Keamanan Berselancar Melalui Hotspot

Kiki Nur Fitria
kikiinur@gmail.com
http://kikiiblablabla.blogspot.com

Dalam keseharian kita sering mendengar istilah Hotspot atau bahkan kita sendiri sering menggunakan fasilitas tersebut. Tanpa kita sadari sebenarnya ada beberaba bahaya yang tersembunyi di HotSpot. Koneksi Internet gratis melalui WLAN atau yang lebih dikenal dengan istilah Hotspot di kafe, hotel, bandara, perkantoran atau bahkan di sekolah atau di kampus menjadi daya tarik tersendiri. Tetapi, tetap saja ada ancaman selalu mengiringi fasilitas gratis tersebut.

SMS adalah teknologi yang dulu pernah menjadi tren sebelum pengiriman pesan teks, gambar atau video telah dapat difasilitasi oleh layanan seperti Yahoo Messenger, Skype, atau WhatsApp Messenger melalui Internet di WLAN. Resikonya, pesan tersebut belum dienkripsi sehingga rentan disadap pengguna hotspot lainnya.

Saat ini banyak sekali tempat-tempat yang menggunakan fasilitas hotspot tersebut. Hal ini ditenggarai karena mayoritas pengguna mobile device lebih memilih koneksi Wi-Fi gratis daripada menggunakan koneksi yang disediakan operator yang tarifnya tidak murah.

Apapun yang murah pasti ada resikonya, Hotspot WLAN menjadi lokasi favorit pengintai data karena tidak memerlukan keahlian layaknya seorang hacker.

Berikut cara kerja dan tips keamanan saat berselancar di Hotspot:

1. Pilih koneksi yang aman.

Tidak semua area menawarkan beberapa pilihan koneksi. Tapi kalau tersedia, pilih jaringan nirkabel yang menyediakan kunci keamanan jaringan atau yang mencantumkan sertifikat keamanan. Jaringan seperti ini menyandikan setiap informasi yang dikirim sehigga membantu melindungi komputer anda dari pihak yang tidak bertanggung jawab.

2. Aktifkan firewall.

Firewall membantu melindungi komputer jinjing dengan mencegah pihak tak berwenang mengkakses melalui internet atau jaringan. Semua sistem operasi Windows memiliki fitur firewall.

3. Sembunyikan file dan printer sharing

Nonaktifkan file dan printer sharing sehingga mencegah komputer lain mengakses komputer anda melalui jaringan.

4. Buat semua folder private.

Hal ini untuk menyulitkan hacker mengakses file anda.

5. Sandikan file

Lindungi berkas dengan menyandikannya, sehingga setiap orang yang mencoba membuka atau memodifikasinya harus memasukkan kata kunci.

6. Jangan pernah mengetikkan nomor kartu kredit atau kata kunci.

Demi keamanan, jangan pernah memberikan nomor kartu kredit dan informasi finansial lainnya saat bekerja di area hotspot. Para hacker kerap memakai cara yang memancing orang memberikan data pribadi seolah-olah permintaan itu datang dari sistem yang sah.

Jika terpaksa harus mengetikkan data pribadi, pastikan muncul ikon gembok(padlock) di pojok kanan jendela browser dan alamat web dimulai dengan “https”. “S” berarti secure/aman, yang standar hanya “http”

7. Matikan jaringan nirkabel saat tidak digunakan

Jika anda tidak sedang menjelajahi internet atau mengirim email, tapi tetap memakai komputer di area hotspot, nonaktifkan koneksi nirkabel komputer anda. Jika menggunakan kartu Wifi eksternal, cabut saja. Jika memakai kartu Wifi internal, buka Control Panel -> Network Connection. Klik kanan di Connection dan pilih Disable.

Ancaman; HotSpot WLAN bekerja layaknya stasiun Radio. Semua orang yang berada dalam jangkauan sinyal hotspot Wi-Fi bisa menerima data. Artinya semua orang dengan aplikasi untuk smartphone dan tablet atau tool untuk notebook dapat melakukan pengintaian data dengan sangat mudah. Berapa banyak hotspot didaerah anda? Apa nama hotspot tersebut? Base station mana yang digunakan dan apa jenis enkripsinya?Apa saja perangkat yang terhubung dan alamat IP-nya? Adakah file sharing pada perangkat tersebut? Semua informasi ini berguna untuk menyerang suatu target.

Informasi WLAN bisa didapat dengan network scanner standar yang tersedia bebas dan legal, seperti Zenmap, Inssider, atau Wi-Fi Analyzer.

Biografi Penulis

 **Kiki Nur Fitria**. Menyelesaikan sekolah SMA pada tahun 2009 di SMA 9 Semarang. Sekarang sedang melanjutkan studi di Politeknik Negeri Semarang, mengambil jurusan D4 Teknik Telekomunikasi konsentrasi Jaringan Radio Komputer. Berbagai artikel menarik lain tersedia secara gratis di situs blog *http://kikiiblablabla.blogspot.com*