INTERNET OF THINGS DEVICE SECURITY

CYBER SECURITY AWARENESS MONTH 2020

WHAT ARE IoT DEVICES?

Internet of Things devices (known as IoT devices) is a common catchall name for day to day devices that have been given a way to connect to the internet. IoT devices communicate and interact over the internet and some have the ability to be remotely controlled and monitored. In the UK, it is reported that around a third of households have more than five IoT devices from IoT watches, radios, doorbells, TVs, toasters, and lights.

By 2025 there are globally expected to be 64 billion IoT devices in use. Of course, growth does carry several benefits at supporting our everyday lives, but, as soon as you connect anything to the internet, security and privacy issues are going to arise and it's important you are aware and know how to manage them.

Many low budget IoT devices utilise little to no security in order to keep costs down. This is one way security issues can emerge.

WHAT ARE THE SECURITY ISSUES?

Limited / No software updating tools: Updates are critical for maintaining security in all devices, but IoT devices even more so. Many IoT devices come without the ability to perform automatic updates. Because many devices are low budget, manufacturers either do not implement this or they stop supporting the device entirely when a new model is released. It is important to check to see if you can update your device.

Default / Weak passwords: Many IoT devices come with default passwords. It is important that you change this default password, because default passwords are often easy for cyber criminals to get hold of. It is important to recognise here that this is not the password you use to connect to the IoT device but the password that protects the IoT device. When buying a IoT device, it's important to check if you can change the default password.

INTERNET OF THINGS DEVICE SECURITY

CYBER SECURITY AWARENESS MONTH 2020

Knowledge and awareness: IoT devices are a new technology and therefore we can't be expected to know everything. Although the majority of the security issues are manufacturing issues, the way we as individuals interact with them can open up vulnerabilities, which is why being informed and aware is so important. Social engineering attacks will almost certainly begin to target IoT devices. Cyber criminals follow the numbers: the more popular a technology or app is, the more criminals will target it.

Eavesdropping: IoT devices can have the capacity to listen and record conversations, so it's important to be careful what we say in front of them.

CASE STUDY

Ring cameras have been accused of multiple breaches. In one case, 4 days after a camera was installed, an attacker allegedly hacked into the camera and began talking to an 8-year-old girl. Ring did not implement two-factor authentication for customers or require them to establish a complicated password when setting up their device. Both these security flaws are common routes that criminals take advantage of when targeting IoT devices.

TOP TIPS

- ✅ Check if your IoT device has automatic updates enabled, if it doesn't then enable updates if you can
- ✅ The National Cyber Security Centre (NCSC) recommend that your password is made up of three well-chosen random words. For example: fogautumngoat. Be sure to include numbers, capital letters & symbols: F0g@utuMnG0@t.
- ✅ Many IoT devices now offer two-factor authentication, its important you enable this as an added layer of security to help protected you in case the password for your IoT device gets compromised. For more information on passwords and 2FA, read our recent account security guide.
- ✅ If you receive a communication that you're not expecting (whether by your IoT device, Whatsapp, email, phone call, SMS message or any other way) that is asking you to do something and makes you feel emotional (rushed, happy, panicked, embarrassed or anything else), be aware this could be social engineering.
- ✅ When having private conversations, be it for work or personal, be aware of IoT devices that could have a listening feature enabled.