Protect Yourself Tips: Computers

1. **Update passwords**. Keep administrative names and passwords updated.

Top 10 worst passwords in 2017:
123456
password
12345678
qwerty
12345
123456789
letmein
1234567
football
iloveyou

2. **Set wireless networks to "no broadcast"…** and password-protect them.

U.S. Computer Emergency Readiness Team's "Securing Wireless Networks" - handout
https://www.us-cert.gov/ncas/tips/ST05-003

3. **Must-haves: anti-virus, anti-malware.** Make sure you have both an anti-virus and anti-malware programs installed. There are several good, free options for personal use from companies such as AVG and Malware Bytes.

4. **Turn on your firewall.** This will prevent intruders from entering your system via the Internet—a must-have in these cyber times.

5. **Turn on automatic updates.** This will make sure you have the latest software patches for your operating system and web browser, which are usually published to fix known bugs and security flaws.

6. **Update security programs,** such as anti-virus and anti-malware and firewalls to protect your computer. Viruses can destroy your data, and malware will steal your personal information.

7. **Update all third-party programs**, including Microsoft Office, Adobe products and browsers such as Firefox, Chrome and Safari. Hackers often target third-party applications with known vulnerabilities.

8. **Drive power**. Uninstall programs and apps you don't use. Run a disk cleanup and defragmenter in Windows or use an application such as AppCleaner or AppZapper in Mac OS.

9. **Manage your startups.** This is as easy as running "msconfig.exe" in Windows or finding "Login Items" in your Mac System Preferences. The fewer programs that automatically load, the more system resources available, the faster your computer.

10. **Power down**. Be sure to power down your computer when not in use.

11. **If sensitive information is stored on the hard drive, protect it with encryption** and by regularly backing up your data to a separate disk and, where possible, a remote site or facility.

12. **Before disposing of your computer, remove all storage drives**. Do not rely on the "delete" or trash function to remove files containing sensitive information.

13. **Store personal files and data backups securely in your home**, especially if you have roommates, employ outside help, or have service work done in your home. Be sure to turn on all security settings built into your computer, and password-protect your computer and files with sensitive personal or account data.