OUCH! | Oktober 2014

Surat Berita Bulanan berkenaan Kesedaran Keselamatan Untuk Pengguna Komputer

OUCH!

DALAM ISU KALI INI...

- Pengenalan
- Lima Langkah Utama

Lima Langkah untuk Kekal Selamat

Pengenalan

Apabila teknologi semakin memainkan peranan penting dalam kehidupan kita, ia juga akan menjadinya semakin kompleks. Dengan peredaran teknologi yang begitu pantas, mengikuti perkembangan nasihat keselamatan boleh menyebabkan kekeliruan. Ianya seolah-olah sentiasa terdapat panduan baru tentang apa yang perlu dan tidak perlu anda lakukan. Walaubagaimanapun, sekiranya perincian tentang bagaimana untuk kekal selamat bertukar dari masa ke masa, terdapat beberapa perkara asas yang boleh anda lakukan untuk melindungi diri anda. Tidak kira teknologi apa yang anda gunakan atau di mana anda menggunakannya, kami mengesyorkan lima langkah berikut.

Editor Jemputan

Fokus utama Lenny Zeltser adalah melindungi operasi IT para pelanggannya di NCR Corp dan mengajar 'malware combat' di SANS Institute. Lenny aktif di Twitter sebagai **@lennyzeltser** dan menulis blog tentang keselamatan di **blog.zeltser.com**.

Lima Langkah Utama

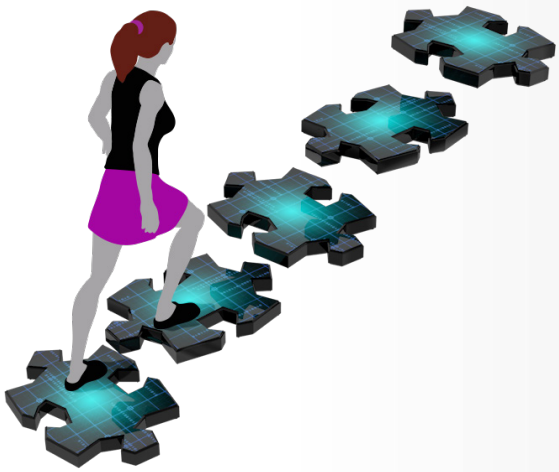
Setiap langkah di bawah merupakan gambaran ringkas. Untuk mengetahui lebih lanjut tentang setiap langkah tersebut, sila semak bahagian Sumber di akhir surat berita ini.

1. **Anda**: Pertama, sentiasa ingat bahawa teknologi sahaja tidak dapat melindungi anda. Penyerang telah mempelajari cara yang paling mudah untuk melepasi kebanyakan teknologi keselamatan iaitu dengan menyerang anda. Jika mereka mahukan kata laluan anda atau maklumat kad kredit, cara paling mudah untuk mereka adalah dengan memperdayakan anda untuk memberi maklumat tersebut. Sebagai contoh, mereka boleh menyamar sebagai sokongan teknikal Microsoft dan menghubungi anda tentang jangkitan pada komputer anda, sedangkan mereka hanyalah penjenayah siber yang mahukan capaian kepada komputer anda. Ataupun mereka akan menghantar e-mel menerangkan bahawa bungkusan anda tidak dapat dihantar dan meminta anda untuk klik pada pautan untuk mengesahkan alamat anda, sedangkan realitinya mereka mahu anda ke laman sesawang yang tidak selamat yang boleh menggodam komputer anda. Pada dasarnya, perlindungan terhebat adalah diri anda sendiri. Sentiasalah berwaspada, dengan menggunakan akal anda boleh mengesan dan menghalang kebanyakan serangan.

2. **Kemas kini**: Pastikan komputer, peranti mudah alih, aplikasi dan apa sahaja yang bersambung dengan rangkaian menggunakan versi perisian yang terkini. Penjenayah siber sentiasa mencari kelemahan dalam teknologi yang anda gunakan. Apabila mereka mengetahui kelemahan ini, mereka menggunakan program khas untuk mengekploitasi kelemahan tersebut dan menggodam ke dalam apa sahaja teknologi yang anda gunakan, termasuklah rangkaian, komputer dan peranti mudah alih anda. Sementara itu, syarikat yang mencipta teknologi yang

Lima Langkah untuk Kekal Selamat

anda gunakan, bekerja keras untuk memastikan ianya yang terkini. Setelah kelemahan diketahui, mereka akan mencipta tampalan untuk membaikinya dan mengeluarkan tampalan tersebut kepada orang awam. Dengan memastikan komputer dan peranti mudah alih anda dapat dikemas kini, anda mengurangkan bilangan kelemahan yang diketahui, menjadikannya lebih susah untuk seseorang menggodam anda. Untuk memastikan ia sentiasa dikemas kini, benarkan kemas kini automatik bila-bila mungkin. Semua teknologi yang bersambung dengan rangkaian boleh menggunakan kaedah ini, termasuk TV yang bersambung dengan internet, pemantau bayi, penghala (router) rumah, konsol permainan atau suatu masa nanti termasuklah kereta anda. Jika sistem operasi komputer, peranti mudah alih atau sebarang teknologi yang anda gunakan tidak lagi mempunyai sokongan dan tidak lagi menerima sebarang kemas kini, kami mengesyorkan mendapatkan versi baharu yang di sokong.



Dengan mengikuti lima langkah utama ini, perlindungan anda bertahan lebih lama dan anda dapat memanfaatkan teknologi terkini dengan sepenuhnya.

3. **Kata Laluan**: Langkah seterusnya untuk melindungi diri anda melibatkan penggunaan kata laluan yang unik dan kukuh untuk setiap peranti, akaun dalam talian dan aplikasi. Kata kunci di sini adalah unik dan kukuh. Kata laluan yang kukuh bermaksud sesuatu yang tidak mudah di teka oleh penggodam atau program automatik mereka. Jangan gunakan satu perkataan, sebaliknya, gunakan frasa laluan yang panjang yang mempunyai beberapa perkataan dan beberapa simbol dan nombor sebagai langkah yang selamat. Unik bermaksud menggunakan kata laluan yang berbeza untuk setiap peranti dan akaun dalam talian. Dengan itu jika satu kata laluan dikompromi, semua akaun dan peranti anda yang lain masih selamat. Tidak dapat mengingati kesemua kata laluan unik dan kukuh tersebut? Jangan bimbang, begitu juga kami. Itulah sebabnya kami mengesyorkan anda menggunakan pengurus kata laluan, iaitu aplikasi khas untuk telefon pintar atau komputer yang mampu menyimpan kesemua kata laluan anda dalam format penyulitan dengan selamat. Akhir sekali, jika akaun anda menyokong pengesahan dua kali, kami amat mengesyorkan supaya anda menggunakannya kerana ia merupakan salah satu cara terbaik untuk melindungi akaun anda.

4. **Penyulitan**: Langkah ketiga yang kami syorkan adalah penggunaan penyulitan. Penyulitan memastikan hanya mereka yang anda percayai boleh mencapai maklumat anda. Maklumat boleh disulitkan dalam dua keadaan: pegun dan bergerak. Menyulitkan maklumat dalam keadaan pegun bermaksud melindunginya apabila ia disimpan seperti fail di dalam cakera keras atau cakera mudah alih USB. Kebanyakan sistem operasi membenarkan anda menyulitkan maklumat secara automatik dengan menggunakan fungsi seperti Penyulitan Penuh Cakera. Kami mengesyorkan anda menggunakannya sekerap mungkin. Menyulitkan maklumat yang bergerak bermaksud menyulitkan maklumat semasa ia dipindahkan dari komputer atau peranti anda kepada yang lain, contohnya ketika

Lima Langkah untuk Kekal Selamat

anda sedang melakukan perbankan dalam talian. Cara mudah untuk mengetahui penyulitan digunakan atau tidak adalah dengan memastikan alamat laman sesawang yang anda lawati bermula dengan “https:” dan mempunyai simbol mangga yang berkunci di sebelahnya.

5. **Sandaran**: Kadang-kala, tidak kira bagaimana anda berjaga-jaga, salah satu dari peranti atau akaun anda mungkin dikompromi. Jika ini berlaku, pilihan yang anda ada untuk memastikan komputer atau peranti mudah alih anda bebas dari perisian yang tidak selamat adalah dengan memadamnya secara penuh dan membinanya dari awal. Penyerang mungkin akan menghalang anda daripada mencapai fail peribadi anda serta gambar dan maklumat lain yang terdapat pada sistem yang telah di kompromi. Pilihan yang ada adalah dengan mengembalikan semula maklumat peribadi anda dari sandaran. Pastikan anda membuat sandaran sekerap mungkin untuk semua maklumat penting dan pastikan anda boleh mengembalikannya. Kebanyakan sistem operasi dan peranti mudah alih menyokong fungsi sandaran automatik.

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

Email Phishing Attacks:	http://www.securingthehuman.org/ouch/2013#february2013
Securing Your New Tablet:	http://www.securingthehuman.org/ouch/2013#december2013
Strong Passwords:	http://www.securingthehuman.org/ouch/2013#may2013
Password Managers:	http://www.securingthehuman.org/ouch/2013#october2013
Two-Step Verification:	http://www.securingthehuman.org/ouch/2013#august2013
Encryption:	http://www.securingthehuman.org/ouch/2014#august2014
Personal Backup and Recovery:	http://www.securingthehuman.org/ouch/2013#september2013

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

