



ماهنامه آگاهی از امنیت اطلاعات برای شما

## سرقت هویت: پیشگیری، شناسایی و پاسخگویی

### مقدمه

در عصر دیجیتال امروزی، اطلاعات شخصی شما بیش از هر زمان دیگری ارزشمند است. متأسفانه، این نیز آن را به یک هدف اصلی برای سرقت هویت تبدیل می کند. درک این تهدید، شناسایی آن، و دانستن اینکه چگونه از خود محافظت کنید، عناصر ضروری برای محافظت از زندگی دیجیتال آنلاین شما هستند.

### سرقت هویت چیست ؟

سرقت هویت زمانی اتفاق می افتد که شخصی به طور غیرقانونی اطلاعات شخصی شما - نام شما، شماره های شناسایی مانند شماره امنیت اجتماعی یا شماره پاسپورت، یا جزئیات کارت اعتباری را برای ارتکاب کلاهبرداری یا سایر جرایم به دست می آورد. یک شکل رایج سرقت هویت، سرقت هویت مالی است که در آن شخصی از اطلاعات شما برای کلاهبرداری مالی استفاده می کند. مثلاً هویت شما را می دزدند و به نام شما کارت اعتباری، رهن یا وام خودرو می گیرند و شما باید قبوض را بپردازید. با این حال، انواع دیگری از سرقت هویت وجود دارد مانند سرقت هویت پزشکی که در آن شخصی اطلاعات پزشکی شما را می دزدد و برای اقدامات پزشکی که هرگز دریافت نکرده اید، به نام شما بیمه پزشکی می گیرد. یکی دیگر از موارد سرقت هویت مربوط به مالیات است، زمانی که یک مجرم از شماره شناسایی مالیاتی شما برای ارسال اظهارنامه مالیاتی به نام شما و ادعای بازپرداخت متقلبانه استفاده می کند. سپس وقتی سعی می کنید اظهارنامه مالیاتی تشکیل دهید، نمی توانید پول خود را پس بگیرید زیرا قبلاً به شخص دیگری ارسال شده است.

### اقدامات پیشگیرانه

برای محافظت از خود چه کاری می توانی انجام دهی؟ متأسفانه، آنطور که به نظر می رسد آسان نیست، زیرا بسیاری از سازمان ها در حال حاضر اطلاعات شما را در اختیار دارند و حفاظت از آن به عهده آنهاست. با این حال، چند قدم کلیدی وجود دارد که می توانید انجام دهید.

- رمز های عبور قوی: یکی از موثرترین راه ها برای محافظت از خود این است که هر یک از حساب های خود را با یک رمز عبور منحصر به فرد و طولانی ایمن کنید و در صورت امکان، احراز هویت چند عاملی را فعال کنید.
- به روز رسانی منظم نرم افزار: با فعال کردن به روزرسانی خودکار در همه دستگاه های شما، مطمئن شوید دستگاه های شما با جدیدترین وصله های امنیتی و ویژگی ها به روزرسانی شده اند.
- کارتهای اعتباری: از کارت های اعتباری برای خریدهای آنلاین استفاده کنید، هرگز از کارت های نقدی استفاده نکنید، زیرا کارت های اعتباری محافظت بسیار بیشتری در برابر تقلب به شما می دهند. ایده دیگر این است که از یک کارت اعتباری فقط برای خریدهای آنلاین و از یکی دیگر برای خریدهای حضوری استفاده کنید. برخی از خدمات، کارت اعتباری مجازی یا یک بار مصرف را برای هر خرید آنلاین ارائه می دهند.
- مسدود کردن اعتبار: مسدود کردن اعتبار، گزارش اعتباری شما را قفل می کند و از کلاهبرداران جهت باز کردن حساب های جدید به نام شما جلوگیری می کند. این کار را می توان به صورت رایگان با تماس با دفاتر اعتباری بزرگ انجام داد. این ممکن است گزینه ای در همه کشورها نباشد.

## کشف سرقت هویت

تشخیص زود هنگام یکی از قوی ترین راه هایی است که می توانید از خود محافظت کنید. هر چه زودتر تشخیص دهید هویت شما توسط شخص دیگری مورد استفاده قرار گرفته است، زودتر می توانید اقدام کنید. برخی از رایج ترین نشانه های سرقت هویت عبارتند از:

- صورتهای مالی غیرمعمول: به طور منظم تمام صورت حساب های بانکی و کارت اعتباری خود را کنترل کنید. شما نیاز دارید به دنبال هرگونه هزینه یا انتقال پولی باشید که می دانید انجام نداده اید. یک راه عالی برای انجام این کار، فعال کردن اعلان های خودکار است. به این ترتیب هر زمان که هزینه ای برای کارت اعتباری شما وجود دارد یا تغییری در حساب پس انداز یا چک شما وجود دارد، بلافاصله به شما اطلاع داده می شود.
- گزارش های اعتباری نامنظم: سالانه گزارش های اعتباری خود را برای فعالیت مشکوک بررسی کنید. شما به دنبال هر وام جدیدی به نام خود باشید که می دانید انجام نداده اید یا اگر تغییرات عمده ای در رتبه اعتباری خود دارید.
- صورتحساب ها یا اعلان های مرموز: اگر شروع به دریافت صورتحساب برای اقلامی می کنید که می دانید هرگز خریداری نکرده اید، یا اگر توسط آژانس های پرداخت برای صورتحساب های پرداخت نشده برای اقلام یا خدماتی که هرگز خریداری نکرده اید با شما تماس گرفته اند، محتاط باشید.
- انکارهای غیرمنتظره: اگر به طور غیرمنتظره ای بازپرداخت مالیات یا درخواست اعتبار یا وام شما رد شد، علت آن را بررسی کنید.

## پاسخ به سرقت هویت و نجات از آن

اگر نگران هستید که هویت شما به خطر افتاده است، فوراً اقدام کنید.

- سریعاً گزارش دهید: در صورت مشکوک شدن به حادثه فوراً گزارش دهید. برای مثال، اگر در حساب بانکی یا کارت اعتباری خود فعالیت جعلی را شناسایی کردید، با بانک خود تماس بگیرید. همچنین، گزارشی را برای مجریان قانون محلی ارسال کنید. این می تواند در اثبات جرم و کمک به شما در بازپرداخت هرگونه هزینه یا ثبت ادعاهای بیمه بسیار مهم باشد.
- هشدارهای تقلب و مسدود شدن اعتبار: در گزارش های اعتباری خود یک هشدار تقلب قرار دهید و اگر قبلاً این کار را نکرده اید، مسدود کردن اعتبار را در نظر بگیرید. علاوه بر این، برای حذف اطلاعات تقلبی، با دفاتر اعتباری همکاری کنید.
- همه چیز را مستند کنید: هنگام تماس با سازمان ها برای بازپایی، مطمئن شوید که سوابق مفصلی از ارتباطات و اقدامات انجام شده خود را نگه دارید، و شامل افرادی که با آنها صحبت کرده اید، چه تاریخ/زمانی و چه مواردی در مورد آن صحبت شده است را ذکر کنید.
- رمزهای عبور را تغییر دهید: گذرواژه ها را برای همه حساب های کلیدی خود به روزرسانی کنید. اگر یک برنامه مدیریت رمز عبور برای ردیابی همه رمزهای عبور جدید خود ندارید، در نظر بگیرید که یکی تهیه کنید.

## نتیجه

با درک اینکه سرقت هویت چیست و با به کارگیری این اقدامات ارائه شده، می توانید خطر قربانی شدن خود را تا حد زیادی کاهش دهید.

## منابع

برنامه های مدیریت رمز عبور: <https://www.sans.org/newsletters/ouch/power-password-managers>

ایمن سازی حساب های مالی: <https://www.sans.org/newsletters/ouch/securing-financial-accounts>

مسدود شدن اعتبار: <https://www.usa.gov/credit>

گزارش سرقت هویت: <https://www.identitytheft.gov>

ترجمه شده برای عموم توسط: مجید هدایتی، هومن خجاو

IOUCH توسط SANS Security Awareness منتشر شده است و تحت مجوز 4.0 Creative Commons BY-NC-ND می باشد. شما آزاد هستید که این ماهنامه را برای بقیه اشتراک گذاشته یا آن را توزیع نمایید به شرطی که آن را به فروش نرسانده یا تغییری در آن ایجاد نکنید. هیئت تحریریه: Walter Scrivens, Phil Hoffman, Alan Waggoner, Leslie Ridout, Princess Young.