Surat Berita Bulanan berkenaan Kesedaran Keselamatan Untuk Pengguna Komputer

Adakah Saya Digodam?

Pengenalan

Tidak kira betapa selamatnya anda, sama seperti memandu kereta, lambat laun anda mungkin akan berdepan dengan kemalangan. Berikut adalah klu untuk membantu anda menilai jika anda telah digodam dan jika ya, apa yang patut anda lakukan. Lebih awal anda mengetahui sesuatu yang buruk telah berlaku, lebih banyak peluang anda untuk membaiki masalah tersebut.

Klu Yang Anda Telah Digodam

- **Program anti-virus akan menjana amaran jika sistem anda dijangkiti. Pastikan amaran tersebut dijanakan oleh perisian anti-virus dan bukan tetingkap timbul dari laman sesawang yang cuba menipu supaya anda menelefon suatu nombor atau memasang sesuatu. Tidak pasti? Buka program anti-virus anda.**
- **Anda mendapat tetingkap timbul memberitahu komputer anda telah disulitkan dan anda perlu membayar wang tebusan untuk mengembalikan fail tersebut.**
- **Pelayar membawa anda ke laman sesawang selain dari yang anda mahukan.**
- **Komputer atau aplikasi sentiasa rosak, dan terdapat ikon untuk aplikasi yang tidak diketahui atau tetingkap ganjil timbul.**
- **Kata laluan anda tidak lagi berfungsi walaupun anda tahu ianya betul.**
- **Rakan-rakan bertanya mengapa anda menghantar mereka e-mel-e-mel spam dan anda tidak pernah menghantarnya.**
- **Terdapat transaksi pada kad kredit atau pengeluaran bank yang tidak pernah anda lakukan daripada akaun.**

Bagaimana Hendak Bertindak

Jika anda syakanda telah digodam adalah lebih baik untuk bertindak secepat mungkin. Jika ianya berkenaan kerja, jangan cuba untuk menanganinya sendirian. Laporkan insiden ini dengan serta-merta. Jika sistem atau akaun persendirian anda telah digodam, berikut adalah beberapa langkah yang boleh diambil.

Tukar Kata Lalauan: Ini termasuklah menukar bukan sahaja kata laluan pada komputer dan peranti mudah alih, bahkan akaun dalam talian anda. Jangan gunakan komputer yang telah digodam untuk menukar kata laluan, dan gunakan sistem lain yang anda pasti adalah selamat. Jika anda mempunyai banyak akaun mulakan dengan yang paling penting. Jika anda tidak dapat mengingati kesemua kata laluan anda, gunakan pengurus kata laluan.

Kewangan: Bagi isu berkaitan dengan kad kredit atau akaun kewangan, hubungi bank atau syarikat kad kredit secepat mungkin. Gunakan nombor yang dipercayai seperti nombor di belakang kad kredit, penyata bank atau lawati laman sesawang mereka dari komputer yang dipercayai. Sebagai tambahan pertimbangkan untuk meminta bank membekukan fail kredit anda.

Anti-virus: Jika perisian anti-virus anda memaklumkan terdapat jangkitan pada fail, ikuti langkah yang dicadangkan. Kebanyakan perisian anti-virus akan memberikan pautan yang boleh anda ikuti untuk mengetahui lebih lanjut mengenai jangkitan tersebut.

Pasang Semula: Jika anda tidak boleh membaiki komputer yang telah dijangkiti atau mahu memastikan sistem anda selamat, pasang semula sistem operasi. Jangan pasang semula dari sandaran, sebaliknya sandaran digunakan untuk memulihkan fail peribadi anda. Jika anda rasa tidak mampu untuk melakukannya sendiri, dapatkan khidmat pakar untuk bantuan. Atau jika komputer atau peranti anda sudah lama, mungkin ianya lebih mudah untuk digantikan dengan yang baru. Akhirnya jika anda telah selesai membina semula atau membeli yang baru, pastikan ia dikemaskini dan bolehkan kemaskini secara automatik.

Sandaran: Kunci kepada melindungi diri anda adalah dengan bersedia dari awal dengan melakukan sandaran dengan kerap. Banyak solusi akan menyandarkan fail anda setiap hari atau setiap jam secara automatik. Tidak kira solusi mana yang dipilih pastikan anda mampu memulihkan fail tersebut. Selalunya pemulihan data dari sandaran adalah cara terakhir untuk anda kembali pulih selepas digodam.

Penguatkuasaan Undang-undang: Jika rasa terancam, laporkan kepada penguatkuasa undang-undang tempatan. Jika anda telah menjadi mangsa kepada kebocoran data dan berada di Malaysia, anda boleh merujuk kepada http://www.pdp.gov.my/index.php/my/.

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/.

Editor Jemputan

Dr. Johannes Ullrich *(@johullrich) merupakan Dekan Penyelidikan di SANS Technology Institute, Pengarah SANS Internet Storm Center dan juga seorang felo SANS. Beliau mencipta rangkaian kerjasama sensor DShield dan menjadi hos podcast berita keselamatan rangkaian harian Internet Storm Center.*

Sumber

Sandaran:	https://www.sans.org/u/JGP
Ungkapan Laluan:	https://www.sans.org/u/JGU
Pengurus Kata Laluan:	https://www.sans.org/u/JGZ
Apakah Perisian Hasad:	https://www.sans.org/u/JH4
Pembekuan Kredit:	https://krebsonsecurity.com/2018/09/credit-freezes-are-free-let-the-ice-age-begin/