BE CYBER SMART.

CYBERSECURITY IS EVERYONE'S RESPONSIBILITY

MAKE SURE YOU ARE DOING YOUR PART!

WHY SHOULD YOU CARE?

- YOUR PRIVACY ISN'T A LUXURY – IT'S A SECURITY MEASURE
- CYBER ATTACKS CAN BE SUCCESSFUL WITH LITTLE TO NO TECHNICAL KNOWLEDGE OR ABILITIES
- MOST CYBERCRIME BEGINS WITH SOME SORT OF MALWARE. YOU, YOUR FAMILY, AND YOUR PERSONAL INFORMATION IS ALMOST CERTAINLY AT RISK IF MALWARE FINDS ITS WAY ONTO YOUR COMPUTER OR DEVICES.
- TECHNOLOGICAL SECURITY MEASURES CAN ONLY PROTECT YOU SO MUCH- YOU ARE YOUR BEST DEFENSE
- CYBER SELF-DEFENSE BASICS CAN GO A LONG WAY TO KEEPING YOU AND YOUR DATA OUT OF THE HANDS OF BAD ACTORS.

TAKE STEPS TO PROTECT YOURSELF ONLINE

- Secure your networks
  - Unsecure or “open” networks allow for many cyber attacks. Protect your network by using the strong encryption (WPA2/WPA3)
  - Utilize multiple networks(i.e., guest) to control “who” can access “what” while connected.
- Use a trusted Anti-Virus/Anti-Malware software
- Keep software updated to the latest versions and set security software to run regular scans
- Double your login protection by using **Multi-Factor Authentication**
  - By enabling MFA you are ensuring that the only person who has access to your account is you!

PASSWORD CONSCIOUSNESS

Password or credential stuffing is a cyberattack that tries “stuffing” already comprised username and passwords from one site into another site in hopes that the user uses the same login information across platforms.

- Use Different Passwords across different systems and accounts
- Try to use the longest password allowed
- Always use a mix of uppercase and lowercase letters, numbers, and symbols
- Change your passwords every few months
- Use a password manager
- Utilize account compromise reporting tools(credit reporting, dark web scans, etc.)

SECURELY MANAGE YOUR MOBILE APPLICATION

- Many connected devices are supported by a mobile application
  - These applications run in the background of your mobile device gathering information about users.
- Only download apps from trusted vendors and sources
- Check and manage your app permissions
- Do not put your personal information at risk:
  - Say “no” to privilege requests that don’t make sense
- Enable multi-factor authentication on apps as an added level of security
- Update apps regularly

MANAGE YOUR INTERNET OF THINGS (IOT)

New Internet-connected devices provide a level of convenience in our lives, but they require that we share more information than ever

Each device we add to our connected world represents another infiltration point for cybercriminals

WHAT SHOULD YOU DO?

- **Change your device's factory security settings from the default password**
  - **Get creative and create a unique password for your IoT devices.**
  - **Do not reuse the same password for all devices**
  - **Not using the default password is one of the most important steps to take in the protection of IoT devices**
- **Regularly check for firmware/software updates on IoT devices**
- **Accurately manage device permissions**
  - **Have an approved list of devices which IoT devices can connect to and communicate with**
- **Consider placing IOT devices on a separate/dedicated network if available**

QUESTIONS?

DO YOUR PART, BE CYBER SMART