestions to enhance this campaign and make it more useful for the community. Please send your input to CIO@ttu.edu.

Message from the CIO

After months of planning, strategizing, brainstorming, researching, and gathering data, we are officially launching the Safe Computing Practices Message campaign for Texas Tech University and surrounding area. Beginning with a keynote speech at the Chamber of Commerce Technology Luncheon on November 3, I will begin scheduling various educational workshops, roundtables, forums, and discussions aimed at raising awareness and understanding of information technology security awareness. I invite you to visit our Safe Computing Practices Web site at http://www.safecomputing.ttu.edu. An informed community is an empowered, safe IT neighborhood! In this issue, we discuss the threat of Spyware and how to protect your system(s). In addition, we will provide an Overview of the Safe Computing Campaign and highlight the “Do you know about...” series designed to provide simple, useful computing tips on timely and relevant issues. As always, I invite your comments and suggestions; simply email CIO@ttu.edu. As we approach the holiday season, a peak time for security threats and hacking, I encourage you to take advantage of educational materials and opportunities to increase your own knowledge and to protect your system, data, and personal information.

-Sam Segran
Associate Vice President for IT and Chief Information Officer

TTU Compliance with the DMCA | TTU Privacy Policy | State of Texas | Texas Public Information Act | Texas Tech University Health Sciences Center
Copyright 2004 Texas Tech University | All Rights Reserved | Updated: November 08, 2004 | Texas Tech Operator: (806) 742-2011
Texas Tech University Location: 2500 Broadway - Lubbock, Texas
Hear Ye! Hear Ye!

Announcing the

"Do you know about..." Series!

Designed to offer practical computing tips and suggestions, the "Do You Know About..." (DYKA) series debuted several weeks ago. Based on our customer service assessments and customer support evaluation, each week we identify a timely topic and provide simple, practical tips for addressing the issue or concern. The "Do You Know About..." series is a weekly TechAnnounce that will target a timely and TTU-relevant technology topic. We have already addressed email scams/hoaxes, file sharing, connecting a new computer to TTUNet, and password security.

You can find an archive of previous DYKA's at: http://www.ttu.edu/safecomputing/ttu/dyk/.

If you have input or topic suggestions, please email the Office of the CIO at cio@ttu.edu.

Fighting the Electronic Blues: E-mail Hoaxes and Scams, Part I

E-mail has become the largest distribution technique for hackers and other electronic criminals. Counting on customer naiveté and gullibility, hackers craft malevolent e-mail strategies designed to prey on our vulnerabilities. Knowledge and caution are the best defense against such foul play. Throughout the next several issues, we will outline common hoaxes and scams.

In general, we suggest a few simple practices:

- Never open an e-mail attachment from a person that you do not know.
- Even if you recognize the sender's name, do not open an e-mail attachment unless you are expecting a document.
- If you receive an unexpected attachment from a known recipient, call and confirm that they sent you a document.
- If you receive an ad, special prize announcement, or any request to visit a Web site, delete the message and do not click on the Web address.
- Do not send personal information (SSN, Driver's License, etc.) through e-mail.

In a nutshell, be cautious and skeptical! Given some of the devastating results that hoaxes and scams can cause, err on the side of safety.

Spyware is software that:

- Installs itself on a PC without the consumer's knowledge
- Tracks computer usage
- Difficult to remove
- Can have both commercial intent (targeted ads) or criminal intent (password collecting)

Different Kinds of Spyware

- **Adware** - Tracks browsing and search habits and/or delivers targeted pop up ad.
- **Keyloggers** - Records username and password information and/or program activity to monitor usage.
- **Browser Hijackers** - Changes some aspect of the browser: the homepage, default search engines, and favorites.
- **Dialers** - Modem hijackers that dial international or 900 numbers.

Crime Prevention: How Does Spyware Attack?

- Voluntary software downloads
- Browser security holes
- Human Weakness
- Fake Anti-Spyware
- Malicious installation (by someone at your company or institution)