Welcome to week 4 of National Cyber Security Awareness Month! This week's topic is "Your Evolving Digital Life". We will concentrate on all of the gadgets and devices that we can now connect to the Internet, from watches to coffee pots to refrigerators. We will also discuss issues with a security technology we use every day and don't even think about - the key fob for our cars.

It used to be that the Internet was just something that people, using devices such as desktops and laptops, connected to for information and to share ideas. Now, almost anything can be connected to the Internet, even things we would not normally think about being "Internet ready". Refrigerators are now available that allow a user to look up recipes or check the weather while standing in front of them. There are coffee and tea pots that are Internet connected, allowing the owner to start them up from their phones. While it might be convenient to start a pot of coffee from the road before you get home, it is not necessarily a good idea to turn on unsupervised devices containing heating elements. All of these devices must connect, usually using wireless networking technology, and few of them offer any kind of real security. Recently, a flaw was discovered that resulted in certain Internet connected tea pots to expose the wireless network password used to connect it to the owner's home network.

While on the topic of home networks it would be prudent to mention that all consumer wireless routers have default passwords set by the manufacturer that should be changed immediately when they are first set up. The same goes for any similar device - if it grants access to something, it should not use a default password. Be sure to check the documentation for the proper procedure to reset the default password.

When was the last time you worried about the security of your car's remote lock key fob? For most people, the answer is never, but recent advances in technology now potentially render vulnerable over 90% of the current keyless entry systems installed in cars. The attacker must have physical access or be in close proximity to the car, but the process is simple and the cost of the parts is under $40. It is unlikely that current cars will ever receive an upgrade to correct this problem, so here are some tips to reduce this threat.

- Whenever possible, you should park in secure environments like enclosed garages.
- Understanding that the previous tip is not practical for most people, you should at least avoid parking cars in remote, isolated areas.
- Every so often, perform a visual inspection of your car, particularly underneath it. The device required to circumvent the keyless entry system must be placed on or near the target car. Anything that looks out of place should be more closely inspected, particularly if it has exposed circuitry or looks "homemade".
- Be aware of your surroundings as you approach your car. The current version of this device requires some human coordination to circumvent the security, so be aware of people lurking in the area or sitting in parked cars. This is also good advice in general for your physical safety.

With everything starting to connect for various reasons to the Internet, our digital lives will continue to evolve and we must make an effort to stay aware of the risks involved.