The "Internet of Things"

A consequence of our ever increasing interconnected world is that the "things" in our lives know us, track us, know where we are, how we got there, what we are doing. The "things" in our lives leave a digital trail of our "life's breadcrumbs."

Your safety can now depend on a password. Have you made it hard enough to keep people from gaining access to a car, a home or a computer or phone? Has your Wi-Fi become another door that a criminal can enter through? While you cannot be responsible for the quality of products in your world, a change of habits can limit your risk of harm when you use them.

As an example, if you put all of your wealth in a strong metal box, what kind of lock would you choose to secure it? A simple gym locker padlock or one that your bank uses to secure their own vault.

Even conveniences like a Bluetooth headset for a phone can let others listen in on your conversations if not set up securely. Technology can be a convenience but it carries a responsibility to learn how to set it up correctly. If you cannot, get professional help. Use it responsibly and maintain it properly Today's cyber criminals can be hiding behind you at the coffee house or on the other side of the world.

Community and Education Since 1969
Central Florida
Crime
Prevention
Association

emal@cfcpa.org

www.CFCPA.org

**Central Florida Crime
Prevention Association
P.O. Box 432
Goldenrod, FL 32733**

Central Florida Crime Prevention Association

Staying Ahead of Crime

Staying Safe in an Interconnected World

Form 8-2016

We live in an interconnected world. Invisible networks like the Internet connect everyday devices. Wi-Fi is in our cars, home security, cameras, thermostats, locks, phones, appliances, cable TV boxes, medical devices, even door bells. Even simple things like Bluetooth, garage door openers, car keyless remotes are all wireless networks. And all networks can pose risks to your personal safety.

So What is the Risk?

Any device, when connected to a network, can be breached. We call this hacking. It simply means that if you have a Wi-Fi enabled lock on your front door, your network connection has become an entry point into your home. A criminal can enter your home through its connected devices, taking personal information like banking passwords, control the devices to know if you are home, even gain physical access to your home and control your locks. When you are interconnected, sharing your habits, your whereabouts, can pose a risk to personal safety or the safety of your family members. Even a photo shared through social media can contain your exact location. Post that you are on vacation and you might be broadcasting that your home is empty.

Staying Safe

Here are some basic rules to follow that reduce the risks associated with interconnectivity:

Passwords: They are your primary defense against hacking. Use long complex passwords. Upper, lower case, include numbers and special characters. Change them frequently on your financial accounts. Never use common names or words that can be associated to you. Never share them, never use the same password for everything.

Factory Default Settings: Never leave devices such as a router, phone, earpiece, or computer set with the factory logins and passwords.

Update your devices regularly: Hackers take advantage of vulnerabilities in software. When a manufacturer sends an update to fix security problems, use them.

Wi-Fi: For your home Wi-Fi use the most secure settings (WPA2) and a complex password. Hide your network name (SSID) so others cannot find your Wi-Fi easily. Be very wary of free Wi-Fi spots. Make sure your phone, tablet or computer have firewalls that protect you. Never keep highly confidential information on a device if you use free Wi-Fi.

Bluetooth: This is not a secure network. It was meant to attach peripherals to smart devices. Never leave them in “pairing” discoverable mode and don’t use the default pairing PIN. When you no longer need a Bluetooth Connection, delete it.

Keyless Entry: While short in range, they can be intercepted to capture entry codes. Be aware of anyone suspicious nearby and consider using your manual key.