PROTECTING YOUR PERSONAL DEVICES

Your personal phone, tablet, or laptop likely contains a lot of personal information. A device unattended for even just few minutes could put your data at risk.

Set a Password on Your Device	♦ Change your password frequently. ♦ Create strong passwords – use at least 8 characters with upper/lower case letters, numbers and special characters. ♦ Set a short time to require the password. ♦ Enable encryption if it isn't active by default. ♦ Set auto wipe with too many failed password attempts. ♦ Change your password frequently. ♦ Consider using a Password Manager software that securely stores your passwords electronically.
Enable Security Features	Consider enabling the following features on your devices: ♦ Change your password frequently. Find My Phone ♦ Security questions/two factor authentication to make any changes to the security settings on the account associated with the device (AppleID, Google account, Microsoft account) ♦ Alerts that notify you if your account is used/access using an unregistered device
Use Caution When Using Public Charging Stations	♦ Read before you click. ♦ You could accidently authorize access to all of your data on your device, if you are not careful.

SAFEGUARDING YOURSELF AGAINST HACKERS

Phishing involves emails, texts, phone calls that are meant to trick you into sharing your personal information, including IDs and passwords, or stealing them from your device by loading malware onto your device will explode during the Holiday Season. This also goes for Facebook, Instagram, and Twitter posts.

Beware of Fake Messages

- Watch out for Delivery Tracking information pretending to be from USPS, FedEx or UPS.
- Be cautious of Order Confirmation emails for high priced items.
- Take caution with Special Sale notifications and sign-ups.
- Review the “From” field for erroneous emails pretending to be someone important.
- Scrutinize domain names as they may be slightly different.
- Take special notice to subject lines with phrases such as “extremely urgent” or “due payment”.

Use Caution Clicking on Attachments or Links

- If it is from a company you do business with, go to their webpage directly.
- If it is from someone you know, send them a message asking if they sent you the communication.

Never Respond to an Email that asks for Your Personal Information

Do Not Share Personal Information over the Phone Unless You Initiated the Call

Cover your Webcam with Tape

Enable Two-Factor Authentication

Provides a second layer of security and sends you a message if an attempt is made to access your email or a social media account.

Encrypt Websites

If sending or accessing confidential information on a website, consider protecting your data by using HTTPS Everywhere.

Protect Your Computer’s Hard Drive

Consider activating the data encryption feature on your personal device.

Use Caution with Sensitive Web Searches

Consider using an alternative search for sensitive web searches.