



State of Utah

Enterprise Security Office

Monthly Security Tips

NEWSLETTER

July 2011

Volume 6, Issue 7

Cyber Crime: How It Happens And How You Can Protect Yourself

From the Desk of EISO

An increasing number of domestic and international criminals are using the Internet for illegal purposes. Computers and other electronic devices can be used to commit crimes. This newsletter will discuss who are potential targets, the nature of computer and cyber crime, and what you can do to be safe.

Why are you a target?

Information, whether personal or business related, is becoming increasingly valuable to criminals. Where personal information, such as bank account, credit card, or social security numbers, is stored, whether on your personal computer or with a trusted third party such as a bank, retailer or government agency, a cyber criminal can attempt to steal that information which could be used for identity theft, credit card fraud or fraudulent withdrawals from a bank account, among other crimes.

How can you be attacked in a Cyber Crime?

Simply by connecting to the Internet you are making yourself a potential target of criminals. Everyday, criminals use automated tools to scan for unprotected or vulnerable computers. Criminals may target you specifically or you may be the subject of a random attack. Whether a specific target or just a random attack, there are two main ways by which your computer can be affected by cyber crime:

Your computer is used to steal your personal information: Two examples are trojans and spyware. Trojans are a form of malware masquerading as something the user may want to download or install, that may then perform hidden or unexpected actions, such as allowing external access to the computer. A Trojan may be used to install spyware such as 'keylogging' software, which records keystrokes including passwords and then forwards the 'keylogged' information to the attacker.

Your computer is used to facilitate other crimes and attacks on others: Computers can be hijacked to provide storage of illegal images or illegal downloads of music. Hijacked computers could also be used as a platform to launch attacks or commit crimes against others.

The best way to protect yourself from cyber crime is to use common sense, be prepared and take precautions.

How Can You Stay Safe?

- Keep your operating system updated/patched. Set it to "auto update".
- Use anti-virus and anti-spyware software and keep them updated.
- Do not visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Secure your transactions. Look for the "lock" icon on the browser's status bar and be sure "https" appears in the website's address bar before making an online purchase. The "s" stands for "secure" and indicates that the communication with the webpage is encrypted.
- Be cautious about all communications you receive including those purported to be from "trusted entities" and be careful when clicking links contained within those messages.
- Do not respond to any unsolicited (spam) incoming e-mails.
- Do not open any attachments contained in suspicious emails.
- Do not respond to an email requesting personal information or that ask you to "verify your information" or

to "confirm your user-id and password."

- Beware of emails that threaten any dire consequences should you not "verify your information".
- Do not enter personal information in a pop-up screen. Providing such information may compromise your identity and increase the odds of identity theft.
- Have separate passwords for work related and non-work related accounts.

Resources for more information:

MS-ISAC Tip -- Surf Safe On The Internet

msisac.org/daily-tips/Surf-Safe-on-the-Internet.cfm

US-CERT Shopping Safely Online

us-cert.gov/cas/tips/ST07-001.html

National Cyber Security Alliance

staysafeonline.org/in-the-home/protect-yourself

FTC Identity Theft Site

ftc.gov/bcp/edu/microsites/idtheft/

For more monthly cyber security newsletter tips, visit: www.msisac.org/awareness/news/

*The information provided in the Monthly Security Tips Newsletters is intended to increase the security awareness of an organization's end users and to help them behave in a more secure manner within their work environment. While some of the tips may relate to maintaining a home computer, the increased awareness is intended to help improve the organization's overall cyber security posture. This is especially critical if employees access their work network from their home computer. **Organizations have permission and are encouraged to brand and redistribute this newsletter in whole for educational, non-commercial purposes.***

Brought to you by:



MULTI-STATE
Information Sharing
& Analysis Center™

A DIVISION OF |  CENTER FOR
INTERNET SECURITY



SECURITY
.UTAH.GOV