

OUCH!

DALAM ISU INI...

- Ungkapan Laluan
- Menggunakan Ungkapan Laluan dengan Selamat
- Sumber

Ungkapan Laluan

Pengenalan

Kata laluan merupakan sesuatu yang anda gunakan hampir setiap hari, dari menggunakan emel, perbankan dalam talian, membeli barangan atau menggunakan telefon pintar. Bagaimanapun, kata laluan merupakan salah satu titik kelemahan anda kerana jika orang lain mengetahui atau dapat meneka kata laluan anda, mereka boleh menggunakan akaun anda, yang membolehkan mereka memindahkan duit, membaca emel atau mencuri identiti anda. Itulah sebabnya kata laluan yang kukuh adalah penting untuk melindungi diri anda. Sungguhpun begitu, kata laluan juga selalunya mengelirukan, sukar untuk diingati dan sukar untuk ditaip.

Dalam surat berita ini anda akan mempelajari cara mencipta kata laluan kukuh yang mudah untuk anda ingat dan mudah untuk ditaip – dinamakan ungkapan laluan.

Editor Jemputan

My-Ngoc Nguyen (disebut Me-Nop Wynn) merupakan seorang pengajar bertauliah SANS dan juga CEO/Perunding Utama di Secured IT Solutions. Beliau merupakan pakar yang memiliki memegang sijil-sijil terbaik dengan lebih 14 tahun pengalaman membangun, mematangkan, dan menguruskan program keselamatan siber untuk pelbagai industri dan sektor. Twitter: [@MenopN](#) LinkedIn: My-Ngoc 'Menop' Nguyen.

Ungkapan Laluan

Cabaran yang kita semua tempuhi adalah penjenayah siber telah membangunkan kaedah yang canggih dan efektif menggunakan teknik daya kasar (brute force) untuk kata laluan. Ini bermaksud orang yang berniat jahat boleh mendapatkan kata laluan anda jika ianya lemah atau mudah diteka. Langkah penting untuk melindungi diri anda adalah dengan menggunakan kata laluan yang kukuh. Selalunya, ianya dilakukan dengan mencipta kata laluan yang kompleks, namun ianya sukar untuk diingati, mengelirukan dan sukar untuk ditaip. Sebaliknya, kami menyarankan anda menggunakan ungkapan laluan, iaitu perkataan-perkataan bersiri atau satu ayat. Lebih banyak aksara ungkapan laluan anda ada, maka lebih kukuhlah ia. Kelebihannya ialah ia lebih mudah diingati dan ditaip tetapi masih sukar untuk digodam penyerang siber. Berikut merupakan dua contoh berbeza.

Kata laluan-saya-kukuh

Minum teh pada pukul 1.23

Apa yang menjadikan ungkapan laluan ini sangat kukuh bukan sahaja sebab ianya panjang, tetapi ia juga menggunakan huruf besar dan simbol (ingat, jarak dan tanda baca merupakan simbol). Pada masa yang sama ungkapan laluan ini mudah diingati dan ditaip. Anda boleh menjadikan ungkapan laluan anda lebih kukuh jika anda menggantikan huruf dengan simbol

Ungkapan Laluan

dan nombor, seperti menggantikan huruf 'a' dengan simbol '@' atau huruf 'o' dengan nombor kosong. Jika laman sesawang atau program menghadkan bilangan aksara yang boleh anda gunakan sebagai kata laluan, gunakan kesemua aksara yang dibenarkan.

Gunakan Ungkapan Laluan Anda dengan Selamat

Anda juga perlu berhati-hati bagaimana anda menggunakan ungkapan laluan. Penggunaan ungkapan laluan tidak akan membantu jika mereka yang berniat jahat boleh mencuri atau membuat salinan dengan mudah.

1. Gunakan ungkapan laluan yang berbeza untuk setiap akaun atau peranti anda. Sebagai contoh, jangan gunakan ungkapan laluan yang sama untuk kerja atau akaun bank yang anda gunakan pada akaun peribadi seperti Facebook, YouTube atau Twitter. Dengan cara ini, jika salah satu akaun anda digodam, akaun anda yang lain masih selamat. Jika anda mempunyai terlalu banyak ungkapan laluan untuk diingati (sesuatu yang biasa), pertimbangkan untuk menggunakan pengurus kata laluan. Ia adalah satu program khas yang menyimpan kesemua ungkapan laluan anda dengan selamat. Dengan cara ini anda hanya perlu mengingati ungkapan laluan untuk komputer anda atau peranti dan program pengurus kata laluan.
2. Jangan sesekali kongsi ungkapan laluan anda atau strategi untuk menciptanya dengan sesiapa, termasuklah rakan sekerja dan penyelia anda. Ingat, ungkapan laluan adalah rahsia; jika orang lain mengetahuinya ungkapan laluan anda tidak lagi selamat. Jika anda secara tidak sengaja berkongsi dengan orang lain, atau percaya bahawa ungkapan laluan anda telah dikompromi atau dicuri, tukar serta-merta. Kecuali anda mahu berkongsi ungkapan laluan dengan seorang ahli keluarga yang sangat dipercayai jika berlaku kecemasan. Salah satu cara yang boleh anda gunakan adalah dengan menulis ungkapan laluan anda (pastikan ianya bukan berkaitan kerja) dan simpan di tempat yang selamat, dan kongsi lokasi tersebut dengan ahli keluarga yang dipercayai. Dengan cara tersebut jika sesuatu berlaku pada anda dan perlukan bantuan, akaun anda boleh dicapai oleh orang tersayang.
3. Jangan gunakan komputer awam, seperti yang terdapat di hotel-hotel atau kafe internet untuk log masuk akaun anda. Memandangkan sesiapa sahaja boleh menggunakan komputer ini, ianya mungkin dijangkiti dan menangkap kesemua ketukan kekunci. Hanya log masuk ke akaun anda menggunakan komputer atau peranti yang dipercayai.
4. Hati-hati dengan laman sesawang yang memerlukan anda untuk menjawab soalan peribadi. Soalan ini digunakan jika anda terlupa ungkapan laluan anda dan perlu menetakannya semula. Masalahnya adalah jawapan kepada soalan ini selalunya boleh didapati dari internet, atau dari laman Facebook anda. Pastikan jika anda menjawab soalan peribadi anda menggunakan maklumat yang tidak terdapat secara terbuka atau maklumat palsu yang anda cipta. Jika anda



Ungkapan laluan adalah cara yang lebih mudah untuk mengingati kata laluan yang lebih kukuh.

Ungkapan Laluan

tidak mampu untuk mengingat jawapan kepada soalan-soalan tersebut, cari tema lain seperti watak dalam filem dan jawab berpandukan watak tersebut. Pilihan lain adalah sekali lagi menggunakan pengurus kata laluan, kerana kebanyakannya turut membolehkan anda menyimpan maklumat tambahan ini.

5. Kebanyakan akaun dalam talian juga menawarkan sesuatu yang dipanggil pengesahan dua faktor, juga dikenali sebagai penentusahan dua faktor. Ini memerlukan lebih dari ungkapan laluan anda seperti kod laluan dihantar kepada telefon pintar. Pilihan ini lebih selamat dari ungkapan laluan itu sendiri. Jika boleh, sentiasa bolehkan penggunaan kaedah pengesahan yang lebih kukuh.
6. Peranti mudah alih selalunya memerlukan PIN untuk capaian. Ingat PIN adalah suatu bentuk kata laluan. Semakin panjang PIN anda, semakin selamat. Banyak peranti mudah alih membenarkan anda untuk menukar PIN anda kepada ungkapan laluan yang sebenar atau menggunakan biometric seperti cap jari.
7. Jika anda tidak menggunakan apa-apa akaun lagi, pastikan anda tutup, padam atau lupuhkan ia.

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://snc.skmm.gov.my/>.

Sumber

- Pengurus kata laluan: <https://securingthehuman.sans.org/ouch/2015#october2015>
- Penentusahan dua faktor: <https://securingthehuman.sans.org/ouch/2015#september2015>
- Lock Down Your Login: <https://lockdownyourlogin.com>
- SANS SEC301 - Five day course on cyber security basics: <https://sans.org/sec301>

OUCH! diterbitkan oleh program SANS "Securing The Human" dan diedarkan di bawah lesen [Creative Commons BY-NC-ND 4.0](https://creativecommons.org/licenses/by-nc-nd/4.0/). Kebenaran diberikan untuk mengedarkan surat berita ini atau menggunakannya dalam mana mana program kesedaran selagi tiada perubahan dibuat kepada kandungan asal.

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

