Zeiss field machines, public Wi-Fi risks and IoT scanning

End of support for old field machines

Zeiss have recently announced that they are withdrawing support contracts for many of their older 7 series Humphrey Field Analysers (HFAs) in November 2017. They have confirmed maintenance contracts can continue, but repairs will only be possible while they have spare parts available. This might not be for long as they are stopping manufacture of spares for these models. This change will absolutely result in lots of old HFAs being replaced with the newer 8 series devices.

One knock-on advantage of only keeping the more modern HFAs in use is that they will all be network compatible and thus compatible with Zeiss Forum. Some units have shied away from considering the Forum software as it would mean replacing some of the older field machines. This is worth knowing as clinicians interested in Forum may want to look at options for putting it into place when any old HFAs are being replaced.

Internet access on the go

Internet access while away from home is becoming more necessary. Many of us rely on public Wi-Fi, but are the risks and downsides worth it? What is the alternative?

The risks and disadvantages

The noteworthy issues are speed and security. Public Wi-Fi is often slow, as the bandwidth is being shared by all the users. It may only take one person to watch Netflix for the experience to reduce for all other users. Security is a more significant concern. Here are some easy to implement measures to reduce your exposure.

1. Avoid sensitive activities on public Wi-Fi. For the most part this means avoiding internet banking or similar. Public Wi-Fi always carries risks, as you may accidentally connect to something that you think is a Wi-Fi hotspot, but actually is a fake hotspot set up for malicious purposes.
2. Pick the network you use carefully. The safer and faster services are likely to be those offered by shops and cafes, rather than generic 'Free Wi-Fi'. The latter group generally have poor performance and less security.
3. Password protected is better. If you have the choice, use a network that requires you to ask at the counter for the password (or read it off a sign). These networks tend to use the fairly robust security built into Wi-Fi.
4. HTTPS Everywhere. If you must use free Wi-Fi regularly consider installing this add-on into your computer browser. It is compatible with Chrome and Firefox. The software automatically ensures your computer always connects to the secure (HTTPS) version of a website, if one exists.

If you want to avoid these issues, the alternative is to use your own network connection instead. This can be achieved by tethering your phone or buying a mobile hotspot and data contract.

Tethering from your phone

Most smartphones allow you to share your internet connection with other devices, like a laptop computer or iPad. Unless you have a generous contract, it's very easy to run out of data. The other issue with this method is that it can run down your phone's battery rapidly.

Mobile hotspot

From a security (and speed) standpoint this is the best option. The main issue is extra cost. Prices between companies vary significantly, but for a pay monthly contract in the UK expect to pay at least £10 per month. A costlier contract will provide more data. There is merit in taking out a monthly contract initially. This will allow you to determine how much data you need per month. All the UK mobile companies offer mobile hotspots, so it's worth choosing one with good reception in the areas you travel.

What about using data overseas?

Roaming charges have come down dramatically over the years, especially when roaming in Europe (well, the EU actually). The main UK mobile providers all have different approaches to roaming at present. Some (like Three) let you use your contract minutes and data in the EU (and some other countries) at no extra cost. Most of the other companies either give you a bit of data free or they charge you a few pounds per day to use your home allowance. Outside of Europe, similar options exist but at higher cost.

Of note, the law requires data roaming charges to be abolished in the EU by June 2017. Most companies are likely to behave as Three currently do, by offering our contract amounts when abroad, for no extra cost. It's not clear if this will affect roaming charges outside the EU. It's also not yet clear if BREXIT will result in higher roaming charges for British citizens when in EU countries.

No more ransom! (www.nomoreransom.org)

This reputable site hosts very good advice about avoiding the ransomware attacks that are becoming ever more popular. As we've previously stated, avoiding ransomware is the best approach. The site does detail steps that can be taken after infection to regain access to your files. This is unfortunately only the case in a minority of attacks. Most require handing over money to the attackers to regain access to your files. If you are ever unfortunate enough to succumb to such an attack, this is the site to visit. It will help you determine the attack vector and any possible solutions.

Scan your Internet of Things

IoT is a fairly recent acronym (meaning Internet of Things). It defines all the devices that now connect to the internet that are not typical smartphones, tablets or regular computers. Examples of IoT devices are the network connected thermostats, doorbells, light bulbs, mains switches and, of course, fitness trackers. Just like computers, these devices are prone to malware. Unfortunately, many of the manufactures of such devices don't design robust network security into the products. Worse still, many are never updated and they become susceptible to internet wide automated takeovers. Such an attack occurred on Friday 21 October 2016. The attack disrupted the internet on a large scale, especially in the US. More interesting is the fact that the bulk of the devices causing the attack were hijacked home routers and internet connected cameras with poor security.

There is a search engine for devices sat on the internet with poor security. It's called Shodan. The 'Internet of Things Scanner' (from Bulldog security) allows you to easily search Shodan for your own network to see if any vulnerabilities are detected. If problems are found the scanner doesn't really help you much to sort the problem, but at least it lets you know. Here is the link: http://iotscanner.bullguard.com

SECTION EDITOR

David Haider,
Consultant Ophthalmologist and Chief Clinical Information Officer,
Bolton Foundation Trust, UK.

E: david@drhaider.co.uk
Twitter: @drdavidhaider

The author has no proprietary or financial interests in the products discussed.