Cybersecurity Essentials

1. **Use strong passwords.**
Do not use the same password over and over. Make sure it is at least 12 characters long.

2. **Use two-factor authentication.**
This security setting sends a PIN number to your phone when you sign in to a website. This helps verify your identity.

3. **Store your passwords safely.**
It is best to use password management software. If you write passwords down, do not store them somewhere where a visitor or family member can easily access them.

4. **Be wary of "phishing."**
It is common for criminals to send emails that appear to come from friends, relatives, or companies asking for personal information. Do not share personal information such as credit card numbers over email.

5. **Don't enter login or payment information to unsecured sites.**
Secure website will display a green "padlock" icon and the text "https" in the top left of your browser window.

6. **Avoid clicking links in emails.**
Clicking links in emails can download malware onto your computer.

7. **Backup your computer.**
Backup your computer to the cloud or a physical external hard drive weekly so that you can recover files if your computer is compromised or stolen.

8. **Don't trust pop-up windows.**
Windows that pop up unexpectedly asking for login information or encouraging you to download something are almost never legitimate.

9. **Keep your computer updated.**
Software updates are important for "patching" holes in your computer's security.

10. **Don't share personal information on social media.**
Criminals often look to social media for personal information they can use to impersonate you online. Do not share location, birthdays, and similar information on social media.