Surat Berita Bulanan berkenaan Kesedaran Keselamatan Untuk Pengguna Komputer

OUCH!

DALAM KELUARAN INI...

Frasa Laluan

Latar Belakang

Kata laluan merupakan sesuatu yang anda gunakan hampir setiap hari, dari membuat capaian kepada e-mel dan perbankan dalam talian sehinggalah membeli makanan atau menggunakan telefon pintar anda. Pun begitu, kata laluan merupakan titik kelemahan anda yang utama, jika seseorang mempelajari kata laluan anda mereka boleh mencuri identiti anda, memindahkan wang anda atau capaian kepada maklumat peribadi anda. Kata laluan yang kukuh adalah penting untuk melindungi diri anda. Dalam surat berita ini, anda akan pelajari bagaimana untuk mencipta kata laluan kukuh yang mudah untuk diingati dengan menggunakan sejenis kata laluan yang dipanggil frasa laluan.

Editor Jemputan

Guy Bruneau merupakan seorang perunding keselamatan kanan di IPSS Inc., pengajar SANS dan pengendali ISC. Guy mempunyai SANS GSE dan telah tamat program SANS Cyber Guardian. Anda boleh mengikuti Guy di Twitter **@GuyBruneau** dan di **handlers.sans.org/gbruneau**.

Frasa Laluan

Cabaran yang kita hadapi adalah penjenayah siber telah mencipta cara yang canggih untuk meneka, atau “brute force” kata laluan, dan mereka semakin handal. Ini bermakna mereka boleh mengkompromikan kata laluan anda sekiranya ia lemah atau mudah untuk diteka. Langkah penting untuk melindungi diri anda adalah dengan menggunakan kata laluan yang kukuh. Lebih banyak aksara yang anda gunakan untuk kata laluan anda menjadikannya lebih sukar untuk penyerang meneka. Walaubagaimanapun, kata laluan yang panjang dan kompleks kadangkala sukar untuk diingati. Sebaliknya, kami mengesyorkan anda menggunakan frasa laluan, ini merupakan frasa atau ayat yang mudah untuk diingati, tetapi sukar untuk digodam. Berikut adalah satu contoh.

Di manakah King Julian?

Apa yang menjadikan frasa laluan ini sangat kukuh bukan sahaja pada kepanjangan 21 aksaranya, tetapi ia menggunakan huruf besar dan simbol (Ingat, ruang kosong dan tanda baca merupakan simbol). Anda boleh menjadikan frasa laluan anda lebih kukuh dengan menggantikan huruf dengan nombor dan simbol, seperti menggantikan huruf ‘a’ dengan simbol ‘@’ atau huruf ‘o’ dengan nombor kosong. Jika ada laman sesawang atau program yang mengehadkan bilangan aksara yang boleh digunakan untuk kata laluan, gunakan jumlah aksara maksimum yang dibenarkan.

Frasa Laluan

Menggunakan Frasa Laluan dengan Selamat

Anda juga perlu berhati-hati bagaimana anda menggunakan frasa laluan. Frasa laluan tidak berguna jika mereka yang berniat jahat dengan mudah mencuri atau melakukan salinan pendua.

Frasa laluan merupakan salah satu cara paling efektif yang boleh diambil untuk melindungi identiti dan maklumat anda.

1. Pastikan anda menggunakan frasa laluan yang berbeza untuk setiap akaun atau peranti yang anda gunakan. Sebagai contoh, jangan gunakan frasa laluan yang sama untuk kerja atau akaun bank dengan akaun peribadi seperti Facebook, Youtube atau Twitter. Dengan cara ini, jika salah satu akaun anda digodam, akaun lain masih lagi selamat. Jika anda mempunyai frasa laluan yang banyak untuk diingati (iaitu perkara biasa), pertimbangkan untuk menggunakan pengurus kata laluan. Ini merupakan program khas yang menyimpan kesemua frasa laluan untuk anda. Dengan cara ini, anda hanya perlu mengingati frasa laluan kepada komputer dan pengurus kata laluan anda.

2. Jangan sesekali berkongsi strategi anda menjana frasa laluan anda kepada orang lain, termasuklah rakan sekerja. Ingat, frasa laluan adalah rahsia, jika orang lain mengetahui frasa laluan anda ia tidak lagi selamat. Jika anda dengan tidak sengaja berkongsi frasa laluan dengan sesiapa, atau percaya yang kata laluan anda telah dikompromi atau dicuri, pastikan anda menukarnya dengan serta-merta.

3. Sama seperti kata laluan, elakkan daripada menggunakan frasa laluan yang mudah diteka atau yang sering digunakan. Sebagai contoh, frasa “Four score and seven years ago” adalah kurang bagus kerana ia diketahui umum.

4. Jangan gunakan komputer awam, seperti yang terdapat di hotel dan pusat sumber, untuk log masuk kerja atau akaun bank. Memandangkan sesiapa boleh menggunakan komputer ini, ia mungkin dijangkiti oleh kod yang berniat jahat yang menyimpan semua ketukan kunci. Hanya log masuk kepada kerja atau akaun bank menggunakan komputer atau peranti mudah alih yang dipercayai.

5. Hati-hati dengan laman sesawang yang memerlukan anda untuk menjawab soalan peribadi. Soalan ini digunakan jika anda terlupa frasa laluan anda dan perlu untuk menetapkannya semula. Masalahnya jawapan kepada soalan ini kebiasaannya boleh didapati di internet, atau paparan Facebook anda. Pastikan jika anda menjawab soalan peribadi ini anda tidak menggunakan maklumat yang terdapat secara terbuka atau maklumat yang anda cipta. Pengurus kata laluan boleh membantu anda kerana kebanyakannya membenarkan anda untuk menyimpan maklumat tambahan ini.

Frasa Laluan

6. Kebanyakan akaun dalam talian menawarkan sesuatu yang dipanggil pengesahan dua faktor, juga dikenali sebagai penentu sahan dua langkah. Di sinilah anda perlu lebih dari frasa laluan untuk log masuk, seperti kod laluan dihantar kepada telefon pintar anda. Pilihan ini lebih selamat daripada hanya menggunakan frasa laluan sahaja. Apabila mungkin, sentiasa gunakan langkah pengesahan yang lebih kukuh.

7. Peranti mudah alih selalunya memerlukan PIN untuk melindungi capaian kepadanya. Ingat bahawa PIN hanyalah satu bentuk kata laluan. Lagi panjang PIN anda, lebih selamat. Kebanyakan peranti mudah alih anda membenarkan anda untuk menukar nombor PIN anda kepada frasa laluan.

8. Akhir sekali, jika anda tidak lagi menggunakan sebarang akaun, pastikan anda tutup, padam atau nyah aktifkannya.

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

Two-step Verification:	http://www.securingthehuman.org/ouch/2013#august2013
Password Managers:	http://www.securingthehuman.org/ouch/2013#october2013
Social Engineering:	http://www.securingthehuman.org/ouch/2014#november2014
Common Security Terms:	http://www.securingthehuman.org/resources/security-terms

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