Buletin Bulanan Kesadaran Keamanan bagi Pengguna Komputer

Stop Pengelabuan

Sekilas

Surel dan layanan pesan (seperti Skype, Twitter atau Snapchat) merupakan salah satu cara utama berkomunikasi. Setiap hari, kita tidak hanya menggunakan teknologi ini untuk bekerja namun juga untuk bertutur sapa dengan teman dan keluarga. Lantaran demikian banyak orang tergantung pada teknologi ini, menjadikannya salah satu modal utama para penyerang siber, inilah yang dinamakan pengelabuan (phishing). Berikut ini akan dibahas apa itu pengelabuan dan bagaimana cara mengenalinya sekaligus menghentikan sebuah serangan, baik di lingkungan kerja atau rumah.

Apa itu Pengelabuan

Pengelabuan adalah satu jenis serangan yang menggunakan surel atau layanan pesan untuk mengelabui Anda sehingga melakukan tindakan yang seharusnya tidak dilakukan, seperti klik pranala berbahaya, berbagi sandi atau membuka lampiran surel yang terinfeksi. Penyerang berupaya keras membuat pesan menyakinkan dan memainkan emosi seperti menciptakan situasi terburu-buru atau memancing rasa ingin tahu. Mereka mampu membuat seolah-olah pengirimnya adalah seseorang atau sesuatu yang Anda tahu, seperti teman atau perusahaan terpercaya yang sering dipakai. Atau bahkan menggunakan logo bank Anda atau memalsukan alamat surel sehingga penampilan pesan jadi lebih meyakinkan. Penyerang kemudian mengirimkan pesan itu ke jutaan orang. Mereka tidak tahu siapa yang akan terpancing, namun mereka tahu, semakin banyak terkirim, semakin banyak orang akan menjadi korban.

Lindungi Diri

Umumnya, aman-aman saja membuka dan membaca surel atau pesan. Agar sebuah serangan pengelabuan berhasil, diperlukan upaya untuk memperdaya Anda agar melakukan sesuatu. Namun, ada beberapa ciri dari sebuah serangan, berikut adalah yang paling umum ditemui:

- Terciptanya situasi genting, membutuhkan " tindakan segera" agar terhindar dari suatu bencana seperti ancaman penutupan akun atau ancaman penjara. Penyerang ingin menciptakan suasana terburu-buru sehingga Anda berbuat kesalahan.
- Memaksa Anda menerobos atau mengabaikan aturan dan prosedur di tempat kerja
- Munculnya rasa ingin tahu atau sesuatu yang berlebihan (tidak, Anda tidak menang lotere)

- Sapaan umum seperti “Pelanggan Yth”. Sebagian perusahan atau teman pasti tahu nama Anda.
- Meminta informasi sensitif, seperti nomer kartu kredit, sandi atau informasi lain yang seharusnya sudah diketahui pihak pengirim yang benar.
- Pesan yang mengaku berasal dari oganisasi sah, tapi memakai tata bahasa dan ejaan yang buruk, menggunakan alamat surel pribadi seperti @gmail.com
- Pesan berasal dari sumber resmi (mungkin atasan Anda) namun alamat balasan (Reply-To) mengacu ke alamat surel pribadi.
- Anda menerima pesan dari seseorang yang dikenal, namun gaya dan pilihan katanya tidak seperti biasanya. Bila curiga, telepon saja pihak pengirim untuk memastikan kebenarannya. Mudah sekali bagi seorang penyerang siber untuk menciptakan sebuah pesan seakan berasal dari teman atau rekan kerja.

Akhirnya, akal sehat adalah perlindungan terbaik. Bila sebuah surel atau pesan tampak aneh, mencurigakan atau terlalu mengada-ada, mungkin saja itu sebuah upaya penyerangan.

Versi Bahasa Indonesia

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

Editor Tamu

Tonia Dudley mengembangkan dan menjalankan program Security Awareness sejak 2011, termasuk program pelatihan pengelabuan yang terkenal. Info lengkap di www.linkedin.com/in/toniadudley.

Sumber Pustaka

Rekayasa Sosial:	https://www.sans.org/u/Cb1
Mengajarkan Pentingnya Keamanan:	https://www.sans.org/u/Cb6
Kiat Aman Surel:	https://www.sans.org/u/Cbg
Tipu Daya CEO:	https://www.sans.org/u/Cbl
OUCH! Translations and Archives:	https://www.sans.org/u/Cbq

Lisensi