IT Documentation

InfoSec Secure Computing Tips

Author: John Glynn
Date: 31th August 2016

Secure Computing Tips

Tip #1 - Keep your passwords strong: The best strategy for protecting your information is to use a strong password that contains upper and lowercase letters as well as numbers and symbols. Consider using numbers and symbols that resemble letters to strengthen your password while keeping it easy to recall, e.g., "B@seb@11" instead of "baseball."

Tip #2 - Don't leave a computer you're logged into unattended or unprotected: It only takes a few seconds for someone to use an open browser to collect login information and copy passwords, so make sure to shut down the browser or lock your screen if you're going to be away from your computer, even for just a minute or two.

Tip #3- Password-protect mobile phones and tablets:

- Lock your device with a PIN or password - and never leave it unprotected in public.
- Only install apps from trusted sources.
- Keep your device's operating system updated.
- Don't click on links or attachments from unsolicited emails or texts.
- Avoid transmitting or storing personal information on the device.
- Most devices are capable of employing data encryption - consult your device's documentation for available options.
- Use Apple's Find my iPhone or the Android Device Manager tools to help prevent loss or theft.
- Backup your data.

Tip #4- Don't fall for phishing scams: So-called "phishing" scams occur when a cyber-thief calls or emails while posing as banking or merchant account official and attempts to collect login information. A sophisticated scammer can create a website that looks very much like a legitimate site. Never give out sensitive account information via email or over the phone. Instead, call the company directly.

Tip #5- Regularly update your software to eliminate security weaknesses:

- Windows, Macs and virtually all browsers regularly provide free software updates. Take advantage of this to close security loopholes!
- Turn on Automatic Updates for your operating system
- Make sure to keep browser plug-ins (Flash, Java, etc.) up to date.

Tip #6 - Be careful what you click

Avoid visiting unknown websites or downloading software from untrusted sources. These sites often host malware that will automatically, and often silently, compromise your computer.

If attachments or links in email are unexpected or suspicious for any reason, don't click on it.

Tip #7 - Backup, Backup, BACKUP!

Backing up your machine regularly can protect you from the unexpected. Keep a few months' worth of backups and make sure the files can be retrieved if needed.

Here are some additional tips to help keep you safe and secure online:

Use a firewall - Mac and Windows have basic desktop firewalls as part of their operating system that can help protect your computer from external attacks.

Use public wireless hot-spots wisely - follow these tips (link is external) for staying safe.

Be conscientious of what you plug in to your computer (flash drives and even smart phones can contain malware).

Be careful of what you share on social networking sites.

Monitor your accounts for suspicious activity.

Bank or shop online only on trusted devices and networks - and logout of these sites when you've completed your transactions.