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

هشدار

در شماره ی قبل خواندیم که چگونه استوارت هولدن مدیر یک بنگاه آموزش تجارت در بریتانیا در نوامبر سال ۲۰۱۰ با از دست دادن ۲۳۰۰۰ پوند قربانی پدیده ی سرقت اطلاعات شد.

در سال ۲۰۰۵ نیز سامانتا گرین کارمند واحد حسابداری یک شرکت خصوصی در برایتون انگلستان قربانی سرقت اطلاعات شد. سامانتای ۳۶ ساله زمانی که در حال برداشت از حساب بانکی اش بود متوجه شد که به حدنصاب محدودیت اعتبار برداشتی رسیده است. او پس از کنترل صورت حساب خود با چندین تراکنش خرید اینترنتی که توسط او انجام نشده بود مواجه شد. او بلافاصله با سایتهای خرید آنلاین و بانک مربوطه تماس گرفت و آنها را در جریان مساله قرار داد ولی آنها تراکنش ها را مشکوک ارزیابی نکردند.

ولی اصل ماجرا این بود که سارقان و جاعلان هویت و اطلاعات با استفاده از اطلاعات محرمانه و شخصی سامانتا توانستند به اطلاعات حساب بانکی وی دست یابند و او را به مبلغ ۳۰۰۰ پوند متضرر سازند. این در حالی بود که بانک سامانتا پس از دریافت گزارشی مبنی بر استفاده ی کارت اعتباری سامانتا در استرالیا و آمریکا حساب بانکی او را مسدود کرد و این ضربه ی بزرگی در زندگی سامانتا از نظر اقتصادی محسوب می شد.

۸۱ درصد مردم انگلستان سرقت هویت را از جیب زنی، زورگیری، و سرقت منزل مهمتر میدانند و نگران آن هستند. این در حالی است که متوسط ۴۶۷ روز طول می کشد تا هویت فرد تبهکار شناسایی شود.

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.

طبق گزارشات سالانه ی این کمیسیون، تعداد این شکایات هر ساله رو به افزایش است بطوریکه از میزان شصت هزار شکایت در سال ۲۰۰۲ میلادی به صد و هفتاد هزار شکایت در سال ۲۰۰۴ طی دو سال رسیده است. یعنی رشد سالانه بالغ بر ۲۵ درصد.

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 هویت افراد می باشد. تبهکاران با سرقت این اطلاعات فرد قربانی را مورد سوء استفاده و جعل هویت قرار میدهند.

**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 مختلفی 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 و شخصی و حقوقی ما و یا سازمان ما باشد و بیش از آن چیزی که ما فکر می کنیم حاوی اطلاعات مهم می باشد.**

اسناد و مدارکی که در ظرف زباله ی ما قرار دارند، شامل ایمیل های چاپ شده، 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 اطلاعات رقبا و بازار،گزارش جلسات، اطلاعات مشتریان، قراردادها 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 یخچال ۳۰ فوت دودرب با سیستم یخ ساز اتوماتیک مواجه شویم.

روش های ساده و قابل توجهی که برای بالابردن 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 و غیره...

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 سطح آموزش افراد و پرسنل سازمانها در ارتباط با میزان رفتار امنیتی آنها بسیار پایین است. طی این تحقیق مشخص شد که ۷۸ درصد شرکتها و سازمانهای نمونه گیری شده در این تحقیق دارای سیاست های پیشگیری در حوزه ی سرقت اطلاعات می باشند اما از این میزان فقط ۲۹ درصد آموزش داده می شود. طی این تحقیق اعلام شد که درصد بالایی از پرسنل سازمانها و ادارات از اینکه آیا اطلاعات مورد استفاده ی آنها در سطح امنیتی بالایی نگهداری میشود یا خیر اطمینان خاطر ندارند.

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 دردسر ساز خواهد شد.

**امروزه برای از بین بردن این اطلاعات قابل دسترس، از دستگاه های کاغذخردکن بمنظور امحاء 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 ۲ الی ۶ طبق استاندارد بین المللی DIN تعریف شده اند. بدین معنی که هرچه عدد بزرگتر باشد سایز 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 نمائید. سطوح پائینی جهت مصارف خانگی و شخصی و سطوح بالا جهت مصارف سازمانی و استراتژیک کاربرد دارند.

برای تهیه ی یک کاغذخردکن می بایست به موارد زیر توجه کرد:

در حالت کلی دو نوع کاغذ خردکن وجود دارد: رشته ای و پودری. که از این میان خردکن های پودری با خردکردن کاغذ به قطعات بسیار کوچک با توانایی تبدیل یک کاغذ A۴ به بیش از ۱۵۰۰۰ ذره، امنیت بالاتری دارند.

شماره ی سطح امنیتی از ۲ تا ۶

تعداد برگهای ورودی جهت افزایش سرعت کار

میزان حجم مخزن خرده کاغذ به لیتر

و توان موتور الکتریکی.

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.

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


کاغذ خُرد کن و سی دی خُرد کن های نیکیتا
روشی حرفه ای برای مقابله با سرقت اطلاعات ...

گروه امحاء اسناد نیکیتا

nikita®

کاغذ خُردکن های خانگی، اداری و صنعتی در سطوح امنیتی مختلف

www.nikita.ir مورمشتریان ۹۴-۸۸۸۴۹۲۹۳-۰۲۱