Surat Berita Bulanan berkenaan Kesedaran Keselamatan Untuk Pengguna Komputer

4 Cara Mudah untuk Kekal Selamat

Gambaran Keseluruhan

Menjadikan kesemua teknologi selamat dan terjamin boleh kelihatan berlebihan dan mengelirukan. Walaubagaimanapun, tanpa mengira teknologi yang digunakan dan cara anda menggunakan teknologi tersebut, berikut adalah empat langkah mudah yang akan membantu anda untuk kekal selamat.

1. Anda: Pertama sekali, tiada sebarang teknologi boleh melindungi anda sepenuhnya melainkan diri anda sendiri sebagai pertahanan terbaik. Penyerang ambil maklum cara terbaik untuk mendapatkan maklumat yang mereka mahukan adalah dengan menyasarkan anda, daripada komputer atau peranti lain. Jika mereka ingin mendapatkan kata laluan anda, maklumat kad kredit atau mengawal komputer anda, mereka akan cuba untuk menipu anda untuk memberikan maklumat tersebut kepada mereka, kebiasaannya dengan mencipta unsur mendesak. Contohnya, mereka boleh menghubungi anda dengan menyamar sebagai pekerja sokongan teknikal Microsoft dan mendakwa komputer anda telah berjangkit, sedangkan mereka merupakan penjenayah siber yang inginkan capaian kepada komputer anda. Atau mungkin juga mereka menghantar satu e-mel amaran mengenai bungkusan yang tidak berjaya dihantar dan mendesak anda untuk klik pada satu pautan untuk mengesahkan alamat surat-menyurat anda, sedangkan perkara itu adalah helah mereka supaya anda melawat laman web berhasad yang akan menggodam komputer anda. Pada dasarnya, pertahanan terbaik terhadap penyerang siber ialah diri anda sendiri. Fikirkan dengan logik akal dan anda boleh mengesan dan menghentikan kebanyakan serangan.

2. Frasa Laluan: Kelajuan pengkomputeran moden telah menjadikan kata laluan 8-aksara yang digunakan dulu ketinggalan zaman dan mudah untuk diserang. Apabila sesebuah laman meminta anda untuk mencipta kata laluan, anda perlu mencipta frasa laluan yang kuat dan unik. Frasa laluan ialah sejenis kata laluan yang menggunakan satu siri kata-kata yang mudah, seperti “lebah madu hujan”. Semakin panjang frasa laluan anda, semakin kuat kata laluan anda. Frasa laluan yang unik bermaksud anda menggunakan frasa laluan berbeza untuk setiap peranti atau akaun dalam talian anda. Dengan cara ini, apabila satu frasa laluan anda telah dikompromi, semua akaun dan peranti anda yang lain masih selamat. Tidak ingat semua frasa laluan anda? Gunakan pengurus kata laluan, iaitu program khusus yang menyimpan semua frasa laluan anda dengan selamat dan disulitkan (dan mempunyai pelbagai ciri menarik yang lain).

Akhir sekali, anda perlu membolehkan pengesahan dua-langkah (atau dikenali sebagai dua-faktor atau pengesahan pelbagai-faktor). Selain menggunakan kata laluan, penambahan langkah kedua, seperti penerimaan

kod yang dihantar ke telefon pintar anda atau sebuah aplikasi yang akan menjana kod untuk anda. Pengesahan dua-langkah barangkali merupakan cara yang paling penting untuk anda ambil bagi melindungi akaun dalam talian dan adalah langkah yang lebih mudah seperti yang disangka.

3. Mengemaskini: Sentiasa pastikan setiap komputer, peranti mudah alih, program dan aplikasi yang sedang anda gunakan dipasang dengan perisian yang terkini. Penyerang siber sentiasa mencari kelemahan baru dalam perisian yang dipasang pada peranti yang anda gunakan. Selepas kelemahan ditemui, mereka akan menggunakan program khas untuk mempergunakan kelemahan tersebut dan menggodam peranti yang sedang anda gunakan. Sementara itu, syarikat pengeluar perisian bagi peranti tersebut sentiasa bekerja keras untuk mengeluarkan kemas kini. Dengan memastikan komputer dan peranti yang sedang anda gunakan dipasang kemas kini terbaru dengan segera, anda menjadikan lebih sukar untuk mereka yang ingin menggodam anda. Bagi memastikan anda sentiasa menggunakan kemas kini semasa, anda hanya perlu membolehkan kemas kini automatik sekiranya boleh. Aturan ini digunapakai bagi hampir kesemua teknologi yang berhubung dengan rangkaian, termasuk televisyen yang berhubung dengan rangkaian internet, alat pengawasan bayi, kamera keselamatan, penghala rumah, konsol permainan termasuk kereta anda.

4. Sandaran dan Mendapatkan Semula: Kadang-kadang, walaupun anda berhati-hati, anda masih boleh digodam. Sekiranya perkara tersebut terjadi, cara untuk mendapatkan semula semua maklumat peribadi anda adalah melalui data sandaran. Oleh itu, sentiasa pastikan sandaran dilakukan secara berkala untuk semua maklumat penting dan sahkan anda boleh mendapatkan semula data anda daripada sandaran tersebut. Kebanyakan sistem operasi dan peranti mudah alih menyokong sandaran automatik ke pemacu luaran atau ke awan.

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

Pengajar Bertauliah SANS ***Steve Anson*** *memberi panduan kepada pasukan keselamatan maklumat dan agensi kerajaan di sekeliling dunia untuk meningkatkan tahap keselamatan mereka. Steve merupakan penulis buku Applied Incident Response dan berkongsi pengetahuan beliau secara percuma kepada pengamal keselamatan di* www.AppliedIncidentResponse.com.

Sumber

Pengendalian Sosial:	https://www.sans.org/u/W3G
Penipuan Menyasar Individu:	https://www.sans.org/u/W3Q
Menghasilkan Kata Laluan yang Mudah:	https://www.sans.org/u/W3V
Ada Salinan Sandaran?:	https://www.sans.org/u/W40