Surat Berita Bulanan berkenaan Kesedaran Keselamatan Untuk Pengguna Komputer

OUCH!

DALAM KELUARAN INI...

Media Sosial

Mukadimah

Laman media sosial seperti Facebook, Twitter, Instagram dan LinkedIn merupakan sumber yang menakjubkan, membolehkan anda untuk bertemu, berhubung dan berkongsi dengan orang-orang di seluruh dunia. Walaubagaimanapun, kuasa ini semua hadir dengan risiko, bukan sahaja kepada anda, malah rakan dan majikan. Dalam isu kali ini, kami menerangkan bahayanya dan bagaimana untuk menggunakannya dengan selamat.

Editor Jemputan

Tanya Baccam merupakan seorang perunding keselamatan. Beliau telah pun menjadi pengarang dan pengajar SANS lebih sedekad, termasuk SEC502, SEC542, SEC401, MGT414, AUD507 dan banyak lagi kursus. Ikuti beliau di twitter di **@tbaccam**.

Privasi

Kebimbangan yang lazim dengan media sosial adalah untuk melindungi maklumat peribadi anda. Bahaya yang mungkin mengundang termasuklah:-

- **Impak Kepada Masa Hadapan**: Sesetengah organisasi membuat carian laman media sosial sebagai sebahagian semakan latar belakang. Pencatatan atau gambar yang mengaibkan dan kurang senang, tidak mengira umur, boleh menghalang anda daripada diambil bekerja atau naik pangkat. Sebagai tambahan, banyak universiti melakukan semakan yang serupa untuk pendaftaran pelajar baharu. Tetapan privasi mungkin tidak dapat melindungi anda kerana organisasi ini boleh meminta anda untuk “Like” atau mengikuti laman mereka atau sesetengah pencatatan boleh diarkibkan pada banyak laman.
- **Serangan Terhadap Anda**: Penyerang siber dapat menganalisis catatan anda dan menggunakannya untuk mendapatkan akses kepada maklumat organisasi anda. Sebagai contoh, mereka boleh menggunakan maklumat yang anda kongsi untuk meneka jawapan kepada soalan rahsia untuk menetap semula kata laluan dalam talian, mencipta e-mel khas yang menyasarkan anda yang dipanggil “spearfishing”, atau menyamar sebagai anda dan menelefon seseorang dalam organisasi. Sebagai tambahan serangan ini boleh digunakan pada dunia nyata, seperti mengetahui di mana anda tinggal dan bekerja.
- **Membahayakan Majikan Anda Dengan Tidak Sengaja**: Penjenayah atau pesaing boleh menggunakan maklumat sensitif yang anda catat tentang organisasi atau majikan anda. Sebagai tambahan, catatan anda boleh menjatuhkan reputasi organisasi anda. Pastikan anda menyemak polisi organisasi anda sebelum mencatat apa-apa maklumat tentang kerja anda, sebagai tambahan sesetengah catatan media sosial anda mungkin di pantau.

Perlindungan yang paling berkesan adalah dengan mengehadkan apa yang anda catat. Ya, tetapan privasi boleh memberikan sedikit perlindungan, namun ia selalunya mengelirukan dan bertukar dengan kerap tanpa pengetahuan anda. Sesuatu yang anda sangkakan hanyalah sesuatu yang persendirian sebelum ini boleh berubah menjadi umum dalam sekelip mata

Media Sosial

kerana pelbagai sebab. Tambahan pula, privasi catatan anda adalah selamat bersama siapa yang anda kongsi. Semakin ramai orang yang anda kongsi, maka lebih tinggi kemungkinan maklumat tersebut akan menjadi umum. Anda seharusnya menganggap apa sahaja yang anda catat boleh atau akan menjadi umum dan tetap di internet.

Akhirnya, waspada dengan apa yang rakan anda catat mengenai anda. Jika mereka membuat catatan yang membuat anda kurang selesa, minta mereka menurunkannya. Jika mereka enggan dan tidak ambil peduli, hubungi media sosial tersebut dan minta laman tersebut untuk membuang kandungan tersebut untuk anda. Pada masa yang sama, sentiasa hormati apa yang anda catat tentang orang lain.



Laman media sosial menyeronokkan dan berkuasa, tetapi berhati-hati dengan apa yang anda kongsikan dan dengan siapa anda berbuat demikian.

Keselamatan

Sebagai tambahan kepada isu privasi, berikut merupakan beberapa langkah untuk membantu melindungi aktiviti akaun media sosial anda:-

- **Log Masuk**: Lindungi setiap akaun dengan kata laluan yang kukuh, kata laluan yang unik dan jangan dedahkan kepada sesiapa pun. Sebagai tambahan, banyak laman media sosial menyokong pengesahan yang lebih kukuh, seperti pengesahan dua langkah. Sentiasa gunakan langkah pengesahan yang lebih kukuh ini apabila mungkin. Akhirnya, jangan gunakan akaun media sosial untuk log masuk kepada laman lain, jika ianya digodam kesemua akaun anda akan terdedah.
- **Tetapan Privasi**: Jika anda menggunakan tetapan privasi, pastikan anda semak dan uji sekerap mungkin. Laman media sosial sering mengubah tetapan ini dan ianya mudah untuk membuat kesilapan. Sebagai tambahan, terdapat banyak aplikasi dan perkhidmatan yang membenarkan anda untuk tag lokasi kepada kandungan yang anda catat (dipanggil geotagging). Semak tetapan ini sekerap mungkin jika anda mahu lokasi anda peribadi.
- **Penyulitan**: Laman media sosial menggunakan penyulitan yang dinamakan HTTPS untuk melindungi hubungan talian kepada laman tersebut. Sesetengah laman seperti Twitter dan Google+ menggunakannya secara lazim, manakala yang lainnya memerlukan anda untuk membenarkannya secara manual. Semak tetapan akaun media sosial anda dan benarkan HTTPS sebagai hubungan secara lazim apabila mungkin.
- **E-mel**: sentiasa berwaspada dengan e-mel yang kononnya dari laman media sosial, ini mungkin merupakan serangan penipuan yang dihantar oleh penjenayah siber. Cara paling mudah untuk menjawab kepada mesej seperti itu adalah dengan log masuk kepada media sosial anda secara terus, mungkin dari penanda yang telah disimpan, dan baca dan balas kepada sebarang mesej atau makluman dari laman sesawang.
- **Pautan Berniat Jahat/Penipuan**: Sentiasa berwaspada dengan pautan atau penipuan yang berpotensi yang dicatat pada laman media sosial. Orang jahat menggunakan media sosial untuk menyebarkan serangan mereka. Hanya kerana sesuatu mesej dipos oleh seorang rakan ia tidak bermakna mesej tersebut adalah daripada mereka, akaun mereka mungkin telah dikompromi. Jika terdapat ahli keluarga atau kenalan yang mencatat mesej aneh

Media Sosial

yang tidak dapat anda sahkan (seperti mereka telah dirompak dan memerlukan anda menghantar wang), hubungi telefon mudah alih mereka atau apa cara sekali pun untuk memastikan mesej tersebut adalah daripada mereka.

- **Aplikasi Mudah Alih**: kebanyakan laman media sosial menyediakan aplikasi mudah alih untuk mendapat akses kepada akaun dalam talian. Pastikan anda memuat turun aplikasi mudah alih ini dari sumber yang dipercayai dan telefon pintar anda dilindungi oleh kata laluan yang kukuh. Jika telefon pintar anda tidak dikunci semasa anda kehilangannya, sesiapa boleh mendapat akses kepada laman media sosial anda melalui telefon pintar anda dan membuat catatan sebagai anda.

Laman media sosial merupakan cara yang bagus untuk berhubung dan terus berhubung dengan dunia. Jika anda mengikut tip yang diberikan di sini, anda dapat menikmati pengalaman dalam talian yang lebih selamat. Untuk belajar lebih lagi mengenai cara penggunaan laman media sosial anda dengan selamat atau melaporkan aktiviti yang terlarang, semak laman keselamatan media sosial 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

Kata-kata laluan:	http://www.securingthehuman.org/ouch/2015#april2015
Dua langkah penentusahan:	http://www.securingthehuman.org/ouch/2013#august2013
Menggunakan Aplikasi Mudah Alih Secara Terjamin:	http://www.securingthehuman.org/ouch/2015#january2015
Mendidik Kanak-Kanak mengenai Keselamatan Siber:	http://www.securingthehuman.org/ouch/2015#june2015
Keselamatan Facebook:	https://www.facebook.com/safety

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