



INFORMATION TECHNOLOGY SERVICES

Email your topic suggestions, questions, and comments to itsecurity@sfasu.edu

Cyber-Security Newsletter

August 2011

STEPHEN F. AUSTIN STATE UNIVERSITY

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

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. Every day, 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.

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



Cyber-Security Newsletter

August 2011

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, 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:

National Cyber Security Alliance

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

FTC Identity Theft Site

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

Last Words: Is There a Hacking Epidemic?

For years, security professionals have said that organizations need to apply good security practices to a wide variety of threats. Password security best practices such as encryption, changing your password periodically, using non-dictionary words, and using complex passwords have been around since 1979 [Morris and Thompson, 1979]. Similarly, hacking has been around for decades. Hacker groups such as "Anonymous" and "LulzSec" continue to gain notoriety. Is there a hacking epidemic? Is the public paying closer attention? Read more on this from a quorum of cybersecurity experts at <http://www.freakonomics.com/2011/07/19/why-has-there-been-so-much-hacking-lately-or-is-it-just-reported-more-a-freakonomics-quorum/>

Source: [Morris and Thompson, 1979] R. H. Morris and K. Thompson. UNIX password security. *Communications of the ACM*, 22(11):594, November 1979

Produced by:

Brought to you by:



US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM



MS-ISAC