Surat Berita Bulanan berkenaan Kesedaran Keselamatan Untuk Pengguna Komputer

OUCH!

DALAM ISU INI...

Membeli-belah Dalam Talian Dengan Selamat

MusimTempoh Waktu untuk Berhati-hati

Musim cuti perayaan semakin menghampiri kita dan jutaan orang di seluruh dunia akan mencari hadiah yang terbaik. Kebanyakan dari kita memilih untuk membeli secara dalam talian demi mencari tawaran yang menarik dan mengelak dari perlu beratur panjang dan bersesak dengan orang ramai. Malangnya, inilah juga masa yang ditunggu-tunggu oleh penjenayah untuk melakukan penipuan dalam talian atau penipuan kewangan. Bulan ini kami akan menerangkan bahaya membeli-belah secara dalam talian dan cara untuk melindungi diri anda.

Editor Jemputan

Jonathan Homer (**@JonathanLHomer**) merupakan peneraju dalam industri Kesedaran Keselamatan Siber dan aktif dengan kedua-dua sektor swasta dan kerajaan. Kepakaran Jon adalah penglibataninteraksi bersama para hadirin dan teknik latihan yang canggih.

Kedai Palsu Dalam Talian Palsu

Walaupun kebanyakan kedai dalam talian adalah sah, sesetengah daripadanya tidak, kerana ia adalah laman sesawang palsu yang dibangunkan oleh penjenayah. Penjenayah mencipta laman sesawang palsu ini dengan meniru rupa atau menggunakan nama kedai yang diketahui umum. Mereka kemudiannya menggunakan laman sesawang ini untuk memburu mangsa yang sedang mencari tawaran yang terbaik. Apabila anda membuat carian dalam talian untuk harga terendah anda mungkin akan di arahkan ke salah satu laman sesawang palsu ini.

Apabila memilih laman sesawang untuk membeli sesuatu produk, sentiasa berhati-hati dengan iklan di laman sesawang yang menawarkan harga terlalu murah berbanding dengan laman sesawang lain atau laman yang menawarkan produk yang telah habis dijual di seluruh negararata dunia. Sebab mengapa produk mereka terlalu murah atau boleh didapati adalah kerana barangan yang bakal anda terima adalah tidak sah, palsu atau barangan curi, atau lebih teruk anda tidak akan menerima barangan anda langsung. Lindungi diri anda dengan melakukan perkara berikut:

- Pastikan laman tersebut mempunyai alamat e-mel dan nombor telefon untuk jualan atau soalan khidmat sokongan berkenaan soalan. Jika laman tersebut tampak mencurigakan, hubungi dan bercakap dengan seseorang.
- CariLihat tanda-tanda yang mencurigakan seperti kelemahan tatabahasa dan ejaan.
- Sentiasa mencurigai jika laman tersebut kelihatan sama seperti laman yang diketahui umum yang pernah anda gunakan sebelum ini, tetapi nama domain laman atau nama kedai tersebut sedikit berbeza. Sebagai contoh, anda mungkin kerap mengunjungi laman https://amazon.com untuk semua pembelian Amazon anda. Tetapi sentiasa berhati-hati jika anda dapati anda berada di laman yang berpura-pura menjadi Amazon dengan URL http://store-amazon.com.

Membeli-belah Dalam Talian Dengan Selamat

- Taip nama kedai tersebut atau URL di dalam enjin carian dan lihat apa komen oleh orang lain mengenai laman tersebut sebelum ini. Cari terma seperti “penipuan (scam)”,”tidak akan lagi (never again)” atau “palsu (fake)”. Kurangnya komensemakan juga merupakan petanda kurang baik kerana ianya menunjukkan laman itu masih baru.

Ingat, hanya kerana laman tersebut tampak profesional tidak bermakna ianya sah. Jika terdapat sesuatu pada laman tersebut yang mencurigakan, ambil masa untuk periksa. Jika anda tidak selesa dengan laman tersebut, jangan gunakannya. Sebaliknya, gunakan laman yang anda percaya dan pernah gunakan sebelum ini. Anda mungkin tidak akan mendapat tawaran yang hebat atau item yang paling hangat, tetapi paling tidak anda akan mendapat produk yang tulen dan laporan kredit yang baik.

Lindungi diri anda semasa dalam talian dengan membeli-belah dari laman yang anda percaya dan mempunyai reputasi yang tinggi.

Komputer Anda / Peranti Mudah Alih

Sebagai tambahan kepada membeli-belah di laman yang selamat, anda perlumahu pmemastikan komputer atau peranti mudah alih anda adalah selamat. Penjenayah siber akan mencuba untuk menjangkiti peranti anda supaya mereka boleh memperoleh maklumatnuai akaun bank, maklumat kad kredit, dan kata laluan. Ambil langkah-langkah berikut untuk sentiasa memastikan peranti anda selamat:

- Jika anda mempunyai kanak-kanak di rumah, pertimbangkan untuk memiliki dua peranti, satu untuk anak-anak anda dan satu lagi untuk dewasa. Kanak-kanak mempunyai sifat ingin tahu dan berinteraksi dengan teknologi., Nnatijahnya mereka lebih berisiko tinggi untuk dijangkiti. Dengan menggunakan komputer atau tablet yang khas untuk transaksi dalam talian, seperti perbankan dalam talian dan membeli-belah, anda mengurangkan risiko untuk dijangkiti. Jika peranti yang berbezalainan bukanlah satu pilihan, buat akaun yang berlainan untuk komputer yang dikongsi, dan pastikan anak-anak anda bukantidak mempunyai kelebihan pentadbir.
- Hanya buat sambungan kepada rangkaian tanpa wayar yang anda selia, seperti di rumah atau rangkaian yang anda percayai semasa membuat transaksi. Penggunaan Wi-Fi awam seperti di kedai kopi dan sebagainya mungkin bagus untuk membaca berita tetapi bukan untuk membuat capaian kepada akaun bank anda.
- Sentiasa pasang kemas kini terbaru dan kemas kini perisian antivirus. Ini menjadikannya lebih sukar untuk penjenayah siber untuk menjangkiti peranti anda.

Kad Kredit Anda

Semak penyata kad kredit anda untuk memastikan cas yang mencurigakani. Anda patut semak penyata anda dengan kerap, paling kurang sekali sebulan. Sesetengah penyedia kad kredit memberi anda pilihan untuk memaklumkan anda melalui

Membeli-belah Dalam Talian Dengan Selamat

e-mel atau pesanan teks setiap kali cas dikenakan ke atas kad kredit anda atau apabila cas melebihi amaun yang di tetapkan. Satu lagi pilihan adalah untuk memiliki satu kad kredit hanya untuk membuat pembelian dalam talian., dDengan cara ini jika iainnya telah di kompromi anda hanya perlu menukar kad tersebut tanpa memberi impak kepada aktiviti pembayaran anda yang lain. Jika anda percaya penipuan telah berlaku, hubungi syarikat kad kredit anda dan terangkan situasi anda. Ini juga adalahmerupakan salah satu sebab mengapa kad kredit adalah lebih baik dari kad debit untuk pembelian dalam talian. Kad debit mengambil wang terus dari akaun anda, dan jika berlaku penipuan, telah berlaku ianyaadalah lebih sukart untuk mendapatkan wang anda kembali.

Akhir sekali, terdapat teknologi terkini yang membolehkanungkinkan anda untuk membuat bayaran tanpa mendedahkan nombor kad kredit anda. Pertimbangkan kad kredit yang menjana nombor kad kredit yang unik untuk setiap pembelian dalam talian anda, atau gunakan perkhidmatan pembayaran yang diketahui umum, seperti PayPal, yang tidak memerlukan anda tidak perlu untuk memberikan nombor kad kredit anda kepada pembekal.

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

Five Steps to Staying Secure:	https://www.securingthehuman.org/ouch/2014#october2014
Securing Your Home Network:	https://www.securingthehuman.org/ouch/2014#january2014
Securing Your Tablet:	https://www.securingthehuman.org/ouch/2013#december2013
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