OUCH! | Juli 2015

Buletin Bulanan Kesadaran Keamanan bagi Pengguna Komputer

OUCH!

Dalam Edisi Ini...

Media Sosial

Sekilas

Situs media sosial seperti Facebook, Twitter, Instagram dan LinkedIn sangat menakjubkan, memungkinkan Anda bertemu, berinteraksi dan berbagi dengan orang lain diseluruh penjuru dunia. Namun dibalik semua kehebatan itu tersembunyi resiko, tidak saja bagi Anda namun juga bagi keluarga, teman dan organisasi. Dalam edisi kali, akan dibahas bahaya apa yang mungkin muncul serta bagaimana menggunakan beragam situs itu secara cermat dan aman.

Editor Tamu

Tanya Baccam lama bekerja sebagai konsultan keamanan. Pengarang dan instruktur di SANS selama lebih dari satu dekade. Hadir di Twitter sebagai **@tbaccam**.

Privasi

Salah satu hal penting di media sosial adalah perlindungan informasi pribadi. Bisa saja terjadi hal-hal seperti dibawah ini:

- **Dampak Masa Depan**: Banyak organisasi memindai situs media sosial sebagai bagian dari pemeriksaan latar belakang (background check). Beragam foto atau unggahan, walaupun sudah dilakukan sejak dulu, bisa menghambat proses rekrutment atau promosi jabatan. Selain itu, beberapa universitas melakukan hal yang sama dalam proses seleksi siswa. Pilihan privasi mungkin tidak memberikan perlindungan sebab organisasi tersebut bisa saja meminta Anda untuk “Like” atau bergabung ke dalam lembar situs atau beberapa unggahan tertentu sudah tersimpan di berbagai situs.
- **Serangan Pribadi**: Penyerang dunia maya sanggup menganalisa unggahan Anda dan menggunakan informasi itu untuk memperoleh banyak hal mengenai diri dan organisasi Anda. Sebagai contoh: mereka bisa menggunakan informasi yang diunggah untuk menebak jawaban “secret questions” pada saat reset sandi, menciptakan surel khusus ditujukan ke Anda (dikenal sebagai spearfishing) atau menelpon seseorang di organisasi berpura-pura sebagai Anda. Selain itu, upaya serangan ini bisa merambah ke hal-hal lain seperti identifikasi lokasi tempat kerja dan rumah Anda.
- **Merugikan Organisasi**: Pihak yang berniat jahat atau pesaing bisa memanfaatkan unggahan informasi sensitif organisasi untuk menyerang organisasi, Selain itu, unggahan Anda berpotensi menimbulkan reputasi negatif pada organisasi/perusahaan. Pastikan memahami kebijakan organisasi/perusahaan perihal apa saja yang bisa diunggah seputar perkerjaan Anda, lagi pula mungkin saja unggahan ke media sosial selalu diawasi.

Perlindungan terbaik adalah dengan membatasi apa yang diunggah. Memang benar, pilihan pengaturan privasi memberikan beberapa proteksi tapi sering kali tidak mudah dilakukan dan bisa berubah setiap saat tanpa sepengetahuan penggunanya.

Media Sosial

Apa yang dianggap bersifat pribadi bisa saja berubah menjadi hal umum karena berbagai alasan. Selain itu privasi sebuah unggahan tergantung pada siapa Anda berbagi. Semakin banyak berbagi, semakin besar kemungkinan informasi tersebar luas. Ingat untuk selalu beranggapan bahwa apapun yang diunggah akan bisa dan bakal menjadi informasi umum dan bagian terpadu dunia internet.

Selanjutnya, waspadalah terhadap segala sesuatu mengenai diri Anda yang diunggah oleh orang lain. Bila unggahan tersebut membuat Anda tidak nyaman, mintalah untuk menariknya lagi. Bila permintaan ini ditolak atau diabaikan, hubungi situs media sosial itu dan mintalah bantuan untuk menghapus unggahan tersebut. Sebaliknya, jangan sembarangan mengunggah informasi mengenai orang lain.

Situs media sosial memang menyenangkan dan sangat bermanfaat, bijaklah dalam berbagi dan berteman.

Keamanan

Selain urusan privasi, beberapa langkah dibawah ini bisa berguna untuk melindungi akun media sosial dan aktifitas online.

- **Login**: Lindungi setiap akun dengan sandi yang kuat, unik serta tidak berbagi sandi dengan orang lain. Perlu diketahui pula, banyak situs media sosial menggunakan proses pengecekan lebih detil, sebagai contoh adalah proses verifikasi dua tahap. Selalu gunakan metode otentifikasi yang paling kuat bila ada. Ingat untuk tidak menggunakan akun media sosial untuk login ke situs lain sebab bila terjadi peretasan maka semua akun tersebut menjadi tidak aman lagi.
- **Pengaturan Privasi**: Bila menggunakan pengaturan privasi, pastikan melalukan pengecekan dan pengujian berkala. Situs media sosial tidak jarang mengubah pengaturan privasi dan kekeliruan bisa dengan mudah sekali terjadi. Selain itu, banyak program aplikasi dan servis yang memungkinkan pemberian tanda lokasi pada unggahan (geotagging). Secara berkala lakukan pemeriksaan terhadap pengaturan ini apabila Anda tidak bermaksud berbagi informasi lokasi.
- **Enkripsi**: Situs media sosial menggunakan enkripsi HTTPS untuk mengamankan sambungan internet ke situs tersebut. Beberapa situs seperti Twitter dan Google+ menggunakan metode ini secara otomatis, sementara yang lain mungkin mengharuskan Anda untuk mengaktifkan HTTPS. Periksalah pengaturan akun media sosial dan aktifkan fitur HTTPS bila mungkin.
- **Surel**: Waspada terhadap surel yang menyatakan berasal dari situs media sosial, ini bisa saja merupakan serangan yang dilakukan kriminalis siber. Cara paling aman menjawab pesan sepert itu adalah dengan mengakses situs media sosial tersebut (mungkin alamat situs sudah disimpan), membaca dan membalas pesan atau pemberitahuan langsung dari situs tersebut.

Media Sosial

- **Tautan Berbahaya/Palsu**: Berhati-hatilah terhadap tautan mencurigakan yang diunggah ke media sosial. Banyak pihak beritikad tidak baik menggunakan cara seperti itu. Hanya karena sebuah pesan dikirim oleh seorang teman tidak berarti pesan itu benar-benar berasal dari orang itu karena bisa saja terjadi akun orang tersebut sudah dibobol. Bila ada anggota keluarga atau teman mengirimkan pesan aneh yang sulit dimengerti (cerita perampokan atau permintaan pengiriman uang), lakukan percakapan langsung via telepon guna memastikan apakah benar mereka mengirim pesan itu.
- **Aplikasi Alkom**: Kebanyakan situs media sosial menyediakan aplikasi alkom (alat komunikasi) untuk mengakses akun online. Pastikan aplikasi ini diunduh dari sumber terpercaya dan alkom dilengkapi dengan sandi yang kuat. Bila alkom tidak dalam keadaan terkunci pada saat hilang, orang lain bisa dengan mudah mendapatkan akses ke situs media sosial dan melakukan banyak hal atas nama Anda.

Media sosial merupakan sarana ampuh berkomunikasi dan mengikuti perkembangan dunia. Dengan bijak mengikuti berbagai saran diatas, Anda akan bisa menikmati dunia online dengan lebih aman. Untuk mengetahui lebih banyak bagaimana menggunakan situs media sosial serta cara melaporkan aktifitas tanpa ijin, kunjungi halaman keamanan situs media sosial yang dipakai.

Selanjutnya

Untuk berlangganan buletin bulanan OUCH! Kesadaran Keamanan, mengakses arsip buletin OUCH! dan mengetahui lebih banyak solusi kesadaran keamanan SANS, silakan kunjungi http://www.securingthehuman.org.

Versi Bahasa Indonesia

BIPIMax memberikan Pelatihan Optimasi Proses Bisnis (LSS) dan Pengenalan Keamanan & Proteksi Informasi. Informasi lengkap: http://www.bipimax.net

Sumber Pustaka

Frasa Sandi:	http://www.securingthehuman.org/ouch/2015#april2015
Verifikasi dua tahap:	http://www.securingthehuman.org/ouch/2013#august2013
Aman menggunakan Aplikasi Alkom:	http://www.securingthehuman.org/ouch/2015#january2015
Keamanan Dunia Siber bagi Anak:	http://www.securingthehuman.org/ouch/2015#june2015
Facebook Security:	https://www.facebook.com/safety

Dewan Redaksi: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Diterjemahkan oleh: T. Gunawan