



Issued 12/31/17

Hacking public Wi-Fi – How You're At Risk

Nastassja Poorter, enterprise sales director at Dynamic Recovery Services (DRS), an ICT services and solutions provider, said 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. 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 3rd 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, user names and passwords," said Poorter. "People should never, under any circumstances, do online banking transactions or share any personal information with others while using public Wi-Fi." 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,” Poorter said. Another 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 said. “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,” said Poorter. “Sidejacking, or session hijacking, is a method an attacker will use to essentially steal a user’s access to a Web site by using a packet sniffer to get their hands on an unencrypted cookie that grants access to the site in question.

The cyber crook can 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 said 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.