Buletin Bulanan Kesadaran Keamanan bagi Pengguna Komputer

OUCH!

Dalam Edisi Ini...

- **Sekilas**
- **Phishing**
- **Lindungi Diri Anda**

Phishing (Surel Pengelabuan)

Sekilas

Surel digunakan sebagai salah satu cara berkomunikasi. Sehari-hari tidak terbatas digunakan untuk urusan pekerjaan namun juga bertutur sapa dengan teman dan handai-taulan. Selain itu, surel digunakan diberbagai perusahaan sebagai sarana pendukung jasa layanan online seperti konfirmasi pembelian online atau penyediaan laporan perbankan. Lantaran demikian banyak orang tergantung pada surel, menjadikannya salah satu sasaran serangan kriminalis siber. Edisi ini akan mengupas seluk beluk phishing sebagai metode serangan surel sekaligus cara pencegahannya.

Editor Tamu

Dr. Lance Hayden adalah Managing Director Berkeley Research Group. Ahli dibidang budaya dan perilaku keamanan, pengarang buku People-Centric Security: Transforming Your Enterprise Security Culture terbitan McGraw-Hill. Lance hadir di www.linkedin.com/in/drhayden.

Phishing

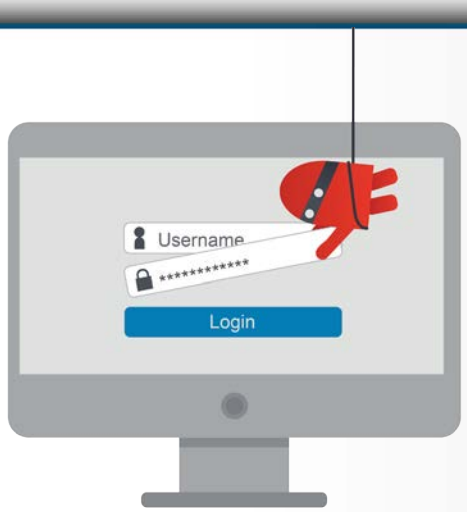
Phishing diartikan sebagai serangan yang menggunakan surel atau mekanisme pengiriman pesan lainnya seperti media sosial dengan tujuan memperdaya penggunanya agar mengklik tautan atau membuka sebuah lampiran. Bila hal ini terjadi, bisa saja terjadi pencurian data penting dan/atau penularan virus ke komputer. Perancang surel phishing selalu menciptakan surel aspal (asli tapi palsu). Bisa saja dengan membuatnya sedemikian rupa agar nampak seperti dikirim oleh teman atau perusahaan yang sudah dikenal dan bahkan menggunakan logo dari bank atau memalsukan alamat surel sehingga sekilas susah dibedakan dengan aslinya. Surel ini akan dikirim ke jutaan orang. Tidak ada yang tahu siapa yang akan menjadi korbannya, namun semakin banyak surel ini dikirim berarti semakin besar kemungkinan berhasil. Phishing mirip dengan menjala ikan, tidak ada yang tahu apa yang akan terjaring namun semakin besar ukuran jala tentunya akan tambah banyak ikan bisa diperoleh. Beberapa cara Phishing dibawah ini lazim digunakan dalam menjaring korbannya:

- **Memanen Informasi**: tujuan pelaku adalah mendapatkan beragam informasi pribadi seperti sandi, nomer kartu kredit atau informasi perbankan. Hal ini dilakukan dengan mengirimkan tautan (link) lewat surel dengan tujuan untuk mengarahkan Anda ke sebuah situs web asli tapi palsu. Situs ini bakal meminta Anda memberikan informasi akun serta data pribadi. Ketahuilah bahwa situs itu palsu, setiap informasi yang dimasukkan akan jatuh ke pihak pelaku.
- **Tautan Berbahaya**: Bertujuan untuk mengambil alih kendali peralatan. Hal ini dilakukan dengan mengirimkan

Phishing (Surel Pengelabuan)

surel yang berisi sebuah link. Bila link tersebut di-klik, sebuah situs web akan menyerang peralatan Anda dan bila sukses, akan menularkan virus kedalamnya.

- **Lampiran Berbahaya**: Tujuannya sama, untuk menularkan program berbahaya serta mengambil alih kontrol peralatan. Bedanya, pelaku akan mengirimkan sebuah berkas (file) seperti dokumen Word. Membuka lampiran itu berarti mengaktifkan serangan yang berpotensi akan mengambil alih kontrol peralatan Anda.
- **Penipuan**: banyak surel phishing merupakan berita rekaan belaka. Pelaku berusaha mengelabui Anda dengan menyatakan bahwa Anda terpilih sebagai pemenang lotere, berpura-pura sebagai program amal yang butuh dana atau meminta Anda memindahkan uang jutaan dollar. Bila surel ini ditanggapi, mereka akan meminta pembayaran atas jasa yang sudah dilakukan atau berusaha mendapatkan akses ke rekening bank dan menguras dana yang ada didalamnya.



Berpikirlah dengan jernih untuk melindungi diri Anda. Bila surel atau pesan tampak tidak lazim, mencurigakan atau terlalu mengada-ada, bisa saja itu sebuah serangan phishing.

Lindungi Diri Anda

Secara umum, membuka dan membaca surel atau pesan tentu aman-aman saja. Upaya phishing baru akan sukses bila pelaku berhasil memperdaya sang korban sehingga melakukan sebuah tindakan/aksi. Dibawah ini adalah beberapa tanda yang mengindikasikan sebuah surel bertujuan tidak baik:

- Surel tersebut menciptakan suasana genting, perlu perhatian/tanggapan secepatnya agar terhindar dari sesuatu yang bersifat merugikan seperti penutupan akun. Dalam kondisi mendesak itulah Anda diharapkan melakukan tindakan yang keliru.
- Tiba-tiba Anda mendapatkan surel dengan lampiran atau sebuah surel yang membujuk Anda agar membuka sebuah lampiran. Contoh: Sebuah surel menjelaskan bahwa lampiran yang ada berisi daftar karyawan yang akan diberhentikan, informasi gaji karyawan atau surat tuntutan pajak.
- Sebagai pengganti nama Anda, surel itu menggunakan sapaan umum “Pelanggan Yth”. Biasanya perusahaan atau teman akan menyapa dengan menggunakan nama Anda.
- Surel tersebut meminta informasi penting yang sensitif seperti nomer kartu kredit atau sandi.

Phishing (Surel Pengelabuan)

- Surel itu berkilah berasal dari organisasi resmi, namun terdapat banyak kesalahan tata bahasa atau ejaan, lagi pula menggunakan alamat surel pribadi seperti @gmail.com, @yahoo.com atau hotmail.com.
- Tautan terlihat aneh dan tidak resmi. Cara mengetahuinya adalah dengan meletakkan kursor mouse diatas tautan untuk melihat alamat lengkap tautan tersebut. Cara paling aman adalah dengan melakukan copy and paste tautan tersebut ke halaman baru browser atau ketik saja alamatnya.
- Bila menerima pesan dari seseorang yang dikenal namun nada percakapan dan pilihan kata yang dipakai tampak mencurigakan. Lakukan pengecekan langsung lewat telepon untuk memastikan. Mudah bagi orang lain untuk menciptakan surel seakan-akan berasal dari teman atau rekan kerja.

Bila Anda yakin sebuah surel merupakan phishing, jangan ragu untuk segera menghapusnya. Ingat, pikiran jernih dan akal sehat tetap merupakan perlindungan terbaik.

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

Rekayasa Sosial:	https://www.securingthehuman.org/ouch/2014#november2014
Lima Langkah Tetap Aman:	https://www.securingthehuman.org/ouch/2014#october2014
Saya Diretas, Selanjutnya Bagaimana:	https://www.securingthehuman.org/ouch/2014#may2014
OnGuard Online:	https://www.onguardonline.gov/phishing
SANS Security Tip of the Day:	https://www.sans.org/tip_of_the_day.php

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