Internet-Connected Devices or the “Internet of Things (IoT)

Devices connected to the IoT include routers, printers, thermostats, refrigerators, webcams and home automation hubs powered by artificial intelligence, such as Amazon Alexa and Google Assistant. There are also smart locks, smartwatches and many more gadgets that we keep at home, carry or even wear. If an internet-connected device performs a non-critical function, why does it need any cyber security at all? Put differently, are security measures necessary only when a device might cause harm if it is hacked? Why would you still want to secure something like a garage door opener?

Because any IoT device can be the target of a hacker, and any hacked device can be weaponized.

The Mirai botnet involved approximately 150,000 internet-enabled security cameras that were hacked and turned into a botnet which launched a distributed denial of service (DDoS) attack that took down internet access for a large portion of the eastern United States.

Manufactures with added internet connectivity to devices we sometimes use means that a single remote attack can scale to hundreds of thousands or millions of devices. Once the decision is made to connect a device to the internet, that device has the potential to transform from a single-purpose device to a general-purpose computer capable of launching a DDoS attack (an incident in which a network of computers floods an online resource with high levels of unwanted traffic so that it is inaccessible) against any target in the world. The Mirai botnet is also a demonstration that a manufacturer does not need to sell many devices to create the potential for a “weaponized” device.

Minimum security settings do not guarantee that a device will not be hacked. However, they greatly minimize certain types of attacks and make it possible to detect and respond when a hacker gains a toehold in your network. If a device doesn’t have security settings,

human practices must be implemented to compensate for the missing features.

Why Should We Care?

- New Internet-connected devices provide a level of convenience in our lives, but they require that we share more information than ever.
- With more connected “things” entering our homes and our workplaces each day, it is important that everyone knows how to secure their digital lives.

Simple Tips

- If You Connect IT, Protect IT. Whether it’s your computer, smartphone, game device, or other network devices, the best defense is to stay on top of things by updating to the latest security software, web browser, and operating systems. If you have the option to enable automatic updates to defend against the latest risks, turn it on.
- Only download apps from trusted vendors and sources.
- Some best practices for implementing IoT security settings
- Change default passwords and credentials
- While this advice may seem like common sense, it's important to note that criminals are aware of the default password, and they will use that to gain control of the device. Passwords continue to be the weakest link in the IoT, or any other network connected device.
- Consider updating your IoT device’s software. Many manufacturers are aware of the security risks and provide updates to their device’s software that can prevent your device from being hacked.