Surat Berita Bulanan berkenaan Kesedaran Keselamatan Untuk Pengguna Komputer

Hentikan Memancing Data

Pengenalan

E-mel dan perkhidmatan pesanan (seperti Skype, Twitter atau Snapchat) adalah salah satu cara utama kita berkomunikasi. Kita bukan sahaja menggunakan teknologi ini untuk kerja malahan untuk berhubung dengan rakan dan keluarga. Memandangkan ramai orang di seluruh pelosok dunia bergantung kepada teknologi ini, ia telah menjadi salah satu kaedah serangan utama oleh penyerang siber, iaitu kaedah serangan yang dipanggil memancing data (phishing). Pelajari apakah itu memancing data dan bagaimana anda boleh mengenali dan menghentikan serangan ini, tidak kira di rumah mahupun di tempat kerja.

Apakah itu Memancing Data

Memancing data adalah suatu jenis serangan yang menggunakan e-mel atau perkhidmatan pesanan untuk memperdayakan mangsa supaya mengambil tindakan yang tidak sepatutnya mereka ambil, seperti klik pada pautan hasad, berkongsi kata laluan atau membuka lampiran e-mel yang terjangkit (?). Penyerang bekerja keras untuk menjadikan mesej-mesej ini meyakinkan dan bermain dengan emosi anda, seperti memerlukan tindakan segera atau ingin tahu. Mereka boleh menjadikan emel tersebut seperti ianya datang daripada seseorang atau sesuatu yang anda tahu, contohnya kawan atau syarikat yang sering digunakan. Atau mereka juga boleh menambahkan logo bank atau memalsukan alamat e-mel supaya mesej tersebut tampak tulen. Penyerang kemudiannya menghantar mesej ini kepada berjuta orang. Mereka tidak tahu siapa yang akan memakan umpan ini, apa yang mereka tahu lebih banyak e-mel yang mereka hantar lebih ramai orang yang akan menjadi mangsa.

Melindungi Diri Anda

Dalam hampir kesemua kes, membuka dan membaca e-mel atau mesej adalah baik sahaja. Untuk memastikan serangan memancing data berfungsi, penjahat perlu memperdayakan anda untuk melakukan sesuatu. Mujurlah terdapat petunjuk yang sesuatu mesej itu adalah suatu serangan. Berikut adalah antara yang lazim:

- Memerlukan tindakan segera, mendesak sebelum sesuatu perkara buruk berlaku, seperti mengugut untuk menutup akaun atau menghantar anda ke penjara. Penyerang mahu anda bergegas melakukan kesilapan.
- Memberi tekanan supaya anda memintas atau mengabaikan polisi atau prosedur di tempat kerja.
- Mempunyai rasa ingin tahu yang tinggi atau terlalu bagus untuk dipercayai (tidak, anda tidak memenangi loteri itu).

- Ucapan pembuka yang umum seperti “Pelanggan yang dihormati”. Kebanyakan syarikat atau rakan mengetahui nama anda.
- Meminta maklumat sensitif, seperti nombor kad kredit atau kata laluan atau sebarang maklumat yang sepatutnya diketahui oleh si penghantar.
- Mesej tersebut menyatakan ia adalah dari organisasi yang rasmi, tetapi menggunakan tatabahasa yang lemah atau ejaan atau e-mel persendirian seperti @gmail.com.
- Mesej tersebut datang dari alamat yang rasmi (seperti bos anda) tetapi mempunyai alamat balas kepada orang lain atau akaun e-mel persendirian.
- Anda menerima mesej daripada seseorang yang anda kenali, tetapi nada atau perkataan tidak menggambarkan individu tersebut. Jika anda ragu-ragu, telefon penghantar untuk memastikan mereka menghantarnya. Amat mudah bagipenyerang mencipta suatu mesej yang tampak seperti dihantar oleh kawan-kawan atau rakan sekerja.

Akhir kata pertimbangan akal adalah pertahanan terbaik anda. Jika suatu e-mel atau mesej tampak pelik, mencurigakan atau terlalu bagus untuk dipercayai, ia mungkin serangan memancing data.

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

Tonia Dudley telah membangun dan menjalankan program kesedaran keselamatan semenjak tahun 2011, termasuklah membina program latihan memancing data yang telah memenangi anugerah. Anda boleh mencari beliau di www.linkedin.com/in/toniadudley.

Sumber

Social Engineering:	https://www.sans.org/u/Cb1
Helping Others Secure Themselves:	https://www.sans.org/u/Cb6
Email Do’s and Don’ts:	https://www.sans.org/u/Cbg
CEO Fraud:	https://www.sans.org/u/Cbl
OUCH! Translations and Archives:	https://www.sans.org/u/Cbq

lesen