Top 10 Cyber Security Tips

Personal Edition

Your personal devices contain private information that you do not want leaked to the world. Ensure that your devices are protected at home, at work, and on the go.

1	**Defend your computer in depth by using anti-virus software and firewalls** – These two components are absolutely essential and no computer system should be operated without anti-virus and firewall software.
2	**Keep your operating system and software programs up-to-date with the latest security patches** – Ensure that updates are applied regularly to the operating system and ALL the software programs installed on the device. Ensure that automated updating features of the operating system and various software programs are enabled and scheduled. This is necessary as vulnerabilities in software programs are discovered daily.
3	**Be cautious when surfing the web and opening emails** – Verify that the website or email does not have malicious intent. Do not download attachments or click on links within an email if you are unsure of its authenticity. Remember to only install software from a legitimate source.
4	**Use encryption when storing data locally on your computer hard drive or on portable devices –** Encryption is a way to protect sensitive information from unauthorized disclosure, alteration or loss. The encryption process makes information unreadable unless decrypted by an authorized user with the correct key or password.
5	**Remember to change your password(s) regularly** – One way to remember is to change your password at home or on your device is when you have had to change it at work. Immediately change it if you suspect that it has been compromised. Remember that your password should be complex, hard to guess, and never shared!
6	**Use secure wireless networks** – Verify that the wireless network you are using is secured with a password and encrypted using Wi-Fi Protected Access 2 (WPA2).
7	**Create a separate user profile/account on your home PC for your work activities** – This method isolates your work activities from your personal activities and other users on the computer.
8	**Use secure file deletion software to permanently erase files** – If specialized deletion software is not used, only the identification numbers for the files are erased, and not the contents of the file. This means that the files and their contents can be recovered.
9	**Set the screen saver to come on automatically** – This type of timeout control ensures that your workstation or device is secure while not in use. Typically, the screen saver will activate after 15 minutes of inactivity and will require a password to resume the session.
10	**Educate yourself** – Become familiar with the various threats to your personal devices and learn about the tools and practices to mitigate the risks.

Created December 2016