Surat Berita Bulanan berkenaan Kesedaran Keselamatan Untuk Pengguna Komputer

OUCH!

DALAM ISU INI...

Phishing

Pengenalan

E-mel merupakan salah satu cara utama kita berkomunikasi. Kita bukan sahaja menggunakannya setiap hari untuk kerja tetapi juga untuk terus berhubung Antara rakan dan ahli keluarga. Sebagai tambahan e-mel merupakan kaedah utama untuk syarikat memberikan perkhidmatan dalam talian seperti pengesahan pembelian atas talian atau ketersediaan penyata bank anda. Memandangkan ramai orang di seluruh dunia bergantung kepada e-mel, ia telah menjadi salah satu kaedah serangan utama yang digunakan oleh penjenayah siber. Dalam surat berita ini kami akan menerangkan tentang phishing, kaedah serangan e-mel yang biasa digunakan, dan langkah yang boleh anda ambil untuk menggunakan e-mel dengan selamat.

Editor Jemputan

Dr. Lance Hayden merupakan pengarah urusan untuk Berkeley Research Group. Seorang pakar dalam budaya keselamatan dan tingkah laku, beliau juga merupakan pengarang buku People-Centric Security: Transforming Your Enterprise Security Culture terbitan McGraw-Hill. Anda boleh jumpa beliau di **www.linkedin.com/in/drhayden**.

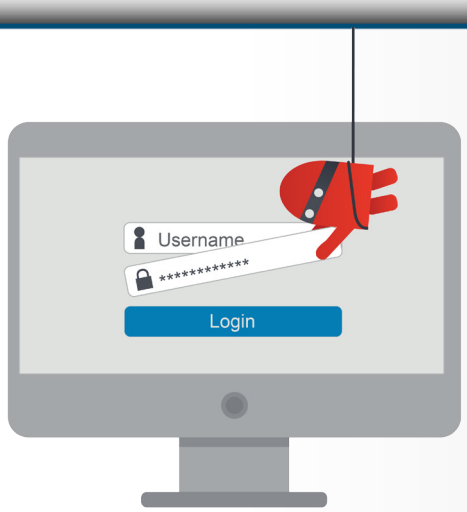
Phishing

Phishing merujuk kepada serangan menggunakan e-mel atau perkhidmatan pesanan seperti laman media sosial yang menipu anda untuk mengambil tindakan, seperti klik pada pautan atau membuka lampiran. Dengan menipu mangsa dengan serangan yang sedemikian anda berisiko kehilangan maklumat sensitif dan/atau komputer anda dijangkiti. Penyerang bekerja keras untuk menjadikan phishing mereka tampak meyakinkan. Sebagai contoh mereka akan mengarang e-mel yang tampak sama seperti datangnya dari seseorang atau sesuatu yang anda kenali, seperti kenalan atau syarikat yang anda percaya dan sering berurusan. Mereka akan menambah logo bank anda dan memalsukan alamat e-mel supaya ianya tampak sah. Kemudian penyerang akan menghantar e-mel ini kepada berjuta penerima. Mereka tidak tahu siapa yang akan menjadi mangsa, apa yang mereka mahu adalah lebih banyak e-mel yang dihantar, kebarangkalian untuk berjaya adalah lebih tinggi. Phishing hampir sama menggunakan jaring untuk menangkap ikan, anda tidak akan tahu apa yang dapat anda tangkap tetapi lebih besar jaring anda lebih banyak ikan yang akan anda dapat. Ada beberapa cara penyerang menggunakan phishing untuk mendapatkan apa yang mereka mahukan.

- **Menuai Maklumat**: Matlamat penyerang adalah untuk menuai maklumat peribadi seperti kata laluan, nombor kad kredit atau maklumat perbankan. Untuk melakukan ini mereka akan menghantar e-mel dengan pautan yang akan membawa anda ke laman yang tampak sah. Laman ini kemudiannya akan meminta maklumat akaun anda atau maklumat peribadi anda. Walaubagaimanapun laman tersebut adalah palsu, sebarang maklumat yang anda beri akan dihantar terus kepada penyerang.

Phishing

- **Pautan Berniat Jahat**: Matlamat penyerang adalah untuk mengawal peranti anda. Untuk melakukan ini mereka akan menghantar e-mel kepada anda dengan pautan. Jika ada klik pada pautan tersebut, ia akan membawa anda kepada satu laman yang akan melancarkan serangan ke atas peranti anda, jika berjaya ia akan menjangkiti sistem anda.
- **Lampiran Berniat Jahat**: Matlamat penyerang adalah sama, untuk menjangkiti dan mengawal peranti anda. Tetapi mereka tidak menghantar pautan sebaliknya fail yang dijangkiti, seperti dokumen Word. Membuka lampiran tersebut akan melancarkan serangan, berkemungkinan memberikan penyerang kawalan kepada sistem anda.
- **Penipuan**: Sesetengah e-mel phishing tidak lebih dari penipu yang telah beralih kepada digital. Mereka akan cuba untuk membodohkan anda dengan mengatakan anda telah menang loteri, menyamar sebagai badan amal yang memerlukan sumbangan atau meminta bantuan untuk memindahkan berjuta-juta dolar. Jika anda membalas kepada sebarang e-mel tersebut, mereka akan menyatakan mereka memerlukan bayaran pendahuluan untuk perkhidmatan mereka atau capaian kepada akaun bank anda, menipu duit anda.



Pertahanan terbaik adalah menggunakan akal. Jika e-mel atau pesanan tampak pelik, mencurigakan, atau terlalu bagus untuk dipercayai, ia berkemungkinan merupakan serangan phishing.

Melindungi Diri Anda

Hampir semua kes, membuka dan membaca e-mel atau pesanan adalah tidak mengapa. Untuk serangan phishing berlaku penjenayah perlu menggunakan muslihat untuk anda melakukan sesuatu. Mujurlah terdapat petunjuk sesuatu pesanan tersebut adalah serangan, berikut adalah yang lazim di jumpai:

- E-mel tersebut sedikit mendesak, memerlukan anda untuk bertindak secepat mungkin sebelum sesuatu buruk berlaku, seperti akaun anda ditutup. Penyerang mahukan anda terburu-buru melakukan kesilapan sebelum berfikir.
- Anda menerima e-mel dengan lampiran yang tidak anda jangkakan atau e-mel tersebut memujuk anda untuk membuka lampiran tersebut. Antara contoh adalah e-mel menyatakan ia mempunyai lampiran maklumat yang tidak di umumkan lagi, maklumat penggajian pekerja atau surat dari IRS mengatakan anda sedang di saman.
- E-mel tersebut menggunakan kata ganti nama seperti “Dear Customer” sebaliknya dari menggunakan nama anda. Kebanyakan syarikat atau rakan akan menggunakan nama anda.
- E-mel tersebut meminta maklumat sensitif anda, seperti no kad kredit atau kata laluan.
- E-mel tersebut menyatakan datang dari organisasi yang rasmi, tetapi mempunyai tatabahasa dan ejaan yang teruk, atau menggunakan alamat e-mel peribadi seperti @gmail.com atau hotmail.com.

Phishing

- Pautan tersebut tampak pelik atau tidak rasmi. Salah satu cara adalah dengan menuding tetikus pada pautan tersebut sehingga ada pop-up menunjukkan ke mana pautan tersebut akan membawa anda. Jika pautan dalam e-mel tidak sama dengan destinasi pada pop-up, jangan klik. Pada peranti mudah alih menekan dengan jari anda pada pautan tersebut akan mengeluarkan pop-up yang sama. Langkah yang lebih selamat adalah dengan menyalin dan menampal URL dari e-mel ke dalam pelayar atau taip pautan yang betul.
- Anda menerima pesanan dari seseorang yang anda kenali, tetapi nada atau perkataan tidak menggambarkan beliau. Jika anda berasa was-was, telefon penghantar untuk mendapat kepastian bahawa mereka menghantarnya. Ianya mudah untuk penyerang siber untuk mencipta satu emel yang nampak seperti datangnya dari rakan atau rakan sekerja.

Jika anda percaya sebarang e-mel atau pesanan adalah serangan phishing, padamkannya. Akhir sekali pertahanan terbaik adalah dengan menggunakan akal.

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 http://www.securingthehuman.org.

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://www.securingthehuman.org/ouch/2014#november2014
Five Steps to Staying Secure:	https://www.securingthehuman.org/ouch/2014#october2014
I'm Hacked, Now What?:	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

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