



## October is National Cybersecurity Awareness Month

### If You Connect It, Protect It!

The line between our online and offline lives has become indistinguishable. Technology has taken us to an always online state. Making it smaller, faster and cheaper; providing faster speeds — 4G, now 5G brings the world and all the information out there and puts it readily into our hands. This always online state offers us endless opportunities. Unfortunately, it also offers the same to fraudsters.

Follow this simple rule of thumb — if you connect it, protect it. This means that if your device connects, in any way to the internet, it must be protected. What you do depends on the device and how it connects.

#### Smart Phones:

Today's smart phones are more than telephony devices, they are full blown computers. As such, they need to be protected just like a computer. Here are some best practices you should be following:

- Setup device encryption to protect the data in your phones' storage.
- Setup up a login password/PIN/Pattern so unauthorized users cannot access your phone and its files.
- Install antivirus software. Ensure that you keep it up to date.
- Update your applications and O/S. These updates help keep your phone secure.
- Only install applications from know good sources, such as the Apple Store or Google Play.

#### Mobile Devices/Computers:

You protect these devices in the same fashion:

- Where applicable, enable device encryption to protect the data on the device. For Windows 10 PCs, think Bitlocker.
- Setup up a logon password/PIN/Pattern so unauthorized users cannot access your device. Remember to make passwords long, and complex by using letters (capital and lowercase), numbers, and special characters. Passphrases work best! Passwords should always be unique, never reuse them.
- Install antivirus software. Ensure that you keep it up to date.
- Update your applications and O/S. These updates help keep your device secure.
- Only install reputable software. Illegally installing software is a crime. These downloads can hurt your system by introducing viruses and malware.

#### Other Devices:

Smart devices, such as thermostats and smart speakers are great conveniences, but they all come with risk. Be sure that user IDs and passwords for such devices are secure and unique. Securing these devices is a special skill, don't be afraid to hire a consultant to do this. The cost is well worth the added security.

#BeCyberSmart this #CybersecurityAwarenessMonth



**Do Your Part  
Be Cybersmart!**