Beware of getting hacked through public Wi-Fi

As much as public Wi-Fi is great for convenience - it's free, saves on mobile data, and is often faster when it comes to downloading - hackers love public Wi-Fi too, and for different reasons.

© gstockstudio via www.123RF.com

There are several ways cyber crooks can access an individual's private information, and even steal their identity or capture their banking logins through public Wi-Fi.

Man-in-the-middle (MITM) attacks

One of the ways in which they can do this, is through Man-in-the-Middle (MITM) attacks, during which a hacker intercepts communications between two parties. While they may think their communications are private, and that data is being shared directly between the server and the client, the link is, in fact, being intercepted by a third party. The attacker can then alter the communication, and display, for example, a fake or phishing website, or send a message of his own.

"Public Wi-Fi is particularly susceptible to attacks of this nature, due to the fact that any HTTP site data being transmitted is unencrypted, effectively rendering your data public. Through compromised routers, attackers can steal reams of personal information, and give an attacker access to financial logins, private messages, usernames and passwords. People should never, under any circumstances, do online banking transactions or share any personal information with others while using public Wi-Fi."

What can you do?

So what can users do? Check for secure sites, ones that have https:// instead of just http in front of them. "Certificates denoted by the 's' mean the website is more secure and offers a decent level of encryption, so only use such sites when accessing personal information," says Poorter.

The next thing users of public Wi-Fi need to be aware of are ‘Evil Twin’, or fake, Wi-Fi connections. “In these attacks, a cybercriminal sets their service identifier (SSID) to be the same as an access point (AP) at the local hotspot or wireless network. He can then disrupt or disable the genuine AP by disconnecting it, directing a denial of service attack against it, or creating radio frequency interference around it. This is particularly cunning, as it bypasses any security systems a public Wi-Fi hotspot might have in place,” she explains.

She advises users to be very suspicious should two network connections show up that have a similar name, and if possible, make use of a virtual private network (VPN). This will establish a level of encryption between the user and a website, so any data that could potentially be intercepted is unreadable to a cybercriminal unless they have the decryption key, which they don’t.

Packet sniffing

According to her, the next danger associated with public Wi-Fi is packet sniffing. “Every time there is data transmitted over the Internet, irrespective of whether it's an email, Google Search or retail transaction, the data is broken down into digital information that is sent in data packets. The packets are labelled and addressed with instructions explaining where they are going to. Millions of data packets move between destinations all the time, uninterrupted,” she explains.

“However, and here’s the caveat: If someone has installed sniffing hardware or software somewhere on the network, they can eavesdrop, snatch that data in mid-transmission just long enough to ‘sniff’ or inspect it, and if found to be interesting or valuable, quickly capture and copy it before sending it on its way. This is done without anyone being the wiser. Packet sniffing is like wiretapping for the internet.”

Packet sniffers can read emails, see passwords, view your web history, and more alarmingly, capture account information such as logins and credit card numbers in detail. “Again, I recommend turning to strong encryption, in the form of a VPN to avoid this scourge,” says Poorter.

Sidejacking

“Another danger of public Wi-Fi is sidejacking, or session hijacking. In these instances, an attacker will essentially steal a user’s access to a website by using a packet sniffer to get their hands on an unencrypted cookie that grants access to the site in question. This technique allows the cyber crook to impersonate the user, as the session cookie is already providing access to the Web site's content. Alarmingly, sidejacking bypasses encryption to some degree.”

Poorter says although attackers can’t read a password through this technique, they could still download malicious software that could, and get their hands on enough information to make stealing your identity a breeze. “Again, make use of https:// and VPNs to secure against this type of threat.”