Cybersecurity Wellness

Safe, secure computing requires **knowledge**, **awareness** and ongoing **action**. Computers are pervasive in our lives in devices we use every day. Now with many working at home, secure home computing is critical. Cyber security begins with you. Protect your privacy, identity and finances with these top tips.

1. Use a **password manager** (Keeper**,** SplashID, 1Password or LastPass). Use strong passwords by combining uppercase and lowercase letters with numbers and symbols to create a strong, secure password. Do not use the same password for multiple accounts or sites. Do not share your passwords. Do not write it down.

2. Use **multi-factor authentication** when available especially on financial accounts and email preferable using an authenticator app versus text messages.

3. Beware of **phishing** in emails and phone calls. Always be careful clicking on attachments or links in email or web sites. Ignore unsolicited emails, and be wary of attachments, links and forms in emails that come from sources you do not trust, you do not know or seem "phishy." **If** it's unexpected or suspicious, do not click on it. Avoid untrustworthy downloads from freeware or shareware sites.

4. An out of date, unpatched computer, tablet or mobile device is more likely to have vulnerabilities. **Update software** on computing devices (anything that connects to the Internet). Configure your computers for automatic updates. Check that anti-virus software is always up to date.

5. Lock your devices when not in use. Never leave your devices unattended, especially in public places. Require biometric (e.g. facial recognition) or password authentication for device access If you keep sensitive information on a flash drive or external hard drive, lock it up. **Physical security** of your device is just as important as technical security.

6. Use **end point security** (e.g. Windows Defender) protect your computer from malware, ransomware and viruses. Be careful what you plug in to your computer. Malware can be spread through infected flash drives, external drives and smartphones.

7. Connect securely and **secure your network**. Use secure WiFi (e.g. Wi-Fi Protected Access 3). Change your default router password. Use a security gateway or firewall. Update and/or upgrade your router and wireless access points.

8. When browsing the web use **secure, encrypted connections**. Ensure you are on a HTTPS (Hypertext Transfer Protocol Secure) site. With unencrypted connections your data is vulnerable in transit. Sensitive browsing, such as banking or shopping, should only be done on a device you control and on a network that you trust. Whether a friend's phone, a public computer or free WiFi, your data can be stolen.

9. **Backup** your data regularly and automatically to protect you from the unexpected. Keep several months' worth of backups and verify the files can be restored.

10. Watch what you are **sharing on social networks**. Criminals will befriend you and gain access to information that helps them gain access to more valuable data.

11. Offline, be wary of **social engineering**, where someone attempts to gain information from you through manipulation. If someone calls or emails you asking for sensitive information, say no. Call the company directly to verify credentials before giving out information.

12. **Monitor** your accounts and transactions for suspicious activity. If you notice something unfamiliar, it may be a sign that you were compromised. Many financial institutions offer activity notifications for your protection.

13. **Stay Informed**: Stay current with the latest security threats and developments. The following are additional resources.

14. When in doubt **ask and expert**. Better safe than sorry.

Further Reading

- 11 security tips to help stay safe in the COVID-19 era - Microsoft Security
- Securing Your Remote Office (cisecurity.org)
- Stay Safe Online - Stay Safe Online
- Guide to Internet security
- Computer Security Tips