OUCH! | Januari, 2015

Surat Berita Bulanan berkenaan Kesedaran Keselamatan Untuk Pengguna Komputer

OUCH!

DALAM ISU KALI INI...

Penggunaan Apps Mudah Alih Secara Selamat

Pengenalan

Peranti mudah alih seperti telefon pintar dan tablet telah menjadi salah satu teknologi utama yang kita gunakan dalam kehidupan seharian dan dunia kerjaya. Apa yang menjadikan peranti mudah alih begitu serba boleh adalah kewujudan berjuta-juta apps yang boleh kita pilih. Apps membolehkan kita menjadi lebih produktif, berkomunikasi dan berkongsi dengan sesiapa dengan pantas, belajar dan berlatih atau berseronok. Walaubagaimanapun, kuasa yang dibawakan oleh semua apps mudah alih ini datang dengan risiko. Berikut adalah beberapa langkah yang boleh diambil untuk menjamin dan mengekalkan keselamatan apps mudah alih anda.

Editor Jemputan

Chris Crowley merupakan perunding bebas, pengarang kursus dan pengajar kanan SANS. Beliau aktif di Twitter **@CCrowMontance** dan di Google plus: **+ChrisCrowley**.

Mendapatkan Apps Mudah Alih

Langkah pertama adalah memastikan anda memuat turun dari sumber yang selamat dan boleh dipercayai. Ingat, sesiapa pun boleh membangunkan apps mudah alih, jadi anda perlu berhati-hati dari mana anda dapatkannya. Penjenayah siber semakin pandai mencipta dan mengedarkan apps mudah alih yang dijangkiti yang kelihatan sahih. Jika anda memasang salah satu apps yang telah dijangkiti, penjenayah ini kemudiannya dapat mengawal peranti mudah alih anda termasuklah membaca e-mel anda, mendengar percakapan anda dan menuai senarai kenalan. Hanya dengan memuat turun dari sumber yang dipercayai dan dikenali anda boleh mengurangkan kebarangkalian untuk memasang apps yang dijangkiti. Apa yang anda mungkin tidak sedari adalah jenama peranti mudah alih anda menentukan pilihan anda.

Bagi peranti Apple seperti iPad atau iPhone, anda hanya boleh memuat turun apps mudah alih dari persekitaran yang diuruskan, iaitu Apple app store. Kelebihannya adalah Apple melakukan semakan keselamatan ke atas kedua-dua apps dan pembuatnya. Walaupun Apple tidak dapat menangkap semua orang jahat atau apps yang dijangkiti, persekitaran yang diuruskan ini membantu mengurangkan risiko untuk anda memasang apps yang dijangkiti. Sebagai tambahan, jika Apple menemui apps di dalam stornya yang dipercayai telah dijangkiti, mereka akan mengeluarkannya dengan segera. Telefon Windows menggunakan pendekatan yang sama untuk menguruskan apps mereka.

Peranti mudah alih android pula berbeza. Android memberikan anda fleksibiti dengan membenarkan anda memuat turun apps dari mana-mana sumber di internet. Walaupun begitu, dengan fleksibiliti ini anda perlu lebih bertanggungjawab. Anda perlu lebih berhati-hati dengan apps mudah alih yang anda muat turun dan pasang kerana bukan

Penggunaan Apps Mudah Alih Secara Selamat

Kunci untuk menggunakan apps mudah alih dengan selamat adalah dengan hanya memasang apps dari sumber yang dipercayai dan pastikan apps anda dikemas kini dan kebenarannya disahkan.

semuanya disemak. Google menyelenggarakan kedai apps mudah alih sama seperti Apple yang dipanggil Google Play. Apps yang anda muat turun dari Google Play secara asasnya telah disemak. Oleh yang demikian kami mencadangkan supaya anda memuat turun apps mudah alih untuk peranti Android hanya dari Google Play. Elakkan dari memuat turun apps Android dari laman sesawang lain, kerana sesiapa sahaja termasuk penjenayah siber boleh mencipta dan menyebarkan apps mudah alih berniat jahat dan menipu anda untuk menjangkiti peranti mudah alih anda. Sebagai perlindungan tambahan, pertimbangkan untuk memasang antivirus pada peranti mudah alih anda.

Untuk mengurangkan lagi risiko, elakkan apps yang baharu, mempunyai jumlah muat turun yang rendah atau yang mempunyai sedikit komen positif. Semakin lama apps tersebut tersedia atau lebih banyak komen positif yang diperoleh, berkemungkinan besar apps tersebut boleh dipercayai. Sebagai tambahan, hanya pasangkan apps yang perlu anda gunakan. Tanya diri anda, adakah saya perlu menggunakan apps ini? Setiap apps bukan sahaja membawa keterdedahan yang baharu tetapi juga isu privasi. Jika anda berhenti menggunakan sebarang apps, buangkannya dari peranti mudah alih anda (pasangkan semula kemudian jika anda perlu menggunakannya).

Akhir sekali, anda mungkin berkeinginan untuk melakukan jailbreak atau root peranti mudah alih anda. Ini adalah proses menggodam dan memasang apps yang tidak diluluskan atau menukar fungsi sedia ada yang asal. Kami mengesyorkan supaya anda tidak melakukan jailbreaking atau rooting, bukan sahaja ia melepasi atau memintas kebanyakkan ciri keselamatan yang dibina dalam peranti mudah alih anda, bahkan ia juga membatalkan jaminan dan kontrak sokongan.

Keizinan

Setelah anda memasang apps mudah alih dari sumber yang dipercayai, langkah seterusnya adalah memastikan ianya ditala dengan selamat dan menjaga privasi anda. Memasang dan/atau menala apps mudah alih selalunya memerlukan anda memberi beberapa keizinan. Sentiasa fikir dahulu sebelum membenarkan sebarang capaian, adakah apps anda memerlukan kebenaran tersebut untuk berfungsi? Sebagai contoh, sesetengah apps menggunakan perkhidmatan geo-lokasi. Jika anda membenarkan apps sentiasa tahu kedudukan anda, anda juga membenarkan pembuat app tersebut menjejaki setiap pergerakan anda, mereka juga boleh menjualnya kepada pihak ketiga. Jika anda tidak mahu memberikan kebenaran kepada apps, cari apps lain yang memenuhi keperluan anda. Ingat, anda mempunyai banyak pilihan di luar sana. Peranti Apple membenarkan sesetengah kebenaran ditukar dalam tetapan atau ketika digunakan, seperti capaian kepada maklumat geo-lokasi. Peranti mudah alih Windows dan Android ada-

Penggunaan Apps Mudah Alih Secara Selamat

lah berbeza, mereka menggunakan pendekatan semua-atau-tiada. Jika anda tidak memenuhi semua kebenaran yang dikehendaki, anda tidak mungkin boleh memasang apps tersebut.

Mengemaskini Apps

Apps mudah alih, sama seperti sistem operasi komputer atau peranti mudah alih, mesti dikemas kini untuk memastikan ianya yang terkini. Penjenayah sentiasa mencari kelemahan dalam apps. Mereka melancarkan serangan untuk mengeksploitasi kelemahan tersebut. Pencipta yang membangunkan apps anda juga mencipta dan mengedarkan kemas kini untuk membaiki kelemahan dan menjaga peranti anda. Semakin kerap anda semak dan memasang kemas kini, semakin bagus. Kebanyakan platform membolehkan anda untuk membuat tetapan kepada sistem untuk mengemas kini apps mudah alih secara automatik. Kami mencadangkan tetapan ini. Jika ini tidak mungkin, kami mencadangkan anda menyemak sekurang-kurangnya setiap dua minggu untuk kemas kini apps mudah alih anda. Walaupun begitu, apabila apps anda dikemas kini sentiasa pastikan anda sahkan sebarang kebenaran baharu yang ia perlukan.

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 http://www.securingthehuman.org.

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

Social Engineering:	http://www.securingthehuman.org/ouch/2014#november2014
Disposing Your Mobile Device:	http://www.securingthehuman.org/ouch/2014#june2014
Securing Your New Tablet:	http://www.securingthehuman.org/ouch/2013#december2013
Common Security Terms:	http://www.securingthehuman.org/resources/security-terms
SEC575: Mobile Device Security Course:	http://www.sans.org/sec575

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

