SANS SECURITY AWARENESS

OUCH!

Surat Berita Bulanan berkenaan Kesedaran Keselamatan Untuk Pengguna Komputer

Serangan Panggilan Telefon dan Penipuan

Pengenalan

Apabila berfikir tentang penjenayah siber anda mungkin fikirkan seorang perancang jahat yang duduk di belakang sebuah komputer sambil melancarkan serangan canggih melalui Internet. Walaupun kebanyakan penjenayah siber pada hari ini menggunakan teknologi seperti e-mel atau mesej segera, penjahat turut menggunakan telefon untuk memperdayakan mangsa mereka. Terdapat dua kelebihan menggunakan telefon. Pertama, tidak seperti e-mel, hanya beberapa teknologi sahaja yang mengawasi panggilan telefon dan boleh mengesan dan menghentikan serangan. Kedua, lebih mudah bagi penjahat menyampaikan emosi mereka melalui telefon dan kemungkinan mereka memperdayakan mangsa adalah lebih tinggi. Mari belajar bagaimana kita boleh mengenali dan menghentikan serangan ini.

Bagaimana Serangan Panggilan Telefon Berfungsi?

Pertama anda perlu memahami apa yang penyerang ini mahukan. Mereka selalunya mahukan duit, maklumat atau capaian kepada komputer anda (atau ketiga-tiganya). Mereka melakukan perkara ini dengan memperdayakan anda untuk melakukan apa yang mereka mahu. Penjahat ini menghubungi mangsa diseluruh dunia, dengan mencipta situasi yang sangat mendesak. Mereka menakutkanmangsa supaya tidak keruan lantas mangsa tidak dapat berfikir dengan rasional, dan mereka menggesa mangsa untuk melakukan kesilapan. Antara contoh yang biasa termasuklah:

Pemanggil berpura-pura bahawa mereka adalah dari pihak berkuasa cukai kerajaan atau perkhidmatan memungut cukai dan memberitahu mangsa ada cukai yang tertunggak. Mereka menjelaskan bahawa jika mangsa tidak membayar cukai tersebut mangsa akan dipenjarakan, kemudian mendesak mangsa untuk membuat bayaran dengan menggunakan kad kredit melalui telefon. Ini adalah penipuan. Kebanyakan jabatan hasil termasuklah LHDN tidak akan membuat panggilan atau menghantar e-mel kepada orang ramai. Semua makluman cukai rasmi akan dihantar menggunakan surat biasa.

Pemanggil berpura-pura mereka adalah dari Sokongan Teknologi Microsoft dan memberitahu bahawa komputer mangsa telah dijangkiti. Setelah mereka meyakinkan bahawa komputer mangsa telah dijangkiti, mereka mendesak supaya mangsa membeli perisian mereka atau memberikan capaian kepada komputer. Microsoft tidak akan menghubungi anda di rumah.

Mangsa menerima mel suara automatik mengatakan akaun bank mereka telah dibatalkan dan meminta mangsa menghubungi satu nombor untuk mengaktifkannya semula. Apabila mangsa menghubungi mereka akan dilayan oleh sistem automatik yang meminta mangsa untuk mengesahkan identiti dan menjawab pelbagai soalan peribadi. Ini sememangnya bukan dari pihak bank, penjenayah sebenarnya sedang merekodkan semua maklumat untuk tujuan penipuan identiti.

Melindungi Diri Anda

Perlindungan terbaik ketika menghadapi serangan panggilan telefon adalah diri anda sendiri. Ingat perkara berikut.

Sekiranya anda menerima panggilan dan ianya mencemaskan, mendesak anda melakukan sesuatu, sentiasa mencurigainya. Walaupun panggilan tersebut tampak OK pada mulanya, tetapi kemudian mula berasa pelik, anda boleh hentikannya pada bila-bila masa.

Jika anda percaya panggilan telefon tersebut adalah satu serangan, hentikan perbualan. Jika anda mahu memastikan panggilan telefon tersebut adalah sah, pergi ke laman organisasi tersebut (seperti bank anda), dapatkan nombor telefon sokongan dan buat panggilan terus kepada mereka. Dengan cara itu anda dapat pastikan bahawa anda bercakap dengan organisasi yang betul.

Jangan percayakan ID-Pemanggil, penjahat selalunya akan memperdayakan nombor pemanggil supaya ia tampak dari organisasi yang sah atau mempunyai kod kawasan yang sama seperti nombor telefon anda.

Jangan sesekali benarkan pemanggil mengambil kawalan kepada komputer atau memperdayakan anda untuk memuat turun perisian. Ini adalah salah satu cara penjahat menjangkiti komputer anda.

Jika panggilan telefon datang dari seseorang yang anda tidak kenali secara peribadi, biarkan panggilan tersebut pergi terus ke mel suara. Dengan cara ini anda boleh melihat semula panggilan pada masa terluang. Lebih baik lagi, bolehkan fungsi "Do Not Disturb" yang terdapat pada kebanyakan telefon kini.

Penipuan dan serangan melalui telefon sedang meningkat. Diri anda sendiri adalah perlindungan terbaik untuk mengesan dan menghentikannya.

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

Jen Fox *menawarkan perkhidmatan kesedaran keselamatan, kejuruteraan sosial dan penilaian risiko sebagai Perunding Kanan Keselamatan di All Covered. Cari Jen di Twitter sebagai* @j_fox.

Sumber

Consumer Information about Identity, Privacy, & Online Security:
https://www.consumer.ftc.gov/topics/privacy-identity-online-security

Lapor Penipuan Telefon di: https://aduan.skmm.gov.my

Kejuruteraan Sosial: https://www.sans.org/u/Fi5