Surat Berita Bulanan berkenaan Kesedaran Keselamatan Untuk Pengguna Komputer

OUCH!

DALAM ISU INI...

Penipuan Melibatkan Ketua Pegawai Eksekutif (CEO)

Apakah Penipuan Melibatkan CEO?

Penjenayah siber amat licik -mereka sentiasa menggunakan cara baharu untuk mendapatkan apa yang mereka mahu. Salah satu cara yang amat berkesan adalah menjadikan orang seperti anda sebagai sasaran. Penyerang siber menyedari bahawa mereka yang lalai atau tidak sedar merupakan lubuk di dalam mana-mana organisasi, bagaimanapun mereka lupa terdapat orang yang berpengetahuan seperti pembaca OUCH! boleh menjadi pertahanan terbaik organisasi mereka.

Editor Jemputan

Angela Pappas adalah pengarah keselamatan maklumat dan kesedaran di Thomson Reuters. Angela bertanggungjawab sebagai duta program, e-Pembelajaran dan mendidik pekerja tentang phishing.

Penjenayah siber telah membangunkan serangan terbaru yang dinamakan Penipuan CEO, juga dikenali sebagai Kompromi E-mel Perniagaan (Business Email Compromise, BEC) Dalam serangan ini, penjenayah siber berpura-pura menjadi CEO atau eksekutif kanan yang lain dari organisasi anda. Penjenayah kemudiannya menghantar e-mel kepada pekerja seperti anda untuk memperdayakan anda melakukan sesuatu yang tidak patut anda lakukan. Serangan seperti ini sangat efektif kerana penjenayah siber telah melakukan kajian yang teliti. Mereka mencari dari laman sesawang anda maklumat seperti lokasi, eksekutif-eksekutif dan organisasi lain yang bekerjasama dengan anda . Penjenayah siber kemudiannya mempelajari sebanyak mungkin tentang rakan sekerja anda dari laman seperti LinkedIn, Facebook atau Twitter. Apabila mereka tahu struktur organisasi anda mereka akan menyelidik dan menjadikan salah seorang pekerja sebagai sasaran. Mereka mencari sasaran berpandukan matlamat mereka. Jika penjenayah siber tersebut menyasarkan wang, sasaran mereka mungkin pegawai dari jabatan akaun. Jika mereka mencari maklumat cukai, sasaran mereka mungkin sumber manusia. Jika mereka mahu capaian pelayan pengkalan data, sasaran mereka mungkin sesiapa dari jabatan teknologi maklumat.

Apabila mereka telah mengetahui apa yang mereka mahu dan sasaran mereka, mereka akan mula merangka serangan mereka. Selalunya mereka akan menggunakan phishing sasaran. Phishing adalah apabila penyerang menghantar e-mel kepada berjuta orang dengan matlamat untuk memperdayakan mereka untuk melakukan sesuatu, sebagai contoh membuka lampiran yang dijangkiti atau melawati laman berniat jahat. Phishing sasaran sama seperti phishing; namun begitu, bukannya menghantar e-mel umum kepada berjuta orang kerana mereka menghantar e-mel khas mensasarkan kumpulan kecil dan mereka yang terpilih. E-mel phishing sasaran ini tampak sangat tulen dan sukar dikesan. Seringkali e-mel tersebut datang daripada seseorang yang anda kenali atau pernah bekerja bersama, seperti rakan sekerja atau mungkin juga

© SANS Institute 2016

Penipuan Melibatkan Ketua Pegawai Eksekutif (CEO)

dari bos anda. E-mel tersebut tampak tulen kerana mereka mungkin menggunakan istilah atau perkataan yang digunakan rakan sekerja anda; mereka mungkin menggunakan logo organisasi anda atau mungkin juga tandatangan seorang eksekutif. E-mel seperti ini selalunya akan membangkitkan rasa cemas atau mendesak, meminta anda mengambil tindakan segera tanpamemaklumkan sesiapa. Matlamat penjenayah siber adalah untuk menggesa anda melakukan kesilapan. Berikut merupakan tiga senario yang biasa diguna:

Penipuan CEOmerupakan serangan hebat yang dapat melepasi kebanyakan pertahanan keselamatan anda. Pada akhirnya pertahanan yang terbaik adalah diri anda.

Pemindahan Wayar: Penjenayah siber mahukan wang. Ini bermakna mereka telah selidik siapa yang bekerja di jabatan akaun atau kumpulan yang menguruskan kewangan organisasi anda. Penjenayah kemudiannya mengarang dan menghantar e-mel berpura-pura menjadi bos mereka; e-mel tersebut memberitahu mereka terdapat satu kecemasan dan duit perlu dipindahkan kepada akaun tertentu secepat mungkin.

Penipuan Cukai: Penjenayah siber mahu mencuri maklumat tentang pekerja supaya mereka boleh menyamar sebagai pekerja untuk penipuan cukai. Mereka selidik organisasi anda dan mengenalpasti siapa yang menguruskan maklumat pekerja, sebagai contoh, seseorang dari sumber manusia. Dari situ, penjenayah siber menghantar e-mel palsu menyamar sebagai eksekutif kanan atau seseorang dari jabatan perundangan, meminta menghantar dokumen tertentu dengan segera.

Menyamar Sebagai Peguam: Tidak semua serangan Penipuan CEO melibatkan hanya e-mel; cara lain seperti telefon boleh digunakan. Dalam senario ini, penyerang bermula dengan menghantar emel kepada anda dengan menyamar sebagai pegawai kananyang memberitahu anda bahawa seorang peguam akan berhubung berkenaan satu perkara penting. Penjenayah kemudiannya menghubungi anda dan menyamar sebagai seorang peguam. Penjenayah akan membangkitkan rasa cemas sambil mereka bercerita tentang perkara sulit dan sensitif masa. Rasa cemas ini memperdayakan anda untuk terus bertindak.

Melindungi Diri Anda

Jadi apa yang boleh anda lakukan untuk melindungi diri dan organisasi anda? Logik akal merupakan pertahanan terbaik anda. Sekiranya anda menerima pesanan dari bos atau rakan sekerja anda dan ia tidak kelihatan betul, berkemungkinan ia adalah suatu serangan. Petunjuk termasuklah membangkitkan rasa cemas atau mendesak, tandatangan yang tampak tidak kena, nada tertentu yang anda tidak jangkakan, atau nama yang digunakan dalam e-mel tersebut berbeza dengan

© SANS Institute 2016

Penipuan Melibatkan Ketua Pegawai Eksekutif (CEO)

apa yang biasa penghantar memanggil anda. Satu lagi petunjuk adalah penyerang menggunakan alamat emel atau nombor telefon yang tidak pernah anda lihat, atau menggunakan alamat e-mel yang hampir serupa tetapi tidak sama dengan rakan sekerja atau bos anda. Sekiranya anda ragu-ragu, hubungi individu tersebut menggunakan nombor telefon yang dipercayai atau bersemuka dengan mereka (jangan balas melalui e-mel) dan sahkan bahawa mereka yang menghantar e-mel tersebut. Jangan sesekali melangkau polisi dan tatacara keselamatan. Organisasi anda mungkin mempunyai polisi yang menerangkan langkah yang perlu diambil untuk membenarkan pemindahan wang atau melepaskan maklumat sulit. Permintaan yang cuba untuk melangkaui polisi tersebut, tidak kira walaupun ianya dari sumber yang nyata, seharusnya dianggap mencurigakan dan perlu ditentusahkan sebelum sebarang tindakan diambil. Sekiranya anda menerima permintaan seperti ini dan tidak pasti akan tindakan susulan, hubungi penyelia anda, meja bantuan atau kumpulan keselamatan maklumat dengan segera.

Mari Belajar Lebih Lanjut!

Langganilah surat berita bulanan berkenaan Kesedaran Keselamatan Untuk Pengguna Komputer OUCH!, akseslah arkib OUCH!, dan belajar lebih lanjut mengenai penyelesaian kesedaran keselamatan SANS dengan melayari laman sesawang kami di securingthehuman.sans.org/ouch/archives.

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/.

Sumber

Social Engineering:	https://securingthehuman.sans.org/ouch/2014#november2014
Phishing:	https://securingthehuman.sans.org//ouch/2015#december2015
What is Malware:	https://securingthehuman.sans.org/ouch/2016#march2016
Two-step Verification:	https://securingthehuman.sans.org/ouch/2015#september2015
Tip of the Day:	https://www.sans.org/tip-of-the-day

OUCH! diterbitkan oleh program SANS “Securing The Human” dan diedarkan di bawah lesen Creative Commons BY-NC-ND 4.0. Kebenaran diberikan untuk mengedarkan surat berita ini atau mengunakannya dalam mana mana program kesedaran selagi tiada perubahan dibuat kepada kandungan asal.

Editor: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley
Translated by: Muhamad Hashimi, Rahayu Aziz, and Sheikh Ahmad Raffie