

# WI-FI HOTSPOT

## Selamatkah Penggunaannya?



CyberSecurity  
MALAYSIA  
An agency under MOSTI

Oleh: Azira  
Abd. Rahim



### Langkah-langkah Keselamatan

Penggunaan Wi-Fi Hotspot membolehkan kita melayari internet tanpa wayar yang kini boleh di dapat di tempat-tempat umum seperti pusat membeli belah, pusat rekreasi, hotel, kafe, lapangan terbang, perpustakaan dan sebagainya. Kebiasaannya talian Wi-Fi ini boleh dilakukan sehingga 300 kaki dari jarak lokasi Hotspot tersebut.

Wi-Fi berfungsi dengan membenarkan penyambungan komputer adik-adik ke internet tanpa wayar dan tidak memerlukan pelan data dan isyarat selular. Kini, kebanyakan tempat telah menawarkan kemudahan Wi-Fi secara percuma untuk para pelanggannya.

Tetapi, tahukah adik-adik bahawa kita perlu melindungi diri sewaktu menggunakan perkhidmatan ini. Malah kita juga perlu tahu bagaimana untuk memastikan maklumat dan identiti adik-adik kekal selamat.

Menggunakan Wi-Fi awam secara automatik boleh mendedahkan adik-adik kepada ancaman keselamatan siber yang jarang wujud di rangkaian berbayar. Jika adik-adik perlu menggunakan Wi-Fi awam, mari kita semak langkah-langkah keselamatan untuk menyimpan maklumat adik-adik dengan selamat.

### 1 Hanya Gunakan Web Encrypted

Adik-adik boleh mengetahui sama ada laman web yang adik-adik layari itu selamat atau tidak dengan menggunakan "https" dan SSL (Secure Sockets Layer). Sesetengah laman web ini juga disertakan dengan ikon kunci pada URL di sebelah https://. Ini akan menunjukkan bahawa sambungan adik-adik ke laman web yang dikehendaki tidak mudah diintip oleh penggodam komputer dan disambungkan dengan lebih selamat.

### 2 Aktifkan Firewall Peribadi Anda

Firewall bertujuan meningkatkan tahap perlindungan komputer adik-adik daripada penggodam mengakses komputer menerusi rangkaian Wi-Fi. Kebiasaannya, komputer adik mungkin sudah tersedia dengan perisian firewall tetapi untuk kepastian adik boleh rujuk kembali tetapan firewall ini. Untuk pengguna Windows, adik perlu pergi ke Panel Kawalan, Sistem dan Keselamatan dan Firewall. Untuk pengguna Mac, adik boleh cari perisian firewall di bawah Pilihan Sistem dan Keselamatan.

### 3 Jangan Aktifkan Signal Wi-Fi

Jangan aktifkan akses ke signal Wi-Fi di setiap masa. Hanya aktifkan sambungan kepada Wi-Fi awam apabila adik-adik perlu menggunakanannya. Jika tidak memerlukannya, adik perlu mematikan sambungan Wi-Fi tersebut. Lebih banyak masa yang dihabiskan di rangkaian, adik-adik akan memberi lebih banyak peluang kepada penggodam untuk memecah masuk dan melakukan sesuatu seperti mencuri maklumat peribadi dan sebagainya. Maka, sila log keluar sebaik sahaja selesai berurus.

### 4 Kemas Kini Perisian Keselamatan Internet

Untuk memastikan kawalan malware, spyware dan virus komputer agar tidak menyerang komputer adik-adik, pastikan peranti akses Wi-Fi dipasang dengan perisian antivirus yang terkini di pasaran. Kebanyakan virus boleh merebak dan tersebar melalui e-mel, maka adik-adik perlu berhati-hati terutamanya ketika membuka lampiran e-mel serta pastikan aplikasi sistem OS Windows sentiasa dikemaskini.

### 5 Pastikan kata laluan dilindungi

Sekiranya adik-adik menggunakan Wi-Fi di rumah, pastikan adik-adik menggunakan kata laluan untuk melindungi router daripada diketahui oleh penjenayah siber. Ini kerana sekiranya mereka dapat mengakses router di rumah adik, mereka berupaya menukar tetapan sekaligus mengintip aktiviti dalam talian adik. Pastikan kata laluan yang dipilih mengandungi gabungan nombor, huruf dan simbol yang unik supaya dapat menyukarkan orang lain untuk meneka.

### 6 Membuat laporan untuk sebarang insiden pencerobohan

Laporkan insiden pencerobohan atau lain-lain insiden keselamatan siber kepada pembekal perkhidmatan internet anda atau hubungi Pusat Bantuan Cyber999 kami melalui email di cyber999@cybersecurity.my atau talian telefon bimbit +60192665850 untuk mendapatkan bantuan.

Sekiranya, komputer adik-adik telah dijangkiti virus atau digodam, cabut sambungan kabel internet di komputer adik-adik sebelum memuat turun perisian virus yang terkini. Lampirkan juga maklumat yang terperinci yang diperolehi dari perisian firewall dan anti-virus semasa membuat laporan.