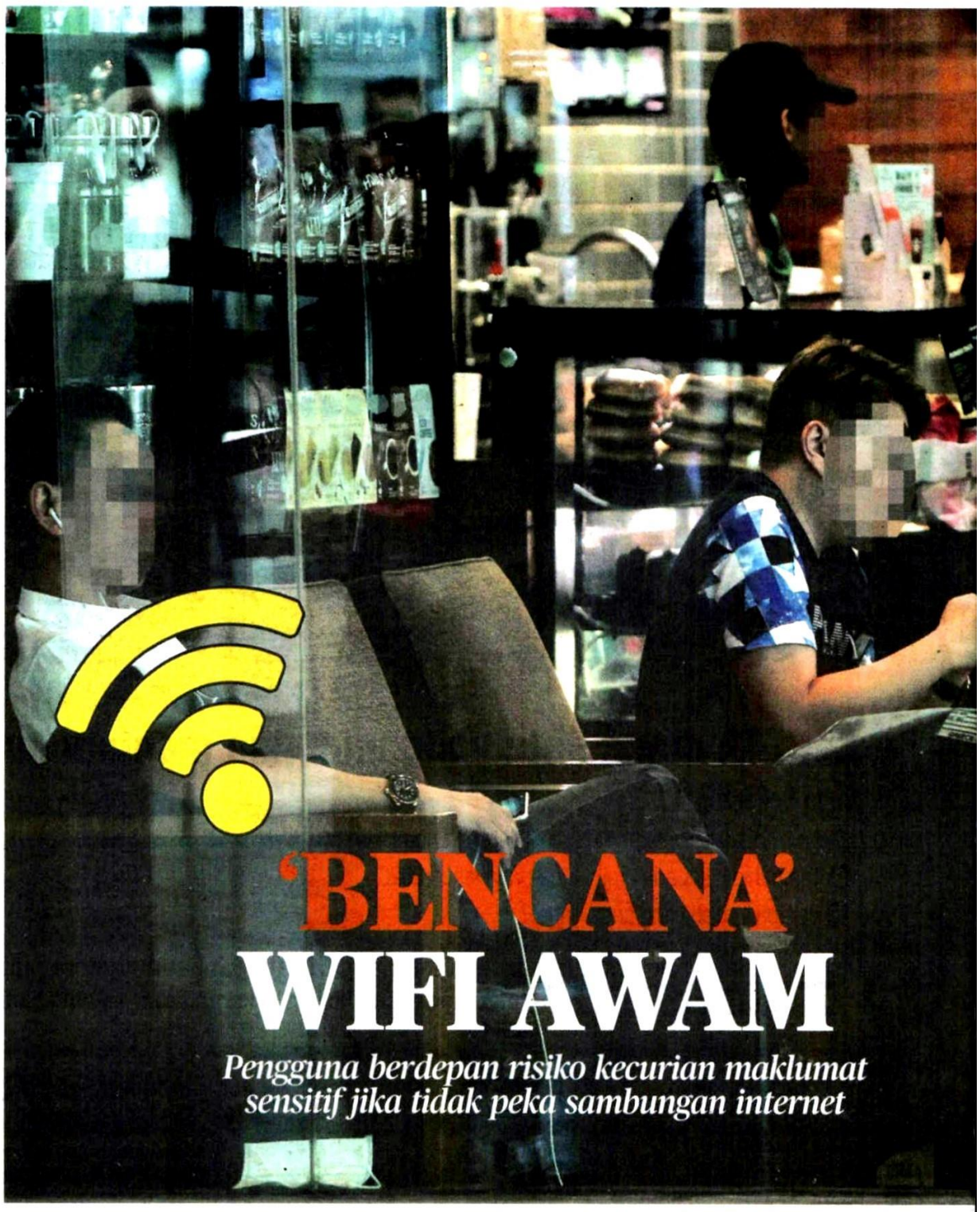
PERSATUAN BANK BANK DALAM MALAYSIA
THE ASSOCIATION OF BANKS IN MALAYSIA

Headline: 'Bencana' Wifi Awam
Publication/Portal: Harian Metro
Date: 23 february 2020

Language: Malay
Section: Lokal
Page: 10



'BENCANA' WIFI AWAM

Pengguna berdepan risiko kecurian maklumat sensitif jika tidak peka sambungan internet

Oleh Muhammad Saufi Hassan dan Ekhwan Haque Fazlul Haque
am@hmetro.com.my

Subang Jaya

Awas setiap kali pengguna melakukan sambungan internet menerusi jaringan tanpa wayar (WiFi) awam (*Public WiFi*) kerana ia mungkin sambungan 'pendua' yang sengaja dicipta penggodam untuk mendapatkan data peribadi pengguna termasuk maklumat perbankan.

Jika anda gemar melakukan transaksi perbankan tanpa menyemak sambungan internet terutamanya sambungan WiFi awam, ada kemungkinan penggodam sudah mengetahui kata laluan serta maklumat sensitif pengguna untuk dieksploitasi demi mendapatkan wang dengan cara paling mudah.

Pengguna kebiasaannya tidak mengetahui sambungan internet awam itu asli ataupun sambungan pendua memandangkan penggodam mencipta jaringan itu yang mirip dengan WiFi awam sedia ada termasuk menggunakan nama umum seperti *Free Public Wifi*, *Free Kafe Wifi* dan beberapa nama lain.

Hasilnya, tatkala peranti pintar pengguna sudah disambungkan menerusi WiFi awam itu, penggodam mempunyai akses pintu belakang (*back door*) untuk merakam transaksi perbankan, malah berupaya melihat data sensitif tersimpan di dalam peranti.

Penggodam juga berupaya mengetahui alamat e-mel pengguna, kata laluan perbankan, nombor kad kredit dan akses kepada storan peranti pengguna.

Mencipta WiFi awam pendua begitu mudah dan ia dilakukan kurang 120 saat dan data peribadi seseorang bertukar tangan tanpa sedar jika pengguna tidak prihatin berhubung sambungan Internet digunakan.

Lokasinya tidak terhad kerana boleh dilakukan di mana saja khusus kepada tempat tumpuan umum seperti kafe, lapangan terbang, stesen kereta api dan sebagainya.

Penggodam hanya memerlukan penghala (*router*) dengan sambungan Internet dan sebuah komputer riba untuk melakukan rakaman interaksi (*hand-shake*) antara peranti mangsa dan komputer riba penggodam.

Selepas itu, setiap pergerakan elektronik pengguna sepanjang menggunakan sambungan itu dirakam termasuk laman web yang digunakan, akses maklumat kepada kenalan dalam peranti dan fail yang disimpan.

Pakar keselamatan siber, Fong Choong Fook berkata, penggodam kebiasaannya menyasarkan pengguna yang membuka laman web perbankan elektronik untuk mendapatkan data sebelum digunakan untuk kepentingan peribadi.

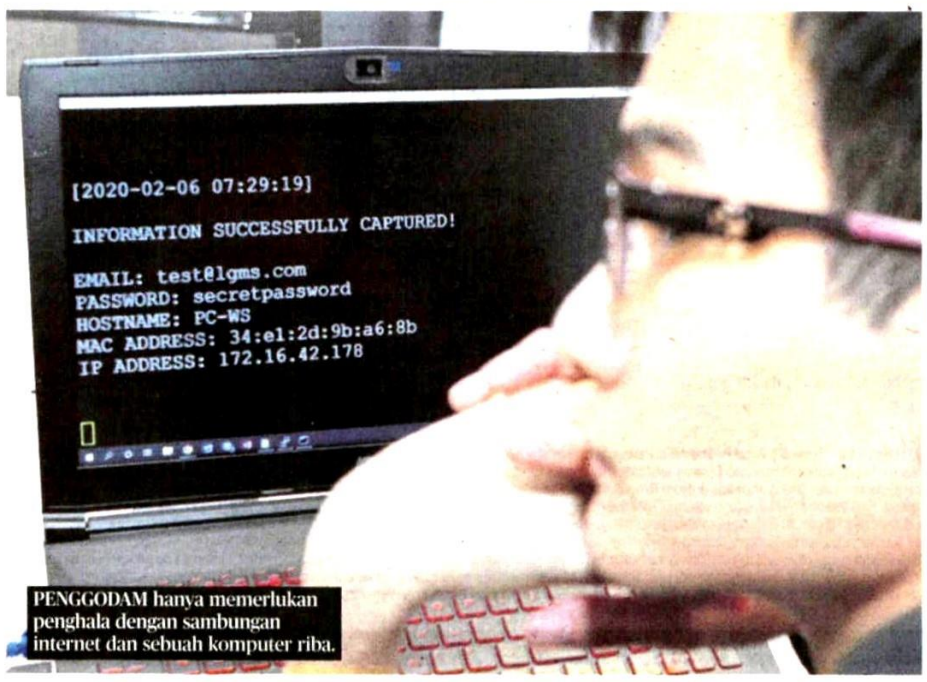
Menurutnya, menerusi sistem WiFi dicipta penggodam, semua maklumat termasuk kata laluan boleh diperoleh dengan mudah tanpa disedari pemilik akaun sehingga menyedari baki wang di dalam akaun berkurangan.

"Penggodam boleh menyamar sebagai pelanggan atau pengunjung sesebuah lokasi sebelum mencipta WiFi yang menggunakan nama yang sama dengan premis yang disasarkan tanpa disedari.

"Alatan penghala boleh disimpan di dalam beg penggodam tanpa disedari sesiapa dan pengunjung yang disasarkan pula tidak sedar sambungan Internet mereka sebenarnya WiFi pendua yang khusus dicipta untuk 'menggali' data sesiapa saja pengguna yang melakukan sambungan kepada jaringan terbabit.

"Kaedah itu digunakan untuk mengetahui maklumat laman sosial seseorang dan tidak hairan akaun mangsa digunakan untuk memuat naik sesuatu status pelik," katanya.

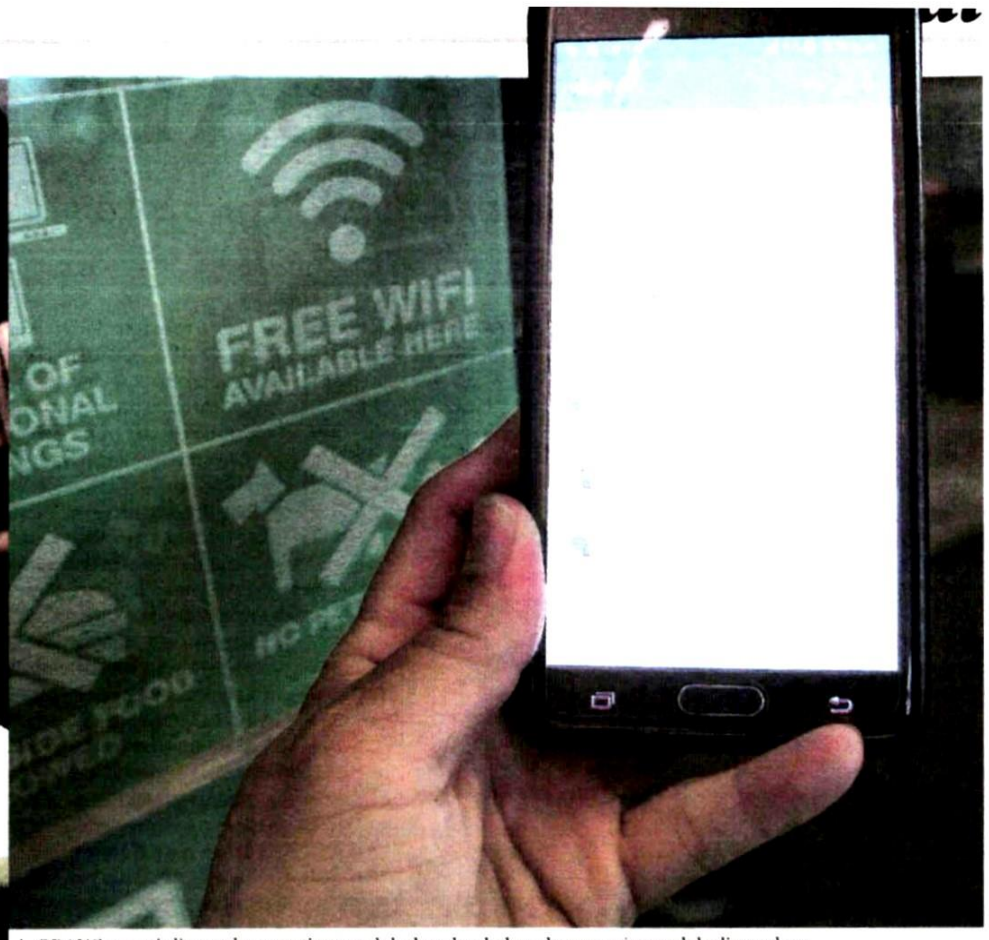
Beliau yang juga Ketua Pegawai Eksekutif LE Global Services Sdn Bhd (LGMS), berkata buat masa ini penggodam dilihat lebih cenderung mendapatkan kata laluan untuk perbankan elektronik kerana mampu mengaut keuntungan



PENGGODAM hanya memerlukan penghala dengan sambungan internet dan sebuah komputer riba.

PENGGODAM juga boleh mencuri maklumat laman sosial seseorang.

ORANG ramai perlu berhati-hati ketika menggunakan sambungan WiFi awam.



ORANG ramai disarankan sentiasa melakukan log keluar laman yang sudah digunakan.

Elak transaksi guna Wifi awam

Kuala Lumpur: Orang awam dinasihatkan tidak menggunakan sambungan Internet Tanpa Wayar (WiFi) awam untuk melakukan sebarang transaksi kerana ia boleh mengundang kepada ancaman siber.

Melakukan transaksi seperti pemindahan wang atau pembelian dalam talian menggunakan jaringan WiFi awam mendedahkan kepada ancaman pengintipan, penggodaman, kecurian identiti dan eksploitasi maklumat sensitif.

Ketua Pegawai Eksekutif CyberSecurity Malaysia (CSM) Datuk Dr Amirudin Abdul Wahab berkata, pengguna perlu memastikan terlebih dulu jaringan sambungan mereka menerusi peranti pintar atau *laptop* supaya menggunakan data atau internet yang lebih selamat.

"Pengguna perlu memastikan sentiasa melakukan log keluar laman yang sudah digunakan seperti e-mel, media sosial seperti Facebook serta Instagram dan bukan hanya menutup pelayar.

"Kedua, jangan simpan kata laluan di dalam peranti atau peralatan mudah alih. Ketiga, hadkan penggunaan internet atau putuskan pautan ke WiFi di *hotspot* kerana penjenayah siber sentiasa mencuba untuk akses dan mencuri maklumat tanpa pengetahuan pengguna," katanya.

Beliau berkata, langkah seterusnya yang boleh diambil apabila pengguna melakukan transaksi sensitif seperti perbankan internet atau pembelian dalam talian, perlu dipastikan ia dilakukan pada rangkaian yang terjamin keselamatan.

"CSM menasihatkan pengguna menjadikan ini sebagai satu tabiat untuk menutup sambungan *bluetooth* atau perkhidmatan lokasi apabila tidak digunakan.

"Ini untuk mengelakkan peralatan mudah alih anda dikesan dan ceroboh serta mengelak daripada orang asing mengetahui di mana lokasi pengguna," katanya.

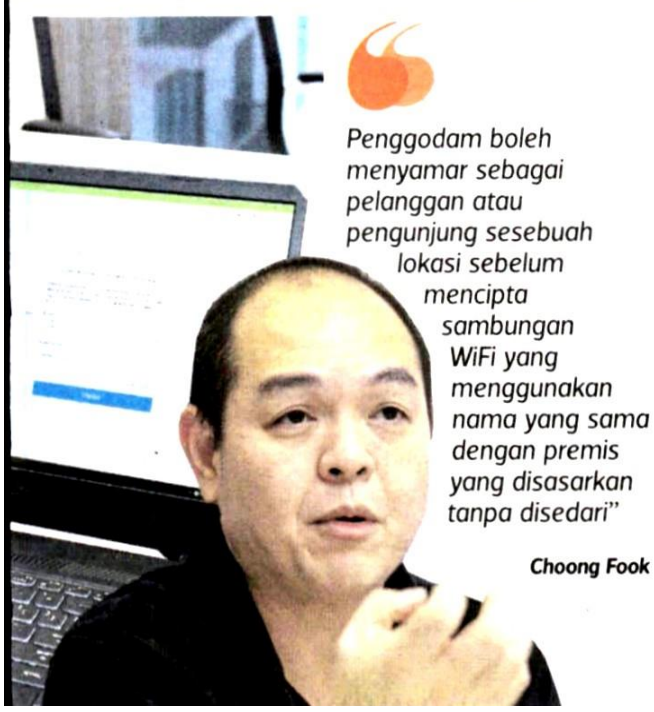
Menurutnya, sekiranya pengguna perlu melayari rangkaian tanpa wayar yang tiada program berkod (enkrip), periksa URL laman web dan jika boleh, gunakan aplikasi pada peralatan mudah alih supaya mengetahui status laman web yang sahih.

Sementara itu, Presiden Persatuan Pengguna Siber Malaysia (MCCA) Siraj Jalil berkata, jaringan internet awam yang tidak meminta kata laluan sangat berbahaya kerana ia boleh disalah guna oleh sesiapa saja.

Menurutnya, jika pengguna mahu melakukan transaksi atau pemindahan data sensitif adalah lebih wajar menggunakan paket data daripada jaringan telekomunikasi.

"Apabila pengguna melakukan sambungan kepada internet awam, ia memberi laluan kepada pemilik jaringan memantau aktiviti maya pengguna termasuk kata laluan yang boleh dirakam.

"Kaedah paling selamat mematikan jaringan Internet awam untuk mengelak sebarang kemungkinan data atau maklumat sensitif pengguna diperhatikan pihak tidak bertanggunjawab," katanya.



"Penggodam boleh menyamar sebagai pelanggan atau pengunjung sesebuah lokasi sebelum mencipta sambungan WiFi yang menggunakan nama yang sama dengan premis yang disasarkan tanpa disedari"

Choong Fook

dengan mudah dan cepat apabila wang dapat digunakan dengan mudah.

Katanya, pada masa akan datang penggodam mampu menggodam sistem dan dokumen rahsia sesebuah organisasi termasuk kerajaan jika sekuriti rangkaian internet tidak dipertingkat.

"Penggodam kini semakin maju dan ia jenayah terancang dilakukan individu untuk mencapai sesuatu matlamat dengan hanya menggodam sistem dan mendapatkan kata laluan.

"Ia nampak ringkas, tetapi kesannya besar seperti yang berlaku kepada beberapa syarikat terkemuka apabila sistem mereka digodam sebelum sejumlah wang diminta untuk memulihkan semula sistem," katanya.

"Jangan simpan kata laluan di dalam peranti atau peralatan mudah alih"
Dr Amirudin