OUCH! | Februari, 2015

Surat Berita Bulanan berkenaan Kesedaran Keselamatan Untuk Pengguna Komputer

OUCH!

DALAM ISU KALI INI...

- **Pra-pemeriksaan**
- **Peranti Hilang/Dicuri**
- **Akses Wi-Fi**
- **Komputer Awam**

Kekal Selamat Ketika Di Perjalanan

Pengenalan

Dalam surat berita ini kita akan melihat bagaimana anda boleh menggunakan internet dan bekerja ketika sedang dalam perjalanan.

Editor Jemputan

Steve Armstrong merupakan Pengarah Teknikal CyberCPR di Logically Secure, pengajar SANS bertauliah dan bekas penulis kursus di SANS. Beliau aktif di Twitter sebagai **@Nebulator** dan di Google plus **+SteveArmstrongSecurity**.

Pra-pemeriksaan

Biarpun rangkaian di rumah atau pejabat anda mungkin selamat, di perjalanan, anda harus sentiasa mengang-gap semua rangkaian lain tidak boleh dipercayai. Anda tidak tahu siapa lagi yang sedang menggunakannya dan ancaman yang mereka bawa. Dengan melakukan beberapa langkah pra-perjalanan yang mudah, anda boleh melind-ungi maklumat anda ketika sedang dalam perjalanan. Seminggu dua sebelum perjalanan:

- Kenal pasti maklumat yang tidak diperlukan dalam peranti yang akan dibawa bersama dan padam maklumat yang tidak perlu. Ini dapat mengurangkan impak jika peranti anda hilang, dicuri atau ditahan oleh pegawai kastam atau keselamatan sempadan. Jika perjalanan anda mengenai kerja, mintalah peranti alternatif daripada penyelia, jika ada.
- Bagi perjalanan antarabangsa, semak jenis penyambung punca kuasa yang digunakan di negara tersebut kerana anda mungkin memerlukan alat penyesuai untuk mengecas peranti. Sebagai tambahan, semak pelan telefon bimbit dengan penyedia perkhidmatan anda. Selalunya penyedia perkhidmatan mengenakan kadar cas yang tinggi untuk penggunaan data antarabangsa, jadi anda mungkin perlu mematikan perkhidmatan data mudah alih atau tukar pelan untuk perjalanan antarabangsa.
- Pasang perisian pada peranti anda supaya ia boleh dijejaki dan juga boleh dipadamkan dari jarak jauh, jika ia hilang atau dicuri. Kebanyakan peranti mudah alih mempunyai fungsi ini dan anda mungkin perlu mengaktifkannya (ingat, fungsi ini memerlukan sambungan internet).

Sehari dua sebelum perjalanan:

- Kemas kini peranti, aplikasi dan perisian anti-virus supaya anda menggunakan versi yang terkini.
- Aktifkan kesemua tetapan keselamatan yang berkenaan pada peranti anda, seperti firewall.
- Kunci semua peranti mudah alih anda dengan kata laluan dan kod pas yang kukuh. Dengan cara ini jika peranti anda hilang atau dicuri, orang lain tidak boleh mengakses maklumat anda.

Kekal Selamat Ketika Di Perjalanan

- Sulitkan kesemua peranti anda supaya jika ia hilang atau dicuri, maklumat di dalamnya tidak boleh dibaca. Sesetengah peranti seperti iPhone melakukannya secara automatik jika anda mempunyai kata laluan atau kod pas pada peranti tersebut.
- Lakukan sandaran penuh untuk semua peranti anda. Dengan ini, jika sesuatu berlaku kepada anda ketika sedang dalam perjalanan anda masih mempunyai maklumat di tempat selamat.

Kunci untuk kekal selamat ketika dalam perjalanan adalah dengan melindungi peranti anda sebelum memulakan perjalanan, pastikan fizikal dan kedudukan peranti selamat pada setiap masa, serta sulitkan semua aktiviti dalam talian anda.

Peranti Hilang/Dicuri

Apabila anda memulakan perjalanan, pastikan keselamatan fizikal peranti-peranti anda. Sebagai contoh, jangan tinggalkan peranti anda di tempat yang mudah dilihat kerana penjenayah boleh memecahkan tingkap kereta dan mengambil barang berharga. Salah satu cara adalah dengan membawa kunci kabel supaya anda boleh mengunci peranti anda secara fizikal, seperti komputer riba semasa anda meninggalkannya. Walaupun jenayah merupakan satu risiko, anda mungkin tidak menyedari bahawa anda lebih berisiko untuk kehilangan peranti anda daripada ia dicuri. Mengikut kajian selama 10 tahun oleh Verizon, seseorang mempunyai kebarangkalian sebanyak 15 kali untuk kehilangan peranti berbanding dicuri. Ini bermakna, sentiasa pastikan peranti bersama anda semasa dalam perjalanan, seperti semasa anda melepasi pos keselamatan di lapangan terbang, meninggalkan teksi atau restoran, meninggalkan bilik hotel atau sebelum anda keluar dari pesawat.

Akses Wi-Fi

Mengakses internet ketika di dalam perjalanan selalunya bermakna anda perlu menggunakan pusat akses Wi-Fi awam seperti yang terdapat di hotel, kedai kopi atau lapangan terbang. Masalah dengan pusat akses Wi-Fi awam adalah bukan sahaja anda tidak tahu siapa yang memasangnya, tetapi anda juga tidak tahu siapa yang sedang mengaksesnya. Oleh itu, ia tidak boleh dipercayai, malah menjadi sebab untuk anda mengambil langkah-langkah melindungi peranti sebelum memulakan perjalanan. Selain itu, Wi-Fi menggunakan gelombang radio untuk menghubungkan peranti anda kepada pusat akses. Ini bermakna sesiapa yang berada dekat dengan anda secara fizikal berkemungkinan boleh memintas dan memantau komunikasi tersebut.

Inilah sebabnya jika anda menggunakan Wi-Fi awam, anda perlu pastikan semua aktiviti dalam talian anda telah disulitkan. Sebagai contoh, apabila anda membuat sambungan dalam talian menggunakan pelayar pastikan laman sesawang yang dilawati juga disulitkan (laman tersebut mempunyai 'https://' pada URL dan imej mangga yang tertutup). Selain itu, anda mungkin mempunyai akaun VPN (Virtual Private Network) yang akan menyulitkan semua aktiviti

Kekal Selamat Ketika Di Perjalanan

dalam talian anda. Akaun VPN akan diberikan oleh majikan anda, atau anda boleh membeli akaun VPN untuk kegunaan peribadi. Jika anda bimbang dengan ketiadaan pusat akses Wi-Fi yang boleh dipercayai, pertimbangkan untuk menambatnya (tethering) kepada telefon pintar anda. (Amaran: Seperti yang telah diberitahu, cara ini mungkin mahal untuk perjalanan antarabangsa. Sila semak dengan penyedia perkhidmatan anda.)

Sumber Awam

Jangan gunakan sebarang komputer awam seperti komputer di lobi hotel, perpustakaan atau di kafe siber. Anda tidak tahu siapa yang menggunakan komputer tersebut sebelum anda menggunakannya dan mereka mungkin telah menjangkiti komputer tersebut dengan sengaja atau tidak. Hanya gunakan peranti yang anda kawal dan percaya untuk sebarang aktiviti dalam talian. Jika anda perlu menggunakan komputer awam, jangan gunakan sebarang perkhidmatan yang memerlukan anda untuk log in atau menaip kata laluan.

Mari Belajar Lebih Lanjut!

Langganilah surat berita bulanan berkenaan Kesedaran Keselamatan Untuk Pengguna Komputer OUCH!, akseslah arkib OUCH!, dan belajar lebih lanjut mengenai penyelesaian kesedaran keselamatan SANS dengan melayari laman sesawang kami di http://www.securingthehuman.org.

Penterjemahan oleh SNSC.

Pusat Keselamatan Rangkaian SKMM (SKMM Network Security Centre- SNSC) beroperasi di bawah Suruhanjaya Komunikasi dan Multimedia Malaysia (SKMM) dengan matlamat menjamin keselamatan maklumat, kebolehpercayaan dan keutuhan rangkaian di Malaysia. Laman Web: http://snsc.skmm.gov.my/.

Sumber

Passwords:	http://www.securingthehuman.org/ouch/2013#may2013
Two step verification:	http://www.securingthehuman.org/ouch/2013#august2013
Encryption:	http://www.securingthehuman.org/ouch/2014#august2014
Securing Your New Tablet:	http://www.securingthehuman.org/ouch/2013#december2013
Verizon DBIR 2014:	http://www.verizonenterprise.com/DBIR/2014/

Editor: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Translated by: Muhamad Hashimi, Rahayu Aziz, and Sheikh Ahmad Raffie