Top 10 Cyber Security Tips

1. **You are an attractive target to hackers.** Don’t ever say “it won’t happen to me.”

2. **Practice good password management.** Use a strong mix of characters, and don’t use the same PW for multiple sites. Don’t share your PW with others, don’t write it down, and definitely don’t write it on a post-it note attached to your monitor.

3. **Back up your data regularly, and make sure your anti-virus software is always up to date, install patches ASAP.**

4. **Never leave your devices unattended.** If you need to leave your computer, phone, or tablet for any length of time – no matter how short – lock it up so no one can use it while you’re gone. If you keep sensitive info on a flash (thumb/pony) drive or external hard drive, lock it up as well.

5. **Always be careful when clicking on attachments or links in email. If unexpected or suspicious for any reason, don’t click it.** Double check the URL of the website the link takes you to: bad actors often take advantage of spelling mistakes to take you to a harmful site.

6. **Sensitive browsing, such as banking or shopping, should only be done on a device that belongs to you, on a network that you trust.** Whether it’s a friend’s phone, a public computer, or a café’s free WiFi – your data could be copied or stolen.

7. **Be conscientious of what you plug in to your computer.** Malware can be spread through infected flash drives, external hard drives, and even smartphones.

8. **Watch what you’re sharing on social networks.** Criminals can befriend you and easily gain access to a shocking amount of information – where you go to school, where you work, when you’re on vacation, your birth date, address – that could help them gain access to more valuable data.

9. **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, it’s okay to say no. You can always call the company directly to verify credentials before giving out any information.

10. **Monitor accounts for any suspicious activity.** If you see something unfamiliar, it could be a sign that you’ve been compromised.