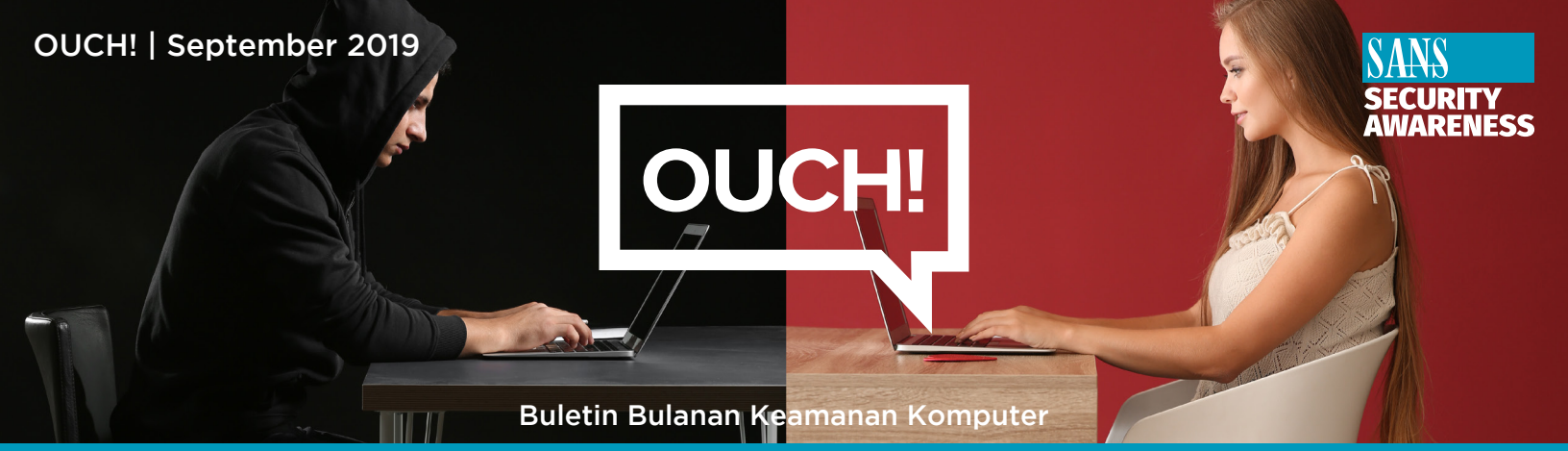
OUCH! | September 2019



OUCH!

SANS SECURITY AWARENESS

Buletin Bulanan Keamanan Komputer

Penipuan via Media Sosial

Sekilas

Banyak dari kita pernah menerima surel penipuan, di tempat kerja atau di rumah. Surel ini nampak seperti surat yang sah/asli, mungkin dari bank, atasan atau toko daring langganan. Itu adalah bentuk serangan, berupaya agar Anda bertindak cepat atau melakukan sesuatu yang seharusnya tidak dilakukan, seperti membuka lampiran terinfeksi, berbagi sandi atau mengirimkan dana. Semakin pintar kita dalam memilah dan menghentikan aksi itu, kriminalis siber juga terus mencoba beragam cara untuk memperdaya.

Upaya untuk mengelabui Anda bisa terjadi disemua media komunikasi, mulai dari Skype, WhatsApp dan Slack hingga Twitter, Facebook, Snapchat, Instagram dan bahkan aplikasi game. Komunikasi berbasis aplikasi atau cara diatas umumnya tidak formal dan terpercaya, itulah alasan kenapa cara itu digunakan untuk mengelabui orang lain. Selain itu, dengan menggunakan teknologi terbaru, seorang penyerang bisa ada di mana saja dan berpura-pura menjadi apa saja sesuai kebutuhan mereka. Hal utama untuk diingat adalah bahwa komunikasi yang terjadi dengan Anda, bisa saja tidak seperti apa yang dibayangkan dan lawan bicara juga tidak seperti yang diharapkan.

Catatan Penting

Berikut ini adalah beberapa tanda bila sebuah pesan yang baru diterima atau posting yang baru dibaca berpotensi sebagai sebuah serangan.

Segera: Sebuah pesan yang meminta "tindakan segera" disertai ancaman pentutupan akun atau ancaman hukuman penjara. Hal ini dirnacang agar Anda melakukan sebuah kesalahan/tindakan sembrono.

Paksaan: Meminta Anda menerabas atau mengabaikan aturan atau kebijakan di tempat kerja

Godaan: Iming-iming sesuatu yang menarik atau diluar kebiasaan seperti menang lotere.

Sensitif: Permintaan akan informasi sensitif seperti nomer kartu kredit atau sandi, atau informasi lain yang selayaknya tidak diketahui orang lain.

Pesan Resmi: Pesan beralamat resmi organisasi namun memiliki banyak kesalahan tata bahasa dan ejaan. Umumnya organisasi pemerintah tidak akan menggunakan media sosial sebagai sarana resmi berkomunikasi dengan Anda. Bila Anda ragu akan keabsahan sebuah pesan, telepon saja organisasi tersebut dengan menggunakan nomer yang tercantum di situs web organisasi tersebut.

Pemalsuan: Anda menerima pesan dari teman atau rekan kerja, namun nada dan gaya bicaranya terasa berbeda. Bila Anda ragu, hubungi pengirim lewat telepon untuk mengecek kebenaran pesan yang dikirim. Mudah bagi seorang penyerang siber membuat sebuah pesan seakan dari seseorang yang dikenal. Dalam beberapa kasus, mereka bisa saja membajak akun teman Anda, dan menggunakan akun itu untuk berkomunikasi dengan Anda. Waspada terhadap SMS, Twitter atau pesan pendek lainnya karena tidak mudah untuk mengetahui pribadi pengirimnya.

Anda adalahbenteng terbaik terhadap semua serangan, penipuan dll. Bila sebuah posting atau pesan terkesan aneh dan?atau mencurigakan, abaikan atau hapus saja. Bila datang dari seseorang yang dikenal, hubungi orang tersebut via telepon untuk memastikan kebenarannya.

Versi Bahasa Indonesia

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

Editor Tamu

Dr. Jessica Barker *(@drjessicabarker) adalah seorang ahli sumber daya manusia khususnya dalam bidang keamanan siber . Beliau adalah CEO Cygenta, selalu penuh semangat mengajarkan keamanan siber, perilaku dan kultur di seluruh dunia. Dr Jessica juga memimpin ClubCISO and pembicara ternama diberbagai forum.*

Sumber Pustaka

Rekayasa Sosial: https://www.sans.org/u/Uz6
Penipuan via Telepon: https://www.sans.org/u/Uzb
Stop That Phish: https://www.sans.org/u/Uzg
Personalized Scams: https://www.sans.org/u/Uzl