Surat Berita Bulanan berkenaan Kesedaran Keselamatan Untuk Pengguna Komputer

OUCH!

DALAM ISU INI...

- Pengenalan
- Bagaimana Pengurus Kata Laluan Berfungsi
- Memilih Pengurus Kata Laluan

Pengurus Kata Laluan

Pengenalan

Salah satu langkah penting yang boleh anda ambil untuk melindungi diri semasa berada dalam talian adalah dengan menggunakan kata laluan yang unik untuk setiap akaun dan aplikasi anda. Malangnya, hampir mustahil untuk mengingati kata laluan yang berbeza bagi semua akaun anda. Inilah sebabnya ramai orang menggunakan semula kata laluan yang sama. Malangnya, penggunaan semula kata laluan yang sama untuk akaun berbeza adalah merbahaya kerana jika seseorang berjaya mendapatkan kata laluan anda, mereka boleh mendapat akses kepada semua akaun dengan kata laluan yang sama. Penyelesaian yang mudah adalah dengan menggunakan pengurus kata laluan (password manager/password vault). Program ini menyimpan semua kata laluan dengan selamat, dan memudahkan anda untuk menggunakan kata laluan yang berbeza untuk setiap akaun. Pengurus kata laluan menjadikannya mudah kerana anda hanya perlu mengingati kata laluan induk pengurus kata laluan sahaja, daripada mengingati kata laluan untuk semua akaun anda.

Editor Jemputan

Chris Christianson merupakan seorang perunding keselamatan yang bekerja di California, berbekalkan lebih 20 tahun pengalaman dan pelbagai sijil teknikal. Beliau telah berucap di pelbagai persidangan dan menyumbang banyak artikel kepada industri. Chris boleh dihubungi di **@cchristianson** dan **https://ismellpackets.com**.

Bagaimana Pengurus Kata Laluan Berfungsi

Pengurus kata laluan berfungsi dengan menyimpan semua kata laluan di dalam pangkalan data, kadang kala disebut peti besi (vault). Pengurus kata laluan menyulitkan kandungan pangkalan data dan melindunginya dengan kata laluan induk yang hanya anda ketahui. Apabila ingin mendapatkan semula kata laluan, seperti log masuk ke perbankan atas talian atau emel, anda cuma perlu menaip kata laluan induk ke dalam pengurus kata laluan untuk membuka pangkalan data anda. Selalunya pengurus kata laluan akan mendapatkan kata laluan secara automatik dan log masuk untuk anda. Ini memudahkan untuk anda menggunakan kata laluan yang unik dan kukuh memandangkan anda tidak perlu mengingatinya.

Sesetengah pengurus kata laluan menyimpan kata laluan di dalam komputer atau peranti mudah alih, dan ada diantaranya yang menyimpan di Awan. Sebagai tambahan, kebanyakan pengurus kata laluan berupaya untuk menyelaraskan kata laluan anda secara automatik merentasi beberapa peranti pengguna. Dengan ini apabila anda mengemaskini kata laluan pada komputer riba, perubahan tersebut akan diselaraskan kepada semua peranti anda. Tidak kira di mana pangkalan data

Pengurus Kata Laluan

disimpan, anda hanya perlu memasang pengurus kata laluan pada peranti untuk menggunakannya.

Apabila pertama kali anda menggunakan pengurus kata laluan, anda perlu memasukkan kata nama dan kata laluan secara manual. Kemudian, pengurus kata laluan boleh mengesan apabila anda membuat percubaan untuk mendaftar akaun dalam talian yang baru atau mengemas kini kata laluan untuk akaun sedia ada dan mengemaskini pangkalan data sewajarnya. Ianya boleh dilakukan kerana kebanyakan pengurus kata lalaunbekerjasama dengan pelayar web . Intergrasi ini membolehkan mereka untuk log masuk anda ke laman sesawang secara automatik.

Pengurus kata laluan merupakan cara yang mudah untuk anda menyimpan semua kata laluan dengan selamat.

Kata laluan induk yang anda gunakan untuk melindungi kandungan pengurus kata laluan adalah kritikal dan perlulah kukuh dan sukar untuk sesiapa menekanya. Malah kami mencadangkan supaya anda menggunakan frasa laluan untuk kata laluan induk, salah satu bentuk kata laluan yang paling kukuh. Jika pengurus kata laluan anda menyokong pengesahan dua langkah, gunakannya untuk kata laluan induk. Akhir sekali, pastikan anda mengingati kata laluan induk anda. Jika terlupa, anda tidak akan dapat akses kepada kata laluan yang lain.

Memilih Pengurus Kata Laluan

Terdapat banyak pengurus kata laluan untuk dipilih. Di dalam seksyen Sumber kami menyediakan pautan kepada ulasan pengurus kata laluan. Sementara itu, untuk memilih pengurus kata laluan yang terbaik untuk anda, ingat perkara yang berikut:

- Pengurus kata laluan sepatutnya mudah untuk digunakan. Jika anda dapati penyelesaian tersebut sukar untuk difahami, cari pengurus lain yang lebih sesuai dengan gaya dan kemahiran teknologi anda.
- Pengurus kata laluan seharusnya berfungsi pada semua peranti yang perlu anda gunakan. Ia juga seharusnya mampu menyelaraskan kata laluan dengan mudah kepada semua peranti anda.
- Gunakan pengurus kata laluan yang terkenal. Berhati-hatilah dengan produk yang baru dalam pasaran dan kurang mendapat maklum balas dari komuniti. Penjenayah siber boleh mencipta pengurus kata laluan yang palsu untuk mencuri maklumat anda. Selain itu berhati-hati dengan penjual yang membangunkan penyulitan mereka sendiri.
- Elakkan daripada menggunakan pengurus kata laluan yang boleh memulihkan kata laluan induk untuk anda. Ini bermakna ia tahu kata laluan induk, dan seterusnya boleh mendatangkan risiko terhadap anda..

Pengurus Kata Laluan

- Apa sahaja penyelesaian yang dipilih, pastikan penjual akan terus membuat tampalan dan kemas kini kepada pengurus kata laluan secara aktif, dan pastikan anda menggunakan versi terkini.
- Pengurus kata laluan tersebut seharusnya mempunyai keupayaan untuk menjana kata laluan yang kukuh untuk secara automatik dan mempamerkan tahapkekukuhan kata laluan yang telah anda pilih.
- Pengurus kata laluan seharusnya memberikan pilihan untuk menyimpan maklumat sensitif lain seperti jawapan kepada soalan keselamatan rahsia, kad kredit atau nombor keahlian penumpang penerbangan kerap anda.

Pengurus kata laluan adalah cara yang terbaik untuk menyimpan semua kata laluan dan maklumat sensitif anda. Walaubagaimanapun, memandangkan ia menyimpan maklumat yang sangat penting, pastikan anda menggunakan kata laluan induk yang unik dan kukuh, yang bukan sahaja sukar untuk penyerang menekanya, malah ianya mudah untuk anda ingati.

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

Top Password Managers of 2017:	https://www.pcmag.com/article2/0,2817,2407168,00.asp
Passphrases:	https://securingthehuman.sans.org/ouch/2017#april2017
Two-step Verification:	https://www.securingthehuman.org/ouch/2015#september2015
Lock Down Your Login:	https://www.lockdownyourlogin.org/
SANS Security Tip of the Day:	https://www.sans.org/tip-of-the-day

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