

1010011
1011100
101100

BAHAGIAN TEKNOLOGI
MAKLUMAT


www.mpkj.gov.my

CELIK IT

3.5"

TIP

**KESELAMATAN
WIFI**




Rangkaian *Wi-Fi* (sering kali di sebut menggunakan nama teknikal 802.11) membolehkan pengguna menghubungkan peranti secara tanpa wayar dengan internet, seperti telefon pintar, konsol permainan video, tablet dan komputer riba.

Disebabkan rangkaian *Wi-Fi* boleh dipasang dengan begitu mudah, ramai yang memasang sendiri rangkaian *Wi-Fi* mereka di rumah. Bagaimanapun, kebanyakan rangkaian *Wi-Fi* di rumah dikonfigurasi secara kurang selamat, hingga membenarkan pengguna yang tidak sah untuk mengakses rangkaian rumah anda atau menyalahgunakan talian internet anda. Untuk memastikan keselamatan dan jaminan rangkaian *Wi-Fi* rumah anda, terjamin disini ada beberapa langkah yang boleh anda ambil.

“Kunci kepada keselamatan rangkaian Wi-Fi rumah anda adalah dengan memastikan hanya anda sahaja yang memiliki akses pentadbir, komunikasi antara peranti dienkrip, dan hanya pengguna yang disahkan boleh menggunakan rangkaian anda.”

Sumber :

- 1) <http://pshotzone.net/securing-wireless/>
- 2) <http://majalahpc.karangkrak.com>



Disediakan Oleh :

Bahagian Teknologi Maklumat
Jabatan Khidmat Pengurusan
Tingkat 2A Menara MPKj
Jalan Cempaka Putih Off Jalan Semenyih
43000 Kajang, Selangor Darul Ehsan

Tel : 03-8737 7899 Faks 03-8734 8705
Laman Web : www.mpkj.gov.my



Tip Keselamatan WiFi Hotspot

1. Matikan penyesuai WiFi anda

Apabila anda tidak berada di rumah atau di tempat kerja, pastikan anda mematikan sambungan WiFi. Jika tidak, komputer anda mungkin disambung ke Hotspot yang berisiko secara automatik tanpa anda sedari.

2. Pastikan firewall aktif

Firewall membantu melindungi komputer dengan menghalang pengguna lain mengakses komputer anda menerusi rangkaian WiFi. Ia bertindak menghalang atau membenarkan maklumat melaluinya.



3. Gunakan Virtual Private Network (VPN)

Apabila memilih untuk menggunakan sambungan WiFi, pastikan ia dilengkapi dengan kunci keselamatan. Maklumat yang dihantar melalui rangkaian ini adalah lebih sulit dan salah satu alternatifnya adalah menggunakan VPN.

Langkah-langkah Mengaktifkan VPN

- Pengguna Windows 7 - Klik Start - Control Panel - Network and Internet - Network and Share Center - Set up a new connection or network.
- Pilih Connect to a Workplace – Next - Use my internet connection (VPN).
- Taip alamat IP dan nama sambungan pada bahagian Destination.
- Masukkan nama pengguna serta kata unik sebelum klik *Connect*



4. Sulitkan data

Anda boleh melindungi fail dengan menjadikannya sulit. Membuka dan mengubah suainya memerlukan kata laluan. Laksanakan prosedur hanya ke atas satu fail pada satu masa. Pertimbangkan untuk melindungi fail yang digunakan semasa bekerja di tempat awam.

5. Gunakan HTTPS dan SSL

Kini, banyak laman web menggunakan fungsi HTTPS bagi menjamin keselamatan sambungan talian perhubungan komunikasi sulit. Akses laman web atau e-mel dimulai dengan https://.

6. Melumpuhkan perkongsian fail dan pencetak

Perkongsian fail dan pencetak membolehkan komputer lain dalam rangkaian mengakses sumber pada



komputer anda. Apabila anda menggunakan komputer mudah alih di tempat Hotspot, lumpuhkan fail dan pencetak daripada perkongsian dan serangan penggadam.

Langkah-langkah menyahaktifkan perkongsian fail

Bagi pengguna Windows 7 - Klik Start - Control Panel - Network and Internet - Network and Sharing Center - Homegroup and sharing options - Change advanced sharing settings - File and printer sharing - Turn off file and printer sharing - Save changes.

7. Pemantauan pintu akses

Jika terdapat kemudahan WiFi di tempat awam, anda pasti terdorong untuk melakukan sambungan. Ini akan menyambung talian ke pusat akses dan menghubungkan anda ke sistem berwayar utama untuk internet. Bagi memastikan sambungan adalah betul, sila semak konfigurasi komputer anda bagi membolehkan sambungan dilakukan.

8. Guna mode privasi pada folder

Komputer yang menggunakan mode privasi adalah lebih sukar digodam.

Langkah-langkah menggunakan mode privasi

- Bagi pengguna Windows 7 - Start - Control Panel .
- Dalam kotak carian, taip Network - Network and Sharing Center - Change advanced sharing settings .
- Klik pada V untuk memperluaskan profil rangkaian semasa anda.
- Di bawah Public folder sharing - Turn off Public folder sharing (people logged on to this computer can still access these folders) - Save changes.

9. OS dan aplikasi 'up to date'.

Hampir setiap minggu akan ada proses kemas kini keselamatan terbaru diumumkan .Kebanyakan virus dan worm yang berisiko mudah merebak dan tersebar melalui e-mel, jadi berhati-hati terutamanya ketika membuka lampiran.



10. Gunakan Antivirus

Pastikan peranti akses WiFi anda dipasang dengan perisian antivirus. Ini adalah untuk kawalan malware dan memastikan anda terlindung dari bahaya lain apabila mengakses WiFi secara terbuka..