PERSATUAN BANK BANK DALAM MALAYSIA
THE ASSOCIATION OF BANKS IN MALAYSIA

Headline: Beware of 'evil twin' WiFi networks, urges CSM
Publication/Portal: The Star
Date: 24 February 2019

Language: English
Section: Focus/ Fokus
Page: 14

Beware of 'evil twin' WiFi networks, urges CSM

THE public should be careful the next time they connect to a free, public WiFi network.

This is because such free Internet access, even if it appears to be from a legitimate provider, could be a cybercriminal's way into your device and data.

In a recent report and video by *Channel NewsAsia*, it was demonstrated that cybercriminals can impersonate free WiFi, such as those provided by airports and other places.

When users log on to the fake WiFi with a similar name as the genuine network, the cybercriminal is able to view what users are doing online and even gain access to their cloud storage.

A demonstration in the video showed a cyber expert being able to impersonate Changi Airport's free WiFi.

After the journalist logged onto the fake Changi Airport WiFi, the expert was able to view what he was browsing and typing in his search engine, among others.

This is called an "evil twin" attack, says CyberSecurity Malaysia (CSM) chief executive officer Datuk Dr Amirudin Abdul Wahab, when commenting on the demonstration.

So far, CSM has yet to receive reports on such incidents in Malaysia.

Nevertheless, the public should be aware of the dangers of such attacks, which can expose victims to being impersonated or their e-banking accounts being compromised.

There are two techniques involved in this cybercrime.

"The first is called the "rogue access point" technique, whereby traffic from the victim can be monitored, intercepted and manipulated by a hacker.

"The attacker can monitor the victim's Internet activity, capture un-encrypted files sent or received by the victim.

"They can also redirect certain websites accessed by the victim, such as fake e-banking websites to harvest their username and password," says Dr Amirudin.

The second technique involves asking the victim to install a malicious app using a fake website in order for the victim to access free WiFi.

"By infecting the victim's smartphone, the attacker has control and access to all of the victim's smartphone resources include media, notes and other personal data.

"For older un-updated smartphones, the attacker may access deeper resources like SMS messages which can be used to manipulate victim e-banking transactions," he explains.

To avoid falling for the "evil twin" attack, users connected to free, public WiFi networks should restrict browsing only to websites that don't require or display sensitive information.

Dr Amirudin also advises the public to check the legitimacy of the network by asking staff to help verify the connection, its requirement and behaviour.

"The public can also use Virtual Private Network (VPN) subscriptions.

"This will encrypt the network traffic between the user's device and the Internet, which can hinder the attacker," he says.

Users are also advised against installing apps from suspicious sources asking for dubious permissions.

"An example of this can be an application that connects the user to the Internet but requires permission to access media, notes and other personal data in the device," Dr Amirudin adds.

For organisations offering free WiFi, he urges them to install detection software or equipment which can identify "rogue access points" in the network.

"Companies should also use a validation system for users to know that they have connected to a legitimate network," he says.