

# اطلاعات تنها چیزی است که اگر از شما سرقت شود، ممکن است اصلا متوجه نشوید



در حالی این اتفاق افتاد که نام کوچک مادر استوارت، اسم رمز تکمیلی ورود به حساب بانکی اینترنتی او بود!

چیزی که در حقیقت اتفاق افتاد این بود که سارقان و جاعلان هویت، با استفاده از اطلاعات محرمانه و شخصی استوارت مانند کارت اعتباری، گواهینامه ی رانندگی، شماره تلفن منزل و جلب اعتماد همسر استوارت توانستند اسم رمز حساب اینترنتی بانک او را پیدا کنند و استوارت را به میزان ۲۳۰۰۰ پوند شامل ۴۰۰۰ پوند برداشت از خودپرداز الکترونیکی، ۲۰۰۰ پوند انتقال حساب به حساب، ۱۴۰۰۰ پوند خرید اعتباری، ۲۰۰۰ پوند خرید یک دوربین فیلم برداری و ۱۰۰۰ پوند خرید از یک فروشگاه پوشاک متضرر سازند.

کمیسیون تجارت فدرال در ایالات متحده در سال ۲۰۰۴ بیش از ۶۳۵۰۰۰ شکایت در مورد سرقت هویت و جعل اسناد محرمانه که چیزی بالغ بر ۵۴۷ میلیون دلار گزارش شده اعلام داشت که از این میزان ۶۱ درصد جعل و کلاهبرداری اسناد و ۳۹ درصد سرقت اسناد محرمانه می باشد. ۸۱ درصد مردم سرقت هویت را از جیب زنی، زورگیری، و سرقت منزل مهمتر میدانند و نگران آن هستند

**سرقت اطلاعات زمانی اتفاق می افتد که اطلاعات محرمانه ی اشخاص و یا سازمان ها توسط افراد غیر کشف میشوند.**

سرقت هویت اولین اقدام برای سوء استفاده از اطلاعات محرمانه و اعتبار افراد می باشد. تبهکاران با سرقت این اطلاعات اعتبار و امنیت مالی و روانی قربانیان خود را تهدید



زمانی استوارت هولدن ۳۴ ساله مدیر یک بنگاه آموزش تجارت بریتانیایی در نوامبر سال ۲۰۱۰ متوجه فاش شدن اطلاعات شخصی خود شد که ۲۳۰۰۰ پوند از حساب بانکی اش برداشت شده بود. او پس از اینکه متوجه شد دلیل افشای اطلاعات شخصی و محرمانه اش، بی احتیاطی او در نگهداری و حفاظت از اوراق هویتش بر روی میز کارش بوده، سخت نگران شد و این نگرانی زمانی جدی شد که همسرش طی یک تماس تلفنی در همان روز به او اطلاع داد که از انجمن بانک شهر به منزل وی تلفن زده اند و نام کوچک مادرش را پرسیده اند.

می کنند. جعل هویت هم پیامد سرقت هویت تلقی میشود و گام بعدی و نهایی تبهکاران در سوءاستفاده و متضرر کردن فرد قربانی است، که شامل جعل اسناد، دسترسی به حساب بانکی، استفاده از سرویس ها و خدمات شهری و شهروندی و غیره میباشد.

**تبهکاران و سارقان از روش های متفاوتی برای دسترسی به این اطلاعات استفاده می کنند.**

روش هایی بسیار ساده، که ما در زندگی روزمره اصلا به آنها توجهی نشان نمی دهیم، شاید بسیار حیرت زده شویم وقتی متوجه شویم که سطل آشغال محل کار و یا محل زندگی ما می تواند مملو از اطلاعات محرمانه، شخصی، حقوقی و یا سازمان ما باشد و بیش از آن چیزی که ما فکر می کنیم حاوی اطلاعات مهم است.

اسناد و مدارکی که در ظرف زباله ی ما قرار دارند، شامل ایمیل های چاپ شده، طرح های بازاریابی، طرح های همکاری حقوقی، مکاتبات تجاری، قبوض آب، برق و تلفن، صورت وضعیت های مالی، فاکتور ها و پیش فاکتور ها، لیست قیمت های نمایندگان، موجودی انبار، محاسبات قیمت تمام شده، گزارشات، تحقیق های بازار، اطلاعات رقبا، گزارش جلسات، مدارک نمایندگی، اطلاعات مشتری، قراردادهای و اطلاعات کارکنان از اسناد هویت افراد فوت شده و غیره باشند.

همچنین علاوه بر اوراق و اسناد مکتوب، امروزه به دلیل پیشرفت روزافزون فن آوری اطلاعات و ارتباطات IT، شاید راه حلی برای از بین بردن یک دیسک فشرده یا کارت اعتباری و هارد دیسک کامپیوترمان نیابیم. اما وقتی متوجه سرقت اطلاعاتمان می شویم که با قبض یا رسید

پرداخت از حساب بانکی مان و یا سند سررسید قسط یک بیخچال ۳۰ فوت دودرب با سیستم یخ ساز اتوماتیک مواجه شویم.

وضعیت مورد بحث در بخش هایی از سازمان ها صورت می گیرند که بترتیب زیر در معرض خطر امنیتی قرار دارند:

۴۵٪ واحد منابع انسانی و اداری

۴۰٪ حسابداری و مالی

۳۸٪ فن آوری اطلاعات و IT

۳۴٪ واحد فروش

۱۷٪ واحد بازاریابی

۱۸٪ واحد شکایات، انتقادات و پیشنهادات

روش های ساده و قابل توجهی که برای بالا بردن ضریب امنیت اطلاعات در سازمان ها و پیشگیری از افشای اطلاعات محرمانه بکار می روند، عبارتند از:

حفاظت اسناد و مدارک، چارت سازمانی قوی، آموزش افراد و پرورش پرسنل مجرب، بالا بردن ضریب امنیت سیستم IT.

اما اسناد مکتوب و اوراق محرمانه و لوح های فشرده حجم بالایی از اطلاعات یک سازمان را تشکیل می دهند. بدیهی است که همواره حجم زیادی از این اطلاعات یا نسخ رونوشت آنها مورد نیاز سازمان نیستند، اما کماکان از حیث اطلاعاتی برای سازمان دارای اهمیت بوده و در صورت افشا در دسر ساز خواهد شد. امروزه برای از بین بردن این اطلاعات قابل دسترس، از دستگاه های کاغذخردکن بمنظور امحاء (نابودسازی) اسناد محرمانه و طبقه بندی شده که جزء سیستم های امنیت اطلاعات بشمار میروند، استفاده می شود. این دستگاه ها در سطوح مختلف امنیتی طراحی گردیده و بسته به نیاز کاربر در هر محیطی قابل استفاده است.

سطوح امنیتی از ۲الی ۶ طبق استاندارد بین المللی DIN تعریف شده اند. بدین معنی که هرچه عدد بزرگتر باشد سباز برش ریزتر بوده و سطح امنیتی بالاتری تامین خواهد

شد. با توجه به اهمیت مدارکی که در اختیار دارید میتوانید سطح امنیتی مورد نیاز خود را انتخاب نمایید. سطوح پائینی جهت مصارف خانگی و شخصی و سطوح بالا جهت مصارف سازمانی و استراتژیک کاربرد دارند.

**در حالت کلی دو نوع کاغذ خردکن وجود دارد:**

۱- نواری یا رشته ای، ۲- پودری. که از این میان خردکن های پودری با خردکردن کاغذ به قطعات بسیار کوچک با توانایی تبدیل یک کاغذ A4 به بیش از ۱۵۰۰۰ ذره، امنیت بالاتری دارند. بعلاوه بسیاری از خردکن های امروزی با قابلیت خرد کردن سوزن، منگنه، کلیپس، CD و کارت اعتباری گستره ی وسیع تری از کاربری این ابزارها را فراهم نموده اند.

اتحادیه امنیت اطلاعات تجاری انگلستان طی یک تحقیق گسترده در سال ۲۰۱۰، میان ۱۴۰۰۰ کارمند در رتبه های مختلف سازمان ها، بر روی سطح امنیت سازمان ها و ارگان های تجاری انگلستان اعلام داشت که به ترتیب اطلاعات درچه وضعیتی بیشترین ریسک سرقت و افشا شدن را دارا می باشند:

طی این تحقیق میزان ریسک افشای اطلاعات:

۶۲٪ بصورت اوراق مکتوب در سطل زباله، ۴۶٪ بر روی مخزن کاغذ چاپگرها،

۴۴٪ روی میز کار افراد، ۳۰٪ در پرورده ها و پوشه ها، ۱۸٪ درصد آماده برای پست،

۱۲٪ در کمده بایگانی و ۶٪ بصورت اطلاعات بر روی کامپیوتر می باشند.

در شماره های بعد به بررسی بیشتر پدیده ی سرقت اطلاعات و روشهای جلوگیری از آن خواهیم پرداخت...

## نیکیتا®

کاغذ خردکن وسیله ی خردکن های نیکیتا  
باتنوع خانگی، اداری و صنعتی

**nikita®**

model: nikita SD 9360

نوع برش : پودری

ظرفیت ورودی کاغذ: ۱۰ برگ A4

سباز برش : ۲\*۹ میلیمتر

سطح امنیت : ۴

سرعت : ۳.۵ متر در دقیقه

حجم مخزن : ۲۷ لیتر

قابلیت خرد کردن سی دی، سوزن، کلیپس

این کاغذ خردکن امحای اسناد را با سطح ۴ امنیتی انجام می دهد و هر برگ کاغذ A4 را به ۳۴۶۵ ذره تبدیل می کند.

تمامی کاغذ خردکن های نیکیتا دارای:

۲۴ ماه گارانتی طلایی

۳ ماه تعویض

۵ سال گارانتی تیغه

۱ سال بیمه حوادث

39 x 36 x 60 cm

برای مقابله با سرقت اطلاعات، هر جا و در هر وضعیت به یک کاغذ خردکن نیکیتا نیاز دارید...



برای مشاهده مدلهای متنوع خردکن های نیکیتا [www.nikita.ir](http://www.nikita.ir)

شرکت سفیر خاورمیانه: تهران، خیابان ایرانشهر شمالی، شماره ی ۲۳۰ طبقه دوم تلفن: ۹۴-۸۸۸۴۹۲۹۳-۱ info@nikita.ir