Consumer Affairs Tabloid

Keeping you in the "KNOW"

287- CITY | Army Community Service Financial Readiness Branch | November 2009

Excerpt from: Federal Bureau of Investigation
www.fbi.gov/pressrel/pressrel09/networking_100109.htm
No, Your Social Networking "Friend" Isn't Really in Trouble Overseas

According to the Internet Crime Complaint Center (IC3), there has been an increase in the number of hijacked social networking accounts reported to www.ic3.gov.

One of the more popular scams involves online criminals planting malicious software and code onto victims' computers. It starts by someone opening a spam e-mail, sometimes from another hijacked friend's account.

Some applications advertised on social networking sites appear legitimate but install malicious code or rogue anti-virus software. These empty applications can give cyber criminals access to your profile and personal information. These programs will automatically send messages to your contacts, instructing them to download the new application too.

Infected users are often unknowingly spreading malware by having links to infected websites posted on their webpage without the user's knowledge. Since the e-mail or video link appears to be endorsed by a friend, social networking contacts are more likely to click on these links.

Although social networking sites are generally a safe place to interact with friends and acquaintances, keep in mind these suggestions to protect yourself while navigating the Internet:

- Be selective when adding friends. Once added, contacts can access any information marked as viewable by all friends.
- Limit access to your profile to only those contacts you trust with your personal information.
- Be careful what you click on. Just because someone posts a link or video to their wall does not mean it is safe.

Excerpt from: GetNetWise
Social Networking Sites http://kids.getnetwise.org/safetyguide/technology/socialnetworking

*Consumer Affairs Note: Even though this article is aimed at parents of children and teens, this information is useful for everyone who uses a social networking site.

Use privacy settings to restrict who can access and post on your child's website. Some social networking sites have settings to limit the information you share with others. Show your child how to use these settings to limit who can view their online profile, and explain to them why this is important. Below are few samples of how to change the preferences in some social networking sites: (click on links to take you to the step by step instructional videos)

Facebook http://kids.getnetwise.org/safetyguide/technology/facebook/facebook-private-audio
Myspace http://kids.getnetwise.org/safetyguide/technology/myspace/myspace-private-audio
Xanga http://kids.getnetwise.org/safetyguide/technology/xanga/xanga-private-audio

Excerpt from: Federal Trade Commission
"Free Security Scan" Could Cost Time and Money www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt121.shtm

Messages telling you to install and update security software for your computer seem to be everywhere. So you might be tempted by an offer of a "free security scan," especially when faced with a pop-up, an email, or an ad that claims "malicious software" has already been found on your machine. Unfortunately, it's likely that the scary message is a come-on for a rip-off.

The free scan claims to find a host of problems, and within seconds, you're getting urgent pop-ups to buy security software. After you agree to spend $40 or more on the software, the program tells you that your problems are fixed. The reality: there was nothing to fix. And what's worse, the program now installed on your computer could be harmful.

These programs are called "scareware" because they exploit a person's fear of online viruses and security threats.

Excerpt from: The Better Business Bureau
http://www.bbb.org/us/article/boo-scareware-attacks-on-the-rise;-bbb-advice-on-how-to-protect-your-computer-12707

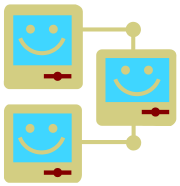
Boo! Scareware Attacks on the Rise; BBB advice on how to protect your computer

Computer experts are reporting that scareware — yet another sneaky technique used by hackers to steal personal information and spread viruses online — is on the rise. Most recently, companies like Google, Twitter and the New York Times are being exploited by hackers as part of a massive scareware attack on consumers.

Never let your guard down. A scareware attack can happen on trusted news sites like the New York Times, in search engines results from Google, and even now on Twitter.

Protect your computer. Install updates to your operating system, purchase antivirus software from a name you trust and keep that software up to date. Also make sure that all security patches and updates are installed for your Web browser and programs like Adobe Flash Player.

Take immediate action during an attack. If you receive a scareware pop up window, experts recommend forcing the window to close through your task manager. To do this, hold down ctrl, alt, and delete at the same time, open your task manager, find the browser in the list of running programs and click "end task." Finally, run an antivirus scan with legitimate, trusted software.



From the Files of Fort Hood's Consumer Affairs Office

Do you have a social network account? You can link up and follow a number of agencies to include the Department of Defense, the Army, Family Support Groups, etc. There is a wealth of information at your fingertips.

Just remember, discretion is the better part of valor. Prospective employers, universities, and even debt collectors troll social networking sites. Anything you post or that your friends post which appears on your account can be used against you.

Please click on the links and read all the articles posted in this tabloid for additional information.

Back issues of the Consumer Affairs Tabloid are available on the Financial Readiness section of the ACS website at www.hoodmwr.com/acs.

Have questions? Email: melody.squires@us.army.mil or call 287-CITY (2489)