Public Wi-Fi Hot Spots: How to Avoid the Hackers
David McLelland - Technology and Online Security Expert

When we're out shopping many of us like to share photos, update social networks or compare shop prices online to make sure we're getting a good deal.

Mobile reception in shopping centres isn't always great, particularly indoors. The data allowance on our smartphones is valuable - and it can be frustrating when we run out, even expensive. We might even be using a tablet or laptop which doesn't have a data plan. So, quite often we look for a Wireless, or Wi-Fi, network to make our browsing faster and potentially cheaper. Public Wi-Fi networks are now all over the place in towns, in coffee shops, shopping centres and even supermarkets.

But how trusting are we about the wireless network we're connecting to?

Just because a Wi-Fi network has a 'friendly-looking' name doesn't mean that it isn't doing unfriendly things. Quite unwittingly we could be giving fraudsters free and open access to our sensitive online data - usernames, passwords and credit card details.

If you open your smartphone/tablet now and look at the Wi-Fi networks nearby, you can probably see many networks that you can connect to. But how do you know that they are who they say they are? Just because it's called something like 'Free Shopping Centre Wi-Fi', does that mean it's safe?

How can you be confident that the Wi-Fi network you're connecting to is a safe/trusted one?

Essentially, this problem is the same as with a phishing email, where you receive an email that pretends to be from your bank, but is actually from a scammer hoping to defraud you of your sensitive information.

As with spam phishing emails, when you log in to a Wi-Fi network, look for signs that all might not be as you'd expect. If there's a login window, are there spelling mistakes in the text? Do the images load? Is the site asking you for unexpected information - your social

network login perhaps, or credit card information? Is it a network that you've heard of before?

If you're at all suspicious then don't risk it, disconnect from the network altogether.

As a general rule, if you need to check your online banking, make online payments or do anything particularly sensitive, you might well be better off using your phone's 3G or 4G which, by design, is much more secure than using public Wi-Fi.

Something you can use to give yourself protection is a 'VPN client' on your smartphone or tablet. This is a little piece of software that encrypts your data on your device meaning it's safe from prying eyes - perfect if you travel a lot or frequently connect to Wi-Fi networks. In fact, a lot of companies use this to let their employees connect to work from a laptop at home. There's lots of information online about VPN apps you can download, but some do charge a fee.

Again, if in doubt - don't connect to that Wi-Fi network. Use your mobile data, wait until you get home, or find a network that you can trust.

As with all security, it's better to be safe than sorry.