HELPFUL TIPS TO STAY SECURE AT HOME

- Create strong passwords and try not to reuse the same password across multiple websites. A strong password is one that is unique and complex, such as 12 characters long, mixing letters, numbers, and special characters. Try not to use your pet's names or your children's birthdates.

- If possible, enable Multi-Factor Authentication (MFA) on as many sites as possible, as it provides another layer of protection not integrated with your computer.

- Try not to post personally identifiable information online, such as anything that can be used to answer any "security" questions on any websites. Try to be cognizant that the internet does not have a <DELETE> key, so anything posted there will always be there.

- Parental controls are available on most internet-enabled devices like computers, smartphones, tablets, and gaming systems.

- Try to use an antivirus program as well as an antimalware program and keep them up to date on all your computers and smart devices.

- Try to use a firewall and keep it up-to-date, such as your home Wi-Fi router or a firewall program, to add another layer of security for your computer and smart devices.

- You may want to disable your “Guest” Wi-Fi network and also use a strong password for your Wi-Fi network and change the password regularly.

- For any “Zoom” or video conference call, webinar, or chat, try to use a password and limit it to only the individuals you want to be on your call.

- If an “online deal” seems too good to be true, it just may be. Try to use shopping websites that you know are reputable sites that you know and trust to prevent fraud and loss.

- Protect yourself against data loss by making regular backups of your important files, such as tax returns, family photo albums, or music libraries. You can use either external devices such as a flash drive (thumb drive), an external USB drive, or an online backup service.