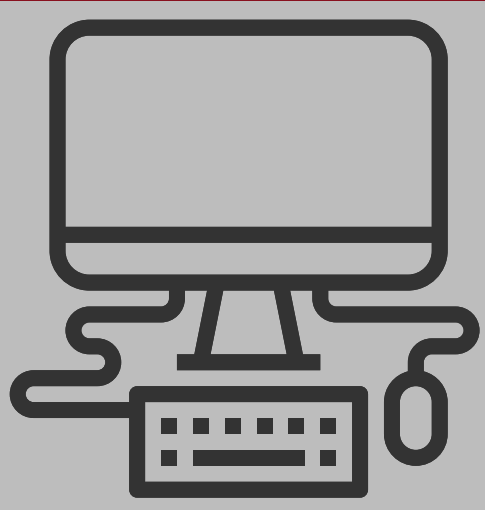
INTERNET SAFETY TIPS

Defense against the Dark Arts.

SYSTEM PRECAUTIONS



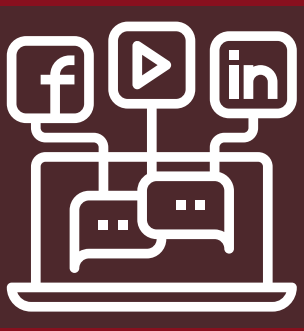
- Keep your computer updated with the latest anti-virus and always allow the system scans to complete.
- Occasionally scan your system with Malwarebytes.
- Run Windows 10 as your operating system.
- Run Windows Updates and always apply updates.
- Enable Internet Firewall on all wireless connections and LAN of home PC.
- Backup data so your computer can be rebuilt if hacked.
- Identify and uninstall strange programs.
- In Task Manager, sort running processes by CPU time, investigate ones that are taking resources. Google the name to identify each process (www.processlibrary.com).

EMAIL PRECAUTIONS

- NEVER open an email attachment from an unknown sender.
- Most legitimate companies will not have spelling and grammatical errors in their emails.
- DO NOT respond to emails requesting financial information of any kind. The IRS, financial institutions, government agencies and law enforcement agencies will NEVER ask for financial information via email.
- DO NOT call 800 numbers listed in an email requesting financial information. Look up the number.
- Any scheme that requires Western Union is a CERTAIN FRAUD.
- Use www.charitynavigator.org to verify any unfamiliar nonprofit organizations are legitimate.
- DO NOT click links in emails from unknown senders.
- Verify tinyurl.com links at www.checkshorturl.com.
- Look at your email in text mode rather than HTML mode (without graphics).

BROWSING PRECAUTIONS

- Shut off pop ups. DO NOT click on pop ups. Close pop ups from the task bar at the bottom of your screen or from Task Manager (Ctrl+Alt+Del).
- DO NOT get faked out by similar looking software. Make sure it's legitimate.
- DO NOT go to sites that you login to on public computers.
- DO NOT click on Boost Performance icons.
- Pay attention to system messages. If you try to run a piece of software, Windows will give you a warning. Read this message and make sure this is what you really want to do.
- DO NOT answer surveys.
- BEWARE of fake Flash Player upgrade messages. Google the Flash Player upgrade to find the correct site.
- Pause cursor over links WITHOUT clicking and look at the bottom left of your screen to figure out where they link to.
- Use dual authentication for online financial accounts.
- When you Google something, the top sites will ALWAYS be ads.



SOCIAL MEDIA PRECAUTIONS

- Verify rumors with www.snopes.com or Google is before sharing it. SLEUTH IT FIRST.
- DO NOT share stupid stuff, like Bill Gates giving everyone $100.
- DO NOT share things from strangers, just like when you were a little kid.
- DO NOT share misinformation or out of date information.
- Use unique passwords for each social media site.

IDENTITY THEFT

- Look up your credit report every year. The heavily advertised site freecreditreport.com is a pay site, www.annualcreditreport.com is the legitimate site.
- Review your social security report: www.socialsecurity.gov/myaccount.
- There is an app called Credit Karma, it will monitor your credit for you, and it is free.
- If you need to report a theft go to www.identifytheft.gov, they have tips on the site to help you as well.
- Get a PIN from your tax preparer so they do not file fraudulent tax returns in your name.
- Make a list of any financial work or personal websites that you use. Make sure you are using unique passwords for each one. Also, make sure those sites are using dual authentication.
- Check to see if your email has been hacked at www.haveibeenpwned.com.

REMEMBER... YOU ARE AN INTERNET NINJA!

1 FENN STREET, PITTSFIELD, MA 01201
(413) 499-0607
WWW.COMPUWORKS.BIZ

CompuWorks
healthy technology
smarter business