# حمله به داده‌ها با یک کلیک

## هکرها با روش‌های مختلفی دست به سرقت اطلاعات کاربران و داده‌های مهم سازمان‌ها می‌زنند

**حمله سایبری تلاشی مخرب برای دسترسی به سیستم‌های رایانه‌ای بدون مجوز با هدف سرقت، افشا، تغییر، غیرفعال کردن یا از بین بردن اطلاعات است. دلایل زیادی پشت یک حمله سایبری وجود دارد؛ از جمله انگیزه‌های سیاسی یا مربوط به انتقام. اما هدف اصلی، سود مالی است، چون یک مهاجم اینترنتی می تواند در جریان این حملات پول زیادی به دست آورد.**

### فیشینگ

**فیشینگ نوعی حمله سایبری است که در آن قربانیان فریب داده می‌شوند تا به هدفی مخرب هدایت شوند. این حملات اغلب شامل لینک‌های جعلی هستند و می توانند از طریق کانال‌های مختلفی مانند ایمیل، متن، رسانه‌های اجتماعی و وب‌سایت‌ها ارسال شوند. هدف حمله ممکن است این باشد که قربانی ویروس‌ها یا بدافزارها را روی دستگاه خود دانلود کند.**

### باج‌افزار

باج‌افزار شـامل رمزگذاری داده‌های یک فرد یا سازمان از طریق بدافزار است که دسترسـی به فایل‌ها، سیستم‌ها یا شبکه‌ها را محدود می کند، اما چرا نام این حمله را باج‌افزار گذاشته‌اند؟ چون مهاجم از قربانی درخواست باج می کند تا اطلاعات او را پس بدهد، ولی بحث خطرناک‌تر این است که پرداخت این باج لزوما به این معنی نیست که داده‌ها پس داده شوند. براساس گزارش سازمان‌های امنیتی بین‌المللی، حملات باج‌افزار در ۵سال گذشته ۱۳درصد افزایش یافته اسـت و میانگین هزینه هر حادثه ۱٫۸۵میلیون دلار است. علاوه بر این، طبق گفته ارائه‌دهنده نرم‌افزار امنیتی Datto ۱۳درصد از کسـب‌وکارهای کوچک و متوسـط در سال گذشـته حمله باج‌افزاری را گزارش کرده‌اند و ۲۴درصد از پاسخ‌دهندگان حداقل یک حمله را گزارش کرده‌اند.

### انواع حملات سایبری و تهدیدات آنلاین

حملات سایبری را می توان به روش‌های مختلفی انجام داد. ۳مورد از رایج‌ترین انواعی که امروزه رخ می‌دهد شامل فیشینگ، باج‌افزار و مهندسی اجتماعی است.

### چه‌کسی پشت حملات سایبری است؟

حملات علیه شرکت‌ها می تواند از منابع مختلفی مانند تیم‌های سـازمان یافته هکری یا حتی افراد معمولی با هدف سـر گرمی رخ بدهد. مهاجمان سـایبری به‌طور کلی به‌دنبـال بهره‌بـرداری از ضعف‌ها و آسـیب‌پذیری‌های موجود در سیستم‌ها و شبکه‌ها هستند. آنها می‌توانند برای دسـتیابی به اهـداف مختلف، کاربران آنلاین را هدف قرار بدهند. یک راه آسان برای طبقه‌بندی این حملات، تهدیدهای خارجی در مقابل تهدیدات داخلی است. تهدیدهای خارجی شـامل مجرمان سازمان‌یافته، هکرهای حرفه‌ای و هکرهای آماتور هستند. تهدیدهای داخلی معمولا کارکسانی است که دسترسی مجاز به دارایی‌های یک شرکت دارند و به‌طور عمدی یا تصادفی از آنها سوءاستفاده می کنند.

### مهندسی اجتماعی

**مهندسی اجتماعی اغلب شامل جعل هویت است. این حمله‌ای برای بازیابی اطلاعات حساس یا فریب‌دادن کاربران است. این مدل حمله ممکن است توسط مهاجمی باشد که با شما تلفنی تماس می گیرد و وانمود می کند که یکی از کارشناسان فناوری اطلاعات از اپراتور تلفن همراه شماست که رمز عبور شما را می خواهد.**

### توسعه آگاهی سایبری

با وجود انواع مختلفی از تهدیدات و مهاجمان سایبری، برای افراد و سـازمان‌ها مهم است که اقدامات امنیتی برای محافظت از خود و داده‌هایشان انجام دهند.

یک مفهوم برای ایجاد محافظت بیشـتر روش «دفاع در عمق» اسـت که در آن از چندین لایه امنیتی برای محافظت از دارایی‌ها در برابر مهاجمان استفاده می‌شود. همانطور که ممکن اسـت اقدامات احتیاطی متعددی برای محافظت از اشیای با ارزش فیزیکی انجام دهید، می توانید برای محافظت از خود از ابزارهای امنیتی در دنیای سایبری استفاده کنید.

برخی از این ابزارها عبارتند از: نرم‌افزارهای ضدویروس، رمزگذاری داده‌ها، فایروال‌ها، سیستم‌های تشخیص نفوذ (IDS) و سیستم‌های پیشگیری از نفوذ (IPS)

همچنین می توانید با ایجاد رمزهای عبور قوی با حروف، کاراکترها و اعداد مختلف، اقدامات پیشگیرانه انجام دهید. در کنـار این عملیات، شـما باید به‌طور منظم رمزهای عبور خود را هر ۶۰ تا ۹۰ روز تغییر دهید، از احراز هویت چندمرحله‌ای استفاده کنید و آنتی ویروس معتبر روی سیستم‌های خود نصب کنید. همچنین اگر متوجه شدید که قربانی یک جنایت سایبری شده‌اید، آن را به مراجع قضایی مربوطه گزارش دهید.

## انواع امنیت سایبری چیست؟

در اینجا با برخی از انواع رایج امنیت سـایبری آشنا می‌شویم:

### امنیت ابری

سیسـتم‌های ابری این روزها نقش مهمی در سازمان‌ها دارند، سرویس‌هایی مانند AWS، GOOGLE، Azure و... تقریبا پای خود را در بیشتر سازمان‌ها باز کرده‌اند. سازمان‌هایی که از این سیستم‌ها استفاده گسترده می کنند و از سرویس‌هایی مانند محیط کار دیجیتال و فضای کار دیجیتال استفاده و اطلاعات خود را روی سرورهای ابری ذخیره می کنند، باید به خطرات احتمالی نیز آگاه باشـند و همواره امنیت سایبری را در اولویت قرار داد و رویه‌های ارائه شده از سوی ارائه‌دهندگان این سرویس‌ها را رعایت کنند.

### امنیت زیرساخت

امنیت زیرسـاخت‌های حیاتی یعنی امنیت سیستم‌های فیزیکی و سایبری که برای جامعه بسیار حیاتی هستند و ناتوانی آنها بر سلامت و ایمنی فیزیکی، اقتصـادی یا عمومی ما تأثیر منفی می گذارد.

### امنیت شبکه

امنیت شبکه، حفاظت از زیرساخت شبکه در برابر دسترسی‌های غیرمجاز، سوءاستفاده یا سرقت است. این سیستم‌های امنیتی شامل ایجاد زیرساخت ایمن برای دستگاه‌ها، برنامه‌ها و کاربران برای همکاری با یکدیگر است.

### امنیت نرم‌افزاری

امنیت نرم‌افزاری شامل تعریف و به‌کارگیری مجموعه‌ای از سیستم‌های دفاعی در نرم‌افزارها و سرویس‌های مورد استفاده در سازمان است. پیش‌نیاز آن ابتدا تعریف یک استراتژی دقیق امنیت سایبری و سپس تعریف دسترسی‌ها به بخش‌های مختلف یک سیستم نرم‌افزاری و همچنین نوع معماری، کدهای اصلی و ایجاد یک سیستم اعتبارسنجی دقیق روی داده‌های ورودی است.

### مدیریت هویت و امنیت داده‌ها

مدیریت هویت به مجموعه قواعد و فرایندهایی اشاره دارد که نیاز به احراز هویت برای دسترسی به اطلاعات در داخل سازمان را تعریف و اجرا می کند. بخـش مهمی از امنیت سـایبری و انتقال اطلاعات به‌عهده کاربران سیستم‌های کامپیوتری اسـت و تعیین و احراز هویت آنها برای کار و دسترسـی به اطلاعات بخش‌های مختلف سازمان اهمیت بالایی دارد.

### امنیت دستگاه‌های قابل حمل

چالش مهم دیگری که امنیت سـایبری با آن روبه‌روست حفاظت از اطلاعات ذخیره شده شخصی و سازمانی روی دسـتگاه‌های قابل حمل مانند تلفن همراه، لپ‌تاپ، تبلت در مقابل دسترسی‌های بدون مجوز، بدافزارها و سرقت اسـت. مقابله با این چالش نیازمند مجموعه آموزش‌هایی است که استفاده‌کنندگان از این دستگاه‌ها، به‌خصوص آن دسته از کارکنانی که از دستگاه‌های سازمانی حاوی اطلاعات حیاتی استفاده می کنند باید با آن آشنا باشند.