**Technology and Security**

The world we live in is becoming more and more technical but seemingly easier to use. That can be deceiving and you should be concerned. Along with technological advances for good comes technological advances for bad. It is staggering how easy it is to access some networks. They have no firewalls and all the devices on the network are open to anyone who understands the carrier they are using. This not only applies to home networks, but business networks and cell phones.

Now with the “Internet of Things” security is going to get more demanding.

Do you have a camera on your PC? Do you have surveillance cameras around your business or home? Are you concerned that people could hack your PC or cameras and watch what is going on?
You should be.

The good thing, or bad thing, depending on how you look at is, is that most of us are not suitable targets for most hackers. However, if you are a politician, a public figure, own a business or have good credit, you should consider taking measures to protect yourself and your business from hackers and people stealing your identity.

The Internet of Things (IOT) is really cool, but if it isn’t maintained, it can be the source of a hack. Every IOT device runs some sort of Operating System (OS) and has Firmware. That OS or Firmware will at some point need to be updated. Those updates usually aren’t to add features, but are to fix a security problem. If you fail to do the updates, you are possibly opening yourself and your business up to a threat and/or hacking. That last sentence applies to just about all technology.

The number one source of potential threats is from smart phones, mainly Android phones, but to some extent iPhones too. Each of our smart phones connect to various wireless networks, few of which are truly secure. Each time you connect and conduct any transaction that is not encrypted, your data has the potential to be captured.

Each time you download and install an APP for your phone, there is a risk that the APP may not be secure.

## What can you do?

- For your phones, make sure any connection to your business network is encrypted.
- Don’t connect to public WiFi.
- Make sure you do a Google on any APP you want to download and install to make sure there are no known issues, this is particularly important with Android devices.
- Install AV and anti-malware software on all devices, especially your phones.
- Make sure there is a way to “Brick” your phone if necessary and that you know how to do it. “Bricking your phone makes it unusable and most phone companies have a way to accomplish that. Contact your carrier for this information before you are compromised!