Surat Berita Bulanan berkenaan Kesedaran Keselamatan Untuk Pengguna Komputer

OUCH!

DALAM ISU KALI INI...

- **Maklumat Anda**
- **Menyeka Peranti Anda**
- **SIM/Kad Storan Luaran**

Melupuskan Peranti Mudah Alih Anda

Pengenalan

Inovasi peranti mudah alih, seperti tablet dan telefon pintar berlaku pada kadar yang menakjubkan. Hasilnya, kebanyakan daripada kita menukar peranti mudah alih sekerap 18 bulan sekali. Malangnya, terlalu ramai yang membuang peranti mudah alih lama mereka dengan mudah tanpa mengambil peduli berapa banyak maklumat peribadi yang terkumpul di dalam peranti mereka. Dalam surat berita kali ini kita akan menyentuh tentang jenis maklumat peribadi yang mungkin tersimpan dalam peranti mudah alih anda dan bagaimana anda boleh menyekanya dengan selamat sebelum melupuskan atau memulangkannya. Jika peranti anda diberikan oleh majikan atau mempunyai maklumat organisasi di dalamnya, pastikan anda semak dahulu dengan penyelia tentang tatacara yang betul untuk melupus dan membuat backup (sandaran) sebelum mengikuti langkah-langkah berikut.

Editor Jemputan

Christopher Crowley (**@CCrowMontance**; **+ChrisCrowley**) merupakan seorang perunding yang berpangkalan di Washington DC. Beliau merupakan pengajar kanan bagi kursus Mobile Device Security and Ethical Hacking (SEC575) di SANS Institute dan pengarang untuk Incident Response Team Management (MGT535).

Maklumat Peribadi Anda

Anda mungkin tidak sedar bahawa peranti mudah alih menyimpan banyak maklumat sensitif yang mungkin melebihi apa yang disimpan di komputer anda. Maklumat biasa yang disimpan oleh peranti mudah alih adalah seperti :

- Tempat tinggal, tempat kerja dan tempat-tempat yang sering anda kunjungi.
- Butiran kenalan dalam buku alamat termasuk keluarga, rakan dan rakan sekerja.
- Sejarah panggilan termasuk panggilan masuk, panggilan keluar dan panggilan tidak dijawab.
- Pesanan ringkas dan pesanan suara.
- Sesi perbualan di dalam aplikasi seperti permainan dan media sosial.
- Sejarah lokasi berdasarkan koordinat GPS dan sejarah menara komunikasi.
- Sejarah pelayaran laman sesawang, cookies dan laman yang di cache.
- Gambar peribadi, rakaman video, audio dan e-mel.
- Kata laluan yang disimpan dan akses kepada akaun peribadi seperti perbankan dalam talian dan e-mel anda.
- Capaian kepada gambar, fail atau maklumat yang di simpan di awan.
- Maklumat mengenai kesihatan, termasuk kadar denyutan jantung anda, tekanan darah atau diet.

Menyeka Peranti Anda

Seperti yang boleh anda lihat, kemungkinan terdapat begitu banyak maklumat sensitif pada peranti mudah alih anda. Tidak kira bagaimana cara anda melupuskan peranti mudah alih anda, seperti mendermakannya, memberinya kepada ahli

© The SANS Institute 2014

Melupuskan Peranti Mudah Alih Anda

keluarga yang lain, menjualnya semula atau dengan membuangnya begitu sahaja, anda perlu pastikan maklumat sensitif anda dipadamkan terlebih dahulu. Sebagai tambahan, anda perlu memadam maklumat yang tersimpan jika anda memulangkan peranti mudah alih atau menukarnya dengan yang baharu. Jika tidak, sesiapa yang memperoleh peranti mudah alih tersebut boleh membuat capaian dengan mudah. Walaubagaimanapun, sebelum anda mula menyeka maklumat anda, anda mungkin perlu membuat sandaran bagi semua maklumat anda, termasuk gambar, video atau apa-apa maklumat lain. Setelah anda menyeka peranti anda, anda tidak akan dapat mengembalikan sebarang maklumat yang disimpan dalam peranti berkenaan.

Apabila melupuskan peranti mudah alih anda, pastikan anda melakukan tetapan semula kilang dan keluarkan SIM dan sebarang kad SD jika peranti anda mempunyainya.

Setelah membuat sandaran maklumat, anda kemudiannya perlu memadamkannya sehingga selamat. Sekadar memadam fail, gambar atau maklumat masih tidak mencukupi. Maklumat yang telah dipadamkan boleh dipulihkan kembali dengan menggunakan alatan percuma yang boleh dijumpai di internet. Sebaliknya anda perlu memadam kesemua maklumat dalam peranti tersebut sehingga selamat, ini yang dipanggil menyeka. Langkah ini menulis semula maklumat dan memastikan ianya tidak boleh dipulihkan. Cara paling mudah untuk melakukannya adalah dengan menggunakan fungsi “tetapan semula kilang” pada peranti anda. Ini akan mengembalikannya kepada keadaan asal seperti anda baharu membelinya. Kami mendapati bahawa tetapan semula kilang merupakan kaedah paling mudah dan paling selamat untuk membuang maklumat daripada peranti anda. Fungsi tetapan semula kilang berbeza mengikut peranti. Senarai di bawah merupakan langkah bagi tiga peranti paling popular:

- Peranti Apple iOS: Settings |General |Reset |Erase All Content and Settings
- Peranti Android: Settings |Privacy |Factory Data Reset
- Telefon Windows: Settings | About |Reset Your Phone

Jika anda masih mempunyai soalan tentang bagaimana untuk melakukan tetapan semula kilang, semak semula manual pengguna atau laman sesawang pengeluar. Ingatlah, memadam maklumat peribadi anda masih tidak mencukupi kerana ia boleh dipulihkan dengan mudah.

SIM & Kad Storan Luaran

Sebagai tambahan, selain maklumat yang tersimpan dalam peranti, anda juga perlu mempertimbangkan apa yang perlu dilakukan pada kad SIM (Modul Pengenalan Pelanggan) anda. Kad SIM digunakan oleh peranti mudah alih untuk membuat panggilan telefon atau sambungan data. Apabila anda membuat tetapan semula pada peranti anda, kad SIM masih menyimpan maklumat tentang akaun anda. Jika anda ingin menyimpan nombor telefon dan menukar kepada peranti baru,

© The SANS Institute 2014

Melupuskan Peranti Mudah Alih Anda

maklumkan kepada jurujual telefon untuk memindahkan kad SIM anda. Jika ianya mustahil, sebagai contoh telefon baharu anda menggunakan kad SIM berlainan saiz, simpan kad SIM lama anda dan siat-siatkannya atau musnahkannya secara fizikal untuk menghalang orang lain daripada menggunakannya semula.

Akhir sekali, sesetengah peranti mengguna pakai kad SD yang berlainan untuk storan tambahan. Kad storan ini lazimnya mengandungi gambar, aplikasi telefon pintar dan kandungan sensitif yang lain. Pastikan anda mengeluarkan sebarang kad storan luaran daripada peranti mudah alih sebelum melupuskannya (untuk sesetengah peranti, kad SD mungkin terselindung di dalam ruangan bateri, berkemungkinan di bawah bateri). Kad ini selalunya boleh diguna semula dalam peranti mudah alih yang baharu, atau boleh digunakan sebagai storan umum pada komputer anda dengan penyesuai USB. Jika mustahil untuk menggunakan semula kad SD anda, sama seperti kad SIM lama anda, kami mengesyorkan ianya dimusnahkan secara fizikal.

Jika anda tidak pasti dengan mana-mana langkah yang disarankan dalam surat berita ini, bawa peranti mudah alih anda ke kedai di mana anda belinya dan dapatkan bantuan daripada juruteknik terlatih. Akhirnya, jika anda mahu membuang sahaja peranti tersebut, pertimbangkannya sebagai sumbangan. Terdapat banyak badan kebajikan yang akan menerima sumbangan anda.

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

NIST SP800-88 Rev. 1: http://csrc.nist.gov/publications/drafts/800-88-rev1/sp800_88_r1_draft.pdf

OUCH! Backups: http://www.securingthehuman.org/ouch/2013#september2013

OUCH! diterbitkan oleh program SANS “Securing The Human” dan diedarkan di bawah lesen Creative Commons BY-NC-ND 3.0. Kebenaran diberikan untuk mengedarkan surat berita ini atau mengunakannya dalam mana mana program kesedaran selagi tiada perubahan dibuat kepada kandungan asal.

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