SANS SECURITY AWARENESS
SafeNet Network & Security Services
شبکه امن اندیشه فردا

وای! نوامبر 2017

ماهنامه ای برای آگاهی کاربران رایانه از امنیت اطلاعات

OUCH!

دراین شماره..

- فروشگاه های آنلاین تقلبی
- کامپیوتر / موبایل شما
- کارت اعتباری شما

خرید آنلاین همراه با امنیت

مقدمه

با نزدیک شدن تعطیلات بسیاری از ما و میلیونها نفر در سراسر دنیا به جستجوی خرید هدایای مناسب میروند. انتخاب بسیاری از ما برای اجتناب از درگیر شدن در صف های طولانی و شلوغ؛ جستجو و خرید اقلام با ارزش بصورت آنلاین است. متاسفانه در این موقع سال بسیاری از مجرمان سایبری هم با راه اندازی وب سایت های خرید اینترنتی تقلبی به دنبال کلاهبرداری و دزدی از دیگران هستند. در ادامه خطرات خرید های اینترنتی و چگونگی انجام آن بصورت امن را برای شما شرح خواهیم داد.

سردبیر مهمان

لنی زلتسر(Lenny Zeltser) سازنده محصولات امنیتی در آزمایشگاه مینروا (Minerva Labs) و مدرس دوره مبارزه با بدافزار در موسسه SANS میباشد .لنی در توییتر با شناسه **@lennyzeltser** فعال بوده و در وبلاگ امنیتی **zeltser.com** مطلب مینویسد.

فروشگاه های آنلاین تقلبی

در حالیکه بسیاری از فروشگاه های آنلاین قانونی هستند تعدادی فروشگاه تقلبی نیز وجود دارند که توسط مجرمان سایبری ایجاد شده اند. مجرمان این کار را با درست کردن سایت های تقلبی که از نظر شکل و قیافه دقیقا مشابه سایت های اصلی هستند و با استفاده از نام و برندهای شناخته شده انجام میدهند. آنها سپس با استفاده از این سایت های مشکل دار افرادی که به دنبال بهترین خرید ممکن هستند را شکار میکنند. زمانیکه شما در حال خرید انترنتی هستید و مهمترین هدف شما خرید های با قیمت های بسیار پایین است قطعا به سمت بسیاری از این سایت های تقلبی هدایت خواهید شد. زمانیکه میخواهید یک سایت را برای خرید اینترنتی انتخاب کنید، مراقب سایت هایی که محصولاتشان را با قیمت بسیار پایین تر از دیگر سایت ها تبلیغ میکنند باشید. دلیل اینکه محصولات آنها بسیار ارزان هستند این است که چیزی که به دست شما خواهد رسید اصلی و یا قانونی نخواهد بود، احتمالا کالای خریداری شده تقلبی و یا دزدی بوده و در برخی مواقع اصلا تحویل خریدار نمیشوند. با بهره گیری از راه های زیر از وقوع این موارد جلوگیری کنید:

- تا جایی که ممکن است، از سایت هایی خرید کنید که از قبل آن را میشناسید و به آنها اعتماد دارید و قبلا از آنها خرید کرده اید.
- بررسی کنید که آیا وب سایت آدرس پستی معتبر دارد و شماره تماسی برای فروش و خدمات پس از فروش درست دارد. اگر سایت مشکوک به نظر میرسید، با شماره آن تماس بگیرید و با افراد آن سایت صحبت کنید. اگر نتوانستید با کسی صحبت کنید، اولین نشانه ای است که شما به یک سایت جعلی برخورد کردید.
- نکات هشدار دهنده میتواند خدمات و کالاها با شرایط عالی باشد یا اشتباهات گرامری و یا نگارش ضعیف، میتواند برای شما هشدار دهنده باشد.
- اگر سایتی بسیار شبیه سایت شناخته شده ای است که قبلا از آن استفاده کرده اید، ولی نام دامنه و یا اسم فروشگاه آن کمی فرق

خرید آنلاین همراه با امنیت

داشت، حتما به آن مشکوک شوید. بعنوان مثال ممکن است شما از سایت آمازون خرید اینترنتی داشتید که آدرس سایت آن https://www.amazon.com است. ولی اگر شما سر از سایتی در آوردید که خود را آمازون میداند ولی آدرس آن چیزی شبیه http://store-amazoncom.com بود، حتما به آن شک کنید.

- نام فروشگاه و یا آدرس سایت آن را در موتور های جستجو تایپ کنید و ببینید مردم در مورد آن سایت چه گفته اند. بدنبال کلماتی نظیر «تقلب»، «کلاهبرداری»، «هرگز»، و یا «جعلی» بگردید. اگر سایت خرید اینترنتی حاوی نظرات دیگران نبود نشان دهنده این است که آن سایت خیلی جدید است و نمیتواند قابل اعتماد باشد.
- قبل از انجام هرگونه خرید اینترنتی مطمئن شوید که ارتباط شما با آن سایت رمزشده است. بسیاری از مرورگرها ارتباطات رمزشده را با علامت قفل و یا حروف HTTPS سبز رنگ قبل از آدرس سایت در سمت چپ بالای صفحه نشان میدهند.

با خرید از سایت های مطمئن و معتبر از خود محافظت کنید.

بخاطر داشته باشید، اگر سایتی طراحی بسیار حرفه ای دارد، نشانگر قانونی و مشروع بودن آن نیست. اگر احساس خوبی در مورد وب سایتی ندارید، از آن استفاده نکنید. درعوض، از یک سایت شناخته شده و قابل اعتماد و یا سایتی که قبلا از آن بصورت امن خرید کردید استفاده کنید. ممکن است نتوانید قیمت های شگفت آور در این سایت ها پیدا نکنید، ولی به احتمال خیلی زیاد کارتان را با یک محصول اصل به پایان خواهید رساند و از دزدیده شدن اطلاعات شخصی و مالی خود نیز جلوگیری خواهید کرد.

کامپیوتر / موبایل شما

لازم است علاوه بر اینکه از یک سایت مشروع و قانونی خرید میکنید، مطمئن شوید کامپیوتر و یا موبایل شما هم امن است یا خیر. مجرمان سایبری سعی میکنند با آلوده کردن تجهیزات شما به حساب های بانکی، اطلاعات کارت اعتباری و رمز عبور های شما دسترسی پیدا کنند. برای امن کردن تجهیزات خود قدم های ذیل را بردارید:

- اگر در خانه کودک دارید، از دو دستگاه استفاده کنید، یکی برای کودکان و دیگری برای بزرگسالان. کودکان به دلیل کنجکاوی که نسبت به تکنولوژی دارند، احتمال بیشتری دارد که دستگاهشان آلوده شود. با استفاده از کامپیوتر و یا تبلت جداگانه که فقط برای معاملات آنلاین ،نظیر خرید اینترنتی و یا بانکداری اینترنتی، استفاده میشود، احتمال آلوده شدن را به حداقل برسانید.
- همیشه از نرم افزار های آنتی ویروس به روز استفاده کنید. با این کار آلوده کردن تجهیزات شما برای مجرمان سایبری بسیار سخت خواهد شد.

خرید آنلاین همراه با امنیت

کارت اعتباری شما

بطور منظم صورتحساب کارت اعتباری خود را برای بررسی برداشت های مشکوک چک کنید، بخصوص زمانی که از کارت خود برای خرید های اینترنتی و یا خرید از یک سایت آنلاین جدید استفاده کردید. بعضی از شرکتهای ارائه دهنده کارت های اعتباری گزینه ای را برای شما فراهم میکنند که بوسیله آن هر زمانی که برداشتی از کارت شما صورت بگیرد و یا بیش از یک مقدار معین از کارت شما برداشت شود با استفاده از پیام کوتاه و یا ایمیل به شما اطلاع خواهند داد. گزینه بعدی داشتن یه کارت دیگر صرفا برای خرید های اینترنتی است، به این ترتیب در صورت به خطر افتادن آن میتوان به سادگی کارت را تغییر داد بدون اینکه برای سایر پرداخت های شما مشکلی ایجاد کند. اگر به این نتیجه رسیدید که از شما کلاهبرداری شده، سریعا با شرکت ارائه دهنده کارت تماس بگیرید. برای انجام خرید های اینترنتی از کارتهای Debit استفاده نکنید. کارتهای Debit مستقیما از حساب بانکی شما پول برداشت میکنند لذا اگر کلاهبرداری صورت بگیرد برگرداندن پول به حساب شما بسیار سخت خواهد بود. در خاتمه، از کارت های اعتباری هدیه و یا کارتهای اعتباری استفاده کنید که برای هر خرید اینترنتی یک شماره کارت منحصر بفرد تولید میکنند. همچنین میتوانید از سرویس های پرداخت شناخته شده نظیر PayPal نیز استفاده کنید که دیگر نیازی به ارائه اطلاعات کارت خود به فروشنده نداشته باشید.

بیشتر بدانید

با مراجعه به آدرس زیر، مشترک ماهنامه OUCH! شوید و به آرشیو خبرنامه آگاهی از امنیت OUCH! دسترسی داشته باشید، و در مورد راه حل‌های افزایش آگاهی‌های امنیتی موسسهSANS بیشتر بدانید.

آدرس: securingthehuman.sans.org/ouch/archives

شرکت شبکه امن، پیشرو در ارائه راهکارهای امنیت شبکه و اطلاعات، خدمات مشاره، آموزش و تست نفوذ. اطلاعات بیشتر در: www.safenet-co.net

منابع

مهندسی اجتماعی:	https://securingthehuman.sans.org/ouch/2017#january2017
چهار قدم برای امن ماندن:	https://securingthehuman.sans.org/ouch/2016#october2016
شبکه خانگی خود را امن کنید:	https://securingthehuman.sans.org/ouch/2016#february2016
نکته امنیتی روز SANS:	https://www.sans.org/tip_of_the_day.php

هیأت تحریریه : Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley
ترجمه شده توسط : سعید میرجلیلی، مجید هدایتی