

## **Computer Safety and Tips**

- Make sure you have virus protection software and keep it up to date.
- Keep all software (including your web browser) current with the most recent updates.
- Keep your firewall turned on.
- Protect your wireless router with a password.
- Never put an unknown flash drive into your computer.
- Never download anything in response to a warning from a program you didn't install or don't recognize that claims to protect your computer or offers to remove viruses.
- Uninstall software that you don't use.

## **Mobile Device Safety**

- Use the passcode lock on your smartphone and other devices. This will make it more difficult for thieves to access your information if your device is lost or stolen.
- Before you donate, sell or trade old devices, be sure to wipe it using specialized software or using the manufacturer's recommended technique.
- Use your mobile device responsibly by carefully selecting which apps you download, what data you share over public Wi-fi and where you leave your device.
- Delete texts from numbers or names which you don't recognize.

## **Internet Safety**

- When shopping online, make sure your browser's padlock or key icon is active. Also look for an S after the http to be sure the website is secure. (Example: https://www)
- Use social networking safely by being selective of friend requests you accept, review what is posted about you, don't post anything that you wouldn't want on a billboard.
- Close your browser when you aren't using the internet.
- Be cautious when using public hot spots.
- Always log off from websites that require your user name and password for access.

## **Email Tips**

- Be wary of suspicious emails.
- Before you open an attachment or click on a link within an email, confirm with the sender that the message is legitimate.
- Don't respond to email or pop-up messages that ask for personal or financial information.
- Don't send personal or financial information via an unsecure email channel.
- Don't respond to emails that bring you news that seems too good to be true; it's probably a scam. Never call the phone number listed within the email, instead look it up using your own means.

## **Password Tips**

- Create strong passwords that are made up of long phrases or sentences that mix capital and lowercase letters, numbers and symbols.
- Don't use the same passwords for different sites.

- Keep your passwords secret and don't share them with anyone.
- Change your user names and password regularly and try to avoid reusing previous user names and passwords.
- Do not use your Social security number as a user name or password.
- Protect your answers to security questions where applicable.

### **Personal Information Safety**

- Don't provide your Social Security number or account information to anyone who contacts you online or over the phone.
- Protect your PINs and passwords and do not share them with anyone.
- Do not reveal sensitive or personal information on social networking websites.
- Shred receipts, bank statements, unused credit card offers, and other paper waste containing sensitive data
- Keep an eye out for missing mail such as bank or credit card statements.
- Try to avoid mailing bills from your mailbox with the flag up.
- Enroll for Online Banking for your financial accounts to closely monitor activity and detect fraudulent transactions.
- Do not sign the back of your credit cards. Instead put "Photo ID Required".
- When ordering checks, don't list a telephone number.
- Place the contents of your wallet on a photocopy machine. Make a copy of both sides of each item. In the event it is lost or stolen, you will know what you had in your wallet and all of the account number and phone numbers to call and cancel.