Online safety in public locations

This document seeks to provide some guidance on the safe use of web compatible devices in public locations like coffee shops, hotels, shopping centres and public houses. It also indicates the risks of enabling Bluetooth in certain situations.

Public or unsecured wifi

When you use a wifi network in a public location, you are effectively logging into a Wireless Access Point just as you would do at home or at work. This isn't inherently risky. However, some of these networks are unsecured. This means that the movement of data across the network takes place without any form of encryption. A capable hacker is able to use software to pull that data directly from the airwaves and store it for future use. Some people understand this risk but assume that providing they don't visit data sensitive sites like banking applications or corporate email, that this risk is acceptable. What they aren't aware of is that the device is likely to be performing background handshakes between applications and the websites that host that data. Thus, although they may not have accessed their email, their email client could be passing their credentials to the website in the background. This makes the password available to a potential hacker.

The key to spotting an unsecured wireless network is the requirement for a password. If there is no password requirement, the network is unsecured. This approach is most ubiquitous in large area wireless networks, such as those deployed in shopping centres, airports and hotels. It is strongly advised that you don't connect to networks of this type. For absolute peace of mind, it is also advised to disable wifi on your device when in range of a network of this type because there is a risk that you have previously connected to a similar network and that your device will remember the connection and reinitialise it.

Wifi honeypots

There is a growing trend for hackers and cyber criminals to set up false wifi networks in key locations. These may mimic the name of the establishment but will generally be unsecured networks. The hope is that people without the establishment's access credentials will spot an open network and connect to that in preference to finding out the password from staff. Having done so, the hacker will intercept all data transferred over that network. Where there is a public and secured network available, it is always advised to connect to the secured network only.

How it works

When your device transfers data to a website it natively does so in plain text format. This is a simple file that just contains the text of the data requested. A password will be clearly visible as will a login ID. When you use an encrypted network, the network itself will scramble this text using a specific algorithm which means that if it is intercepted before it is received by the website that it will be unintelligible. This is why hackers prefer unsecured networks. It is technically possible to take encrypted data and decode it but this is time consuming and, depending on the protocols used and the age of the device, it can be extremely difficult.

As well as log-in data, using unsecured wifi can also carry a risk of some or all of the following issues:

- General interception of data: Including corporate data, intellectual property, media files and the content of all messages from email to instant messaging.
- Viral infection: Having a number of devices available is the perfect way to create what is called a botnet – a chain of linked devices all carrying a malicious piece of code intended to perform a single task. Essentially, the hacker plants a virus on the devices which then are

used to stage a Denial of Service attack on a website or network. The actual attack may not happen for days or months after the virus has been planted meaning that the device owner is very rarely aware that this has happened. A secondary risk is the spread of a ransomware virus where a device is immediately locked and the user is asked for payment to unlock it.

- Bandwidth theft: Most devices hold connection data about multiple networks. This may include your corporate network. In theory, a hacker in range of that network could use those credentials to piggyback on corporate bandwidth or decide to overload that network with multiple connections.
- Using a corporate network for illegal activities: Having gained access to a corporate wifi network, a capable hacker can use it transmit or host illegal activities. This is a common ruse in the transmission of child pornography, the hosting of terror related videos and the transmission of hate speech.

Additional steps to secure privacy

1. Manage your privacy carefully: Hackers are clever and will use anything available in the public realm to clone your identity. Restrict what you make publicly available on social media and carefully manage who you connect to and why. If your device comes with file sharing capabilities, police the settings on these as closely as you can.
2. Restricting device transmissions and Bluetooth: Always keep the "network discovery" settings on your device switched off. These are the easiest way for a hacker to locate your device. For similar reasons, you should keep Bluetooth switched off unless you are in a private place or are moving. Generally speaking, using Bluetooth to connect to your car or to headphones is OK so long as you are moving. Otherwise, your device can be detected within a range of 3m.
3. Use secure connections: Set your browser preferences to use secure transmission protocols such as SSL (Secure Socket Layers) or TLS (Transport Layer Security). This will force your browser to only use sites that display an https:// prefix before the web address, together with the locked symbol. This offers a much higher level of security. You can also download extensions for most devices called "HTTPS Everywhere" which forces a secure connection with every site. The downside of this latter approach is that not all sites have an SSL license so that some web pages will not display if you adopt this approach.
4. Use a VPN: You can establish a VPN connection to the internet on any device. This is a strongly encrypted connection and is difficult to penetrate meaning that hackers tend to move onto easier targets. You can download VPN clients from most major app stores.
5. Firewall and anti-virus: Make sure your device has good protection. Church in Wales devices will ship with a standard firewall and anti-virus software but it is incumbent on the user to ensure that the updates are carried out. For personal devices, it is advisable to use something like AVG or McAfee even if it is only in the free versions. These can be downloaded from most major app stores.

If you require assistance changing any of your settings or wish to improve the security of your device, please contact the IT helpdesk for all Church issued equipment. For personal devices, please contact your provider.

Leon Hughes, Head of Communications and Technology. May 2018.