OUCH! | Jun 2016

Surat Berita Bulanan berkenaan Kesedaran Keselamatan Untuk Pengguna Komputer

OUCH!

DALAM ISU INI...

Penyulitan

Apakah Penyulitan?

Anda mungkin pernah mendengar terma 'penyulitan' dan bagaimana anda harus menggunakannya untuk melindungi diri dan maklumat anda. Bagaimanapun, penyulitan adakala agak mengelirukan dan anda perlu tahu batasnya. Dalam surat berita ini kami akan menerangkan apakah penyulitan menggunakan terma yang mudah, bagaimana ia boleh melindungi anda dan bagaimana cara untuk menggunakannya dengan betul.

Editor Jemputan

Francesca Bosco (**@francibosco**) adalah seorang penyelidik dan pegawai projek, mengendalikan projek-projek jenayah siber, keselamatan siber dan penyalahgunaan teknologi. Beliau bekerja di United Nations Interregional Crime and Justice Research Institute dan beliau adalah turut membangunkan Tech and Law Center.

Anda mempunyai maklumat sensitif yang banyakdalam peranti anda, seperti dokumen peribadi, gambar dan e-mel. Jika salah satu daripada peranti anda hilang atau dicuri, kesemua maklumat sulit anda boleh dicapai oleh sesiapa yang mempunyainya. Sebagai tambahan anda mungkin melakukan transaksi dalam talian sensitif seperti perbankan dan membeli-belah. Jika sesiapa memantau aktiviti ini mereka boleh mencuri maklumat anda seperti akaun kewangan atau nombor kad kredit anda. Penyulitan melindungi anda dalam situasi sebegini dengan memastikan maklumat anda tidak boleh dicapai atau diubahsuai oleh mereka yang tidak bertanggungjawab.

Kaedah penyulitan telah digunakan sejak beribu tahun. Hari ini, penyulitan telah menjadi sangat canggih, tetapi masih digunakan untuk tujuan yang sama – untuk menghantar maklumat dari tempat ke satu tempat dengan memastikan hanya mereka yang dibenarkan dapat membaca maklumat tersebut. Apabila maklumat tidak di sulitkan, ia dipanggil teks kosong(plain-text). Ini bermakna sesiapa sahaja boleh melihat dan membacanya. Penyulitan menukar maklumat ini kepada format yang tidak dapat dibaca yang dipanggil teks sifer(cipher-text). Penyulitan pada hari ini menggunakan operasi matematik yang kompleks dan kunci yang unik untuk menukarkan maklumat anda kepada teks sifer. Kunci inilah yang mengunci atau membuka maklumat anda. Selalunya, kunci ini merupakan kata laluan atau kod laluan.

Apa Yang Boleh Anda Sulitkan?

Secara umumnya terdapat dua jenis data untuk disulitkan, data dalam keadaan rehat (seperti data yang tersimpan dalam peranti mudah alih anda) dan data dalam pergerakan (seperti menerima e-mel atau menghantar pesanan kepada sahabat.

Penyulitan

Menyulitkan data dalam keadaan rehat adalah penting untuk melindungi maklumat sekiranya berlaku kehilangan atau kecurian peranti mudah alih atau komputer. Peranti hari ini sangat berkuasa dan menyimpan maklumat yang banyak, tetapi ianya juga mudah hilang. Sebagai tambahan, media mudah alih yang lain juga boleh menyimpan maklumat sensitif, seperti pemacu USB atau cakera keras mudah alih. Penyulitan penuh cakera(Full Disk Encryption – FDE) adalah kaedah penyulitan yang digunakan dengan meluas di mana ia menyulitkan keseluruhan cakera dalam sistem anda. Ini bermakna semua di dalam sistem tersebut disulitkan untuk anda, anda tidak perlu memilih apa yang perlu disulitkan. Kebanyakan komputer terkini sekarang ini didatangkan dengan FDE, tetapi anda mungkin perlu mengaktifkannya secara manual. Untuk komputer Mac ianya dipanggil FileVault manakala untuk komputer Windows, bergantung kepada versi, anda boleh menggunakan BitLocker atau Device Encryption. Kebanyakan peranti mudah alih juga menyokong FDE. iOS pada iPhone dan iPad mengaktifkan FDE secara automatik sebaik sahaja kod laluan ditetapkan. Bermula dengan Android 6.0(Marshmallow), Google memerlukan FDE diaktifkan secara lalai, dengan syarat perkakasan memenuhi piawaian minimum.

Penyulitan adalah satu cara yang sangat berkesan untuk membantu melindungi maklumat anda, tetapi ianya hanya sekukuh kunci anda.

Maklumat juga sangat terdedah apabila ianya di dalam transit. Jika data tersebut tidak disulitkan, ianya boleh dipantau, diubahsuai dan diambil dalam talian. Inilah sebabnya mengapa anda perlu pastikan sebarang transaksi dan komunikasi sensitif dalam talian disulitkan. Salah satu jenis penyulitan dalam talian adalah HTTPS. Ini bermakna kesemua trafik dari pelayar anda ke pelayan disulitkan. Contoh biasa penyulitan atas talian adalah https:// pada URL, ikon mangga pada pelayar atau bar URL bertukar warna hijau. Satu lagi contoh adalah ketika anda menghantar atau menerima emel. Kebanyakan klien emel menyediakan kebolehan untuk penyulitan yang mungkin perlu anda aktifkan. Contoh ketiga penyulitan data dalam transit adalah di antara dua pengguna yang sedang berbual antara satu sama lain, seperti menggunakan iMessage, Wickr, Signal, Whatsapp atau Telegram. Aplikasi seperti ini menggunakan penyulitan dari hujung ke hujung yang menghalang pihak ketiga dari mencapai data semasa ia dihantar dari satu sistem atau peranti kepada yang lain.

Melakukannya Dengan Betul

Untuk memastikan anda betul-betul dilindungi apabila menggunakan penyulitan, adalah penting bagi anda menggunakannya dengan betul.

Penyulitan

- Penyulitan anda adalah sekukuh kunci anda. Jika seseorang meneka atau mendapat capaian kepada kunci anda, mereka akan mendapat capaian kepada data anda. Lindungi kunci anda. Jika anda menggunakan kata laluan atau kod laluan untuk kunci anda, pastikan ianya kukuh dan unik. Semakin panjang kata laluan anda, semakin sukar untuk penyerang meneka atau menggunakan serangan daya kasar. Jangan lupa kata laluan anda, tanpa kunci tersebut anda tidak dapat lagi menyahsulit maklumat anda. Jika anda tidak dapat mengingati kesemua kata laluan anda kami mencadangkan anda menggunakan pengurus kata laluan.
- Penyulitan anda hanyalah sekukuh keselamatan peranti anda. Jika peranti anda telah digodam atau dijangkiti perisian hasad penyerang siber boleh memintas penyulitan anda. Oleh sebab itu ianya sangat penting bagi anda untuk mengambil langkah tambahan untuk melindungi peranti anda, termasuklah menggunakan antivirus, kata laluan yang kukuh dan memastikan peranti anda dikemas kini.
- Kebanyakan aplikasi dalam talian dan komputer kini menawarkan penyulitan yang kukuh untuk melindungi data dan komunikasi anda. Jika aplikasi yang anda mahukan tidak menyokong penyulitan, pertimbangkan alternatif lain.

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

Encryption Explained:	http://www.howtogeek.com/howto/33949/htg-explains-what-is-encryption-and-how-does-it-work/
Passphrases:	https://securingthehuman.sans.org/ouch/2015#april2015
Password Managers:	https://securingthehuman.sans.org/ouch/2015#october2015
What Is Malware:	https://securingthehuman.sans.org/ouch/2016#march2016
Securing Your New Tablet:	https://securingthehuman.sans.org/ouch/2016#january2016

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