IDShield℠

Investigator Insights

The Internet of Things & Security

It's that time of year when the latest technological advancements get a lot of attention and we see the expanding of the "Internet of Things" (IoT). Perhaps you purchased a personal fitness tracker or read news about internet-connected cars—VW brand chief Herbert Diess recently referred to their new all-electric, internet-connected car as a "smartphone on wheels" when it was spotlighted at the Consumer Electronics Show.

Designed to share information with the purchaser, another internet-connected device or a service, a wide variety of these gadgets exist, including but certainly not limited to:

- A refrigerator that takes photos of its contents each time the door is closed so the owner can check the photos while shopping to determine if a particular item needs to be purchased. And, the fridge integrates with an online shopping app to allow for grocery purchases and deliveries.
- A home lighting system that analyzes your lighting use patterns and mimics them when you are away from home so it's not obvious to outsiders that you are away.
- A health/fitness tracking device that records your exercise activity and sleep rhythms while allowing you to connect with friends also using the device.
- A home monitoring system that allows you to lock/unlock doors and program your thermostat remotely.
- Children's toys such as *Hello Barbie*—a Wi-Fi connected doll with which your child can have a fairly impressive conversation.

What's the goal of these internet connected devices? Supposedly, lives will be enhanced by what these devices can accomplish by sharing data between each other and with the consumer. But, let's look past the bells and whistles for a moment and ask what should be considered when purchasing an internetconnected device. Are there factors that could impact your privacy? Could someone other than you access the device or the data the device collects?

In a recent public service announcement, the Federal Bureau of Investigation (FBI) warned that "weak security capabilities" and "lack of consumer security awareness" can provide criminals with opportunities to exploit these devices. The PSA goes on to list the theft of personal information as one of the potential risks of a connected device.

The primary tip that the FBI shares in their announcement is that you must change the default password that was assigned to the device by its manufacturer. Passwords supplied by the manufacturer may be discoverable on the internet. Create and use a new, unique, strong password as soon as you connect the device to your network.

Other advice includes:

- Isolate IoT devices on their own protected networks
- Disable Universal Plug and Play (UPnP) on routers
- Purchase IoT devices from manufacturers with a track record of providing secure devices
- Update IoT devices with security patches when they become available

- If a device comes with an open Wi-Fi connection, only allow it to operate on a home network with a secured Wi-Fi router
- Consider whether IoT devices are ideal for their intended purpose

Keep in mind that you are the first line of defense. Heed this advice and see more helpful tips in the FBI's public service announcement at: http://www.ic3.gov/media/2015/150910.aspx