IoT (Internet of Things) Security

In our March 2019 Newsletter there was an article about IoT devices – smart household devices such as printers, cameras, smart TVs, nanny cams, appliances, light globes and switches that connect to the internet via your home network.

Many of these devices are insecure. If a hacker broke in to any one of the devices on your network, he or she would have "back door" access to every device on your network, including your PCs and smart phones etc. The hacker would have access to the personal data that these devices that flows to/from the internet and data stored on the devices.

So, not only is it essential to keep your computers secure, but as more and more IoT devices are connected to your home network, it is increasingly important to keep each of these devices secure as well.

The mind boggles!

Avast Smart Home report February 2019

Avast found that at least a third of Australian homes are wide open to cybercriminals via insecure IoT devices! If you have five smart devices, at least one could be insecure.

Avast also scanned 11 million routers worldwide. It found that 59.7% either are vulnerable and 59.1% had never accessed the admin page on their router to update the firmware Out-of-date software/firmware is often the weakest link in the security chain.

Surprisingly, the most common insecure device found by Avast is printers connected by WiFi.

Unfortunately, nothing you install on a home computer or phone can protect the network as a whole - you need to take some extra steps to protect it.

1. **Check the device security**
   Before you purchase an IoT device, check out its security aspects.

2. **Access passwords**
   These devices come with a default administrator username and password that give access to the devices settings, firmware updates etc. Hackers are well aware of these default settings. You should login to the device and change these defaults, otherwise you are leaving the device and your network wide open.

   You should secure your modem/router first by changing the default admin password, and the default Wi-Fi access key (see below).

   And whenever you get a new IoT device, change the default admin password, and the default Wi-Fi access key (done using the device's app or manufacturer's web site).

3. **Firmware**
   All devices have some built-in code called firmware. Firmware is what to device uses to communicate with your operating system or home network. Firmware is different to drivers and apps.

   Firmware can have security holes, so updates are often provided (these updates would probably require your approval. They may be installed automatically, or you may have to manually check and do them using the app that comes with the device.

   Updating firmware is a two-edged sword. Modern firmware installs are quite reliable, but if something goes wrong such as a power failure while the device is updating, it can render the

device inoperable. But these days we need to keep firmware up to date!

EuroSCUG members may remember the talk by Adrianna Shepherd from Cartridge World, Batemans Bay advising not to update firmware on printers because some manufacturers are making changes to prevent the printer accepting cheaper cartridges. In this case, you need to decide if security is more important.

4. **Software**
   Each device would have an app or web site associated with it that gives you control. The device may also have a software driver installed on your PC. You may receive security updates to these apps which you should allow to run automatically.

5. **Summary of basic Security steps**
   - Set strong and unique access passwords on your devices, starting with your modem/router
   - Check for and apply software patches and firmware updates periodically.

Changing default passwords on your Modem/Router

Some modem/routers cannot easily be accessed, you need to check the modem manual to see if (a) you can change anything, and (b) How to do it.

The two of passwords of interest here are ***Modem/Router administration*** password and ***Wi-fi*** password***.***

Modem administration: Access the settings for your modem/router via a web browser or an app provided by the manufacturer or Internet Service Provider. You need a modem admin username and password to access or change your modem settings.

For most people the modem default settings will be something like username: *admin*, password: *admin*. <u>If you change this default admin password, make sure you remember it.</u>

Wi-Fi Network and Password: These settings are used when a device connects to your Wi-fi. The Wifi network has a label called SSID—the default SSID name is often something like "Netgear2536", or "D-link". The SSID name can be changed in most modem/router settings to a more meaningful name like "Julie's Modem" or "26 Freda Place". Associated with the SSID is a password (also called passcode, passphrase, or security key) which the modem requests when a new device wants to access your WiFi.

If you change your Wi-fi password, devices you have previously connected will no longer automatically connect. You need to reconnect them all using the new password.

You may also find that your Internet account username and password is shown on the admin screen. (This what the modem/router uses to connect to the internet via your Internet Service Provider). *Don't try to change your Internet account username/password.*

More advanced network security

Fingbox

This is a simple device that plugs into an Ethernet port in your existing router. There is a Fing app that you install on your phone that communicates with the Fingbox. All you have to do is set up a Fingbox account then away you go. The app lets you know when a device connects to your home network and gives you the option to block it. You can also set it to automatically block any unknown device- it lets you know and you decide to approve it. Features are:

- ***Catch Intruders and Hackers***
  Real-time intruder and hacker alerts means 24/7 monitoring of your network and devices.
- ***Detect Vulnerabilities & Threats***
  Advance warning of vulnerabilities on your network including opened ports, public IP addresses or missing firewalls.
- ***Set Parental Controls***
  Limit internet access and encourage digital downtime for the children and adults on your network.
- ***Know who's Home***
  Assign users to specific devices and know who's home while you're away. Observe unknown devices near your home, even if they're not connected to your Wi-Fi.
- ***Analyze Internet and Wi-Fi Speeds***
  Discover the Wi-Fi speed in specific parts of your home and run automated speed tests to rate your ISP against the competition.
- ***Identify Bandwidth Hogs***
  Analyse the bandwidth Internet megabytes) consumption of your devices to find out what's slowing down your network.

Fing box is available for $149 from https://au.fingbox.com/

Circle With Disney

If you don't have a router with an Ethernet port, a product called *Circle with Disney* is very similar to FingBox but it uses a WiFi connection.
Available from JB Hi-Fi for $99.

D-Fend AC2600 Wi-Fi Router

This is an expensive device (around $500) that provides very good network security. It connects to your current modem/router and monitors all internet traffic using McAfee Secure Home Platform, providing automatic protection for all network devices. The purchase includes free 5 year subscription to McAfee Secure Home Platform. Check with your Service Provider whether this router will work with your internet plan and how to configure your existing modem.
Note that the McAfee Secure Home Platform is a different product to the McAfee security app that runs on computers/phones. It is pre-installed on the router.

For further information, see
https://www.dlink.com.au/home-solutions/DIR-2680_D-Fend_AC2600_Wi-Fi_Router
https://securehomeplatform.mcafee.com/

Sources:
https://www.gadgetguy.com.au/product/review-fingbox-dont-fing-online-without/?display=all
https://www.gadgetguy.com.au/avast-ye-landlubbers-cyber-pirates-can-pillage-your-smart-home/
https://www.gadgetguy.com.au/five-steps-to-secure-your-iot-home-network-you-need-to/
https://au.fingbox.com/

John Allen