## Cybersecurity Checklist:

### 11 things to do to help protect yourself from online criminals.

1. **Have computer security programs running and regularly updated to look for the latest threats**. Install anti-virus software to protect against malware (malicious software) that can steal information such as account numbers and passwords and use a firewall to prevent unauthorized access to your computer.

2. **Be smart about where and how you connect to the Internet for banking or other communications involving sensitive personal information.** Public Wi-Fi networks and computers at places such as libraries or hotel business centers can be risky if they do not have up-to-date security software.

3. **Get to know standard Internet safety features**. For example, when banking or shopping online, look for a padlock symbol on a page (this means it is secure) and https:// at the beginning of the web address. This signifies that the website is authentic and encrypts data during transmission.

4. **Ignore unsolicited emails asking you to open an attachment or click on a link if you are not sure it is who truly sent it and why.** Cybercriminals are good at creating fake emails that look legitimate but can install malware. Your best bet is to either ignore the unsolicited requests to open attachments or files or to independently verify that the supposed source actually sent the email to you by making contact using a published email address or telephone number.

5. **Allow you smartphone to work for you when using your debit card at the gas pump.** Cybercriminals will go to extreme measures to steal your identity and your bank information with the use of skimmers placed indiscreetly at gas pumps. The best way to detect skimmers is to ensure that Bluetooth is enabled on your device when at the pump. If the Bluetooth attempts to connect to a device at the pump most likely there is a skimmer in the card insert. Do not use that pump!

6. **Be suspicious if someone contacts you unexpectedly online and asks for your personal information.** A safe strategy is to ignore unsolicited requests for information no matter how legitimate they appear, especially if they ask for information such as a social security number, bank account number and passwords.

7. **Use the most secure process you can when logging into financial accounts.** Create strong passwords that are hard to guess, change them regularly, and try not to use the same passwords or PINs for several accounts.

8. **Be discreet when using social networking sites.** Criminals comb those sites looking for information such as someone's place of birth, mother's maiden name or a pet's name, in case those details can help them guess or reset passwords for online accounts.

9. **Be careful when using smartphones and tablets.** Do not leave your mobile device unattended and use a device password or other method to control access if it's stolen or lost.

10. **Parents and caregivers should include children in their cybersecurity planning**. Talk with your child about being safe online, including the risks of sharing personal information with people they don't know, and make sure the devices they use to connect to the internet have up-to-date security.

11. **Small business owners should have policies and training for their employees on topics similar to those provided in this checklist, plus other issues that are specific to their business.** For example, consider requiring more information beyond a password to gain access to your business's network, and additional safety measures such as requiring confirmation calls with your financial institution before certain electronic transfers are authorized.