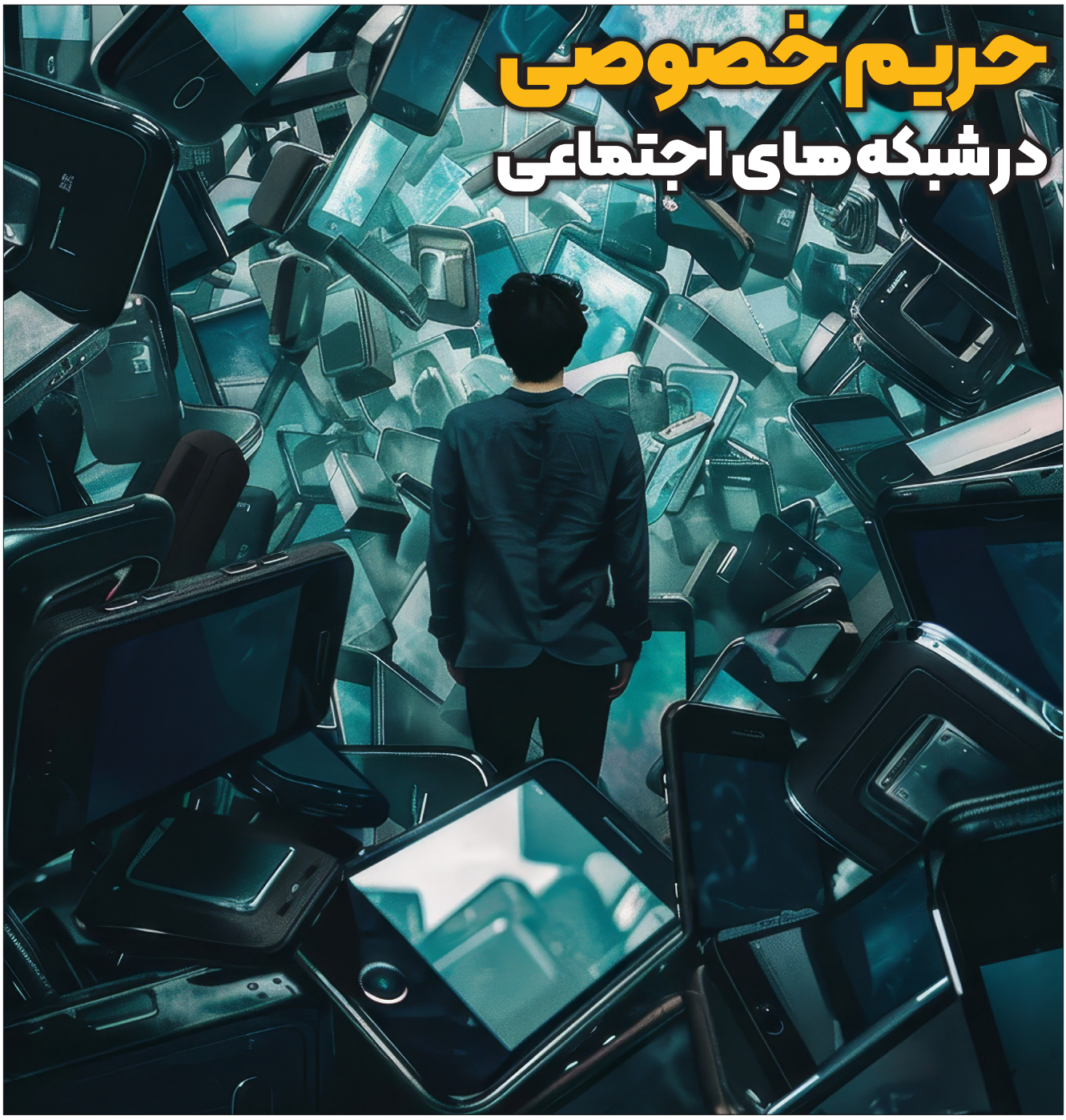
شرکت آب منطقه‌ای گلستان

نشریه داخلی شرکت آب منطقه‌ای گلستان/ شماره سوم/ خرداد ماه ۱۴۰۴



حریم خصوصی در شبکه‌های اجتماعی

چطور اطلاعات شخصی خود را از چشمان کنجکاو حفظ کنیم؟ ‹ 07

وقتی لوکیشن و اطلاعات شما بدون اطلاع‌تان منتشر می‌شود ‹ 13

PRIVACY

BRUCE SCHNEIER

داده ها مشکل آلودگی عصر اطلاعات
است و حفاظت از حریم خصوصی
چالش زیست محیطی است.

نشریه داخلی شرکت آب منطقه‌ای گلستان

شماره سوم ـــ خرداد ماه ۱۴۰۴

فهرست

سرمقاله
دنیایی که همه‌چیز را می‌بیند؛ چرا حریم خصوصی اهمیت دارد؟ 06

مقاله اصلی
چطور اطلاعات شخصی خود را از چشمان کنجکاو حفظ کنیم؟ 07

راهنمای عملی
افزایش امنیت در شبکه‌های اجتماعی 10

سناریو
وقتی لوکیشن و اطلاعات شما بدون اطلاع‌تان منتشر می‌شود 13

موضوع ویژه یک
دفتر کار در خانه؛ راهی باز برای مهاجمان؟ 16

موضوع ویژه دو
خرید آنلاین یا هدیه‌ای برای هکرها؟ 19

بدافزارهای شبکه‌های اجتماعی
بدافزارهای پنهان در شبکه‌های اجتماعی 22

آزمون
امنیت یا سهل‌انگاری؟ 25

دکتر امیرحسین رحیمیان

دنیایی که همه چیز را می‌بیند چرا حریم خصوصی اهمیت دارد؟

در جهانی زندگی می‌کنیم که هر حرکت، هر کلیک و هر پست ما می‌تواند ردپایی دیجیتال از خود بر جای بگذارد. شبکه‌های اجتماعی، ابزارهای پیام‌رسان، فروشگاه‌های آنلاین و حتی اپلیکیشن‌های آب‌وهوا، اطلاعاتی درباره ما جمع‌آوری می‌کنند؛ گاهی با رضایت‌مان و اغلب، بی‌آنکه متوجه باشیم.

در گذشته، مفهوم حریم خصوصی به چهارچوب خانه محدود می‌شد؛ اما امروز این مرزها درهم‌شکسته‌اند. گوشی هوشمند ما، تبدیل به همراه همیشگی‌ای شده که هر لحظه در حال ارسال داده است. موقعیت مکانی، علایق، مخاطبین، عکس‌ها، پیام‌ها و حتی نحوه تایپ کردن ما، همه می‌توانند توسط سامانه‌ها، شرکت‌ها و در بدترین حالت، مهاجمان سایبری رصد شوند.

اما چرا باید نگران باشیم؟ چون اطلاعات شخصی امروز، سرمایه‌ای گران‌بهاست. هکرها می‌توانند از ساده‌ترین داده‌ها برای اجرای حملات مهندسی اجتماعی، فیشینگ یا جعل هویت استفاده کنند. شرکت‌ها با تحلیل رفتار آنلاین‌مان، تبلیغات هدفمند و گاه مزاحم ارائه می‌دهند. حتی دولت‌ها و نهادهای مختلف نیز ممکن است در این چرخه نظارتی حضور داشته باشند.

در چنین شرایطی، مسئولیت آگاه‌سازی و ارتقای فرهنگ امنیت دیجیتال بیش از پیش اهمیت پیدا می‌کند. نه تنها کاربران عادی، بلکه کارکنان سازمان‌ها نیز باید نسبت به ارزش اطلاعات‌شان و نحوه محافظت از آن‌ها آگاه باشند. حریم خصوصی دیگر یک انتخاب نیست؛ یک حق است، که حفظ آن نیازمند دانش، دقت و تصمیم‌های هوشمندانه است.

این شماره از ماهنامه، تلاشی‌ست برای بررسی همین موضوعات؛ از تنظیمات امنیتی در شبکه‌های اجتماعی گرفته تا خطرات پنهان در خریدهای اینترنتی و کار از راه دور.

بیایید یک‌بار دیگر، آگاهانه به ردپای دیجیتال‌مان نگاه کنیم.

MAIN ARTICLE

مقاله اصلی

چطور اطلاعات شخصی خود را از چشمان کنجکاو حفظ کنیم؟

در عصر ارتباطات، مرز میان اطلاعات عمومی و خصوصی به شدت تضعیف شده و در بسیاری از مواقع، به دلیل ناآگاهی یا بی‌توجهی، کاربران حجم گسترده‌ای از اطلاعات شخصی خود را در اختیار دیگران قرار می‌دهند، بدون آنکه متوجه پیامدهای احتمالی آن باشند. این مقاله به بررسی ابعاد مختلف این پدیده می‌پردازد و تلاش دارد نشان دهد که چگونه می‌توان با رعایت اصولی ساده، اما مؤثر، از افشای ناخواسته اطلاعات شخصی جلوگیری کرد.

01

حریم خصوصی در عصر دیجیتال واقعیتی در حال انقراض

پیشـرفت فناوری‌هـای دیجیتـال و گسـترش روزافـزون شـبکه‌های اجتماعی باعث شده که افراد بیش از هر زمان دیگری به اشـتراک‌گذاری اطلاعات روی بیاورند. عکس‌های خانوادگی، موقعیت مکانی، علایق شخصی، نظرات سیاسی، وضعیت سلامتی و حتـی اطلاعات مالی، همگی در معرض دید افراد، شـرکت‌ها، موتورهای جسـت‌وجو و گاهی مهاجمان قرار دارند. بسـیاری از این داده‌ها نه از روی عمد، بلکه از طریق رفتارهای معمول کاربران منتشر می‌شوند؛ برای مثال:

- آپلود خودکار عکس‌ها در فضای ابری بدون تنظیمات مناسب
- فعال بودن موقعیت مکانی (GPS) در زمان عکس‌برداری یا پست‌گذاری
- لاگین به حساب‌های کاربری با استفاده از شبکه‌های عمومی
- استفاده از اپلیکیشن‌هایی که مجوزهای بیش از حد درخواست می‌کنند

این موارد، تنها نمونه‌هایی از هزاران رفتار رایج هسـتند که می‌توانند دروازه‌ای به سوی افشای ناخواسته اطلاعات شخصی باز کنند.

02

اطلاعاتی که ناخواسته منتشر می‌شوند

اطلاعاتـی که کاربـران بدون نیت افشـا، در معرض دید قرار می‌دهند، معمولاً شامل موارد زیر است:

- **الف) داده‌های متا (Metadata)**

هر عکس دیجیتال معمولاً حاوی اطلاعاتی درباره زمان، مکان، دسـتگاه و حتی تنظیمات دوربین است. بسیاری از کاربران هنگام بارگـذاری عکس‌ها در شـبکه‌های اجتماعی یا ارسـال از طریق پیام‌رسان‌ها، به این داده‌های پنهان توجهی ندارند. در نتیجه، فردی با کمترین مهارت فنی می‌تواند محل عکس‌برداری، سـاعت دقیق و حتی الگوی زمانی رفت‌وآمد صاحب تصویر را استخراج کند.

- **ب) موقعیت مکانی (Geolocation)**

اپلیکیشـن‌های بسـیاری به طـور پیش‌فرض دسترسـی به موقعیـت مکانـی را فعال نگـه می‌دارند. وقتـی کاربری بدون بررسـی مجوزها، به چنین برنامه‌هایی اجـازه فعالیت می‌دهد، داده‌های مکانی او به صورت پیوسته جمع‌آوری می‌شود. برخی

پلتفرم‌ها حتی اطلاعات لحظه‌ای کاربر را با مخاطبان یا حتی عموم به اشتراک می‌گذارند.

ج) اطلاعات خانوادگی و ارتباطی

با انتشار عکس‌های خانوادگی، تبریک‌های مناسبتی، یا شرکت در چالش‌های به ظاهر بی‌ضرر (مانند «اولین شماره تلفن همراهت چی بوده؟»)، کاربران ناخواسته بخشی از اطلاعات هویتی خود و نزدیکان‌شان را علنی می‌کنند. این اطلاعات می‌توانند در حملات مهندسی اجتماعی، بازیابی رمز عبور و جعل هویت نقش مهمی داشته باشند.

د) علایق، دیدگاه‌ها و باورها

نظراتی که در فضای مجازی منتشر می‌کنیم، فالو کردن صفحات خاص، یا حتی لایک کردن برخی پست‌ها، همه می‌توانند برای ساختن یک نمایه روان‌شناختی از ما مورد استفاده قرار گیرند. این نمایه‌ها برای اهداف تبلیغاتی، هدایت سیاسی یا حتی فریب و اخاذی بسیار ارزشمند هستند.

03
مسیرهایی که مهاجمان از آن وارد می‌شوند

ناشران بدخواه اطلاعات شخصی، اغلب نیازی به هک کردن ندارند؛ آنچه می‌خواهند، معمولاً پیش روی‌شان است. برخی از رایج‌ترین مسیرهای سواستفاده عبارتند از:

مهندسی اجتماعی (Social Engineering)

ترکیبی از اطلاعات پراکنده مانند نام فرزند، محل کار، تاریخ تولد و شماره تلفن می‌تواند زمینه‌ساز تماس‌های جعلی، ایمیل‌های فیشینگ یا سوءاستفاده در قالب درخواست‌های دوستانه شود.

بدافزارهای جاسوسی (Spyware)

اپلیکیشن‌های رایگان یا جعلی با پوشش خدماتی ساده، با دسترسی به دوربین، میکروفون، لیست مخاطبین و فایل‌های شخصی، داده‌های گسترده‌ای را جمع‌آوری و ارسال می‌کنند.

شبکه‌های اجتماعی و درز اطلاعات

افزونه‌ها، آزمون‌های سرگرم‌کننده و اپلیکیشن‌های جانبی در پلتفرم‌هایی مثل فیسبوک یا اینستاگرام، ممکن است با هدف جمع‌آوری داده‌های رفتاری و اطلاعات تماس طراحی شده باشند.

04
مسئولیت ما چیست؟ چگونه مراقب باشیم؟

در دنیای دیجیتال، تنها دانستن خطر کافی نیست؛ بلکه باید رویکردی فعال و مسئولانه اتخاذ کنیم. برای جلوگیری از افشای ناخواسته اطلاعات شخصی، رعایت نکات زیر ضروری است:

بررسی تنظیمات حریم خصوصی

شبکه‌های اجتماعی گزینه‌هایی برای محدودسازی دسترسی به محتوا ارائه می‌دهند. بررسی دوره‌ای این تنظیمات و انتخاب گزینه‌های محافظت‌شده می‌تواند میزان دسترسی دیگران به اطلاعات‌مان را کنترل کند.

عدم انتشار اطلاعات حساس

اطلاعاتی مانند آدرس منزل، شماره کارت، کد ملی یا وضعیت فرزندان نباید به هیچ وجه در فضای عمومی منتشر شوند — حتی در استوری‌های موقتی.

استفاده از احراز هویت دو مرحله‌ای

فعال‌سازی 2FA در سرویس‌های مهم مانند ایمیل، بانکداری و شبکه‌های اجتماعی، سطح امنیت حساب‌های کاربری را به‌طور چشم‌گیری افزایش می‌دهد.

نصب آنتی‌ویروس و بررسی مجوز اپ‌ها

پیش از نصب هر برنامه‌ای، لازم است میزان دسترسی‌های درخواستی آن بررسی و فقط در صورت ضرورت تأیید شود. همچنین به‌روزرسانی منظم سیستم‌عامل و اپ‌ها اهمیت زیادی دارد.

حذف ردپاهای دیجیتال

موتورهای جست‌وجو یا ابزارهایی مانند «Have I Been Pwned» می‌توانند در شناسایی حساب‌های نشت‌کرده یا اطلاعات عمومی‌شده مفید باشند. حذف یا محدودسازی این داده‌ها می‌تواند دامنه افشای اطلاعات را کاهش دهد.

05
نقش سازمان‌ها و شرکت‌ها

اگرچه بخش عمده‌ای از امنیت دیجیتال به رفتار کاربران بستگی دارد، اما سازمان‌ها نیز مسئولیت سنگینی در این زمینه دارند. آموزش مداوم پرسنل، تدوین سیاست‌های امنیت اطلاعات، نظارت بر مجوزهای نصب نرم‌افزار در دستگاه‌های سازمانی، و استفاده از ابزارهای ضد نشت اطلاعات (DLP) از جمله اقداماتی هستند که می‌توانند نقش مهمی در حفظ حریم خصوصی ایفا کنند.

همچنین سازمان‌ها باید با آگاهی از قوانین مربوط به حفاظت از داده‌های شخصی، همچون GDPR یا مصوبه‌های بومی، چارچوب مشخصی برای جمع‌آوری، نگهداری و حذف اطلاعات کاربران داشته باشند.

06
نتیجه‌گیری: امنیت، انتخابی یا الزام؟

در جهانی که الگوریتم‌ها، داده‌ها و رصد دیجیتال به بخشی اجتناب‌ناپذیر از زیست انسان تبدیل شده‌اند، حفظ حریم خصوصی نه یک انتخاب، بلکه یک ضرورت است. هر کلیک، هر پست، و هر اشتراک‌گذاری، پیامی است که می‌تواند یا در خدمت ما باشد، یا علیه‌مان به کار رود. آگاهی، اولین گام در مسیر حفاظت از اطلاعات است. اما این آگاهی باید با عمل همراه شود؛ عملی که از تصمیم‌های روزمره در فضای مجازی آغاز می‌شود. دکمه‌ی «ارسال» را که فشار می‌دهیم، یک سؤال از خود بپرسیم: آیا مایلم این اطلاعات را در اختیار کسی قرار دهم که نمی‌شناسم؟ اگر نه، شاید زمان آن رسیده که دوباره تنظیمات حریم خصوصی‌مان را بازبینی کنیم.

A PRACTICAL GUIDE

••• راهنمای عملی

افزایش امنیت در شبکه‌های اجتماعی

با رشد سریع شبکه‌های اجتماعی و نقش پررنگ آن‌ها در زندگی فردی، کاری و اجتماعی افراد، حفاظت از اطلاعات شخصی در این فضا به یکی از دغدغه‌های اصلی کاربران تبدیل شده است. امنیت در شبکه‌های اجتماعی دیگر تنها یک توصیه یا انتخاب اختیاری نیست، بلکه یک الزام جدی برای کاهش ریسک‌های سایبری، حفظ حریم خصوصی و جلوگیری از سواستفاده‌های احتمالی است.

کاربران، اغلب بدون بررسی دقیق، اطلاعات زیادی را در اختیار پلتفرم‌ها، مخاطبان و گاهی حتی مهاجمان قرار می‌دهند. در این مقاله، مجموعه‌ای از اقدامات ضروری و قابل اجرا برای افزایش امنیت در شبکه‌های اجتماعی مطرح می‌گردد تا کاربران بتوانند با اطمینان بیشتری در این فضا حضور یابند.

بررسی و تنظیم دقیق تنظیمات حریم خصوصی (Privacy Settings)

اولین گام برای محافظت از حساب کاربری در هر شبکه اجتماعی، بررسی دقیق تنظیمات حریم خصوصی است. بسیاری از پلتفرم‌ها به‌طور پیش‌فرض اطلاعات کاربران را در حالت عمومی (**Public**) قرار می‌دهند. این بدان معناست که پست‌ها، لیست دوستان، لایک‌ها و اطلاعات پروفایل برای همه افراد قابل مشاهده است.

توصیه‌ها:

- در اینستاگرام، حساب کاربری را به حالت **Private** تغییر دهید تا تنها فالوورهای تأییدشده بتوانند محتوای شما را ببینند.
- در تلگرام، امکان مشاهده شماره تلفن، عکس پروفایل و زمان آخرین بازدید را محدود کنید.
- در لینکدین، مشخص کنید چه کسانی می‌توانند ارتباط برقرار کنند یا رزومه شما را مشاهده نمایند.
- در فیسبوک و **X** (توییتر سابق)، محدودسازی دسترسی به استوری‌ها، پست‌ها و فهرست دوستان اهمیت زیادی دارد.

تنظیمات حریم خصوصی باید به‌صورت دوره‌ای بازبینی و به‌روزرسانی شوند، چرا که برخی پلتفرم‌ها به‌مرور تغییراتی در ساختار خود ایجاد می‌کنند که ممکن است بر سطوح دسترسی تأثیر بگذارد.

استفاده از رمز عبور قوی و منحصربه‌فرد

بسیاری از نفوذها و حملات سایبری، به دلیل استفاده از رمزهای عبور ساده یا تکراری رخ می‌دهند. استفاده از گذرواژه‌ای که شامل حروف بزرگ و کوچک، اعداد و نمادها باشد، به‌مراتب امن‌تر از رمزهایی مانند ۱۲۳۴۵۶ یا **password** خواهد بود.

اصول انتخاب رمز عبور امن:

- حداقل ۱۲ کاراکتر داشته باشد.
- ترکیبی از حروف بزرگ، کوچک، عدد و نشانه باشد.
- برای هر حساب کاربری، رمز عبور مجزا تعریف شود.
- از نام فرزند، تاریخ تولد یا شماره تلفن خودداری شود.
- در صورت امکان، از مدیر رمز عبور (**Password Manager**) استفاده گردد.

فعالسازی احراز هویت دو مرحله‌ای (Two-Factor Authentication – 2FA)

احراز هویت دومرحله‌ای، یکی از مؤثرترین روش‌ها برای جلوگیری از دسترسی غیرمجاز به حساب‌های کاربری است. در این روش، حتی در صورتی که رمز عبور افشا شود، مهاجم نمی‌تواند بدون کد ثانویه وارد حساب شود.

روش‌های رایج **2FA**:

- کد پیامکی (**SMS Code**): ارسال کد یکبار مصرف به تلفن همراه
- اپلیکیشن‌های احراز هویت (مانند **Google Authenticator**)
- کلید امنیتی سخت‌افزاری (مانند **YubiKey**)

اکثر پلتفرم‌های معتبر، از جمله اینستاگرام، گوگل، فیسبوک، لینکدین و تلگرام، از این قابلیت پشتیبانی می‌کنند. توصیه می‌شود بلافاصله پس از ساخت حساب، این گزینه فعال گردد.

شناسایی و پرهیز از لینک‌های مشکوک و فیشینگ

یکی از رایج‌ترین روش‌های هک حساب‌های کاربری، ارسال لینک‌های فیشینگ است. این لینک‌ها کاربر را به صفحاتی جعلی هدایت می‌کنند که ظاهری مشابه سایت اصلی دارند و کاربر را به وارد کردن اطلاعات کاربری وادار می‌کنند.

راهکارها:

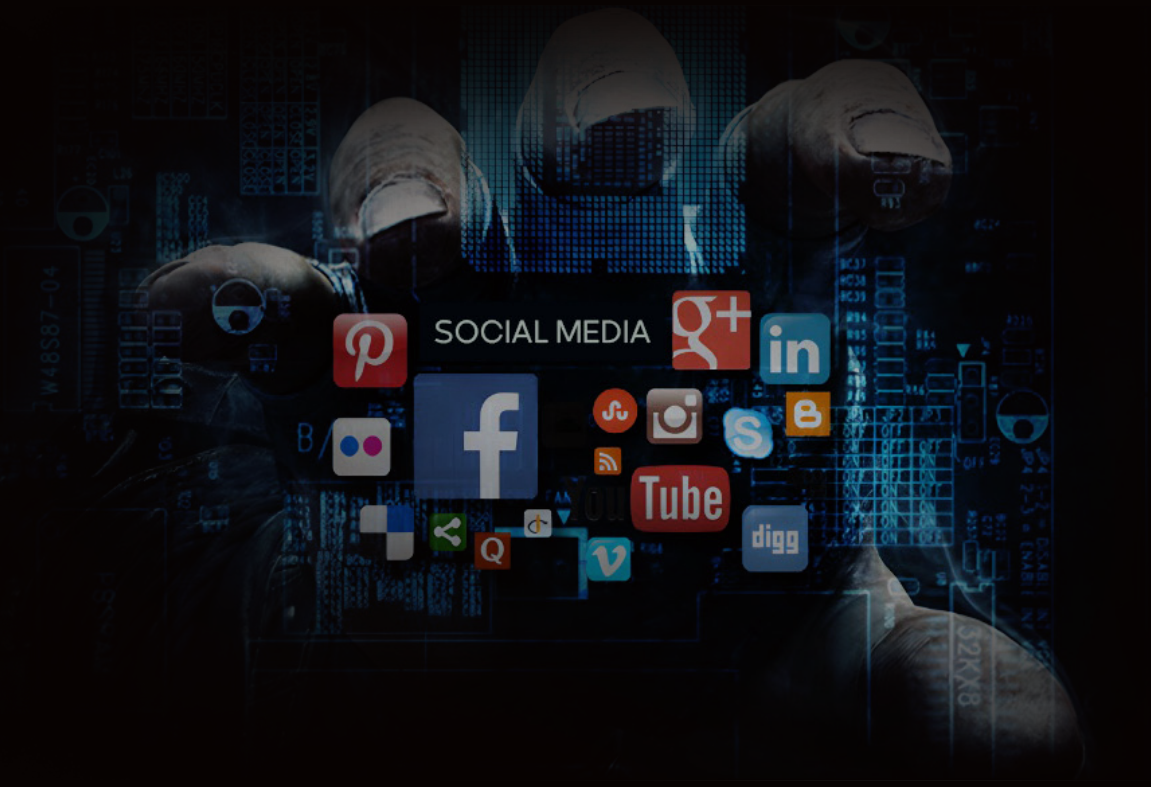
- روی لینک‌هایی که از سوی افراد ناشناس ارسال می‌شود، کلیک نکنید.
- به آدرس **URL** دقت کنید؛ آدرس‌های فیشینگ معمولاً حروفی جابه‌جا دارند یا پسوند دامنه غیرمعمولی دارند.
- از آنتی‌ویروس و افزونه‌های مرورگر ضد فیشینگ استفاده کنید.
- از کلیک بر روی لینک‌های کوتاه‌شده (**short links**) اجتناب کنید، مگر آن‌که مطمئن باشید منبع آن معتبر است.

بررسی اپلیکیشن‌ها و سرویس‌های جانبی متصل به حساب کاربری

بسیاری از کاربران بدون توجه، به اپلیکیشن‌ها یا سرویس‌های شخص ثالث اجازه دسترسی به حساب‌های شبکه‌های اجتماعی خود می‌دهند. این اپ‌ها ممکن است اطلاعات پروفایل، فالوورها، پیام‌ها یا حتی اجازه ارسال پست را دریافت کنند.

توصیه‌ها:

- لیست اپلیکیشن‌های متصل به هر حساب را به‌صورت دوره‌ای بررسی و موارد غیرضروری را حذف کنید.
- از نصب اپ‌هایی با عناوین جذاب اما ناشناخته (مانند "مشاهده بازدیدکنندگان پروفایل") خودداری کنید.
- در فروشگاه‌های اپلیکیشن، به مجوزهای درخواستی و نظر کاربران دقت کنید.
- اپلیکیشن‌های رسمی را مستقیماً از فروشگاه‌های معتبر



مانند Google Play و App Store دریافت نمایید.

مدیریت دقیق حضور دیجیتال (Digital Footprint)

هر فعالیت شما در فضای مجازی، بخشی از ردپای دیجیتال‌تان را شکل می‌دهد. از ثبت‌نام در وب‌سایت‌ها گرفته تا کامنت‌هایی که می‌گذارید، همگی قابل ردیابی هستند. مهاجمان می‌توانند از این اطلاعات برای هدف‌گیری حملات مهندسی اجتماعی استفاده کنند.

نکات کلیدی:

- اگر در سایتی ثبت‌نام کرده‌اید اما دیگر از آن استفاده نمی‌کنید، حساب را حذف کنید.
- نام خود را در گوگل جست‌وجو کنید و نتایج ناخواسته را بررسی و در صورت امکان حذف نمایید.
- از ابزارهایی مانند Firefox Monitor یا HaveIBeenPwned برای بررسی نشت داده‌های خود استفاده کنید.
- در کامنت‌ها، پیام‌ها یا پست‌ها از انتشار اطلاعات حساس خودداری کنید.

به‌روزرسانی مستمر اپلیکیشن‌ها و سیستم‌عامل

بسیاری از به‌روزرسانی‌های نرم‌افزاری، حاوی وصله‌های امنیتی هستند که آسیب‌پذیری‌های کشف‌شده را اصلاح می‌کنند. عدم بروزرسانی به‌موقع اپلیکیشن‌ها یا سیستم‌عامل تلفن همراه، می‌تواند زمینه‌ساز نفوذ از طریق باگ‌های شناخته‌شده شود.

نکته مهم:

- بروزرسانی خودکار را در تنظیمات فعال نگه دارید.
- حتی اپ‌هایی که کمتر استفاده می‌شوند نیز باید به‌روزرسانی شوند.
- اپ‌هایی که دیگر نیاز ندارید را حذف کنید تا سطح حمله کاهش یابد.

نتیجه‌گیری

شبکه‌های اجتماعی، گرچه ابزارهایی قدرتمند برای ارتباط، یادگیری و اشتراک‌گذاری هستند، اما در عین حال می‌توانند بسترهای بالقوه‌ای برای تهدیدات امنیتی نیز باشند. کاربران مسئول، با آگاهی و اقدام به‌موقع، می‌توانند از این فضا به‌صورت ایمن و هوشمندانه بهره‌مند شوند.

رعایت اصولی مانند انتخاب رمز عبور قوی، فعال‌سازی احراز هویت دومرحله‌ای، پرهیز از لینک‌های مشکوک، کنترل مجوزها و بررسی دوره‌ای تنظیمات حریم خصوصی، جزو ابتدایی‌ترین اما مؤثرترین اقداماتی هستند که هر فرد باید در فضای دیجیتال رعایت کند.

در پایان، به یاد داشته باشیم که امنیت، یک محصول نیست؛ بلکه یک فرآیند مداوم است که نیازمند توجه، یادگیری و انطباق با تهدیدات جدید است.

SCENARIO

سناریو ...

وقتی لوکیشن و اطلاعات شما بدون اطلاع‌تان منتشر می‌شود

وقتی گوشی در جیبتان است و احساس امنیت می‌کنید، شاید ندانید که موقعیت مکانی و اطلاعات شخصی‌تان در پس‌زمینه در حال جمع‌آوری و حتی اشتراک‌گذاری است؛ آن هم بدون اجازه یا آگاهی شما. اپلیکیشن‌ها، شبکه‌های اجتماعی و حتی مرورگرها می‌توانند داده‌هایی مانند لوکیشن، مخاطبان و رفتار آنلاین شما را ثبت و منتقل کنند. این داده‌ها ممکن است به شرکت‌ها، تبلیغ‌دهندگان یا حتی افراد ناشناس فروخته یا افشا شوند. در دنیایی که هر حرکت دیجیتال قابل ردیابی است، آگاهی و مدیریت دسترسی‌ها، گامی مهم در مسیر حفظ حریم خصوصی و امنیت دیجیتال شماست.

بخش اول: آغاز ماجرا

نگار، کارشناس روابط عمومی یک شرکت فناوری، فردی فعال در شبکه‌های اجتماعی بود. صفحه اینستاگرامش با بیش از ۱۲ هزار دنبال‌کننده، پر بود از تصاویر جلسات کاری، سفرهای کاری، همایش‌ها و گاه‌گداری عکس‌هایی از زندگی شخصی‌اش. او همیشه سعی می‌کرد حرفه‌ای به‌نظر برسد و از مزایای برندسازی شخصی در فضای دیجیتال بهره ببرد. اما یک نکته را نادیده می‌گرفت: تنظیمات پیش‌فرض گوشی‌اش، همه تصاویر را همراه با موقعیت جغرافیایی ذخیره می‌کرد.

در یکی از روزهای هفته، نگار تصویری از لپ‌تاپش در یک کافه منتشر کرد. کپشن ساده‌ای نوشته بود: «یه روز کاری تو دل آرامش». تصویری عادی به نظر می‌رسید، اما جزئیات آن بسیار بیشتر از چیزی بود که خودش تصور می‌کرد؛ آدرس کافه در فراداده (متادیتا) عکس وجود داشت، موقعیت مکانی به‌صورت خودکار در پست فعال شده بود و پس‌زمینه تصویر نیز نمایی از لوگوی شرکتش را به‌صورت محو نشان می‌داد.

بخش دوم: مهاجم در کمین

مهاجم این ماجرا شخصی به نام «رامین» بود؛ فردی آشنا با مبانی مهندسی اجتماعی و تحلیل داده‌ها. او به‌دنبال نفوذ به یکی از شرکت‌های حوزه زیرساخت اینترنت کشور بود و به‌صورت هدفمند، ردپای دیجیتال کارمندان آن شرکت را دنبال می‌کرد. با جست‌وجویی ساده، به صفحه نگار رسید و متوجه شد او به‌طور مداوم اطلاعاتی از موقعیت‌های حضورش، جلسات سازمانی و نام پروژه‌ها منتشر می‌کند.

با تحلیل ۲۰ پست اخیر، رامین توانست الگوی حضور فیزیکی او را در محل کار و مسیر رفت‌وآمدش شناسایی کند. همچنین، متوجه شد که نگار معمولاً ساعت ۱۰ تا ۱۲ در جلساتی در طبقه پنجم ساختمان شرکت حضور دارد. رامین تصمیم گرفت حمله‌ای هدفمند را طراحی کند؛ نه از طریق هک مستقیم، بلکه از مسیر شخصی‌سازی‌شده، مبتنی بر اطلاعاتی که نگار ناآگاهانه منتشر کرده بود.

بخش سوم: مهندسی اجتماعی در عمل

سه روز بعد، نگار پیامی در دایرکت اینستاگرامش دریافت کرد:

سلام خانم مهندس، من امیر هستم از یک مجموعه‌ی خصوصی، قبلاً در کافه شما رو دیدم و به‌نظر می‌رسید با یکی از همکاران سابق ما در پروژه‌ی فلان همکاری دارید. ما دنبال همکاری با یک متخصص روابط عمومی برای معرفی سرویس جدیدمون هستیم. می‌تونیم یه تماس داشته باشیم؟

نگار که هم نام پروژه را آشنا می‌دید و هم رفتار حرفه‌ای امیر را مناسب می‌دانست، شماره تماس کاری‌اش را در اختیار او گذاشت. تماس برقرار شد. «امیر» در واقع همان رامین بود که با صدایی آرام، دانش فنی و لحنی مؤدبانه، نگار را متقاعد کرد که برای بررسی اولیه همکاری، یک فایل معرفی از طریق واتساپ ارسال کند.

نگار فایل را باز کرد؛ پاورپوینتی که به‌نظر عادی می‌آمد. اما در واقع، این فایل حاوی کد مخفی‌شده‌ی یک بدافزار بود که پس از اجرا، اطلاعات مرورگر و کش‌شده‌های حافظه را به سروری خارجی منتقل می‌کرد.

بخش چهارم: آسیب آرام و خاموش

مهاجم اکنون به اطلاعات مرورگر، کوکی‌ها و حساب‌های فعال نگار دسترسی داشت. از طریق آن، به حساب کاربری وب‌سایت سازمان و نیز پنل مدیریت ایمیل داخلی شرکت نفوذ کرد. پیام‌هایی را که بین واحدهای داخلی تبادل شده بود، خواند و به‌دنبال کلمات کلیدی خاصی همچون «سرور»، «دیتا سنتر» و «دسترسی راه دور» گشت.

رامین حالا نه فقط به اطلاعات کاربر عادی، بلکه به مسیرهای احتمالی نفوذ به زیرساخت فنی سازمان نیز دست یافته بود؛ بدون اینکه نیاز به ابزارهای پیچیده یا آسیب‌پذیری روز صفر داشته باشد. صرفاً با مهارت در تحلیل اطلاعاتی که داوطلبانه و عمومی منتشر شده بودند.

بخش پنجم: نقطه شکست امنیتی

سه هفته بعد، تیم امنیت شرکت متوجه فعالیت‌های مشکوکی در یکی از سرورهای داخلی شد. بررسی‌ها نشان می‌داد که یک دسترسی غیرمجاز از طریق یکی از اکانت‌های روابط عمومی به منابع اطلاعاتی خاصی دست یافته و اقدام به استخراج داده‌هایی کرده که معمولاً در سطح مدیریتی قابل دسترسی هستند.

در ابتدا، تصور بر این بود که مهاجم با شکستن رمز عبور به سیستم نفوذ کرده؛ اما بررسی دقیق‌تر لاگ‌ها و جلسات احراز هویت نشان داد که هیچ رخداد غیرعادی در سیستم‌های دفاعی ثبت نشده است. تحلیل تیم امنیتی به این نتیجه منجر شد که احتمالاً بدافزار از طریق یک فایل ضمیمه در سیستم کاربر اجرا شده است.

بخش ششم: تحلیل امنیتی

این سناریو، گرچه ساختگی به نظر می‌رسد، اما مبتنی بر نمونه‌های واقعی و پرتکراری‌ست که در دنیای سایبری رخ می‌دهند. اشتراک‌گذاری بی‌احتیاط اطلاعات، مخصوصاً در شبکه‌های اجتماعی، بستر مناسبی برای حملات مهندسی اجتماعی، نفوذ به سازمان و سرقت اطلاعات فراهم می‌کند. در اینجا چند نکته تحلیلی مهم از این سناریو استخراج می‌شود:

۱. اطلاعات موقعیتی

فعال بودن GPS هنگام ثبت یا بارگذاری تصویر، می‌تواند دقیق‌ترین مختصات مکانی را به مهاجم بدهد. عکس‌های منتشرشده در اینستاگرام یا حتی واتساپ، در صورت فعال بودن Geotag، حاوی داده‌هایی هستند که به‌راحتی قابل استخراج‌اند.

۲. اطلاعات متنی غیرمستقیم

در بسیاری موارد، کاربران در کپشن‌ها، هشتگ‌ها یا پاسخ

به کامنت‌ها اطلاعاتی درباره زمان، مکان، پروژه‌ها یا همکاران خود منتشر می‌کنند که در نگاه اول بی‌ضرر به نظر می‌رسند؛ اما در مجموع، برای مهاجم ارزشمندند.

۳. هویت‌سازی جعلی

ایجاد شخصیت جعلی اما قابل باور، یکی از رایج‌ترین روش‌های نفوذ است. مهاجم با استفاده از اطلاعات منتشرشده، شخصیتی طراحی می‌کند که با زمینه ذهنی قربانی هماهنگ باشد. در این سناریو، رامین با نام «امیر» و سابقه‌ای مشابه پروژه‌های نگار، اعتماد اولیه را جلب کرد.

۴. حمله از طریق فایل ضمیمه

ارسال فایل با فرمت‌هایی مثل pptx، docx، pdf و حتی jpg، یکی از رایج‌ترین راهکارهای تزریق بدافزار است. این فایل‌ها می‌توانند حاوی ماکروهای مخرب، کد جاوااسکریپت یا لینک‌های پنهان به سرورهای آلوده باشند.

۵. مسئولیت کاربر در امنیت سازمانی

کاربران، بخصوص کارکنان سازمان‌ها، باید درک کنند که هر رفتار دیجیتالی آنان در فضای شخصی، می‌تواند به سطح حملات علیه کل سازمان ارتقا یابد. اشتراک‌گذاری عمومی اطلاعات کاری، یکی از آسیب‌پذیری‌های جدی اما نادیده گرفته‌شده است.

بخش هفتم: چه باید کرد؟ اقدامات پیشگیرانه

در مواجهه با چنین تهدیداتی، چند اقدام پیشگیرانه ضروری و عملی پیشنهاد می‌شود:

غیرفعال کردن ثبت خودکار موقعیت مکانی

تنظیمات دوربین، اپلیکیشن‌ها و شبکه‌های اجتماعی باید به‌گونه‌ای تنظیم شوند که اطلاعات مکانی به‌صورت خودکار ذخیره یا ارسال نشود.

پاک‌سازی متادیتای تصاویر

قبل از انتشار تصاویر در فضای عمومی، بهتر است متادیتا (EXIF) آن‌ها حذف شود. ابزارهایی مانند Photo Exif Editor یا ExifCleaner می‌توانند در این زمینه مفید باشند.

آموزش مداوم امنیت دیجیتال برای کارکنان

سازمان‌ها باید به‌صورت دوره‌ای، آموزش‌هایی درباره مهندسی اجتماعی، حملات هدفمند، فیشینگ، و تحلیل رفتار مهاجم به کارکنان خود ارائه دهند.

بررسی اعتبار افراد قبل از تعامل

در دریافت پیام‌های کاری یا پیشنهاد همکاری، هویت فرستنده باید به روش‌های جداگانه تأیید شود. تماس تلفنی از یک خط رسمی یا بررسی دامنه ایمیل، نمونه‌هایی از این بررسی‌ها هستند.

استفاده از سیستم‌های شناسایی رفتار غیرمعمول

استفاده از سامانه‌هایی که رفتار کاربران را در شبکه تشخیص می‌دهند، می‌تواند در شناسایی زودهنگام نفوذهای مبتنی بر هویت‌دزدی مؤثر باشد.

نتیجه‌گیری

داستان نگار، تصویری واقعی از خطری پنهان است که بسیاری از کاربران، آگاهانه یا ناآگاهانه، با آن مواجه‌اند. تصور غالب این است که خطر سایبری از کدهای پیچیده و هکرهای حرفه‌ای سرچشمه می‌گیرد، اما در واقعیت، نقطه شروع بسیاری از حملات، ساده‌ترین رفتارهای انسانی است. فضای دیجیتال نیازمند سواد رسانه‌ای و امنیتی است. شبکه‌های اجتماعی، با تمام مزایایی که دارند، نباید به دروازه‌ای برای افشای اطلاعات حساس تبدیل شوند. مسئولیت این امر، هم بر دوش فرد است و هم سازمان. با درک تهدیدات و اصلاح رفتارهای ساده اما خطرناک، می‌توان از بسیاری از سناریوهای مشابه جلوگیری کرد.

SPECIAL TOPIC

01
موضوع ویژه

دفتر کار در خانه؛ راهی باز برای مهاجمان؟

تحولات جهانی در سال‌های اخیر، به‌ویژه گسترش همه‌گیری کرونا، شیوه‌های کاری سازمان‌ها را به‌طور چشمگیری تغییر داد. دورکاری از یک مدل استثنائی، به یک راهکار متداول در بسیاری از سازمان‌ها تبدیل شد. اما در کنار مزایای متعدد این الگوی کاری (از کاهش هزینه‌های عملیاتی گرفته تا افزایش انعطاف‌پذیری) تهدیدات امنیتی جدیدی نیز پدیدار شدند. اکنون، خانه بسیاری از کارمندان به «دفتر کار دوم» تبدیل شده، اما این دفتر، اغلب فاقد لایه‌های امنیتی لازم است.

در این مقاله، به بررسی خطرات رایج در دسترسی از راه دور، نحوه استفاده ایمن از ابزارهای اتصال، مسئولیت کاربران در حفظ امنیت تجهیزات شخصی، و تهدیداتی مانند بدافزارهای USB و شبکه‌های WiFi خانگی خواهیم پرداخت.

خطرات رایج هنگام اتصال به شبکه سازمان از منزل

دسترسی از راه دور به منابع سازمانی، اگر بدون تدابیر امنیتی کافی انجام شود، نه تنها باعث افزایش بهره‌وری نخواهد شد، بلکه به بستری برای حملات سایبری تبدیل می‌شود. در ادامه، برخی از مهم‌ترین تهدیدات را بررسی می‌کنیم:

الف) عدم رمزگذاری ترافیک

در صورت عدم استفاده از شبکه‌های رمزگذاری‌شده، داده‌هایی که بین سیستم کاربر و سرور سازمانی ردوبدل می‌شود ممکن است توسط مهاجمان شنود شود. این موضوع در شبکه‌های عمومی یا WiFiهای خانگی ناایمن، بسیار خطرناک‌تر است.

ب) سیستم‌عامل‌های به‌روزنشده

بسیاری از کاربران از رایانه‌ها یا لپ‌تاپ‌های شخصی برای کار از خانه استفاده می‌کنند. این سیستم‌ها ممکن است فاقد وصله‌های امنیتی اخیر باشند و بدین‌ترتیب، زمینه نفوذ از طریق آسیب‌پذیری‌های شناخته‌شده را فراهم کنند.

ج) استفاده مشترک از دستگاه‌ها

کاربرانی که از سیستم خانگی برای کار استفاده می‌کنند، گاه آن را با سایر اعضای خانواده نیز به اشتراک می‌گذارند. این موضوع احتمال نصب برنامه‌های ناامن، کلیک بر لینک‌های مشکوک یا ورود بدافزار را افزایش می‌دهد.

د) ذخیره‌سازی محلی اطلاعات سازمانی

در بسیاری از موارد، فایل‌ها، اطلاعات مشتریان یا مدارک حساس به‌صورت محلی در سیستم شخصی ذخیره می‌شوند. در صورت گم‌شدن یا سرقت دستگاه، این داده‌ها بدون هیچ‌گونه حفاظت باقی می‌مانند.

استفاده ایمن از VPN، RDP و دسکتاپ مجازی

ابزارهای دسترسی از راه دور، در صورتی که به‌درستی پیاده‌سازی شوند، می‌توانند سطح امنیت مناسبی را فراهم کنند. اما چگونگی استفاده و تنظیم این ابزارها نقش تعیین‌کننده‌ای در امنیت نهایی دارد.

الف) شبکه خصوصی مجازی

شبکه خصوصی مجازی راهکاری برای ایجاد تونل رمزنگاری‌شده بین کاربر و شبکه سازمانی است

ب) Remote Desktop Protocols

پروتکل ریموت دسکتاپ، توسط مایکروسافت ارائه شده و امکان دسترسی مستقیم به دسکتاپ سازمانی را فراهم می‌کند. اما این ابزار بدون محافظت مناسب، یکی از اهداف محبوب مهاجمان است.

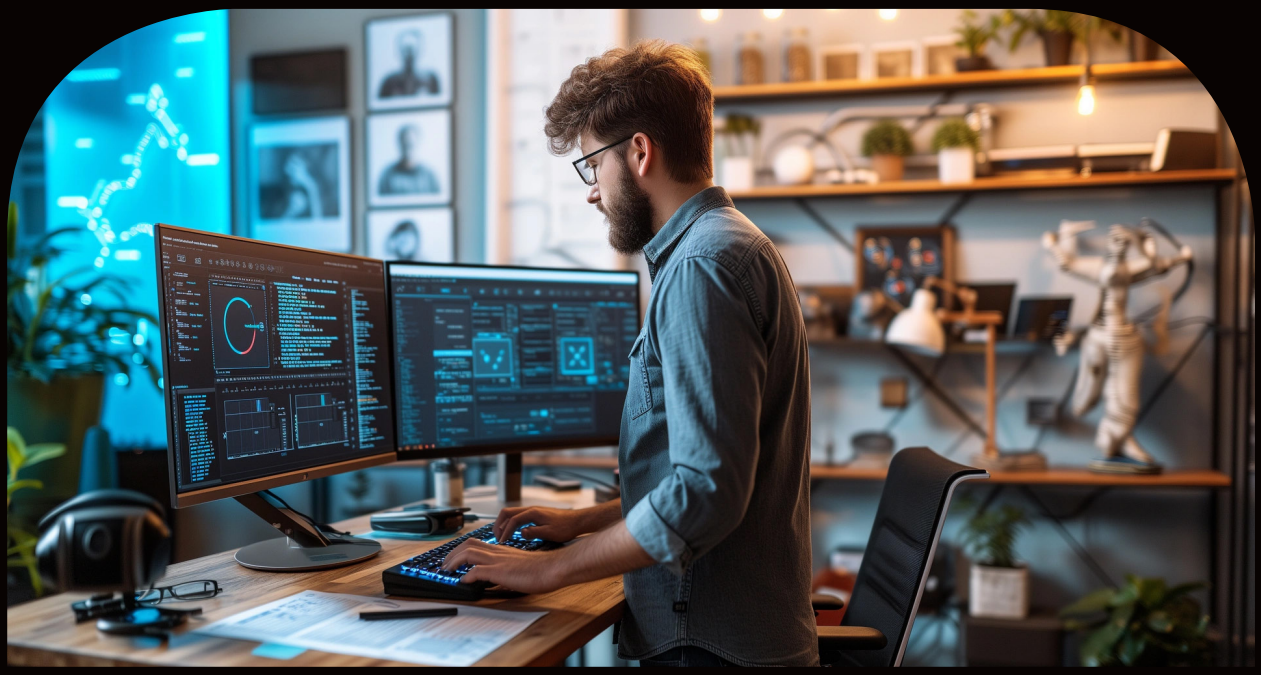
ج) دسکتاپ مجازی

راهکارهایی دسکتاپ مجازی امکان اجرای محیط کاری در بستر امن ابری را فراهم می‌کنند. در این روش، اطلاعات روی دستگاه کاربر ذخیره نمی‌شود و هرگونه فعالیت در محیط ایزوله‌شده انجام می‌گیرد.

مسئولیت کاربر در حفظ امنیت دستگاه‌های شخصی

در مدل دورکاری، کاربر آخرین خط دفاعی سازمان است. اگرچه سازمان‌ها می‌توانند ابزارهای کنترلی متعددی پیاده‌سازی کنند، اما رفتار کاربر نقش تعیین‌کننده دارد.

اقدامات ضروری برای کاربران:



- نصب آنتی‌ویروس معتبر و به‌روزرسانی منظم آن
- اجتناب از نصب نرم‌افزارهای متفرقه از منابع ناشناس
- قفل‌گذاری سیستم و استفاده از رمز عبور قوی
- جداکردن محیط کار از شخصی (مثلاً با استفاده از حساب کاربری مجزا یا سیستم مجازی)
- استفاده از مرورگرهای امن و افزونه‌های ضد تبلیغات و ردیاب‌ها

سازمان‌ها نیز می‌توانند از طریق ابزارهایی سطح پایش امنیتی بر روی دستگاه‌های شخصی را افزایش دهند؛ البته با رعایت ملاحظات حقوقی و حفظ حریم خصوصی کاربران.

تهدیدات مربوط به USB، WiFi خانگی و بدافزارها

الف) حافظه‌های USB

یکی از راه‌های رایج انتقال بدافزار، استفاده از فلش مموری یا هارد اکسترنال آلوده است. در محیط دورکاری، احتمال استفاده از USBهایی که قبلاً در سیستم‌های نامطمئن متصل شده‌اند، افزایش می‌یابد.

پیشنهادات:

- غیرفعال‌سازی خودکار اجرای فایل در زمان اتصال USB
- استفاده از ابزارهای اسکن خودکار USB
- ممنوعیت استفاده از حافظه‌های ناشناس و بدون برچسب در سیاست‌های سازمان

ب) شبکه WiFi خانگی

بسیاری از کاربران از مودم‌های خانگی استفاده می‌کنند که اغلب با رمز عبور پیش‌فرض یا تنظیمات اولیه کارخانه فعال هستند. همین موضوع، نقطه‌ضعف بزرگی در مسیر حمله محسوب می‌شود.

راهکارها:

- تغییر رمز پیش‌فرض مدیریت مودم
- استفاده از رمزگذاری WPA۲ یا WPA۳
- غیرفعال‌سازی WPS
- عدم اشتراک اتصال با همسایگان یا مهمان‌ها
- بررسی دستگاه‌های متصل به مودم به‌صورت دوره‌ای

ج) بدافزارهای رایج در مدل دورکاری

بسیاری از مهاجمان با علم به ضعف امنیتی در شبکه‌های خانگی، بدافزارهایی طراحی می‌کنند که از طریق مرورگر، ایمیل یا حتی پیام‌رسان‌ها وارد سیستم می‌شوند و عملکردهایی نظیر keylogging، سرقت کوکی، ایجاد دسترسی از راه دور و رمزگذاری فایل را انجام می‌دهند.

کاربران باید نسبت به فایل‌های پیوست مشکوک، لینک‌های ناشناس، پیام‌های فیشینگ و به‌روزرسانی‌های جعلی هوشیار باشند. در صورت بروز هرگونه نشانه غیرعادی مانند کند شدن سیستم، باز شدن خودکار مرورگر، نمایش پنجره‌های پاپ‌آپ یا مصرف بالای پردازنده، سیستم باید فوراً بررسی و ایزوله شود.

نتیجه‌گیری

دورکاری، اگرچه مزایای قابل‌توجهی دارد، اما در غیاب رویکردی امنیت‌محور می‌تواند سازمان‌ها را در معرض آسیب‌های جدی قرار دهد. امنیت در این مدل کاری، مسئولیتی مشترک بین کارفرما و کارمند است. سازمان‌ها باید بستر ایمن، ابزارهای مناسب و آموزش مستمر را فراهم کنند، و کاربران نیز باید نسبت به رفتارهای دیجیتالی خود، آگاهی و تعهد کافی داشته باشند.

دورکاری ایمن، تنها در صورتی تحقق می‌یابد که سیاست‌های امنیتی سازمان از دیوارهای فیزیکی شرکت فراتر رفته و به درون خانه‌های کارکنان نیز تسری یابد. در نهایت، «دفتر کار در خانه» نباید دری باز برای مهاجمان باشد؛ بلکه باید به حصاری امن برای ادامه فعالیت‌های سازمانی تبدیل شود.

02
موضوع ویژه

خرید آنلاین یا هدیه‌ای برای هکرها؟

در دنیای امروز، خرید اینترنتی به بخشی جدایی‌ناپذیر از زندگی شهروندان تبدیل شده است. فروشگاه‌های آنلاین، سامانه‌های پرداخت، اپلیکیشن‌های مالی و کیف‌پول‌های دیجیتال، فرآیند خرید و انتقال وجه را سریع‌تر و آسان‌تر از همیشه کرده‌اند. با این حال، سهولت در پرداخت همیشه به‌معنای امنیت نیست. فضای سایبری، فرصت مناسبی برای مهاجمان فراهم کرده تا از طریق تکنیک‌هایی چون فیشینگ، جعل صفحات پرداخت، ذخیره اطلاعات بانکی و مهندسی اجتماعی، به اطلاعات مالی کاربران دست یابند.

در ایـــن مقاله، با نگاهی فنـــی و تحلیلی به مهم‌ترین تهدیدات موجود در حوزه پرداخت الکترونیک، روش‌های شناسایی صفحات تقلبی، عملکـــرد رمز دوم پویا و خطرات ذخیره‌ســـازی اطلاعات کارت‌های بانکی در مرورگر یا سایت‌ها خواهیم پرداخت.

تفاوت درگاه پرداخت رسمی با فیشینگ

درگاه پرداخـــت یکی از مهم‌تریـــن نقاط تماس بین کاربر و ســـامانه بانکی است. اغلب کاربران هنگام پرداخت هزینه خرید اینترنتی، بدون دقت به نشانه‌های اعتبار، اطلاعات حساس خود از جمله شماره کارت، رمز دوم، CVV۲ و تاریخ انقضا را وارد می‌کنند. همین بی‌احتیاطی، زمینه سوءاســـتفاده هکرها را فراهم می‌کند.

درگاه پرداخت رسمی

- پروتکل HTTPS فعال با گواهی معتبر SSL
- آدرس دامنـــه متعلـــق به بانک یا شـــرکت PSP معتبر (مثلاً: https://sep.shaparak.ir)
- وجود نشان اعتماد الکترونیکی (اینماد)
- اســـتفاده از درگاه‌های دارای مجوز بانک مرکزی و شـــرکت شاپرک

درگاه فیشینگ:

- آدرس دامنه جعلی و مشابه با درگاه اصلی (مانند .shepraak com)
- فقدان قفل امنیتی مرورگر یا گواهی نامعتبر SSL
- ظاهر مشابه اما ناقص یا با غلط‌های تایپی
- گاهی حتی با تبلیغ در موتورهای جست‌وجو دیده می‌شود

مهاجمان اغلب از طریق پیامک‌های جعلی، ایمیل‌های فیشینگ، تبلیغات در شبکه‌های اجتماعی یا حتی اپلیکیشن‌های تقلبی، کاربران را به صفحات جعلی هدایت می‌کنند. ورود اطلاعات بانکی در این صفحات، به‌معنای تقدیم بی‌واسطه آن‌ها به مهاجم است.

روش‌های شناسایی صفحات تقلبی بانکی

تشخیص یک صفحه پرداخت جعلی از صفحه واقعی نیازمند دقت و آموزش اســـت. کاربـــران باید مهارت‌هایی بـــرای ارزیابی صحت صفحات بانکی داشته باشند.

معیارهای فنی تشخیص:

- بررسی آدرس سایت: مهم‌ترین مرحله است. دامنه باید دقیقاً مطابق با آدرس رسمی درگاه باشد. هرگونه اضافه یا تغییر مشکوک (مانند نقطه، فاصله یا خط فاصله) باید باعث تردید شود.
- قفل امنیتی مرورگر: در نوار آدرس، علامت قفل (SSL) باید فعال باشد. البته این شرط کافی نیست، چون مهاجمان نیز می‌توانند گواهی SSL دریافت کنند.
- لینک مســـتقیم به صفحه بانک: صفحات پرداخت نباید در داخل آی‌فریم یا دامنه سایت فروشنده بارگذاری شوند. همواره باید به صفحه‌ی بانک هدایت شوید.
- درخواســـت‌های غیرمتعارف: اگر صفحه از شـــما اطلاعات اضافه‌تری خواســـت (مثل رمز کارت، شماره شناسنامه یا ایمیل)، باید مشکوک شوید.
- واکنش غیرعادی مرورگر: هشدارهای مرورگر در مورد امنیت صفحه را جدی بگیرید.

ابزارهای کمکی:

- اپلیکیشن‌هایی مانند افسر سایبری پلیس فتا امکان بررسی امن بودن لینک‌ها را فراهم می‌کنند.
- مرورگرهـــای امن مانند Brave یـــا Firefox با افزونه ضد فیشینگ، قادر به مسدودسازی بسیاری از صفحات جعلی هستند.

رمز دوم پویا؛ چرا و چگونه؟

یکی از مهم‌ترین گام‌ها در افزایش امنیت پرداخت‌های اینترنتی، حذف رمز دوم ایستا و جایگزینی آن با رمز دوم پویا است.

مزایای رمز دوم پویا:

- موقتی و غیربازاســـتفاده: رمز فقـــط برای یک تراکنش معتبر است.
- محدودیـــت زمانی: معمولاً بین ۳۰ تا ۶۰ ثانیه پس از صدور اعتبار دارد.
- مقابله با حملات فیشـــینگ: حتی اگر مهاجم رمز را دریافت کند، زمان لازم برای سوءاستفاده محدود است.
- بی‌نیـــاز از حفظ کردن رمز: امنیت در برابر keyloggerها یا بدافزارهایی که رمز ذخیره می‌کنند.

روش‌های دریافت رمز دوم پویا:

- پیامک بانکی: رمز دوم پویا از طریق پیامک به شـــماره تلفن ثبت‌شده ارسال می‌شود.
- اپلیکیشن رمزساز: برخی بانک‌ها اپ‌هایی طراحی کرده‌اند که با الگوریتم خاص، رمز تولید می‌کنند.

چالش‌های امنیتی:

- اگر گوشـــی آلوده باشـــد، مهاجم می‌تواند پیامک رمز را نیز بخواند.
- اپ‌های رمزساز باید از منابع رسمی نصب شوند و در صورت لو رفتن رمز اول، کافی نیستند.

به‌رغـــم چالش‌ها، اســـتفاده از رمز دوم پویـــا همچنان یکی از مؤثرترین روش‌های کاهش تقلب در پرداخت‌های آنلاین است.

خطرات ذخیره اطلاعات کارت بانکی در مرورگر یا وب‌سایت‌ها

برای ســـهولت در خرید اینترنتی، بسیاری از کاربران اطلاعات کارت بانکـــی خـــود را در مرورگرهـــا یـــا حســـاب‌های کاربری فروشگاه‌ها ذخیره می‌کنند. اگرچه این روش باعث صرفه‌جویی در زمان می‌شود، اما تهدیداتی جدی نیز در پی دارد.

ذخیره در مرورگر:

مرورگرهایـــی مانند کـــروم، فایرفاکس و ســـافاری قابلیت ذخیره‌ســـازی اطلاعات پرداخـــت دارند. امـــا در صورت هک سیستم، نفوذ بدافزار، یا دسترسی فیزیکی افراد دیگر به دستگاه، این اطلاعات قابل سرقت است.

تهدیدات مرتبط:

- کی‌لاگرها که هنـگام ورود اولیه اطلاعات، آن‌ها را ضبط می‌کنند.
- بدافزارهای مرورگر که به اطلاعات ذخیره‌شده دسترسی پیدا می‌کنند.
- حملات فیشینگ درون‌سایتی که داده‌ها را استخراج می‌کنند.
- دسترسی فیزیکی افراد غیرمجاز به سیستم یا موبایل.

ذخیره در سایت فروشگاه‌ها:

فروشگاه‌های آنلاین، گاهی برای خرید سریع‌تر، امکان ذخیره اطلاعـات کارت را فراهـم می‌کنند. اما اگر این وب‌سـایت‌ها به درسـتی از استانداردهای سازمان شـاپرک تبعیت نکنند، داده‌های کاربران می‌تواند به خطر بیفتد.

نمونه‌های واقعی:

- در سـال ۲۰۱۹، اطلاعـات میلیون‌هـا کاربـر در یکـی از فروشگاه‌های آنلاین معروف اروپا نشت پیدا کرد، چون اطلاعات کارت به‌صورت رمزنگاری‌نشده در پایگاه داده ذخیره شده بود.

توصیه‌های امنیتی برای خرید آنلاین ایمن

خرید فقط از فروشگاه‌های معتبر

از سـایت‌هایی خرید کنید که دارای نماد اعتماد الکترونیکی و گواهی SSL معتبر هستند. بهتر است از فروشگاه‌هایی استفاده شود که آدرس دامنه آن‌ها با https آغاز می‌شـود و مالک آن مشخص است.

استفاده از کارت‌های مجزا برای پرداخت اینترنتی

استفاده از کارت‌های بانکی جداگانه با موجودی محدود برای خریدهای آنلاین، خطر سرقت دارایی اصلی را کاهش می‌دهد.

عدم ذخیره اطلاعات در مرورگر

پیشنهاد می‌شـود پس از انجام پرداخت، مرورگر را به‌گونه‌ای تنظیم کنید که اطلاعات را ذخیره نکند یا از حالت ناشناس استفاده کنید.

بررسی دوره‌ای صورت‌حساب‌ها

صورت‌حساب‌های بانکی باید به‌صورت هفتگی بررسی شوند تا در صورت مشاهده هرگونه تراکنش مشکوک، اقدامات لازم انجام گیرد.

فعال‌سازی اعلان تراکنش‌ها

با فعال کـردن اعلان لحظه‌ای تراکنش‌های بانکی، در صورت برداشت غیرمجاز، کاربر سریع‌تر متوجه شده و قادر به اقدام است.

استفاده از رمز دوم پویا و احراز هویت دومرحله‌ای

این دو ویژگی در کنار هم، احتمال موفقیت مهاجم را به حداقل می‌رسانند.

نتیجه‌گیری

در عصر دیجیتال، پرداخت‌های الکترونیک بخشی اجتناب‌ناپذیر از زندگی روزمره شده‌اند. اما همان‌طور که ابزارهای پرداخت توسعه یافته‌اند، روش‌های تقلب و نفوذ نیز پیچیده‌تر شده‌اند. آنچه کاربران را از تبدیل‌شـدن به «قربانی» محافظت می‌کنـد، نه تنها ابزارهای امنیتی، بلکه آگاهی، دقت و رفتارهای دیجیتال هوشمندانه است.

کاربـران بایـد بیاموزند که اطلاعـات بانکـی، همچون رمز گاوصندوق شخصی‌ست. نباید آن را در اختیار هیچ فرد، سایت یا برنامه‌ای گذاشت مگر با اطمینان کامل. خرید آنلاین، اگر با رعایت اصول امنیتی انجام شـود، تجربه‌ای لذت‌بخش و بی‌خطر خواهد بود. در غیر این صورت، تنها چند کلیک ساده کافی‌ست تا تمامی اطلاعات مالی‌تان به «هدیه‌ای برای هکرها» تبدیل شود.

SOCIAL MEDIA MALWARE

بدافزارهای
شبکه‌های
اجتماعی

بدافزارهای پنهان در شبکه‌های اجتماعی

شبکه‌های اجتماعی، با بیش از میلیاردها کاربر فعال روزانه، به یکی از جذاب‌ترین اهداف مهاجمان سایبری تبدیل شده‌اند. حضور گسترده کاربران، حجم بالای تعاملات، و اشتیاق عمومی برای دریافت ابزارها و امکانات بیشتر (مانند افزایش فالوئر، مشاهده بازدیدکنندگان پروفایل، یا مشاهده استوری‌ها به‌صورت ناشناس) باعث شده تا بدافزارها به‌شکلی زیرکانه و فریبنده در این بسترها نفوذ کنند.

این مقاله به معرفی رایج‌ترین نمونه‌های بدافزارهایی می‌پردازد که با پوشش اپلیکیشن‌های جانبی شبکه‌های اجتماعی توسعه یافته‌اند. هدف، آگاهی‌بخشی به کاربران و سازمان‌ها در خصوص تهدیداتی‌ست که گاهی از خود پلتفرم ناشی نمی‌شوند، بلکه از ابزارها و خدمات ثالثی سرچشمه می‌گیرند که برای کاربران جذاب، اما در باطن مخرب هستند.

تروجان‌های تقلبی با عنوان «Story Viewer» یا «Unfollowers»

یکی از رایج‌ترین بدافزارهایی که در فضای اینستاگرام دیده می‌شود، اپلیکیشن‌هایی هستند که به کاربر وعده می‌دهند «بازدیدکنندگان استوری» یا «کاربرانی که آنفالو کرده‌اند» را شناسایی می‌کنند. این اپ‌ها معمولاً با دسترسی کامل به حساب کاربری کاربر (با درخواست وارد کردن یوزرنیم و پسورد) اقدام به جمع‌آوری اطلاعات می‌کنند.

روش کار:

- اپلیکیشن از کاربر درخواست می‌کند تا با اطلاعات واقعی خود وارد شود.
- سپس توکن یا کوکی ورود به حساب را ذخیره کرده و به سرور مهاجم ارسال می‌کند.
- در بعضی موارد، اپ به‌طور کامل کنترل حساب را در دست گرفته و اقدام به ارسال دایرکت، لایک، یا فالو به‌صورت خودکار می‌کند.
- برخی نمونه‌ها حتی با انتشار لینک‌های فیشینگ از طریق دایرکت، به‌عنوان واسطه انتشار بدافزارهای دیگر عمل می‌کنند.

نمونه واقعی:

در سال ۲۰۲۳، یک اپ اندرویدی با عنوان InstaAnalyzer Pro در فروشگاه‌های غیررسمی منتشر شد که پس از نصب، دسترسی کامل به حساب اینستاگرام کاربر را دریافت کرده و به صورت نامرئی از آن برای ارسال پیام‌های جعلی استفاده می‌کرد.

اپلیکیشن‌های لایک بگیر و فالوئر بگیر؛ ظاهر تبلیغ، باطن سرقت اطلاعات

تمایل گسترده کاربران به افزایش لایک، فالوئر و دیده‌شدن بیشتر، بستری مناسب برای مهاجمان ایجاد کرده تا اپ‌هایی با ادعای «افزایش فالوئر تضمینی» یا «لایک رایگان» طراحی کنند. این اپ‌ها اغلب در قالب نرم‌افزار موبایل، ربات تلگرامی، یا حتی افزونه مرورگر عرضه می‌شوند.

تهدیدات اصلی:

- سرقت اطلاعات ورود کاربران از طریق صفحات لاگین جعلی
- استفاده از حساب کاربر برای تعاملات اجباری
- نمایش تبلیغات آلوده یا هدایت به صفحات مخرب
- جاسوسی از داده‌های دستگاه شامل مخاطبین، گالری، و لوکیشن
- نصب بدافزارهای ثانویه به بهانه افزایش سرعت یا بازکردن قفل قابلیت‌ها

بدافزارهای جاسوسی با پوشش اپ‌های پشتیبان‌گیری از چت یا مخاطبین

در پیام‌رسان‌هایی مانند تلگرام، واتساپ یا مسنجر، کاربرانی که نگران از دست رفتن اطلاعات یا چت‌های خود هستند، به دنبال ابزارهای پشتیبان‌گیر می‌روند. مهاجمان با طراحی اپلیکیشن‌هایی تحت عنوان «Backup Chat» یا «Secure Export» کاربران را فریب داده و اطلاعات حساس را به‌راحتی استخراج می‌کنند.

مکانیسم معمول:

- دریافت دسترسی به حافظه، پیامک، تماس‌ها و دسترسی اعلانات
- استخراج چت‌ها، شماره مخاطبین، تصاویر و ویدیوهای ذخیره‌شده
- ارسال داده‌ها به سرور خارجی به‌صورت رمزگذاری‌شده
- گاهی اوقات، این اپ‌ها دارای رابط کاربری واقعی بوده و عملکردی محدود نیز دارند تا جلب‌نظر کاربر را برانگیزند

افزونه‌های مرورگر برای مدیریت شبکه‌های اجتماعی؛ دریچه‌ای برای تزریق کد

بسیاری از کاربران برای راحتی مدیریت همزمان چند پلتفرم (مثل ارسال همزمان به اینستاگرام، لینکدین و توییتر)، از افزونه‌های مرورگر یا سرویس‌های جانبی استفاده می‌کنند. این افزونه‌ها گاه در فروشگاه رسمی مرورگر هم موجود هستند، اما به‌مرور و با دریافت به‌روزرسانی‌های مخرب، به ابزار حمله تبدیل می‌شوند.

اقدامات ممکن:

- تزریق کد جاوااسکریپت به صفحات فعال
- شنود فعالیت مرورگر و کوکی‌های نشست
- هدایت ناخواسته به صفحات تبلیغاتی یا فیشینگ
- تغییر مسیر لینک‌های اشتراکی به آدرس‌های مخرب

جاسوس‌افزارهایی که از نام اپ‌های رسمی سوءاستفاده می‌کنند

در برخی موارد، مهاجمان نسخه‌ای جعلی از اپلیکیشن رسمی یک شبکه اجتماعی طراحی می‌کنند و آن را با نام مشابه منتشر می‌کنند. این نسخه‌ها معمولاً در فروشگاه‌های غیررسمی، کانال‌های تلگرامی یا حتی در قالب فایل نصبی مستقیم به کاربر ارائه می‌شوند.

ویژگی‌های نسخه جعلی:

- ظاهر و آیکون دقیقاً مشابه نسخه اصلی
- عملکرد سطحی مشابه با اپ رسمی (مثلاً نمایش لیست پست‌ها یا پیام‌ها)
- درخواست مجوزهای غیرمعمول (مثل دسترسی به SMS، دوربین یا لیست تماس‌ها)
- جاسوسی از فعالیت کاربر و سرقت اطلاعات لاگین، پیام‌ها و حتی فایل‌ها

نمونه واقعی:

بدافـزاری با نـام Instagram Plus در قالب نسـخه‌ای ارتقاءیافته از اپ اصلی، در سال ۲۰۲۲ توانست بیش از ۵۰ هزار کاربر در منطقه خاورمیانه را آلوده کرده و اطلاعات حساب‌های آنان را به سرورهای مستقر در خارج از کشور ارسال کند.

بدافزارهای خودتکثیر در پیام‌رسان‌ها

در پیام‌رسـان‌هایی مانند واتسـاپ، نمونه‌هایی از بدافزارها مشـاهده شـده که پس از نصـب، به‌صورت خـودکار به تمام مخاطبین کاربـر پیامی حاوی لینک آلوده ارسـال می‌کنند. این روش شـبیه ویروس‌های کلاسـیک عمل می‌کنـد و هدف آن افزایش دامنه آلودگی است.

فرایند:

- دریافت مجوز دسترسی به مخاطبین و پیام‌ها
- ارسال پیام خودکار حاوی لینک آلوده
- فریب کاربران جدید به نصب اپ
- تکرار چرخه

این نوع بدافزارها معمولاً با وعده‌های جذاب مانند «نسـخه طلایی واتساپ»، «مشاهده استوری بدون اطلاع» یا «هک تلگرام دیگران» قربانی را جذب می‌کنند.

راهکارهای پیشگیرانه برای کاربران

در مواجهه با این تهدیدات، رعایت چند اصل ساده می‌تواند تفاوت بزرگی ایجاد کند:

- نصب اپ فقط از فروشگاه‌های رسمی

گوگل‌پلی، اپ‌اسـتور و سـایر مارکت‌های رسمی، هرچند ۱۰۰٪ ایمـن نیسـتند، اما در مقایسـه بـا منابع ناشـناس قابل اعتمادترند.

- بررسی دقیق مجوزها

هیچ اپلیکیشـنی که صرفاً برای مدیریت لایک یا اسـتوری طراحی شـده، نباید به لیسـت تماس‌ها، GPS یا دوربین شما دسترسی داشته باشد.

- استفاده از آنتی‌ویروس معتبر

بسـیاری از آنتی‌ویروس‌ها می‌توانند اپ‌های مشـکوک را پیش از اجرا شناسایی و مسدود کنند.

- فعال‌سـازی احـراز هویـت دومرحله‌ای در شـبکه‌های اجتماعی

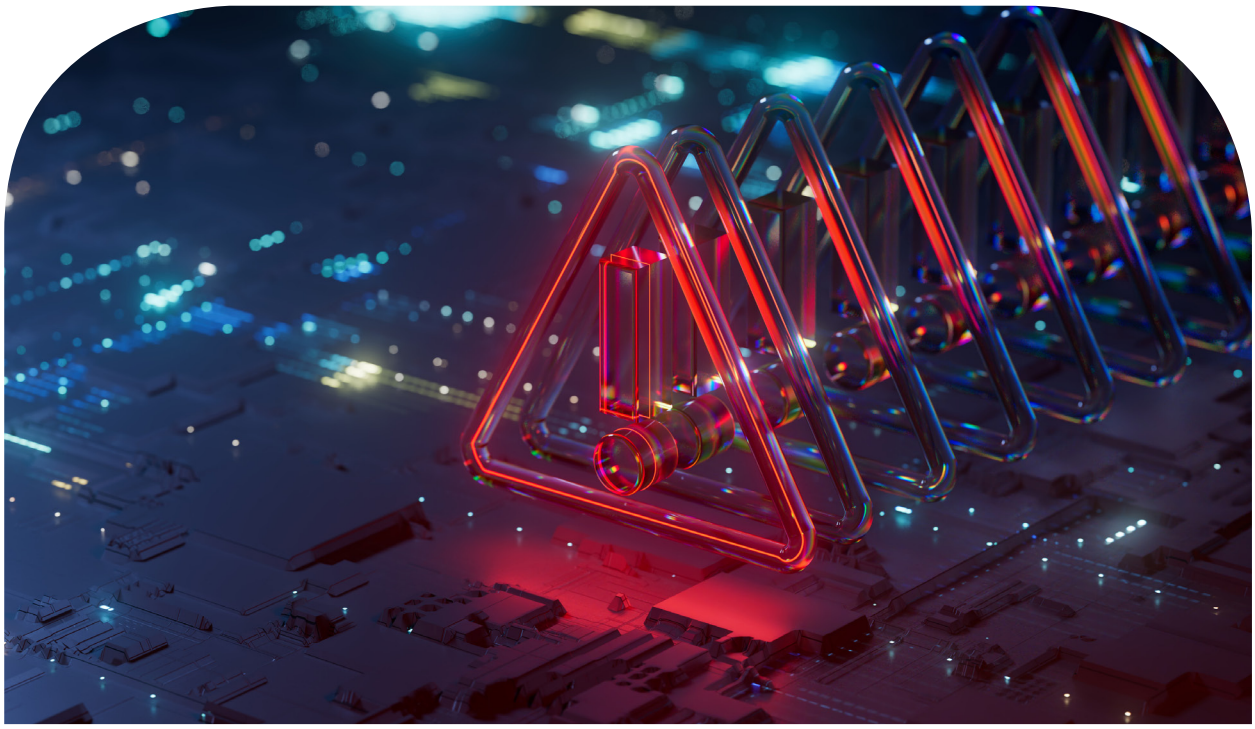
ایـن کار حتـی در صورت سـرقت رمز عبـور، مانع ورود مهاجم می‌شود.

- عدم وارد کردن اطلاعات حساب در اپ‌های جانبی

هیچ ابزار جانبی نباید نیاز به وارد کردن یوزرنیم و پسـورد شـبکه اجتماعی شما داشته باشد. در صورت نیاز به اتصال، تنها از طریق پروتکل OAuth معتبر و ایمن باید انجام شود.

نتیجه‌گیری

بدافزارهـای مرتبط با شـبکه‌های اجتماعـی نه‌تنها تهدیدی برای کاربران عادی، بلکه خطری برای سـازمان‌ها، برندها و حتی زیرساخت‌های حیاتی هستند. مهاجمان با بهره‌گیری از رفتارهای روان‌شـناختی کاربران، آن‌ها را به نصب اپ‌هایی ترغیب می‌کنند که در ظاهر بی‌ضرر و در باطن ابزار جاسوسی یا سرقت اطلاعات هستند. در جهانی که داده ارزشمندترین دارایی افراد و شرکت‌هاست، حفاظت از حساب‌های شبکه‌های اجتماعی باید با همان حساسیتی انجام شود که برای حفاظت از کارت بانکی یا اسناد محرمانه قائل هسـتیم. کاربر هوشمند، همیشه قبل از نصب، کلیک یا وارد کردن اطلاعات، یک‌بار دیگر فکر می‌کند.



TEST

آزمون •••

امنیت یا سهل‌انگاری؟

به هر سؤال زیر پاسخ بله یا خیر بدهید. در پایان، امتیاز خود را براساس تعداد پاسخ‌های بله محاسبه کنید و تفسیر مربوطه را بخوانید.

01 آیا در شبکه‌های اجتماعی از رمز عبور قوی و منحصربه‌فرد استفاده می‌کنید؟

02 آیا احراز هویت دو مرحله‌ای (۲FA) را برای حساب‌های مهم فعال کرده‌اید؟

03 آیا لینک‌های مشکوک یا ناشناس را بدون بررسی باز نمی‌کنید؟

04 آیا تنظیمات حریم خصوصی در اینستاگرام، تلگرام یا دیگر شبکه‌ها را به‌صورت محدود تنظیم کرده‌اید؟

05 آیا از ذخیره اطلاعات کارت بانکی در مرورگر یا اپلیکیشن‌های فروشگاهی خودداری می‌کنید؟

06 آیا از نصب اپ‌های جانبی مشکوک برای افزایش لایک، فالوئر یا مشاهده استوری پرهیز می‌کنید؟

07 آیا دستگاه‌های شخصی‌تان (موبایل، لپ‌تاپ) دارای آنتی‌ویروس فعال هستند؟

08 آیا هنگام اشتراک‌گذاری تصاویر، به حذف موقعیت مکانی (Location) توجه دارید؟

09 آیا با دقت، فایل‌ها و اپ‌هایی که از طریق پیام‌رسان‌ها دریافت می‌کنید را بررسی می‌کنید؟

10 آیا برای خرید اینترنتی فقط از درگاه‌های رسمی استفاده می‌کنید و به آدرس دقیق آن توجه دارید؟

اگر بین ۹ تا ۱۰ پاسخ بله داشتید: عالی – شما رفتار آگاهانه و مسئولانه‌ای در فضای دیجیتال دارید. احتمال قربانی‌شدن در حملات سایبری بسیار پایین است. همین‌طور ادامه دهید.

اگر بین ۶ تا ۸ پاسخ بله داشتید: قابل قبول – نکات مهمی را رعایت می‌کنید، اما هنوز چند ضعف قابل‌بهبود دارید. توصیه می‌شود بر روی نقاط ضعف تمرکز کنید.