ماهنامه ای برای آگاهی کاربران رایانه از امنیت اطلاعات

OUCH!

## دراین شماره..

- فروشگاه اینترنتی جعلی
- کامپیوتر/ دستگاه موبایل شما
- کردیت کارت شما

# خرید اینترنتی امن

## فصل، فصل هوشیاری است

هنگام تعطیلات نزدیک است و بزودی میلیونها نفر در دنیا به دنبال خرید هدیه ایده ال خواهند بود. تعداد زیادی از ما از فروشگاههای اینترنتی خرید خواهیم کرد تا از صف های طولانی و شلوغ در امان بمانیم. متاسفانه الان زمان مورد علاقه مجرمان اینترنتی هم هست تا کلاه برداری مالی و اینترنتی انجام دهند. در این شماره خطرات خرید آنلاین و راههایی که می توانید خودتان را در امان نگه دارید را به شما توضیح می دهیم.

### سردبیر مهمان

جاناتان هومر **(@JonathanLHomer)** پیشقدم مشهور در زمینه صنعت آگاهی امنیت سایبری است و در دولت و بخش خصوصی فعال می باشد.جاناتان متخصص جلب مشارکت مخاطبین و آخرین تکنیک های آموزش است.

## فروشگاههای اینترنتی جعلی

در حالیکه بیشتر فروشگاههای اینترنتی قانونی هستند، تعدادي هم قانونی نیستند، آنها وب سایت های ساختگی هستند که مجرمان راه اندازی کرده اند. مجرمان این وب سایت ها را مشابه ظاهر سایت های خوش نام یا با استفاده از نام سایتهای خوش نام راه اندازی می کنند. سپس از این وب سایت ها برای بدام انداختن مردمی که بدنبال بهترین قیمت ممکن هستند استفاده می کنند. اگر شما کمترین قیمت ممکن را در اینترنت جستجو کنید ممکن است به این سایت های ساختگی هدایت شوید.

هنگام انتخاب وب سایت برای خرید کالایی، در مورد وب سایت هایی که قیمتهایشان بطور قابل ملاحظه ای ارزان تر سایر جاها و سایر وب سایت ها هستند یا وب سایت هایی که محصولاتی را عرضه می کنند که در سراسر کشور قبلا بفروش رفته و چیزی باقی نمانده هوشیار باشید. دلیل اینکه محصولاتشان ارزان ترند یا هنوز موجودند اینست که چیزی که شما دریافت خواهید کرد قانونی نیست، تقلبی است یا دزدی است، یا در بعضی موارد شما هیچ چیز دریافت نخواهید کرد. با انجام کارهای زیر خودتان را محافظت کنید:

- بررسی کنید که وب سایت آدرس پستی و شماره تلفن برای فروش یا پاسخگویی معتبر دارد. اگر وب سایت مشکوک به نظر می رسد، زنگ بزنید و آنرا با مسئولین در میان بگذارید.
- به دنبال شواهد آشکار مثل اشکال گرامری و املایی در نوشته هایشان بگردید.
- اگر وب سایتی از نظر ظاهری بسیار شبیه و کپی یک وب سایت مشهور که قبلا استفاده کرده اید می باشد، که فقط آدرس اینترنتی اش کمی متفاوت است بدان بسیار مشکوک باشید. مثلا، ممکن است شما از وب سایت https://amazon.com برای همه خرید های آمازونی تان استفاده کرده اید. اما نسبت به وب سایتی که از لحاظ ظاهری وانمود می کند که آمازون است و آدرسش https://store-amazon.com است خیلی مواظب باشید.

# خرید اینترنتی امن

- نام فروشگاه یا آدرس اینترنتی اش را در یك موتور جستجو تایپ کنید و ببینید مردم در مورد این وب سایت در گذشته چه گفته اند. بدنبال کلماتی مثل "کلاه برداری" ، "هیچوقت دوباره" یا " قلابی" باشید. کم بودن تعداد یا نبودن نظرات مردم هم علامت خوبی نیست چون نشان می دهد این وب سایت خیلی جدید می باشد.

به یاد داشته باشید، فقط چون سایتی حرفه ای بنظر می رسد بدین معنی نیست که قابل اعتماد هم هست. اگر چیزی در سایتی زنگهای خطر را به صدا در آورد، زمانی را صرف کنکناش کنید. اگر با سایتی راحت نیستید، از آن استفاده نکنید. بجای آن، سایت خوشنامی را که می توانید بدان اعتماد کنید یا در گذشته از آن بطور امنی استفاده کرده اید را پیدا کنید. ممکن است جنس خیلی عالی ای پیدا نکنید اما در عوض محصولی واقعی دریافت خواهید کرد و نیز سابقه اعتبار مالی شما هم خدشه دار نمیشود.

با خرید از وب سایت های مورد اعتماد و خوشنام خودتان را در خرید های اینترنتی بیمه کنید.

## کامپیوتر/ دستگاه موبایل شما

علاوه بر خرید از وب سایت های قانونی، حتما مطمئن باشید که کامپیوتر یا موبایلتان امن است. مجرمان سایبری تلاش خواهند کرد تا دستگاه شما را آلوده سازند تا بتوانند از حساب بانکی، اطلاعات کارت اعتباری ، و رمزهای عبور شما استفاده کنند. با برداشتن این قدم ها دستگاهتان را امن سازید:

- اگر کودك در خانه دارید، دو دستگاه داشته باشید، یکی برای کودك و یکی برای بزرگسالان. کودکان کنجکاوند و با تکنولوژی تعامل دارند، در نتیجه با احتمال بیشتری دستگاهشان آلوده می شود. با استفاده از کامپیوتر یا تبلت جداگانه فقط برای معاملات آنلاین، نظیر بانکداری اینترنتی و خرید، شما شانس آلوده شدن را کاهش می دهید. اگر دو دستگاه ندارید، دو حساب مختلف در یك کامپیوتر مشترك داشته باشید، و اطمینان حاصل کنید که کودکتان مجوز ورود به حساب مدیریت را نداشته باشد.
- فقط به شبکه های وایر لس که خودتان اداره می کنید وصل شوید، شبکه هایی مثل شبکه خانه، یا شبکه هایی که می دانید می توانید برای انجام معاملات مالی اعتماد کنید. استفاده از شبکه های وای فای عمومی مثل شبکه کافی شاپ محلی برای خواندن اخبار عالی هستند اما نه برای دسترسی به حساب بانکی.
- همیشه آخرین بروز رسانی های آنتی ویروس را نصب کنید و آنتی ویرووس بروز رسانی شده را اجرا کنید. اینکار آلوده سازی کامپیوتر شما را برای مجرمان سایبری سخت تر می کند.

## کارت اعتباری شما

همیشه یك چشم به صورتحساب کارت اعتباری تان داشته باشید تا هر گونه هزینه مشکوکی را شناسایی کنید. شما باید صورتحسابتان را مرتب بازبینی کنید، حداقل یك بار در ماه. بعضی شرکت های ارائه دهنده کارت های اعتباری به شما امکان می دهند که هر بار هزینه ای با کارت

# خرید اینترنتی امن

اعتباری شما شد یا هزینه ها ازمیزان مقدار مشخص شده ای بیشتر شد با ایمیل یا پیامك به شما اطلاع بدهند. انتخاب دیگر اینست که یك کارت اعتباری فقط مخصوص خرید های اینترنتی داشته باشید، از این طریق اگر اشتباهی رخ داد شما می توانید بدون اینکه اثری بر دیگر پرداخت هایتان بگذارد کارت اعتباریتان را عوض کنید. اگر معتقدید کلاه برداری انجام شده، سریعا با شرکت ارائه دهنده کارت اعتباریتان تماس بگیرید و شرایط را توضیح دهید. این دلیلی است که استفاده از کارت اعتباری بر استفاده از کارت برداشت از حساب (پرداخت نقدی) برای خرید اینترنتی ارجحیت دارد. کارتهای برداشت از حساب مستقیما از حساب بانکی تان پول برداشت می کنند، و اگر کلاهبرداری صورت بگیرد خیلی بازگرداندن پول به حسابتان مشکل تر خواهد بود.

در ضمن، تکنولوژی جدیدی موجود است که میتوانید بدون افشا کردن شماره کارت اعتباریتان پول پرداخت کنید. سعی کنید از کارت های اعتباری ای که شماره کارت منحصر بفردی برای هر خرید اینترنتی تولید می کنند استفاده کنید، یا از خدمات شناخته شده پرداخت، مثل Paypal که با استفاده از آن لازم نیست شماره کارت اعتباری تان را به فروشنده نشان دهید استفاده کنید.

## 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: http://www.securingthehuman.org

## یادداشت مترجم

سایت www.sycurity.com مرجع امنیت اطلاعات برای کاربران فارسی زبان در سراسر دنیا.

## منابع

| | |
|---|---|
| پنج گام جهت امن ماندن: | https://www.securingthehuman.org/ouch/2014#october2014 |
| امن کردن شبکه خانه: | https://www.securingthehuman.org/ouch/2014#january2014 |
| امن کردن تبلت شما: | https://www.securingthehuman.org/ouch/2013#december2013 |
| نکات امنیتی روز SANS: | https://www.sans.org/tip_of_the_day.php |



هیأت تحریریه : Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
ترجمه شده توسط : سعید میرجلیلی