Contact Information:

Cyber Criminal Intelligence Program

9805 Lowen Road, Building 193

Fort Belvoir, Virginia 22060-5598

Phone: 703.805.3499 (DSN 655)

Fax: 703.805.2351 (DSN 655)

E-mail:

cybercrimintel.cciu@us.army.mil

CCIU Web Page:

www.cid.army.mil/cciu.htm

CID Cyber Lookout
On Point for the Army

"DO WHAT HAS TO BE DONE"

CPF 0020-10-CID361-9H   19 May 2010

HOME COMPUTER SECURITY

OVERVIEW:

The Computer Crime Investigative Unit has determined that several unlawful intrusions into U.S. Government and other domestic computer networks were an indirect result of well-intentioned government and military personnel using their home computers without proper security and safeguards, which led to the compromise of users' access credentials (e.g., username, password, and PIN). Criminals can use legitimate credentials captured from unsuspecting users to gain illegal access to bank, email, and government/corporate accounts as a prelude to further criminal activity such as wire fraud and ID theft.

While government and corporate networks have the benefit of dedicated information technology and security staff, home computers are generally reliant upon individual users for security.

This crime prevention flyer provides ten of the most common and simple protective measures an individual user can implement to mitigate general cyber threats and avoid compromises of computers systems and information.

CID elements are encouraged to brief supported installations and units on the contents of this crime prevention flyer.

TEN HOME COMPUTER SECURITY TIPS:

1 - Use security software that updates automatically. At a minimum, use antivirus, antispyware, and firewall software. Army employees and military personnel may obtain no-cost software from the Army Computer Emergency Response Team at https://www.acert.1stiocmd. army.mil/Antivirus/

2 - Keep your operating system and other software applications (e.g., Adobe Acrobat Reader®, Sun Java®, etc.) updated. Configure them to automatically check for, download, and install security updates.

3 - Use caution when downloading and reading email with attachments. Think twice before opening messages from unknown senders.

4 - Beware of clicking on hyperlinks since they can be masked to direct you to illegitimate sites. Instead, type the web address into your browser yourself. Make sure any website that has your personal or financial information starts with "https://" in the address bar.

5– Use strong passwords consisting of upper and lowercase letters, numbers, and special characters. Protect passwords from disclosure.

TEN HOME COMPUTER SECURITY TIPS (CONTINUED):

6– Protect personal information, and carefully consider what information you post to social networking sites. Criminals can easily obtain the information and use it to answer security questions (names of spouse, parents, children, and pets; home-town; birthdays; etc) that can lead to password resets and unauthorized account access.

7 - Use care when downloading/installing programs, and only download files or plug-ins from trusted websites or sources.

8 - When using a wireless network, adhere to security best practices. See related Cyber Crime Alert Notice.

9– Use the administrator's account only for system administrative tasks such as installing software. For typical tasks, use a standard user's account.

10 - Learn what to do if something goes wrong.

PREVIOUS CYBER CRIME ALERT NOTICES (2CANS) RELATED TO CYBER SECURITY ON THE HOME FRONT:

P2P Might Leave You Up a Tree (28 May 09)

OPSEC on the Cyber Home Front (12 Apr 07)

Wireless (In)Security: Who's Snooping on Your Home Network? (23 Feb 07)

"Vishing" is the New "Phishing" (31 Jan 07)

ADDITIONAL INFORMATION:

OnGuardOnline.gov
http://www.onguardonline.gov/default.aspx

U.S. Computer Emergency Response Team
http://www.us-cert.gov/reading_room/home-network-security/

Switched.com
http://www.switched.com/2010/04/20/10-biggest-security-risks-and-how-to-fix-them-2/

Carnegie Mellon University CERT® Coordination Center
http://www.cert.org/homeusers/HomeComputerSecurity/

Staysafeonline.org
http://www.staysafeonline.org/content/protect-your-computer

CCIU is now using the Interactive Customer Evaluation (ICE) system. Please click on the ICE logo and take a moment to provide us with feedback.

CCIU's "Toucan Lan" keeps an eye on cyber crime issues of interest to the Army community.