راهنمای حفاظت در وب

هرچقدر بیشتر بدانید، قادر به محافظت بهتر از خود خواهیدبود.

مسئله جهانی

در هـر ثانیه، ۱۲ نفر از هر فرد آنلایـن قربانی جرایم اینترنتی (سـایبری) می‌شـود که این رقم در سراسـر جهان به بیش از یک‌میلیون قربانی در یک روز می‌رسد.

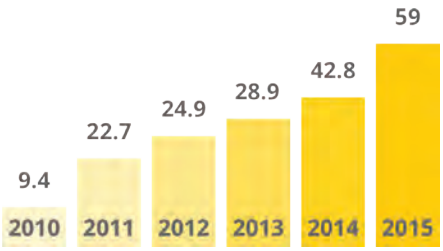
همـه ما مزایا و تسـهیلات امروزی اتصال بـه دنیای دیجیتال را دوسـت داریـم. می‌توانیـم کارهای بانکی، خرید، پسـت الکترونیکی، ارسال متن، به اشتراک گذاری عکس‌ها و بسیاری از کارهای دیگر را به‌صورت مجازی از هر مکانی از طریق لپ‌تاپ، تبلت یا تلفن همراه (موبایل) انجام دهیم.

امـا مجرمان سـایبری (مجـازی) نیز هم‌زمـان و همگام این تکنولوژی ها پیشـرفت می کنند و روش‌های به‌کارگرفته شده توسط هکرها روزبه‌روز پیچیده‌تر می‌شوند. به دلیل تکنولوژی و فناوری مدرن امروزی، دستیابی به اطلاعات شخصی، دستبرد زدن به حسـاب‌های بانکی یا دریافت وام به نام شـما، آسان‌تر شده‌است. آنها می‌توانند به وب‌سـایت‌های دارای نماد اعتماد تجـارت الکترونیکـی و دولتی نفوذ کـرده و اطلاعات هویتی میلیون‌ها نفر را که شما هم شامل آن هستید به دست می‌آورند. با توجه به گزارش ۲۰۱۶ تهدید امنیت اینترنتی سـیمنتک در سال ۲۰۱۵ آسـیب‌پذیری‌های امنیتی عمده‌ای در سه‌چهارم از وب‌سـایت‌های موجود به چشم خورده‌است که این امر شیوه زندگی دیجیتال تمامی افراد را در معرض خطر و ریسـک قرار می‌دهد. هرچقدر بیشتر در مورد جرایم سایبری بدانید، جرایم سـایبری چیست، اطلاعات چگونه به سرقت می روند و در این مـورد چـه کاری می‌توان انجام داد- برای مبـارزه با این جرم گسترده که امکان جلوگیری و دوری از آن وجود ندارد، آماده‌تر خواهیدبود.

۱۲ نفر از هر افراد آنلاین قربانی جرایم سایبری قرار می گیرند.

به طور کلی، بیش از یک‌میلیون نفر در سراسـر دنیا روزانه قربانی این جرایم می‌شوند.

وقایـع شناسـایی شـده مربـوط بـه امنیـت سـایبری (به میلیون)



خطرهای آنلاین متوجه شما، چه مواردی هستند؟

سرقت هویت

سـارقان به منظور دریافت تسـهیلات، وام و یا سایر فعالیت‌های غیرقانونی می‌توانند از هویت شما استفاده کنند.

تراکنش های غیرمجاز (غیر قانونی)

سارقان با استفاده از کارت‌های بانکی (اعتباری) شـما اقدام به خریدهای اینترنتـی غیرمجاز می‌کنند.

صدمه زدن به خوشنامی (شهرت مجازی)

هکرها حساب‌های شـخصی شما را به سرقت برده و از اطلاعات خصوصی شـما علیه خودتان استفاده می‌کنند.

ارقام گزارش شده مربوط به جرایم سایبری

۹ تعداد نقض داده مهم گزارش شده در سال ۲۰۱۵ (منظور از نقض داده مهم، نقض داده‌ای است که در بیش از ۱۰ میلیون رکورد به چشم می‌خورند).

۲۱ تعداد ساعاتی که قربانیان حملات سایبری برای مقابله و برطرف کردن عواقب ناشی از این جرایم سایبری از دست می‌دهند.

۴۵ درصد تعداد کاربرانی که قربانی جرایم سایبری شده‌اند.

۷۵ درصد وب‌سایت‌های قانونی که در آنها به آسیب‌های امنیتی دست یافته شده است.

۱۴۶ تعداد روزهایی که طول می‌کشد تا تخلفات آنلاین انجام‌گرفته، شناسایی شوند.

۵۹۴ تعداد افرادی که در سال ۲۰۱۵ به میلیون نفر، قربانی جرایم سایبری قرار گرفته‌اند.

۱۵۸,۰۰۰ تعداد موارد کلاهبرداری آنلاین گزارش شده در سال ۲۰۱۵.

۲۳۰,۰۰۰ تعداد نمونه‌های جدید بدافزاری منتشر شده در سال ۲۰۱۵ در هر روز.

انواع کلاهبرداری‌ها

درآمدزایی از طریق کلاهبرداری جنسیتی

اگر فردی ناآشنا به‌صورت آنلاین یا از طریق نرم‌افزارهای پیام‌رسانی اجتماعی مانند وی‌چت با کاربر ارتباط برقرار کرده و در قبال ملاقات، قرار عاشقانه یا وعده‌هایی از این دست از شما درخواست خرید کارت‌های خرید/هدیه (به عنوان مثال، کارت‌های خرید آلیپی، آیتونز) کند، در این صورت شما تحت کلاهبرداری جنسیتی قرار گرفته‌اید.

کلاهبرداری از طریق جعل هویت

در صورت دریافت تماس تلفنی غیرمنتظره از سوی کسی که ادعا می‌کند مامور دولتی مانند افسر پلیس، مامور دفتر مهاجرت یا مقام دادگاهی است، دقت کنید؛ چرا که این تماس می‌تواند با هدف کلاهبرداری انجام گرفته‌باشد. در گونه‌ای دیگر از این نوع کلاهبرداری‌ها، تماس‌گیرنده ممکن است که چنین ادعا کند که کارمند یا نماینده بانکی در چین است. آنها چنین بیان می‌کنند که از هویت شما به منظور ارسال بسته‌هایی که حاوی پاسپورت‌های جعلی یا اسلحه‌ها هستند یا درخواست کارت‌های اعتباری بانکی خارج از کشور، استفاده شده‌است. سپس شما را به فردی دیگر که ادعا می‌کند یکی از مقامات چینی است و از شما به خواهش یا حتی با تهدید جزییاتی درباره اطلاعات شخصی از جمله ارقام مربوط به پاسپورت یا حساب بانکی می‌کند، ارجاع می‌دهد.

کلاهبرداری از طریق نرم‌افزار لاین

آیا حساب لاین شما هک شده‌است؟ در کلاهبرداری از طریق نرم‌افزار لاین، هکرها هویت شما را به سرقت برده و از مخاطبان شما درخواست خرید کارت‌های آیتونز یا کارت‌های هدیه برای خود می‌کنند. به گونه‌ای مشابه، ممکن است از شما هم درخواست خرید فوری این‌گونه کارت‌ها از سوی دوستان ارسال شود.

اخاذی سایبری

زمانی که توسط فردی ناآشنا به منظور انجام عملی ناخوشایند برای آنها در محیط مجازی، فریب داده می‌شوید، این افراد بعدها از فیلم‌های ویدئویی و یا تصاویر تهیه شده از این عمل برای اخاذی از شما استفاده می‌کند.

کلاهبرداری از طریق عشق مجازی (اینترنتی)

اگر با شخصی جذاب، معمولا خارجی- در محیط اینترنت دوست شده‌اید و این فرد بعد از مدتی در مورد برخورد به مشکل یا گذراندن اوقاتی سخت با فرد صبحت می‌کند، این حادثه معمولا

تحت عنوان کلاهبرداری از طریق عشق مجازی، تلقی می‌شود. کلاهبردار به منظور به دست آوردن عشق و اعتماد قربانیان خود بر شرح حال ارائه کرده خود پافشاری می‌کند سپس برای اثبات عشـــق طرف مقابل از وی درخواســـت پول می‌کنند. به محض انتقال پول، کلاهبردار ناپدید می‌شود.

کلاهبرداری از طریق خرید آنلاین

اگر کالایی را برای فروش به قیمتی بســـیار مناســـب که به نظر غیرممکن می‌آید در اینترنت مشـــاهده کردید، احتمالا این امر غیر ممکن است.

قربیانیان کلاهبرداری خریـــد آنلاین، تحت تاثیر معامله‌ای در ظاهر خوب قرار می‌گیرند و پول را به حســـاب «فروشـــنده» که قول تحویل کالا را داده‌است، منتقل می‌کنند.

در برخـــی از موارد، فروشـــندگان مبالغـــی اضافی تحت عنوان «عـــوارض گمرکی» یا هزینه های پســـتی تقاضـــا می‌کنند و درنهایت قربانی هرگز کالای مدنظر خود را دریافت نمی‌کند.

کلاهبرداری از طریق سرقت هویت

ممکن است فردی با شما تماس بگیرد و مدعی شود که از سوی ســـازمانی قانونی مامور اطلاع‌رسانی برنده شدن در قرعه‌کشی بخت‌آزمایی است، اما به منظور دریافت این جایزه باید جزییات مربوط به پاســـپورت یا ســـایر اطلاعات خود را در اختیار وی قـــرار دهید. این امر تحت عنوان کلاهبرداری ســـرقت هویت شناخته می‌شـــود، چراکه سازمان‌های قانونی معمولا به جای تماس‌های تلفنی از طریق روش‌های مکاتبه‌ای نوشتاری مانند ایمیل و نامه رسمی، این گونه اطلاع‌رسانی‌ها را انجام می‌دهند.

در صورت داشـــتن هرگونه شـــک و شبهه می‌توانید به منظور تایید اطلاع‌رسانی انجام گرفته با سازمان مزبور تماس بگیرید.

یکی دیگر از راه‌های کلاهبرداری ســـرقت هویت، اســـتفاده از وب‌ســـایت‌های جعلی است که مشـــابه نمونه‌های اصلی خود هســـتند، اما آدرس دسترســـی به آنها دارای تفـــاوت اندکی با یکدیگر هستند. درصورت وارد کردن اطلاعات شخصی و شماره شناسایی شخصی خود در این وب‌سایت‌ها، اطلاعات و پول شما در معرض خطر قرار خواهد گرفت.

یا در تماس تلفنی به منظور کلاهبرداری، ممکن است از سوی فردی که ادعا می‌کند از اطلاعات شـــخصی شـــما برای ارسال مرســـوله‌های غیرقانونی اســـتفاده شده‌است، تماسی دریافت کنیـــد. ممکن اســـت تماس را به فردی دیگـــر ارجاع دهد که مدعی شـــود مســـئول امور مشتریان یا افســـر پلیس است که این فرد از شما درخواست ارائه اطلاعات شخصی‌تان را کند – این اطلاعات شـــامل جزییات حساب بانکی و شماره پاسپورت شماست.

کلاهبرداری از طریق به‌روزرسانی نرم‌افزار

ممکن اســـت تماســـی دریافت کنید که طی آن تماس‌گیرنده مدعی شـــود که کامپیوتر شـــما نیازمند به‌روزرسانی امنیتی یا نرم‌افزاری است. در چنین وضعیتی، به منظور دریافت این به‌روز رسانی، شما نیازمند ارائه شناسه حساب کاربری و رمز عبور خود به فرد تماس‌گیرنده هستید.

گاهی از شـــما خواسته می‌شـــود تا دســـتورهایی خاص را در کامپیوتـــر خود اجرا کنید که بلافاصله بعـــد از این کار متوجه می‌شوید که کنترل کامپیوتر شما در اختیار فردی دیگر است یا از شما خواسته می‌شود تا نرم‌افزاری اضافی را به صورت آنلاین خریداری کنید درحالی که کلاهبرداران اطلاعات کارت اعتباری بانکی یا جزییات حســـاب بانکی شما را برای سوءاستفاده‌های بعدی کپی می‌کنند.

کلاهبرداری شغلی

آیا آگهی‌های شغلی آنلاین مربوط به اسکورت‌های اجتماعی را مشاهده کرده‌اید؟! در این گونه از کلاهبرداری شغلی به قربانیان وعده ملاقات با مشـــتریان ثروتمنـــد در صورت پرداخت هزینه ثبت‌نام؛ داده می‌شـــود. با این حال، پس از پرداخت این هزینه، کلاهبرداران پیش از ناپدید شدن با پول دریافت شده از قربانیان درخواست پرداخت سایر هزینه‌هایی نظیر بیمه و حق عضویت هم می‌کنند.

در آخریـــن گونه از کلاهبرداری شـــغلی، کلاهبرداران تبلیغات شـــغلی مربوط به نایب خریدار، تحصیلدار ســـهام یا مشارکان آزمون سیســـتم وب‌ســـایت‌های محبوب رده‌بندی شده نظیر گامتیری را به‌صورت آنلاین منتشـــر می‌کنند. از مشارکان در این چنین آزمون‌هایی خواســـته می‌شـــود تا اطلاعات شخصی مانند نام، I/C، شماره تلفن همراه، کد امنیتی گوشی موبایل یا گـــذرواژه یک‌بار مصرف (OPT) را ارائه دهند. چنین اطلاعاتی به کلاهبرداران امکان دسترســـی به خطـــوط موبایل قربانیان را می‌دهـــد که بدین‌ترتیب قادر به دریافت تســـهیلات آنلاین می‌شوند.

کلاهبرداری از طریق Money Mule

وقتی فردی که به صورتی آنلاین با وی به آشـــنا شده‌اید از شما درخواست به‌کارگیری حساب بانکی‌تان به منظور دریافت پول یا انتقال پول به حســـابی دیگر از طریق حساب شخصی شما را

می‌کند، بسیار محتاطانه عمل کنید. در چنین وضعیتی از شما تحت عنوان Mule استفاده خواهدشد.

اعضای سندیکاهای کیفری خارجی، اهداف دوست‌یابی خود را بر وب‌سایت‌های شبکه‌های اجتماعی متمرکز کرده‌اند. این مجرمان اغلب خود را در ظاهر افرادی تنها معرفی می‌کنند که به دنبال همدم و دوست هستند. پس از به دست آوردن اعتماد Mule، مجرم از فرد درخواست ایجاد حساب بانکی جدید یا استفاده از حساب موجود برای دریافت پول می‌کند. زمانی که پول در حساب بانکی به صورت سپرده واریز می‌شود از Mule خواسته می‌شود تا پول را به حساب بانکی شخص یا شرکتی دیگر انتقال دهد که معمولا در خارج از کشور حساب بانکی Mule است. از سویی دیگر، سندیکاهای کیفری آگهی‌های شغلی را در پورتال‌های کاریابی آنلاین منتشر می‌کنند. موقعیت شغلی مورد درخواست در این آگهی‌ها مربوط به عاملی است که به‌ازای انتقال پول به شرکتی قانونی، مبلغی را به عنوان درصد دریافت می‌کند.

چگونه مجرمان اطلاعات شخصی شما را به دست می‌آورند

مجرمان سایبری دارای مجموعه‌ای از ابزارها و منابع برای از بین بردن و تباهی زندگی شما هستند.چه در محل کار، چه در محیط بیرونی یا چه در خانه باشید، در زمانی غیرمنتظره ممکن است در معرض جرایم سایبری قرار بگیرید. در ادامه برخی از روش‌های پرکاربرد کیفری که مجرمان برای کلاهبرداری و اجرای جرایم خود می‌کنند، آورده شده‌است.

نقض اطلاعات

اگر اطلاعات شخصی خود در سازمان مالی یا کسب‌وکار – حتی در شرکت‌های بزرگ بیمه یا پزشکی - ذخیره کنید، هویت شما در معرض خطر نقض اطلاعاتی بزرگ قرار می‌گیرد.

بدافزار و ویروس

با توجه به تعداد ویروس‌های جدید، کامپیوتر و اطلاعات شما از طریق وب‌سایت‌ها، برنامه‌های اینترنتی یا شبکه‌های اشتراک‌گذاری فایل، قابل دسترسی و هک هستند.

خرید آنلاین

اگر به اشتباه از وب‌سایت خرده‌فروشی جعلی خرید کرده یا از طریق سیستم‌های پرداخت غیرقانونی ناامن پرداخت‌های خود را انجام دهید، کارت‌های اعتباری و بانکی شما در معرض خطر قرار خواهند گرفت.

کی‌لاگر (ثبت‌کننده ضرب کلید)

مجرمان می‌توانند فناوری‌هایی را در رایانه‌های عمومی، صفحه نمایش‌های پمپ بنزین و صفحه کلید عابربانک‌ها به منظور ثبت و ضبط دکمه‌هایی که در حین وارد کردن گذرواژه خود فشار میدهید، نصب کنید.

فیشینگ

این‌گونه از کلاهبرداری‌ها شامل ایمیل‌های جعلی هستند که به صورتی شگفت‌انگیز مشروع و قانونی به نظر می‌آیند. اگر از شما خواسته شد تا بر لینکی کلیک کرده یا اطلاعاتی را ارائه دهید، سارقان از این طریق می‌توانند گذرواژه‌ها و شماره حساب‌های شما را به دست آورند.

به اشتراک‌گذاری فایل بین دو کامپیوتر

سایت های به اشتراک گذاری فایل میلیون کابر در سراسر جهان را به یکدیگر متصل می نماید. این ارتباط می‌تواند علاقمندان به موسیقی را به ویروس‌ها و شبکه‌های ناامن نیز متصل کند.

ویشینگ (فیشینگ از طریق تماس تلفنی)

کلاهبرداری‌های تلفنی که درخواست ارائه اطلاعات شخصی از طریق تماس مستقیم یا پیام از قبل ضبط شده می‌کنند، به منظور به سرقت بردن هویت شما به‌کار گرفته می‌شوند.

دیدزدن (از روی شانه)

سارقان در حین انجام عمل خرید می‌توانند در پشت سر شما ایستاده و در حین وارد کردن گذرواژه یا شماره شناسایی شخصی، ارقام را مشاهده کنند.

زیر و رو کردن زباله ها

برخی از مجرمان زباله‌های شما را به منظور یافتن صورت‌حساب‌های قدیمی، رسیدها و سایر اطلاعات شخصی دور ریخته شده، زیر و رو کرده و به راحتی اطلاعات شما را به سرقت می‌برند.

تغییر آدرس

سارقان به منظور دریافت اطلاعات شخصی و شماره حساب‌ها، آدرس‌تان را تغییر می‌دهد تا ایمیل‌تان را به آدرس خود هدایت کنند.

سرقت نامه

گاهی اوقات سارقان نامه‌ها را از صندوق‌های پستی بدون قفل برای دستیابی به اطلاعات کارت اعتباری، فرم‌های مالیاتی یا سایر اطلاعات شخصی و مالی می‌ربایند.

کیف پول به سرقت رفته

برخی از سارقان به دنبال چیزی بیش از پول نقد هستند. آنها بیشتر به دنبال کارت‌های اعتباری بانکی، کارت شناسایی و سایر شناسه‌های شخصی شما هستند.

قراردادن پوشش اضافی در دستگاه‌های ATM

سارقان این‌گونه سیستم‌ها را بر دستگاه‌های خودپرداز و سیستم‌های پمپ بنزین نصب می‌کنند تا از این طریق بتوانند اطلاعات شخصی شما را هنگام استفاده از کارت به‌دست بیاورند.

ربودن هویت پزشکی

این‌گونه از سرقت هویت تا زمانی که به منظور معالجه پزشکی یا دریافت بیمه مراجعه نکرده‌اید، قابل شناسایی است. مجرمان با استفاده از هویت شما یا اطلاعات مربوط به بیمه‌تان از سرویس مراقبت‌های پزشکی بهره‌مند می‌شوند.

به سرقت بردن عدم سوءپیشینه

سارقان هویت از اطلاعات شخصی‌تان برای جعل سوابق و ساختن عدم سوءپیشینه استفاده می‌کنند و بدین‌ترتیب جریمه‌های خود را پرداخته نکرده و یا از بازداشت‌شدن خود جلوگیری می‌کنند.

ربودن کارت شناسایی

سارقان از شماره کارت شناسایی ربوده‌شده به منظور ایجاد کارت‌های شناسایی هویت جدید، دسترسی به مدارک یا دستیابی به اطلاعات شخصی و فردی استفاده می‌کنند.

سرقت هویت برای مسائل مالیاتی

با استفاده از کارت شناسایی به سرقت رفته و سایر اطلاعات شخصی، سارقان هویت می‌توانند فایلی را به منظور درخواست مالیات جعلی آماده کرده و بیش از جمع‌آوری فایل توسط شما، این مالیات را دریافت کنند.

چگونه از کلاهبرداری آنلاین پیش از وقوع آن جلوگیری کنند

راهنمایی‌هایی ارزشمند به منظور کمک در محافظت از اطلاعات شخصی‌تان در ادامه آورده شده‌اند.

در ایمیل:

- نامه‌های ارسالی خود را در صندوق‌های پستی فاقد قفل قرار ندهید.
- شماره حساب‌ها یا اطلاعات شخصی خود را بر روی بخش بیرونی پاکت نامه ننویسید.
- اگر محل زندگی خود را برای بیش از یک یا دو روز ترک می‌کنید از مامور پستی درخواست کنید تا بسته‌های پستی شما را برایتان در دفتر پستی نگه دارد.

در خرید آنلاین:

- اطمینان یابید که از وب‌سایتی مطمئن خرید خود را انجام می دهید. دقت کنید وب‌سایتی که از آن به صورت آنلاین خرید می‌کنید در بخش نوار جست‌وجو دارای علامت قفل بوده و همچنین آدرس دسترسی به سایت از "https" استفاده کرده‌باشد.
- از وای‌فای‌های عمومی برای اتصال به اینترنت و انجام امور بانکی یا خرید استفاده نکنید.
- از گذرواژه‌های قوی استفاده کنید و بکوشید تا از گذرواژه‌ای یکسان برای سایت‌های مورد علاقه خود استفاده نکنید.

در کارت‌های اعتباری و ضمانتی پرداخت بدهی

- به جای کارت‌های پیش‌پرداختی (دبیت) از کارت‌های اعتباری استفاده کنید. در هنگام استفاده از کارت‌های اعتباری از امنیت بیشتری برخوردار هستید.
- وضعیت حساب بانکی و کارت‌های خود را به طور کامل برای آگاهی از صحت و درستی آنها بررسی کنید.
- بیش از نیاز خود کارت‌های اعتباری و دبیت را با خود حمل نکنید.

در بانک

- اطلاعات شخصی خود را به فرد تماس گیرنده که مدعی تماس از سوی بانک یا شرکت کارت اعتباری است، ارائه ندهید.
- در صورت امکان به منظور جلوگیری از به سرقت رفتن چک، از واریز نقدی مستقیم استفاده کنید.

در کیف پول خود / در خانه خویش

- به منظور حفظ اسناد و مدارک از دست تبهکاران، آن‌ها را ریزریز کنید.
- کارت شناسایی خود را در کیف پول قرار ندهید.
- تعداد کارت‌های شناسایی را که با خود حمل می‌کنید به حداقل برسانید.

امور آنلاین و کامپیوتری

- از گذرواژه‌های قوی همراه با ترکیبی از حروف بزرگ و کوچک، ارقام و علائم استفاده کنید.
- به ایمیل‌های غیرمنتظره مشکوک که درخواست اطلاعات شخصی‌تان را می‌کنند، دقت داشته‌باشید.
- اگر می‌خواهید کامپیوتر خود را بفروشید و یا دور بیندازید، هارد دیسک آن را به صورت فیزیکی از بین ببرید.