در هر یک از اتاق‌های منزل یا محل کار مکانهای امن را تعیین کنید. این مکان می‌تواند زیر یک میز محکم، یا کنار دیوار داخلی به دور از پنجره باشد.

## جایزه یک میلیون دلاری اپل برای پیدا کردن باگ‌های امنیتی

اپل قصد دارد سال آینده تعدادی از آیفون‌های خود را که به‌طور ویژه برای پژوهشگران امنیتی ساخته شده، ارسال کند، تا آنها حفره‌ها و باگ‌های امنیتی iOS را شناسایی کنند. این شرکت به کسی که بتواند از راه دور به کرنل گوشی دسترسی پیدا کند، یک میلیون دلار جایزه می‌دهد. آیفون‌های مذکور فقط برای کاربرانی که سابقه زیادی در پیدا کردن حفره‌های امنیتی خطرناک در هر پلتفرمی دارند، در دسترس خواهد بود. این دیوایس‌ها همراه با روت شِل، ssh و خصوصیات دیباگینگ پیشرفته به دست کاربران می‌رسند، تا پیدا کردن باگ‌ها آسان‌تر شود. با این وجود باز هم سطح دسترسی محدود است و کاربران تا مرز مشخص‌شده‌ای به فایل‌های سیستم عامل دسترسی دارند.

### اطلاعات شخصی در دنیای اینترنت چیست و چگونه به سرقت می‌رود؟

# خطر در کمین است

**مهرنوش گرکانی | همیشه نگران این هســـتیم که کیف‌مان را در مترو یا خیابان بدزدند و تمام مدارک و اطلاعات شخصی‌مان را از دست بدهیم. این اتفاق سال‌هاست که ما را نگران می‌کند اما چند سالی است که تنها در خیابان و مترو نیست که می‌توانند کیف‌مان را بدزدند و اطلاعات‌مان را با خودشان ببرند و حتی حساب‌مان را خالی کنند، تا به حال هر کدام از ما در دنیای اینترنت و در هر سایتی اطلاعات شخصی‌مان را وارد کردیم، از دنیای اینترنت خریدهای آنلاین انجام دادیم و اطلاعات حساب‌های مالی‌مان را در آن وارد کردیم، حالا این نگرانی برای ما وجود دارد که ممکن است کسی همزمان با ما در همان سایت باشد و اطلاعاتی که وارد می‌کنیم را بدزدد و بعد کلاهبرداری کند یا از حساب‌مان پولی بدزدد. البته که تنها همزمان بودن نیست و یک سارق اطلاعات می‌تواند هر زمانی که بخواهد اطلاعات ما را بدزدد، اگر ما راهکارهای امنیتی را درست استفاده نکنیم.**

**سرقت هویت زمانی اتفاق می‌افتد که شخصی دسترسی غیرمجاز به اطلاعات شخصی شما داشته باشد، این اطلاعات شخصی می‌تواند شامل همه اطلاعات شما باشد که آنها را در دنیای نت وارد می‌کنید؛ نام‌تان، اطلاعات حساب بانکی، عکس مدارک شناسایی یا هر چیز دیگری که برای ارتکاب کلاهبرداری یا جرایم دیگر به آنها نیاز باشد.**

**به این فکر کنید که کسی هویت شما را دزدیده و با آن می‌تواند کلاهبرداری‌های متعدد انجام دهد و هر جرمی که مرتکب شود به نام شما نوشته می‌شود و در هر صورت این شما یید که باید پاسخگو باشید. واضح است که سرقت هویت می‌تواند هزینه‌های زیادی برای شما به همراه داشته باشد و همچنین باعث سردرگمی در زندگی شما شود.**

**یکی از اتهاماتی که آمریکا به شـــرکت هوآوی وارد کرده است همین دزدیدن اطلاعات شخصی کاربران اســـت، البته که هنوز این اتهامات اثبات نشده است اما آمریکا برای تحریم کردن شـــرکت هوآوی این دلیل را هم در نظر گرفته است. بارها در خبرها خوانده‌ایم که اطلاعات یکی از شرکت‌ها لو رفته اســـت یا ایمیل‌های کاربران جی‌میل را هک کرده‌اند. به هر حال ســـرقت اطلاعات شخصی و هویت بین هکرها مرسوم شده و حتی برای نشان‌دادن توانایی‌های خود به بزرگ‌ترین شرکت‌های دنیا هم که شـــده، کاربران را هک می‌کنند. البته این افراد تنها هکرهایی هستند که برای سرگرمی و نشان‌دادن ضعف عملکرد شرکت‌ها دســـت به هک کردن و دریافت اطلاعات شخصی کاربران می‌زنند؛ اما در کنار اینها افرادی هم هســـتند که با هک کردن و به دست آوردن اطلاعات شخصی کاربران کلاهبرداری‌های بزرگ انجام می‌دهند و منبع درآمدی بزرگ برای‌شان است.**

### سرقت هویت آنلاین چیست؟

سرقت هویت هر سال میلیون‌ها نفر را در سراسر دنیا تحت تأثیر قرار می‌دهد و هنگامی رخ می‌دهد که یک کلاهبردار با دستیابی به اطلاعات شخصی شما (PII) به منظور ارتکاب کلاهبرداری، هویت شما را به سرقت می‌برد. سرقت شناسه می‌تواند به روش‌های مختلفی اتفاق بیفتد؛ مثلا سرقت شناســـه آنلاین زمانی اتفاق می‌افتد که شخصی با اســـتفاده از کلاهبرداری مانند وارد کردن نرم‌افزارهای مخرب روی رایانه یا موبایل شما، PII دیجیتال شما را بدزدد و این خلاف روش قدیمی و ساده مثل سرقت کیف پول است. PII دیجیتال شما می‌تواند شـــامل گواهینامه رانندگی و شماره حساب بانکی شـــما و همچنین هرگونه اطلاعات شـــخصی حساس باشـــد که برای تشـــخیص هویت شما مورد استفاده قرار می‌گیرد و به کلاهبرداران اجازه می‌دهد تا خودرا مانند شما معرفی کنند.

بارهـــا در اخبـــار کشـــور خودمـــان شـــنیده‌ایم کـــه کلاهبـــرداران مجـــازی را دســـتگیر کرده‌اند؛ کلاهبرداری‌هایی که برای ما کوچک بوده و برای آنها بزرگ. به این فکر کنید که شـــخصی تنها ۵۰۰ تومان از حساب شما برداشت کند، شاید شما حتی پیگیری نکنید که چرا این رقم از حساب ما کسر شده است اما اگر از حســـاب یک میلیون نفر و از هر نفر ۵۰۰ تومان کسر شود، کلاهبردار ۵۰۰میلیون تومان به جیب زده و شکایتی هم از او نمی‌شود.

باید بدانید شیوع سرقت اطلاعات و هویت دارد بیشتر و بیشتر می‌شود و زندگی مجازی و واقعی ما را به خطر می‌اندازد. حال شـــاید این سوال برای شما مطرح شود که واقعا چه میزان خطر در کمین شماســـت و چطور می‌توانید از این خطرات پیشگیری و جلوگیری کنید؟

### سرقت هویت چطور اتفاق می‌افتد؟

کلاهبرداران از فناوری‌های پیشـــرفته و روش‌های مختلفی برای سرقت PII دیجیتال استفاده می‌کنند. دانستن این‌که این تکنیک‌ها چیست، ممکن است به شما در محافظت از خود کمک کند.

پیتر کین، رئیس دانشگاه و اســـتاد دانشکده حقوق دانشگاه گلدن گیت، می‌گوید: «تخیل و خلاقیت انسان بی‌پایان اســـت؛ به عبارت دیگر، در حالی که لیست زیر نشـــانگر متداول‌ترین روش‌هایی اســـت که مجرمان برای دستیابی به اطلاعات شـــخصی قربانیان استفاده می‌کنند، اما طبق آمار FTC (شـــبکه مصرف‌کننده اینترنت در آمریکا) مطمئنا جامع نیست.»

**سطل زباله (Trash):** دامپســـترها ممکن است بتوانند اطلاعات شخصی شـــما را مثل قبوض قدیمی، شماره‌حســـاب‌های قدیمی، نام آدرس، نام بانک و... به دست آورند. سپس می‌توانند با این اطلاعاتی که از شما به دست آوردند، حساب جدید باز کنند یا حتی خود را به جای شما جا بزنند و سوءاستفاده مالی کنند.

**ایمیل (Mail):** با استفاده از ســـرقت نامه و ایمیل الکترونیکی، مجرمان می‌توانند اطلاعات حساب بانکی شما را بدزدند و به حساب شما دسترسی پیدا کنند.

**فیشینگ (Phishing):** فیشـــینگ زمانی اتفاق می‌افتد که مجرمان ســـایبری برای شما ایمیل‌هایی را ارســـال می‌کنند که گفته می‌شود از یک موسسه مالی یا ســـازمان قابل اعتماد دیگری است و سعی می‌کنند شـــما را طوری ترغیب کنند که روی لینک یا پیوستی که در ایمیل وجود دارد، کلیک کنید و آنها PII شما را سرقت کنند. همه ما ممکن است نامه‌های الکترونیکی از موسسات مالی دریافت کنیم، به طور خاص مجرمان سایبری سعی در فریب مصرف‌کنندگان دارند به‌طوری که شـــما شـــک نکنید و اطلاعاتی که آنها می‌خواهند را غیرمســـتقیم به آنها بدهید. ممکن اســـت شما این نامه‌های فیشینگ را باز کنید یا به آنها پاسخ دهید، این را بدانید که مجرمان فقط در انتظار همین هستند.

**فارمینگ (Pharming):** فارمینگ زمانی اتفاق می‌افتد که ویروسی روی سیســـتم شما وجود داشته باشـــد؛ آنها از همین ویروس استفاده می‌کنند و زمانی که شما وارد مرورگرتان می‌شوید و URL دلخواه‌تان را تایپ می‌کنید، آنها می‌توانند هر چیزی را که شما به مرورگرتان وارد کردید، بدزدنـــد. به این فکر کنید که URL بانک‌تان را وارد می‌کنید و می‌خواهید مبلغی را جابه‌جا کنید، آنها هر چه بنویسید را کپی می‌کنند.

**بدافـــزار (Malicious software):** ممکـــن است شـــما در هنگام دانلود چیزی یک بدافزار را هم به کامپیوتر خود وارد کرده باشـــید، این بدافزار می‌تواند به سیستم شـــما حمله کند و احتمالا PII شما را فاش کند. خرید نرم‌افزار امنیتی را برای سیستم خود در نظر بگیرید و این نرم‌افزار و سیســـتم‌عامل کامپیوترتان را همیشه به روز نگه دارید.

**وب‌ســـایت‌های ناامن:** از خرید آنلاین و ســـایر فعالیت‌ها در وب‌سایت‌هایی که امن نیستند، خودداری کنید و در مـــورد برنامه‌هایی که برای خرید اســـتفاده می‌کنید، احتیاط کنید. فقط از وب‌سایت‌های رسمی و ایمن با پیشوند «https:» استفاده کنید، نه «http:».

**پسورد (password):** پســـوردهای ضعیفـــی که برای حســـاب‌های اجتماعـــی یا مالی خود اســـتفاده می‌کنید، می‌توانند شـــما را آســـیب‌پذیر کنند. سعی کنیـــد از رمزهای عبور منحصربه‌فرد اســـتفاده کنید، چیزی که فقط خودتـــان می‌دانید و حتی نزدیک‌ترین دوستان‌تان هم از آنها اطلاعی ندارند، رمزها را طولانی و قوی بسازید و برای هر حســـاب خود یک رمز در نظر بگیرید. اگر از رمزهای تکراری اســـتفاده کنید، کسی که به یکی از حســـاب‌های شما دسترســـی پیدا کند درواقع همه آنهـــا را خواهد داشـــت. همچنین تأیید هویت چنـــد عاملی را فعال کنید، وقتـــی این گزینه را فعال کنید، لازم اســـت قبل از دسترســـی به حساب کاربری خود، هر دو رمز ورود به یک سیســـتم را بدانید و همچنین به تلفن هوشمندتان یا هر دستگاه دیگری که خودتان انتخاب می‌کنید یک کد ارســـال می‌شود و تنها بـــا واردکردن آن کـــد می‌توانید وارد حســـاب شوید.

**دســـتگاه‌های قدیمـــی (Discarded computers and mobile devices):** بسیاری از مـــا موبایل‌هـــا و کامپیوترهای قدیمی‌مـــان را کنار می‌گذاریم یا ممکن اســـت آنها را برای استفاده به یکی از دوســـتان‌مان بدهیم، همیشـــه این را بدانید که باید دستگاه قدیمی را از هرگونه اطلاعات شخصی‌تان پاک کنید و این پاک کردن نباید قابل برگشت باشد.

## سوءاستفاده از اطلاعات و داده‌ها چیست؟

سوءاستفاده از داده‌ها، استفاده نادرست از داده‌هایی اســـت که هنگام ثبـــت در جایی از مـــا جمع‌آوری می‌شـــود. به طور معمول با توجه به قوانین و سیاست امنیت سایبری شرکت‌ها، سوءاســـتفاده از اطلاعات قابل کنترل است، اما حتی با توجه به تمام این قوانین هرروز سوءاستفاده از داده‌ها و اطلاعات شخصی مردم رو به رشد است. هر کسی که ممکن است به نحوی به اطلاعات یک شرکت دسترسی داشته باشد، می‌تواند از آنها سوءاســـتفاده کند. مثلا کارمندان شـــرکت، پیمانکاران یا حتی متجاوزانی که راه دسترسی را پیدا کرده‌اند.

سوءاســـتفاده‌ها می‌تواند برای ما پیامدهای جدی داشته باشد و این تنها هزینه مالی نیست که می‌تواند ما را متضرر کند بلکه ممکن است حتی جان ما را نیز به خطر بیندازد یا اطلاعات شخصی و خانوادگی‌مان را برای مردم فاش کند و موجب شود زندگی ما به خطر بیفتد. اما این را ما به سادگی نمی‌توانیم متوجه شویم و درواقع برای آن‌که بفهمیم در معرض خطر هستیم، تحقیق و پیشگیری تقریبا برای ما غیرممکن است و نیاز به فرآیندها و فناوری‌هایی دارد که ما به آنها دسترسی نداریـــم. همان‌طور که این مثال‌ها نشـــان می‌دهند، سوءاســـتفاده از داده‌های مبتنی بر تهدید توســـط کارمندان و پیمانکاران در یک سازمان گسترده است و می‌تواند در هر نقطه اتفاق بیفتد.

### نمونه‌های سوءاستفاده از داده‌ها و اطلاعات شخصی Uber (God View)

یک مورد مشـــهور از سوءاســـتفاده داده‌ها در سال ۲۰۱۴ اتفاق افتاد، یک کارمند در شرکت Uber که در آن زمان یکی از ســـریع‌ترین شرکت‌های درحال رشد در جهان بود، خط‌مشی شـــرکت را با استفاده از ابزار «God View» خود برای ردیابی روزنامه‌نگارانی که قرار بود برای مصاحبه و پوشـــش خبری مراسمی که بـــرای Uber بود سوءاســـتفاده کـــرد. نرم‌افزار «God View» برای آن بود که مشتریان و راننده‌های Uber در زمان استفاده از خدمات بتوانند یکدیگر را ببینند و راحت یکدیگر را پیدا کنند. اطلاعات مشتریان با توجه به حفظ حریم خصوصی باید ناشناس می‌ماند، اما این کارمند از آن سوءاستفاده کرد.

### اداره پلیس مینه‌سوتا

در سال ۲۰۱۶، حسابرسان ایالتی در ایالت مینه سوتا دریافتند که بین سال‌های ۲۰۱۳ تا ۲۰۱۵، ۸۸ افسر پلیس در ادارات پلیس سراســـر ایالت از امکانات خود سوءاستفاده کردند و در پایگاه داده گواهینامه رانندگی ایالت برای جســـت‌وجوی اطلاعات در مورد دختران، خانواده، دوســـتان یـــا دیگران سوءاســـتفاده کردند. محققان گفتند که این یک امر غیرمعمول نبوده است و بیش از نیمی از افسران پلیس این ایالت در پایگاه داده، جست‌وجوهای مشکوک انجام داده‌اند.

### اداره پلیس شیکاگو

در ســـال ۲۰۱۶ گزارشی توســـط آسوشیتدپرس مشـــخص کرد که افســـران پلیس در سراسر آمریکا از اطلاعات محرمانه اجرای قانـــون به‌طور غیرقانونی سوءاستفاده می‌کنند و غالبا به جست‌وجوی اطلاعات شخصی افراد نزدیک خود می‌پردازند. در بسیاری موارد، سوءاستفاده از داده‌ها منجر به مواردی از قبیل سرقت شخصی، آزار و اذیت و حتی سرقت هویت می‌شود.

### اطلاعات مربوط به مشتری AT&T

شـــرکت مخابراتی AT&T در سال ۲۰۱۵ بیش از ۲۵ میلیون دلار به کمیسیون ارتباطات فدرال پرداخت کرد. در نتیجه تحقیقاتی که انجام داد، کشـــف کرد کارکنان مراکز تماس بین‌المللی اطلاعات شـــخصی ۲۸۰،۰۰۰ مشـــتری را به صـــورت غیرقانونی فاش می‌کنند و شماره‌های آنها را به اشخاص ثالثی که از آن برای باز کردن قفل تلفن‌های همراه استفاده کرده‌اند، بنابراین دســـتگاه‌ها در شـــبکه‌هایی غیراز AT&T کار می‌کنند.