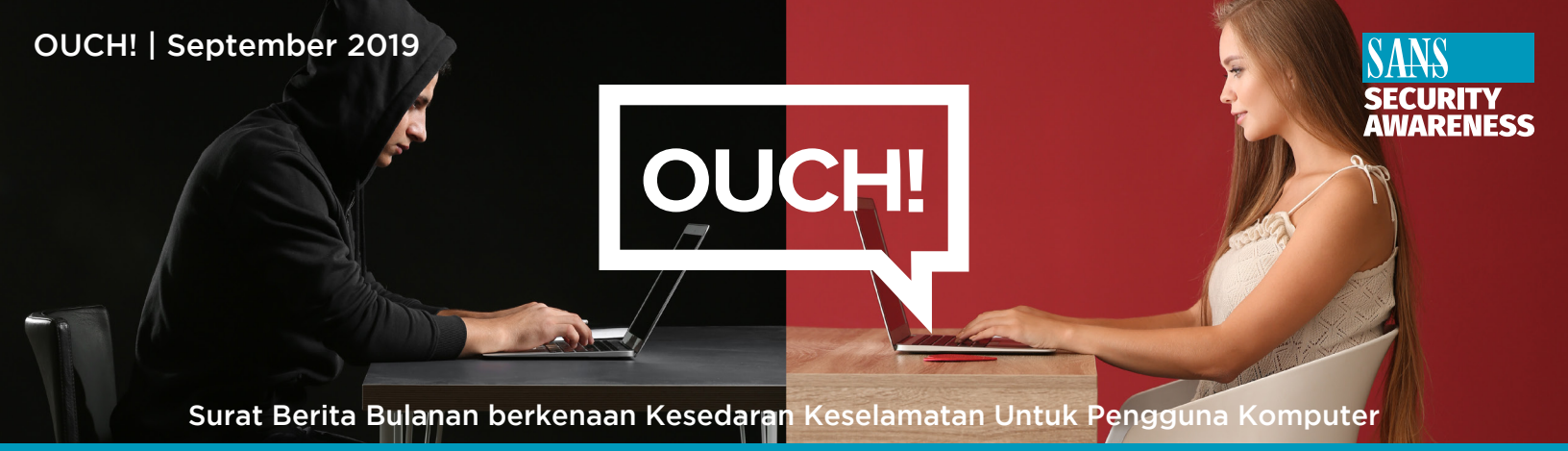
OUCH! | September 2019



SANS SECURITY AWARENESS

Surat Berita Bulanan berkenaan Kesedaran Keselamatan Untuk Pengguna Komputer

Penipuan melalui Media Sosial

Gambaran Keseluruhan

Kebanyakan kita pernah menerima serangan memancing data e-mel (e-mail phishing), sama ada di tempat kerja atau di rumah. E-mel ini kelihatan sah, seperti daripada bank, bos anda atau kedai dalam talian kegemaran. Namun begitu, e-mel ini sebenarnya sejenis serangan, untuk mempercepatkan atau menipu anda membuat tindakan yang tidak sepatutnya anda lakukan, seperti membuka lampiran e-mel berjangkit, berkongsi kata laluan atau memindahkan duit. Cabaran yang wujud ialah semakin maju tindakan kita dalam mengesan dan menghentikan serangan e-mel, semakin penjenayah siber berusaha untuk mencuba cara lain untuk berhubung dan menipu orang lain.

Cubaan untuk menipu boleh terjadi melalui pelbagai jenis komunikasi yang anda gunakan, seperti Skype, Whatsapp dan Slack kepada Twitter, Facebook, Snapchat, Instagram atau aplikasi permainan. Komunikasi melalui platform atau saluran seperti berikut dirasakan kurang formal atau boleh dipercayai, merupakan sebab utama mengapa penyerang menggunakan platform seperti berikut untuk menipu orang lain. Tambahan lagi, dengan kemajuan teknologi terkini menjadikan lebih mudah bagi penyerang yang berada di mana sahaja di dunia untuk berpura-pura menjadi sesiapa sahaja yang mereka mahu. Penting untuk kita berwaspada dalam setiap bentuk komunikasi yang digunakan kerana mungkin tidak seperti yang sepatutnya, dan seseorang tidak semestinya seperti yang mereka tunjukkan.

Poin Penting

Berikut merupakan tanda-tanda yang menunjukkan mesej yang anda terima atau paparan yang anda baca berkemungkinan merupakan satu serangan.

Desakan: Mesej yang diterima mempunyai unsur yang mendesak dan memerlukan “tindakan segera” sebelum sesuatu perkara buruk berlaku, seperti ugutan untuk menutup akaun anda atau menghantar anda ke penjara. Penyerang tersebut ingin menggesa anda untuk melakukan kesilapan.

Tekanan: Menekan anda untuk memintas atau tidak mengendahkan polisi atau prosedur di tempat kerja.

Rasa Ingin Tahu: Rasa ingin tahu yang kuat atau sesuatu yang indah khabar dari rupa. Tidak, anda tidak memenangi sebarang cabutan bertuah.

Maklumat Sensitif: Permintaan untuk maklumat yang sangat sensitif, seperti nombor kad kredit anda atau kata laluan, atau apa sahaja maklumat yang anda rasa tidak patut dikongsi.

Mesej Rasmi: Mesej yang kononnya daripada organisasi kerajaan, tetapi mempunyai tatabahasa dan ejaan yang salah. Kebanyakan organisasi kerajaan tidak menggunakan media sosial untuk komunikasi rasmi dan berhubung secara terus dengan anda. Jika anda tidak pasti sama ada mesej itu sah atau tidak, hubungi semula organisasi tersebut menggunakan nombor telefon yang dipercayai seperti yang tertera di laman web mereka.

Penyamaran: Anda menerima mesej daripada kawan atau rakan sekerja, tetapi nada dan susunan kata-kata tidak kelihatan seperti dari mereka. Jika anda berasa ragu-ragu/sangsi, buat panggilan telefon kepada penghantar mesej untuk mengesahkan mereka yang menghantar mesej tersebut. Mudah bagi penyerang siber untuk mencipta mesej yang kelihatan seperti dihantar dari seseorang yang anda kenal. Dalam sesetengah kes, penyerang boleh mengambil alih akaun rakan anda dan berpura-pura menjadi mereka ketika menghubungi anda. Berhati-hati dengan mesej teks, Twitter dan format mesej pendek yang lain, kerana lebih sukar untuk mengesan personaliti penghantar mesej tersebut.

Diri anda sendiri adalah pertahanan terbaik terhadap penipuan, penyamaran dan serangan yang seumpama dengannya. Jika terdapat paparan atau mesej yang kelihatan ganjil atau mencurigakan, abaikan atau hapuskan sahaja mesej tersebut atau jika mesej tersebut daripada seseorang yang anda kenal secara peribadi, buat panggilan telefon untuk mengesahkan mereka yang menghantar mesej tersebut.

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/.

Editor Jemputan

Dr Jessica Barker *(@drjessicabarker) mengetuai keselamatan siber dari aspek kemanusiaan. Beliau merupakan CEO bersama di Cygenta, di mana beliau meneruskan minat dalam memberikan pengaruh secara positif mengenai kesedaran keselamatan siber, tingkah laku dan kebudayaan di keliling dunia. Beliau merupakan Pengerusi ClubCISO dan seorang penceramah yang terkenal.*

Sumber

Pengendalian Sosial:	https://www.sans.org/u/Uz6
Serangan Panggilan Telefon dan Penipuan:	https://www.sans.org/u/Uzb
Hentikan Memancing Data:	https://www.sans.org/u/Uzg
Penipuan Menyasar Individu:	https://www.sans.org/u/Uzl