OUCH! | Februari, 2017

Surat Berita Bulanan berkenaan Kesedaran Keselamatan Untuk Pengguna Komputer

OUCH!

DALAM ISU INI...

Kekal Selamat Dalam Perjalanan

Pengenalan

Kami mahu anda menikmati teknologi sebaiknya pada sepanjang masa, termasuklah ketika anda mengembara. Surat berita ini meliputi kaedah bagaimana anda boleh berhubung dengan Internet dan menggunakan peranti anda dengan selamat semasa mengembara.

Editor Jemputan

Mark Williams merupakan Arkitek Keselamatan Perusahaan di BlueCross Blueshield, Tennessee. Beliau merupakan pengajar SANS dan presiden ISSA Chattanooga chapter. Beliau banyak mengembara dan memahami isu yang sering dihadapi apabila membawa peranti canggih bersama.

Pra-Semak

Rangkaian rumah atau pejabat anda mungkin selamat, tetapi apabila anda sedang mengembara anda harus menganggap semua rangkaian yang anda sambungi tidak boleh dipercayai. Anda tidak mengetahui siapa yang turut menggunakannya dan apa yang mereka lakukan. Berikut adalah langkah mudah yang boleh anda gunakan untuk melindungi data dan anda sendiri sebelum anda mengembara.

- Maklumat paling selamat adalah maklumat yang tiada pada anda. Kenal pasti data yang anda tidak perlukan pada mana-mana peranti yang dibawa bersama dan padam maklumat tersebut. Ini dengan banyaknya akan mengurangkan impakjika peranti anda hilang, dicuri atau disita oleh kastam atau pihak keselamatan sempadan. Jika perjalanan anda berkaitan dengan kerja, tanya penyelia anda jika organisasi ada membekalkan peranti khusus untuk bekerja diluar kawasan.
- Kunci peranti mudah alih anda dan/atau komputer riba dengan kata laluan atau ungkapan laluan yang kukuh. Dengan cara ini jika ianya dicuri atau hilang, maklumat anda tidak dapat di akses. Sebagai tambahan, dayakan atau pasang penyulitan penuh cakera pada peranti dan komputer riba anda. Untuk kebanyakan peranti mudah alih, fungsi ini diupayakan secara automatik apabila anda menggunakan kunci skrin.
- Pasang atau dayakan perisian pada peranti anda supaya anda boleh menjejak dan juga memadamnya dari jauh, jika peranti hilang atau dicuri.
- Kemas kini peranti anda, aplikasi dan perisian antivirus sebelum pergi supaya anda menggunakan versi terkini. Kebanyakan serangan menumpukan kepada sistem dengan perisian sudah lapuk.
- Lakukan sandaran penuh untuk semua peranti anda. Dengan cara ini jika apa-apa terjadi kepadanya ketika mengembara anda masih mempunyai semua data asal di dalam lokasi yang selamat.

Kekal Selamat Dalam Perjalanan

- Untuk perjalanan antarabangsa, semak pelan perkhidmatan untuk telefon anda dengan penyedia perkhidmatan. Selalunya penyedia perkhidmatan mengenakan cas yang tinggi untuk penggunaan data antarabangsa, jadi anda mungkin mahu menyahdayakan data selular ketika berada di luar negara atau beli kad SIM prabayar tempatan untuk perjalanan antarabangsa.

Untuk kekal selamat semasa mengembara, tingkatkan keselamatan peranti anda sebelum meninggalkan rumah, pastikan ianya selamat secara fizikal dan sulitkan semua aktiviti dalam talian anda.

Peranti Hilang / Dicuri

Sebaik sahaja anda memulakan perjalanan pastikan keselamatan fizikal peranti anda. Sebagai contoh, jangan sesekali tinggalkan peranti anda di dalam kereta di mana orang boleh melihatnya dengan mudah, kerana penjenayah dengan mudah boleh memecahkan cermin kereta dan mengambil apa sahaja barangan bernilai yang boleh mereka capai. Walaupun jenayah adalah salah satu risiko, mengikut satu kajian Verizon seseorang adalah 100 kali lebih cenderung untuk kehilangan peranti dari dicuri. Ini bermakna sentiasa semak berkali-kali jika anda masih mempunyai peranti anda ketika sedang bergerak, seperti apabila anda melepasi prosedur keselamatan di lapangan terbang, meninggalkan teksi atau restoran, daftar keluar dari bilik hotel atau sebelum anda meninggalkan kapal terbang. Pastikan anda memeriksa poket belakang tempat duduk!

Akses Wi-Fi

Mengakses Internet ketika mengembara selalunya bermaksud menggunakan capaian wi-fi awam, seperti di hotel, kedai kopi tempatan atau di lapangan terbang. Dua masalah dengan wi-fi awam: anda tidak dapat memastikan siapa yang memasangnya dan siapa yang berhubung dengannya. Oleh itu ia harus dianggap tidak boleh dipercayai. Malah inilah sebabnya mengapa anda mengambil semua langkah keselamatan perantisebelum anda pergi. Sebagai tambahan, wi-fi menggunakan gelombang radio, ini bermakna sesiapa sahaja yang secara fizikal nya dekat dengan anda berpotensi untuk memintas dan memantau komunikasi anda. Oleh sebab ini, jikamenggunakan wi-fi awam, anda perlu memastikan semua aktiviti dalam talian disulitkan. Sebagai contoh, ketika berhubung dalam talian menggunakan pelayar pastikan laman yang anda lawati disulitkan. Anda boleh memastikannya dengan melihat 'HTTPS://' dan/atau gambar mangga yang berkunci di dalam bar URL atau alamat anda. Sebagai tambahan, anda boleh menggunakan apa yang dipanggil VPN (Rangkaian Peribadi Maya) yang boleh menyulitkan semua aktiviti dalam talian ketita didayakan. Ini mungkin diberikan untuk melakukan kerja, atau anda boleh membeli sendiri VPN untuk kegunaan peribadi. Jika anda bimbang tiada wi-fi yang boleh anda percayai,

Kekal Selamat Dalam Perjalanan

mungkin anda boleh berhubung menggunakan telefon pintar anda. Amaran: seperti yang telah kami maklumkan, kaedah ini boleh menjadi sangat mahal ketika perjalanan antarabangsa, semak dengan penyedia perkhidmatan anda dahulu.

Sumber Awam

Jangan gunakan komputer awam, seperti yang terdapat pada lobi hotel atau di kafe siber, untuk log masuk ke sebarang akaun atau mengakses maklumat sensitif. Anda tidak tahu siapa yang menggunakan komputer itu sebelum anda, dan mereka mungkin telah menjangkiti komputer tersebut secara tidak sengaja atau dengan niat tertentu. Jika boleh, hanya gunakan peranti yang anda percaya dan kawal. Sebaiknya, komputer awam digunakan untuk maklumat umum seperti melihat ramalan cuaca atau mendapatkan berita terkini. Log masuk kepada mana-mana akaun seperti akaun Google mengundang pengodam yang mungkin memerhatikan anda.

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 securingthehuman.sans.org/ouch/archives.

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

Passphrases:	https://securingthehuman.sans.org/ouch/2015#april2015
Backups:	https://securingthehuman.sans.org/ouch/2015#august2015
Malware:	https://securingthehuman.sans.org/ouch/2016#march2016
Encryption:	https://securingthehuman.sans.org/ouch/2016#june2016
OUCH Archives / Translation:	https://securingthehuman.sans.org/ouch/archives

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