The Internet of Things

Rod’s just had a smart thermostat installed. It’s connected to the internet which means he can control his heating remotely with his smartphone from just about anywhere.

Smart devices which are connected to the internet like this, are part of what’s known as the Internet of Things or IoT for short. Some are frivolous, some are useful, and others are potentially life saving. But there’s a problem.

Many of the devices have poor security and cybercriminals are taking advantage of it. Let’s have a look at an example of how easy it can be for hackers, in this case ethical hackers, to get into someone’s network and gain access to all the devices that are connected to it.

A smart kettle connects through Wi-Fi to an app on a smartphone which is used to control it. Access to the kettle’s software is password protected, but the password is in the manual and available to everyone. Using this the ‘hackers’ were able to connect to the kettle and communicate with it.

They found that they could get the kettle to ask the router for its password and therefore they could connect to the network and access anything else on it, including personal and private information and any other networks it’s connected to - such as a work intranet.

But realistically, what are the chances of this happening?

Well, they would be very slim, except that the kettle, like many IoT devices, was on a database. And this particular database shows the locations of all the other kettles which can be hacked in the same way.

This is a simple, but real, example of how criminals are gaining access to our devices and information. Often in ways which we can’t imagine and don’t fully understand.

Later versions of the kettle had much tighter security. But one of the problems at the moment is that there are no set security standards.

Another way IoT devices are being used is in what’s known as a distributed denial of service attack. Here’s how it works.

Essentially an IoT device is a small computer which is connected to the internet, and can therefore be infected with malware just like any other device.

One piece of malware was designed to find IoT devices which could be compromised and infect them with malware. The malware sent the device’s details back to a command and control computer, and then moved on to find the next device.

In this way, thousands of devices were infected with malware which enabled them to be controlled remotely and without the owners knowing. This is known as a botnet, and this particular botnet was used to overload a server by sending it so many messages that it couldn’t cope and it stopped functioning properly.

This may sound far fetched, but these attacks are happening regularly.

The motivation behind them varies but includes hackers testing their skills, activists making political or social points, criminals extorting money, and state sponsored agents attacking large scale infrastructures such as power grids.

If a device can communicate with another device, there’s always the potential that it can be hacked and provide a way into the network the device is connected to. Just as with a house or any other property, a network is only as secure as its weakest point of entry.

We’re used to locking out criminals as best as we can in other areas, and here are some things you can do to protect yourself, and to protect your devices from being used by malicious agents.

Make sure you’re aware of all the IoT devices you have and beware of older products which tend to have little or poor security.

Replace any default passwords with strong, unique ones.

Keep the device’s software, which is known as firmware, up-to-date and avoid devices which can’t be updated.

Also check the product’s, and manufacturer’s, reputation for internet security before you buy.

The Internet of Things brings many advantages. It’s growing rapidly and is being used to create smart cities, businesses and homes. Being aware of the ways these devices are being exploited, and taking simple precautions, will help keep workplaces, homes and families better protected.