Cyber Crime Prevention Flyer

Contact Information:
Cyber Criminal Intelligence Program
27130 Telegraph Road
Quantico, Virginia 22134

Phone: 571.305.4482 [DSN 240]
Fax: 571.305.4189 [DSN 240]

E-mail

CCIU Web Page

CPF 0005-15-CID361-9H **2 June 2015**

Home Computer Security

The number of significant computer security breaches at large companies, government agencies, and other organizations continues to rise. Criminals are relentless in their attempts to steal information. While many civilian and military personnel assume using their government authorized access credentials on their home computer makes everything secure, this is not always the case. If the home system is vulnerable, then those access credentials (username, password, and PIN) and your other personal information are not protected. Thus, possibly giving free reign to bank, email, and government accounts to further criminal activity.

Well-intentioned civilian and military personnel do not have the budget or dedicated information technology and security staff of government and private organizations to secure home systems; however, civilian and military personnel can be proactive by initiating home computer security measures. The Computer Crime Investigative Unit recommends users abide by the following ten common and simple protective measures an individual user can implement to mitigate general cyber threats and avoid potential compromises.

TEN HOME COMPUTER SECURITY TIPS:

1. **Install protective software and ensure the software updates automatically.** Army civilians and military personnel may obtain, for free home use, McAfee antivirus software from the Defense Information Systems Agency at http://www.disa.mil/cybersecurity/network-defense/antivirus/home-use.
2. **Patch, Patch, Patch!** Keep your operating system and other software applications updated. Set your computer for automatic software and operating system updates. An unpatched system is more likely to have vulnerabilities that can be exploited.
3. **Choose strong passwords.** Include letters, numbers, and special characters in passwords, create a different password for each important account, and change passwords regularly. Consider using pass phrases for an added level of safety.
4. **Use caution with email.** Ignore unsolicited emails, and be wary of attachments, links and forms in emails that come from people you do not know, or which seem "phishy."
5. **Use secure connections.** When connected to the Internet, your data can be vulnerable while in transit. When accessing websites using personal credentials, check that the web address starts with "https://" indicating a secure connection.
6. **Backup, Backup, Backup!** Backing up your machine regularly

TEN HOME COMPUTER SECURITY TIPS (CONTINUED):

protects you from the unexpected. Keep a few months' worth of backups and make sure the files can be retrieved if needed.

7. **Be careful what you download.** We live in a digital age in which we can download just about anything to watch, listen, or use. There are hundreds of sites to download legitimate digital content, but there are thousands more that offer bogus, and harmful content, filled with malware designed to steal your financial and other personal information.
8. **Consider what information you post to social networking sites.** Criminals easily obtain personal information from social networking sites and use the information to answer security questions that can lead to password resets and unauthorized account access. Refer to CCIU Cyber Crime Prevention Flyers on Social Networking Safety Tips and Facebook, Twitter, LinkedIn, and Google+ configuration guides.
9. **Use a standard user account.** The standard user account can help protect your computer from malware installation, because the standard user cannot install programs without the administrator password. Use the administrator account only for system administrative tasks such as installing software.
10. **You are a security layer, so stay informed.** Each individual is a line of defense because no 100 percent solution exists for all security issues. Be wary of social engineering and learn what to do if something goes wrong.

Previous CCIU Advisories related to Home Computer Security:

I Don't Want To Plug And Play, Universal Plug and Play (UPnP) Vulnerabilities (6 Feb 2015)

Held for Ransom—Part II, Ransomware, (29 Jan 2015)

Held For Ransom, Ransomware, (4 Sep 2012)

Unsolicited Software or Devices, Cybersecurity Concerns with Unsolicited Software/Devices (5 Feb 2014)

Additional Information:

United States Computer Emergency Readiness Team (US-CERT)
Home Network Security
Cyber Security Tips

OnGuardOnline
Secure Your Computer

University of California, Santa Cruz
Top Ten List of Good Computing Practices

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