Community Cyber Ambassador Newsletter (Vol 6. September 2017)

Creating a safer
Cambridgeshire

Your computer and mobile devices are the gateway to your online world and most people would agree that their lives would be inconvenienced if one or more of their devices were lost, stolen or disabled.

For a criminals however a lost or stolen device can provide an opportunity to make money with many now realising that the information *on* - and accessible *from* - the device such as private data, confidential emails, login details, data on apps, financial information etc can also have a value.

In August 2017, ITV's tonight programme showed how easy cybercriminals could gain access to smart devices in a home by hacking into the Wi-Fi network through an unsecured router. Changing default passwords/PINs on devices (where applicable) can make it more difficult for hackers to discover them.

To see what the hackers did next and for further information about the programme visit: http://www.itv.com/news/2017-08-24/tonight-can-crooks-hack-your-home/

Your home will have at least one form of physical security to prevent criminals from gaining easy access and steal your property and you would look to update your security if you found a weakness (e.g. a broken lock is a weakness and should be fixed immediately). The same principle should be applied to the security around your connected devices within the home (e.g. the previous broken lock example is

Top tips for protecting your connected devices

- **Always** have internet security software loaded, switched on and kept updated on your computer. Download security apps on all your mobile devices too, including Apple devices.
- **Update** software and apps when prompted, including operating systems as these often contain security updates.
- **Think before you click.** Clicking on email attachments or links in emails and social media posts could infect your devices with various types of malware, including ransomware and spyware.
- **Never** give a cold caller remote access to your devices as this could compromise or even disable them. Only an authorised support person who **you have contacted** with a problem, should be allowed to gain access.
- **Always** protect computers and mobile devices with a PIN or password, even if they come with biometric protection.
- Some data and photos are irreplaceable. Back up all your devices regularly in case they become unusable or get lost or stolen.
- Other connected wearable (Smart watches) and household devices (televisions, CCTV cameras etc.) can also be compromised by hackers. To prevent hacking always set a new password or PIN (where applicable) when setting your device up for the first time.

For more top tips on protecting your connected devices visit - www.getsafeonline.org/devices

the equivalent of having no pin/ secure password on your devices)

While criminals are one threat to our connected devices accidents and malfunctions can and will happen and there is a high probability that at least one or more devices in your home might experience at least one of these in the future potentially leading to the loss of your data on the device or a large bill to repair and retrieve the information. Making a regular backup of data that is important to you i.e. photos, music files, documents etc. to a hard drive/USB/DVD and testing the backups will allow you to enjoy your files should the worst happen to your device.

Get Safe Online has a list of top tips to help you protect your computer, smartphone and tablet from not only malware and unauthorised access, but from physical loss and damage too.

You can view all of them at - www.getsafeonline.org/devices

Breaking news

Earlier this week it was confirmed that CCleaner a popular anti-virus programme had been the subject of a malware infection which compromises the security of the machines it is installed on. The tool is used by millions to keep their Windows PCs running smoothly.

CCleaner users have been warned to immediately install the latest version of the software and perform a system scan using the anti-virus software.

Tony Neate, CEO of Get Safe Online, says*: "It's ironic that a tool which is trusted by millions to perform good routine housekeeping on their Windows PCs – including helping to protect their privacy – could now be planting illicit software on their machines which compromises it.*

"In this particular case, it would be difficult for a user to detect that they had downloaded a version of the manufacturer's own software that was infected. However, it does reinforce our advice about setting up automatic updates for all your software and operating systems, and having the best security that you can afford in order to avoid problems."

For the full story and advice on what you should do now visit - www.getsafeonline.org

Next month is **Get Safe Online Week** which will start on 23/10/2017 and will be focused on Phishing. Cambridgeshire Constabulary will be promoting advice on how to keep yourself safe from phishing scams but please do support GSO week by helping us to spread one other message or top tip on how to stay safe online among your community, family and/or friends.

October's newsletter will feature the top tips on keeping yourself safe from Phishing scams.