Cyber Security

Passwords:

- Never give your password out to anyone you don't know. Technicians should not ask for this information over the phone.
- To create a strong password, use at least one capital letter and one number or special character.
- When creating a new strong and easy to memorize password, think of a phrase and use the first letter of each word in the phrase to build your password. For example, "I like to play basketball with friends" could be *il2pbBwf*

WiFi:

- Don't use public WiFi for anything sensitive. In other words, don't do your online banking or bill paying, etc. while on a public WiFi network. A hacker could access information from your personal device.
- 3G and 4G networks are the most secure.
- Turn off the setting allowing your device to automatically connect to hotspots.
- Always log out of websites when using a public computer or public WiFi.

Email:

- Do NOT open attachments, reply to, click links in, or call phone numbers in suspicious emails. If an email appears suspicious, delete it.
- An email can be suspicious if it *appears* to be sent from someone known to you. The email address or subject line may have familiar information.
- Never answer an email that asks you to verify personal information via a link, a reply email, or a phone call.
- If you want to verify an email, find a phone number for the organization named in the email. For example, the email may claim to be from your utility company. Use an external source of information (bills, web browser, phone book) to find the phone number; do NOT use the number in the email.

Websites:

- When entering login information or any personal information, make sure the URL begins with *https* (the s means the information processed on the page is securely encrypted.) The URL is the web address displayed at the top of the web page.

Miscellaneous:

- Never use a thumb / flash drive for which you do not know the source.