Safe Computing Tips (or how to avoid malware!)

Unfortunately, scammers, identity thieves, and hackers have grown more sophisticated in recent years. Today, they are utilizing a vast array of tricks to infect systems with viruses, destroy data on your hard drive, or even steal your identity. ALLCONET would like share some tips about safe computing practices so you can avoid inadvertently installing a virus/malware (in general, bad software!) on a computer.

Samples of tricks used to infect your PC

- **"Your computer is infected."** You stumble across an infected web page, advertisement, or email, and you see a pop-up window advising your computer has been "infected" with one or more viruses, spyware, etc. The pop-up window says to "click here" to download software that will clean your PC. **DO NOT DO THIS.** This is a fake antivirus scam that will infect your PC with viruses and/or malware. The screen below is an example of a fake antivirus window…looks like a real antivirus application, doesn't it?

- **"Phishing."** You receive an email message that appears to come from a financial institution (for example, Wells Fargo Bank, or PayPal) or your Internet Service Provider. Often, the email tells you that there is a problem with your account, and you are prompted to click on a link to fix the problem. **DON'T.** The link is to a web page that either collects your information to use for fraud or identity theft purposes, or one that will infect your PC with a virus. Financial institutions and Internet Service Providers never send messages such as these.

- **Social networking site videos/links.** You receive an email from a friend on Facebook, MySpace, or another social networking site inviting you to watch a hysterical video, check out a hilarious photo, or visit a cool new website, but when you click on the link, you receive a message that a software update is needed. **If you proceed with the software update, you will most likely infect your computer.** And, the virus could then end up in your Facebook profile, sending messages and posting on your friends' walls the exact same message you were tricked by. **NEVER update software from a redirected site on the Internet; instead, go to your browser's website and update it from there.**

Safe Computing Tips (or how to avoid malware!)

- **Fake electronic greeting card.** You get an e-mail telling you to click on a link to receive an e-card sent by someone you know. Unfortunately, the link actually takes you to the virus site, or sometimes the site of an undesirable advertising company. You will be notified that you have to install an "ActiveX" control in order to view the card. If you are foolish enough to bite, your computer will become infected.

- **Fake "returned" mail or fake package delivery notice.** Similar to the fake electronic greeting card, these messages also contain links that can lead to virus installations or very nasty advertising. (porn)

- **Money transfer scam.** Someone tells you, either via Facebook, chat, message, or email, that they are stranded in a foreign country and need money. Coined the "Nigerian 419" virus because many victims claim to be alone in Nigeria, the virus hacks your personal information listed on your profile in order to make it seem like he or she is actually your friend and to make the plea more convincing. Money transfer scams are successful because money wired to another country can be picked up at multiple locations, making the hacker almost impossible to identify or trace. NEVER send money in the mail without contacting the person in a secure form outside of social networking. Facebook has an online form that can be filled out and submitted if you believe your account has been compromised.

Overall recommendations and tips for virus prevention

- **Do not open** any files attached to an email or click on any links within an email from an unknown, suspicious or untrustworthy source.
- **Do not open** any attachments or links in an email unless you know what it is, even if it appears to come from a friend or someone you know. Some viruses can replicate themselves and spread through email. Confirm that your contact really sent an attachment. It is very easy for a hacker to "spoof" someone's email address; in other words, make an email look like it is coming from someone you know…even if it is not.
- **Use common sense.** It's always better to err on the side of safety. If you're unsure about an email attachment or a link in an email, **DELETE THE EMAIL.** Especially if it's from a source you don't recognize. If there are tempting animations on a website that look highly unprofessional, don't download them.
- **Never click "OK" to download, install, or run anything that you did not specifically request.**
- **Install antivirus software and keep it up to date.**
- **Use a firewall. Windows has one built-in; you can find it in control panel.** Using a firewall reduces the chance of malware infection. If you do get infected, it can potentially warn you before the malware sends out information about you or attempts to attack other computers. Please pay attention to these warnings; sometimes they can be obscure.
- **Avoid using a computer account with "administrator" privileges.** An administrator account is necessary to install software and change most Windows settings. For regular use, in Windows Vista or Windows 7 use a normal user account or in Windows XP, a "limited" account. You can add an account and configure its settings under Control Panel, User Accounts. If you are not an administrator and stumble across an infected file or web page, Windows will prompt for permission to run the program. **Unless you were specifically requesting software to install, say NO to this request!**

Safe Computing Tips (or how to avoid malware!)

Other resources for more information

- McAfee Anti-Virus Tips http://home.mcafee.com/virusinfo/anti-virus-tips

- Stephen F. Austin State University Information Technology Security Page, provides a list of current threats and how to avoid them: http://www.sfasu.edu/itsecurity/