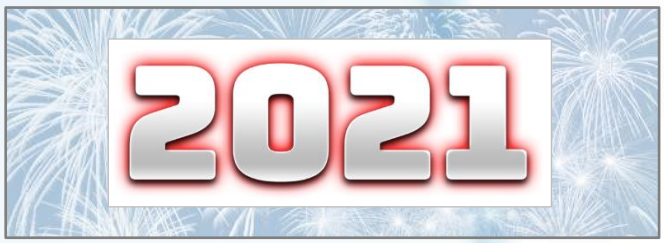
CYBER AWARE

Securing Your Devices

Surrey & Sussex CCU Newsletter



Happy New Year to all our readers! We trust you had a restful festive break after a very unusual year. Almost certainly, many of you will have received some sort of 'electronalogical' gadgetry for Christmas – ranging from computers and mobile phones through to 'Internet of Things' or 'IoT' devices like IP cameras, Home Automation Systems and doorbells. We are here to help get this IoT kit secure so you can make sure you are the only one using them!

What devices do I need to be concerned about?

Security needs to be considered for every device you have. And particular care needs to be taken if it connects to the Internet and accesses online accounts.

Unfortunately, security still isn't very high on the priority list for many companies. One of the biggest issues with IoT devices are those that use default or weak usernames and passwords. If these are not changed, cyber-attackers can access them in the same way that you might. It is also important to understand how the device can be accessed, how you connect to it etc. Remember – if you move to a new house, or your residential circumstances change, you should also consider changing these credentials to prevent previous residents from accessing them.

What are the risks?

It depends on your device. If your heating control is compromised, someone may turn up the heating or turn it off – probably not too serious. If your smart doorbell is compromised, someone could watch comings and goings to your house and potentially listen to conversations in its vicinity. This might cause you an element of concern. If your baby monitor or child's GPS watch gets compromised, things could get a lot more serious. The safest thing to do is to secure all your devices – and the online accounts they access – to prevent any problems.

How do I secure these devices?

The main thing to consider here is the username and password combination – or credentials. Check your product manual to see how to change them. Sometimes you can't change the username of a device but you should always be able to change the password. A strong password is longer than 12 characters, consists of 3 random words and can be strengthened by including capitals, numbers, and symbols. All passwords should be completely different. Here are some examples of a strong password: -

GOOD: DurbanPalmMountain

BETTER: DurbanPa1mM0unta1n

BEST: ~DurbanPa1mM0unta1n!

Are you interested in a free cyber awareness presentation? Our Protect & Prepare team can deliver online presentations to businesses and other groups (20+ attendees) across Surrey & Sussex. These are approximately 1 – 1½ hours in duration and cover a range of current cyber topics.

Please e-mail CyberCrimeUnit@surrey.pnn.police.uk for further information.

SEROCU: serocu.police.uk/cyber | Cyber Aware: www.ncsc.gov.uk/cyberaware | NCSC: www.ncsc.gov.uk

CYBER AWARE

So how do I change these details?

The best place to start is to read any instructions that came with the device. Even though these are often woefully inadequate, they often give an indication as to how to access the device. Sometimes, you may need to download an 'App' to access it. Others may be accessible through your web browser – like your home router. Many devices are compatible with other products such as Amazon Alexa, Apple HomeKit or Google Home so you can control them from your mobile phone.

Remember to store your new usernames and passwords safely and **ALWAYS** factory reset devices you buy second hand or inherit from others.

Device Updates

IoT devices will always have some sort of operating system or code to make them work – often called firmware. Responsible vendors will regularly update this code to enhance security or provide additional functionality. As with your mobile phone and computer, it is always worth updating this firmware to make sure you have the latest version installed.

Why would anyone want to access my IoT devices?

There are many reasons. If organised criminals can compromise these devices, they can use their Internet connectivity to help in Distributed Denial of Service or 'DDoS' attacks. This is when the device becomes part of a 'BotNet' (short for 'Robot Network') and is remotely controlled by an attacker to cause interference with other networks or websites.

Script Kiddies, or unsophisticated hackers, will try and access these devices for fun – or just because they can. This can have unintended consequences, particularly for vulnerable individuals like the elderly.

At a domestic level, control of IP cameras & doorbells could enable someone to watch and listen to a person, and GPS enabled smart devices could be used to obtain real-time locational data for them.

What other security measures should I take?

Many of these devices will be associated with an online account – for example, a FitBit device will store your exercise and personal information in the cloud. As with any other online account, a strong password should be used, and 2-factor-authorisation set up wherever possible. You should also ensure your privacy settings are updated to avoid unintentional sharing of personal data.

As all your devices will be connecting to the Internet through your home router, make sure this is also secured with a strong encryption method like WPA2. Set a strong Wi-Fi password and limit access to your network to trusted individuals.

Where can I get more information?

https://serocu.police.uk/cyber

https://serocu.police.uk/individuals

https://serocu.police.uk/cyber-domestic-abuse

https://www.ncsc.gov.uk/cyberaware

https://www.ncsc.gov.uk/section/information-for/individuals-families

https://www.ncsc.gov.uk/guidance/smart-devices-in-the-home

Are you interested in a free cyber awareness presentation? Our Protect & Prepare team can deliver online presentations to businesses and other groups (20+ attendees) across Surrey & Sussex. These are approximately 1 – 1½ hours in duration and cover a range of current cyber topics.

Please e-mail CyberCrimeUnit@surrey.pnn.police.uk for further information.

SEROCU: serocu.police.uk/cyber | Cyber Aware: www.ncsc.gov.uk/cyberaware | NCSC: www.ncsc.gov.uk