A Doctors.net.uk app and more security woes

Doctors.net.uk gets a new app

The Doctors.net.uk website is well known in the medical community. Its online services started 20 years ago, in 1998! Since then it has retained its core features of providing email accounts and also an online forum for doctors. It also offers e-learning materials, an image library and access to some online medical textbooks.

Recently the company launched an iOS and Android app to interact with its online forums. The app is free and seems well featured and reliable. As doctors.net.uk has a very large community (they claim, over 50,000 doctors) the forum is unsurprisingly very heavily used. The app even provides quick access to the 'Emergency Room' where users can post a question that requires a prompt response. The company quote an impressive four minutes as an average response time in this section. Clearly the app is not ophthalmic specific, though there is a dedicated ophthalmology forum, that can be easily accessed in the app. Image uploading is also supported to assist users in asking clinical questions. The community of users is closed, with individuals needing a degree of vetting with their GMC number to get an account. The forum is used for all manner of clinical and professional questions as well as plenty of general interest topics. The addition of the app will likely be of great benefit to the users and the community. Figure 1 is a screenshot of the new software.

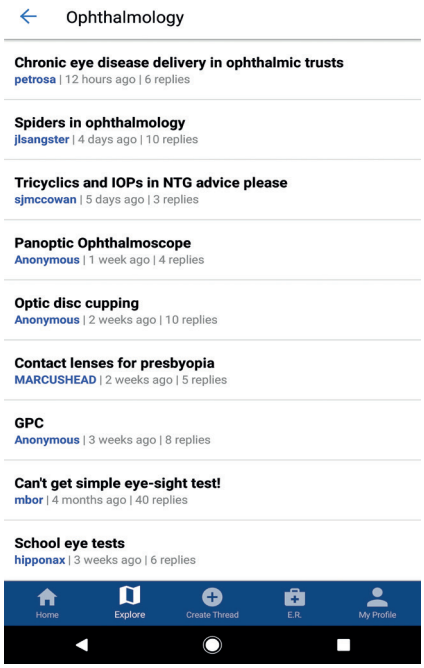

Figure 1: The new Doctors.net.uk app.

Fake accounts on LinkedIn

It has become clear from the large number of cyber attacks in 2017 (including those to the NHS) that our employers are at significant risk of ongoing attacks. In my role I have more visibility of the vast number of malicious emails that are trying to infect our organisations daily.

LinkedIn, the popular business networking website, in increasingly being used as a vector for such attacks.

An attack would likely go something like this...

- An individual receives a Linkedin request from a stranger. The account looks very real, with many contacts and testimonials. The stranger's role may be relevant to the individual receiving the request.
  The individual accepts the connection request and a message conversation ensues that leads to the new contact emailing the individual (on their work email) an attached form to complete.
- The individual receives the form and opens it on their work PC.
- The concealed malware contained in the file infects the PC and starts a business wide network attack.

The take home message is clear. Use care when accepting connection requests from strangers on LinkedIn, even if you seem to have some contacts in common. Also, be especially vigilant to any suggestions that involve you opening attachments or clicking on links in emails from new LinkedIn contacts.

Time to turn Bluetooth off

A new generation of smartphone attacks is being discovered. The most high profile in recent months is called BlueBourne, though this likely represents just the first in a line of new attacks targeting smartphones with Bluetooth enabled. Anyone with a smartphone with Bluetooth switched on could potentially be infected, giving attackers full access to all the stored information on the device. The phone doesn't have to connect to anything, just having Bluetooth switched on is enough to provide a vulnerability. Although some of the bugs that cause these problems have been fixed, more are being found. The only certain way to protect from these attacks is to switch Bluetooth off on the smartphone. This comes at a price though, as handsfree kits in cars and fitbits (to name just two) won't connect without Bluetooth. The best advice seems to be to only have Bluetooth switched on for periods of time when it is needed (e.g. when driving). At other times it makes sense to switch the Bluetooth feature off. With the above in mind it is also worth noting a limitation in the new iPhone control centre, which is accessed from swiping up from the bottom of the screen. The Bluetooth button in the control centre does not completely disable Bluetooth. That can only be done from the proper settings menu. If Bluetooth has been 'switched off' from the control centre it could still be hijacked by one of these new exploits. A screenshot of the new control centre is shown in Figure 2. Have a read of this *Guardian* article if you want to know more about the issues with the Control Centre https://goo.gl/qW7cEG

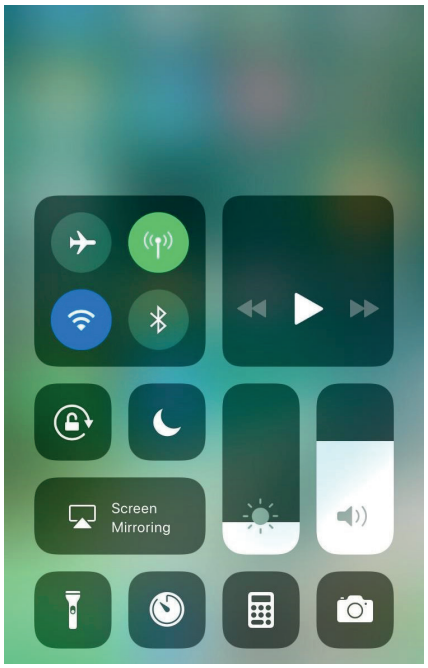

Figure 2: The new iPhone control centre.

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.