IT Security Best Practices

1. Online Accounts
    a. Use unique passwords whenever possible. Do not reuse the same password or variants of the same password for all of your accounts.
    b. An easy way to have a complicated password that is easy to remember is to use a passphrase. Random sentences or puns work well (e.g. Owl be home for Christmas.) Be sure to include spaces and punctuation to increase the complexity of your passphrase.
    c. Use a password manager to keep track of and generate passwords. I like LastPass (www.lastpass.com).
    d. Enable two-factor authentication on your important accounts. Lastpass, Google, Microsoft, Yahoo, Teamviewer, and many other programs all support two-factor authentication.
    e. Make sure any websites that ask for personal or financial information have "https:" at the beginning of the web address. This will ensure your transaction if verified to be with the right site and also makes sure that your communication is encrypted.
    f. Always make sure you are expecting an attachment before opening any email attachment. Conversely, always tell your recipients what you are sending them if you include attachments in your email messages.
2. Personal Computers
    a. Update often (run Windows Update or Apple Software Update).
    b. Use antivirus. Windows Defender, which comes with Windows 10, is a very solid antivirus suite, and it is free. Good alternatives include AVG Antivirus, AVAST Antivirus, and Kaspersky Labs.
    c. Do not install multiple antivirus solutions at the same time or they will slow down your computer significantly.
    d. Download and run Malwarebytes occasionally (once a month unless you're experiencing a problem). Use the free version without the trial for the Pro version. You really only want to use Malwarebytes with manual scans and your antivirus software will handle most other things. (www.malwarebytes.org) P.S. I checked into the claim that Malwarebytes installed or contained malware, but I could find no reference to this. This software is used by millions of IT professionals. I trust it.
    e. Use a modern web browser. Do not use anything older than Internet Explorer 11. I suggest using Microsoft Edge (comes with Windows 10) or Google Chrome. Safari is also fine on Macs.
        i. Install AdBlock Plus on your browser. It is a free plugin for Edge, Firefox, and Chrome. This will block unwanted ads from website and protect you from some seedy links. If a website complains about your using an adblocker, if you trust the site, you can whitelist the site to let its adds through. Forbes.com is an example of a site that might do this.
        ii. Do not install Java or Flash in your browser unless you absolutely must. Both products are horribly insecure and the main vector for malware to reach computes through the web.
    f. If you have a lot of issues with viruses or things breaking on your computer, consider changing your main account to a user account and creating a separate administrator

account. This will force Windows to prompt you for the admin account credentials whenever you need to install something or make a system-wide change. Instructions for changing your account type can be found here: http://www.komando.com/tips/12210/one-change-that-instantly-makes-your-computer-safer/all

g. Make sure your software firewall is enabled. This will protect your computer from network attacks.

h. If you are worried about your data falling into the wrong hands, encrypt your hard drive with Bitlocker (Windows 10 Pro/Enterprise), FileVault (Macintoshes), or Veracrypt for everything else (https://veracrypt.codeplex.com/).

i. Enable Find my Device (Windows) or Find my Mac. This works sort of like Find my iPhone and could help you find a misplaced laptop if it is connected to the Internet.

3. Backups
   a. Backup your data. If you want to be thorough, use offline, online, and offsite approaches.
      i. Offline = use an external hard disk to back up your software. Most hard disks come with their own backup software, but Windows also has a built in backup system called “File History”.
      ii. Online = use a cloud storage system like Carbonite or iDrive for full system backups. If you only care about protecting the files in your My Documents folder or places like that, you can also use services like Dropbox, Google Drive, or OneDrive.
      iii. Offsite = backing up to an external hard disk and storing it somewhere other than where you primarily keep your computer. The idea here is that if something happened to your office location (e.g a fire), you will have a data backup somewhere else away from the fire.
4. Networking
   a. Make sure your home or office network is protected by a physical firewall. Most Internet Service Providers have some sort of firewall built into the cable or fiber modems they use with their services.
   b. Use at least WPA encryption on your WiFi passkeys. If you have an older router, you might be using WEP encryption which is easily broken.
5. General
   a. Protect your phone with a passcode, fingerprint scan, or some other security measure like an Android swipe pattern.
   b. Make sure Find my iPhone or Find my Device is enabled on your phone. This will give you the ability to locate a missing phone or remotely erase a stolen phone and make it so others cannot use the device.
   c. Be wary when installing new software. Make sure you trust the source. If downloading software, make sure you are downloading from the creator’s website. For example, if you are downloading Microsoft Office, make sure it is coming from Office.com. If installing Quickbooks, make sure the file is coming from Intuit.com.
   d. If you are unsure about a website or file, check it on www.virustotal.com