شرکت آب منطقه‌ای گلستان

نشریه داخلی شرکت آب منطقه‌ای گلستان/ شماره چهارم/ تیر ماه ۱۴۰۴

امنیت در عصر شنود دیجیتال

DIGITAL LISTENING

EDWARD SNOWDEN

من نمی‌خواهم در دنیایی زندگی کنم
که هرچه می‌گویم، هر کاری که انجام
می دهم، هر کسی که با آن صحبت
می کنم، هر ابراز خلاقیت و عشق و
دوستی، در آن ثبت شده باشد.

نشریه داخلی شرکت آب منطقه‌ای گلستان

شماره چهارم ـــ تیر ماه ۱۴۰۴

فهرست

دکتر امیرحسین رحیمیان

وقتی خودمان ناخواسته تبدیل به جاسوس خودمان می‌شویم!

در جهان پرشتاب فناوری، جایی که ابزارهای هوشمند هر روز بیش از گذشته در زندگی ما حضور می‌یابند، یک واقعیت تلخ و کمتر شنیده‌شده وجود دارد؛ گاه بدون آن‌که بدانیم، خودمان مسیر افشای اطلاعات حساس را هموار می‌کنیم. در واقع، ما تنها قربانیان حملات سایبری نیستیم، بلکه در بسیاری از موارد، نقش فعال و ناخواسته‌ای در شکل‌گیری آسیب‌ها ایفا می‌کنیم. این مسئله صرفاً به دلیل ناآگاهی یا خطای انسانی نیست، بلکه اغلب ناشی از پدیده‌ای به نام عادی‌سازیِ رفتارهای دیجیتال است؛ یعنی وقتی عادت می‌کنیم که هر اپلیکیشنی را نصب کنیم، هر مجوزی را بدون بررسی تأیید کنیم، یا هر دستگاهی را به شبکه‌مان متصل نماییم، بدون آن‌که به پیامدهای امنیتی آن بیندیشیم.

تکنولوژی‌های روزمره؛ تسهیل‌گر یا تهدید؟

تلفن‌های هوشمند، رایانه‌های همراه، ساعت‌های دیجیتال، دوربین‌های تحت شبکه، اسپیکرهای هوشمند و دستیارهای صوتی مانند Google Assistant یا Alexa، امکانات ارزشمندی را در اختیار ما می‌گذارند. آن‌ها زندگی ما را ساده‌تر کرده‌اند، سرعت تعاملات را افزایش داده‌اند و بهره‌وری سازمانی را ارتقاء بخشیده‌اند. اما همین ابزارها، در صورتی که به درستی مدیریت نشوند، می‌توانند نقش واسطه‌ای ناپیدا میان ما و نشت اطلاعات حساس را ایفا کنند.

برای مثال، میکروفونی که همیشه فعال است، دوربینی که به اپلیکیشن‌های نامطمئن دسترسی دارد، یا اپلیکیشنی که موقعیت مکانی کاربر را به صورت پیوسته ثبت می‌کند، ممکن است عملاً بدون آگاهی ما، حجم زیادی از داده‌های رفتاری، صوتی یا حتی تصویری را جمع‌آوری کرده و به سرورهایی در مکان‌های ناشناخته ارسال کنند.

بدتر از آن، این تهدیدات همواره در پوشش قابلیت‌های کاربرپسند و ظاهر قابل اعتماد پنهان شده‌اند. پیام‌هایی از قبیل «برای ادامه استفاده از این سرویس، لطفاً به برنامه اجازه دسترسی به حافظه، دوربین و مکان جغرافیایی را بدهید» تبدیل به یک امر روزمره شده‌اند و کمتر کسی در سازمان‌ها به‌درستی متوقف می‌شود تا پیامدهای این مجوزها را بررسی کند.

اگرچه بسیاری از سازمان‌ها اقدامات فنی نظیر نصب آنتی‌ویروس، فایروال، یا محدودیت دسترسی شبکه را پیاده‌سازی کرده‌اند، اما تهدیدات نوین عمدتاً از لایه رفتاری و کاربری سرچشمه می‌گیرند. برای نمونه،

تصور کنید یک کارمند سازمان، لپ‌تاپ کاری خود را به شبکه وای‌فای عمومی یا خانگی متصل می‌کند که همزمان چندین دستگاه شخصی، شامل گوشی اعضای خانواده، تلویزیون هوشمند یا حتی اسباب‌بازی‌های متصل به اینترنت نیز روی آن فعال هستند. در چنین شرایطی، داده‌های شغلی ممکن است در معرض ترافیک ناایمن قرار گیرند، بدون اینکه کارمند از آن مطلع باشد.

همچنین، استفاده از اپلیکیشن‌های سرگرمی یا خدماتی در دستگاه‌های سازمانی، بدون بررسی امنیتی، می‌تواند به مهاجمان امکان دهد تا از طریق به‌ظاهر بی‌خطرترین مجاری، دسترسی اولیه به سامانه‌ها را به‌دست آورند. نمونه‌هایی از این نوع نفوذ در گزارش‌های شرکت‌های امنیتی به کرات ثبت شده‌اند؛ جایی که حمله از طریق یک بازی موبایلی ساده یا یک ابزار ویرایش عکس آغاز شده و در نهایت به نشت اطلاعات محرمانه منتهی شده است.

در چنین شرایطی، دیگر نمی‌توان امنیت اطلاعات را صرفاً به ابزارها سپرد. مهم‌ترین ابزار در برابر این تهدیدات، افزایش آگاهی کارکنان و کاربران نهایی است. امنیت در جهان امروز نه‌تنها یک مسئله فنی، بلکه یک مهارت فردی است. آموزش مستمر، مرور سیاست‌های امنیتی سازمان، و ترویج فرهنگ «پیش از کلیک، فکر کن»، از جمله اقداماتی است که می‌تواند سهم کاربر را در حفظ امنیت دیجیتال افزایش دهد.

کاربران باید بدانند که:

- هر مجوزی که به یک اپلیکیشن می‌دهند، می‌تواند کانالی برای استخراج اطلاعات باشد.
- هر دستگاهی که به شبکه متصل می‌کنند، یک مسیر بالقوه برای ورود تهدیدات است.
- هر پیامی که بدون بررسی باز می‌کنند، ممکن است حاوی کدی باشد که بدون اجرا شدن ظاهری، اطلاعات را منتقل می‌کند.

در این شماره از ماهنامه، تمرکز ما بر روی تهدیدهای پنهانی و نظارت‌های دیجیتال ناخواسته خواهد بود؛ تهدیداتی که نه با رمز عبور ضعیف، بلکه با ساده‌ترین رفتارهای روزمره کاربران ایجاد می‌شوند. تلاش کرده‌ایم با تحلیل رفتارهای دیجیتال رایج، ارائه سناریوهای واقعی، معرفی ابزارهای ساده کنترلی، و مهم‌تر از همه، نگاه آموزشی غیرکلیشه‌ای، کمک کنیم تا سطح هوشیاری دیجیتال در میان کارکنان سازمان افزایش یابد.

امنیت سایبری در دهه‌ی جدید، مفهومی فراتر از دیوار آتش و ضدویروس است. امروزه، بخش بزرگی از امنیت، به تصمیم‌های روزانه‌ی ما در استفاده از فناوری وابسته است. اینکه چه اپلیکیشنی نصب می‌کنیم، به چه چیزی اجازه دسترسی می‌دهیم، یا حتی چه چیزی را هنگام صحبت مقابل میکروفون روشن می‌گذاریم. اکنون بیش از هر زمان دیگر، ضروری است که رفتارهای دیجیتال خود را بازنگری کنیم. چرا که در بسیاری از موارد، تهدید از بیرون نمی‌آید، بلکه از درون رفتارهای خود ما آغاز می‌شود.

MAIN ARTICLE

مقاله اصلی

تجسس مدرن: ابزارهایی که از طریق صدا، تصویر، موقعیت و حتی نور از ما جاسوسی می‌کنند

در گذشته‌ای نه‌چندان دور، واژه‌ی جاسوسی یادآور مأمورهای مخفی، میکروفون‌های پنهان‌شده پشت قاب عکس‌ها، و دوربین‌هایی با لنزهای تلسکوپی در فیلم‌های هیجانی بود. اما امروزه، مفهوم جاسوسی به شکلی بسیار پیچیده‌تر و در عین حال، نامحسوس‌تر در زندگی روزمره ما نفوذ کرده است. ما در محیطی زندگی می‌کنیم که بسیاری از ابزارهای شخصی و اداری‌مان ـ از تلفن همراه گرفته تا لپ‌تاپ و حتی ساعت هوشمند ـ به‌طور بالقوه می‌توانند به ابزارهای ضبط و انتقال اطلاعات بدل شوند. تفاوت اصلی دنیای امروز با گذشته اینجاست: اکنون «خودِ ابزارهایی» که به آن‌ها اعتماد داریم، ممکن است بدون آگاهی ما، در نقش چشم‌ها و گوش‌های یک ناظر پنهان عمل کنند.

در این مقاله، به شکلی مستند، ساده و دقیق بررسی خواهیم کرد که چگونه ابزارهای عادی مانند گوشی‌های همراه، میکروفون‌های همیشه‌فعال، وب‌کم‌ها، حسگرهای حرکتی، دستگاه‌های اینترنت اشیا و حتی نور یک مانیتور می‌توانند اطلاعات حساس ما را ثبت و منتقل کنند. این بررسی صرفاً تئوریک نیست؛ بلکه به نمونه‌های واقعی، پروژه‌های تحقیقاتی مستند و گزارش‌های امنیتی معتبر اشاره دارد تا خواننده نه‌تنها با تهدیدات آشنا شود، بلکه نگاه تازه‌ای به امنیت روزمره خود پیدا کند.

01

گوشی‌های هوشمند؛ جاسوسانی در جیب ما

تلفن‌های هوشمند امروزی بیش از آن‌که ابزار ارتباطی باشند، دستگاه‌هایی چندمنظوره‌اند که مجموعه‌ای از میکروفون‌ها، دوربین‌ها، حسگرهای موقعیت‌یاب، سنجش نور، شتاب‌سنج و دستیارهای صوتی را در دل خود جای داده‌اند. همین امکانات گسترده، اگرچه زندگی را آسان‌تر می‌کنند، اما به همان میزان در معرض سوءاستفاده قرار دارند.

الف) شنود محیط با میکروفون پنهان

تعداد زیادی از اپلیکیشن‌های رایگان نصب‌شده روی گوشی، حتی زمانی که ظاهراً بسته هستند، به میکروفون دستگاه دسترسی دارند. برای مثال، گزارش‌هایی وجود دارد که نشان می‌دهد برخی نرم‌افزارهای تبلیغاتی از میکروفون گوشی استفاده می‌کنند تا با شنود صداهای محیط، علایق کاربر را تحلیل کرده و تبلیغات مرتبط‌تری نمایش دهند. هرچند این فرآیند در ظاهر برای هدفی تجاری انجام می‌شود، اما در عمل، ضبط بی‌اجازه‌ی صدای کاربر و ذخیره‌ی آن در سرورهای ناشناس، مصداق آشکار نقض حریم خصوصی است. در برخی کشورها، حتی گزارش شده که گروه‌های هکری پیشرفته از طریق نصب بدافزارهای مخصوص روی گوشی افراد هدف، می‌توانند مکالمات را به‌طور زنده شنود کرده یا محیط اطراف کاربر را بدون اطلاع او ضبط و ارسال کنند.

ب) ردیابی لحظه‌ای از طریق موقعیت مکانی

مکان‌یاب گوشی (GPS) فقط زمانی فعال نیست که کاربر در حال استفاده از نقشه باشد. در واقع بسیاری از نرم‌افزارها ـ حتی اپلیکیشن‌های سرگرمی یا آب‌وهوا ـ بدون دلایل موجه، موقعیت مکانی کاربر را به‌صورت مداوم استخراج می‌کنند. در بسیاری از موارد، کاربر هنگام نصب نرم‌افزار، بدون مطالعه دقیق مجوزها، دسترسی به موقعیت مکانی را صادر می‌کند. با تجمیع این اطلاعات، امکان ترسیم دقیق الگوهای رفت‌وآمد، مکان کار، محل سکونت، حتی ساعاتی که کاربر در خانه نیست، فراهم می‌شود. در سطح کلان، این داده‌ها ممکن است به شرکت‌های تبلیغاتی فروخته شوند یا در صورت نشت اطلاعات، در دسترس مجرمان سایبری قرار بگیرند.

ج) دوربین‌هایی که همیشه آماده‌اند

برخی بدافزارهای پیشرفته توانایی فعال‌سازی دوربین جلو یا پشت گوشی بدون اطلاع کاربر را دارند. حتی در مواردی، نرم‌افزارهای جعلی مثل چراغ‌قوه یا اسکنر QR که در ظاهر بی‌ضرر به‌نظر می‌رسند، در پشت‌صحنه به دوربین دسترسی دارند و تصویر را ثبت و آپلود می‌کنند. متأسفانه کاربر عادی به‌دلیل آشنایی ناکافی با مدیریت مجوزها، متوجه این فعالیت‌ها نمی‌شود.

02

لپ‌تاپ‌ها و رایانه‌ها؛ خاموش اما در حال ضبط

رایانه‌ها، به‌ویژه لپ‌تاپ‌ها، به ابزارهای کاری و خانگی جدایی‌ناپذیر زندگی ما بدل شده‌اند. اما همان‌طور که امکانات آن‌ها گسترده‌تر شده، احتمال سوءاستفاده از این امکانات نیز بیشتر شده است.

الف) وب‌کم‌هایی که چشم مهاجم‌اند

در بسیاری از حملات سایبری هدفمند، مهاجم با ارسال پیوست آلوده یا نصب بدافزار، کنترل کامل بر دوربین لپ‌تاپ را به دست می‌آورد. نکته خطرناک ماجرا اینجاست که در برخی مدل‌های لپ‌تاپ، امکان فیلم‌برداری از کاربر بدون روشن شدن چراغ وضعیت دوربین وجود دارد. نمونه‌های واقعی این نوع جاسوسی حتی در میان روزنامه‌نگاران، فعالان سیاسی و کارمندان سازمان‌های حساس گزارش شده است. برای همین، استفاده از کاور فیزیکی روی دوربین لپ‌تاپ، امروزه نه یک احتیاط افراطی، بلکه یک استاندارد امنیتی محسوب می‌شود.

ب) ضبط صدا حتی در زمان سکوت

یکی دیگر از تهدیدات پیشرفته که به‌طور خاص در تحقیقات دانشگاهی مطرح شده، استفاده از بلندگوهای رایانه برای ثبت صداست. اگرچه در نگاه اول بلندگو وظیفه پخش صدا دارد، اما برخی حملات پیچیده توانسته‌اند از ساختار بلندگوها برای دریافت امواج استفاده کنند و پس از تحلیل آن‌ها، صدای مکالمات محیط را بازسازی نمایند. هرچند این نوع حملات هنوز در سطح عمومی شایع نیست، اما اثبات آن‌ها در محیط‌های آزمایشگاهی، هشداری جدی برای سازمان‌هایی است که نیاز به محافظت حداکثری از اطلاعات دارند.

ج) لپ‌تاپ‌های همیشه روشن؛ دروازه‌ای برای نظارت شبانه‌روزی

بسیاری از کاربران، حتی در پایان روز کاری، لپ‌تاپ خود را خاموش نمی‌کنند؛ بلکه آن را در حالت «Sleep» یا «Hibernate» رها می‌کنند. این موضوع، در صورتی که سیستم آلوده شده باشد، به مهاجم اجازه می‌دهد حتی در زمان عدم استفاده کاربر، به سیستم متصل شود، داده‌ها را منتقل کرده یا فرمان‌های لازم را اجرا کند.

03

شیشه، نور، لرزش: وقتی محیط اطرافتان جاسوسی می‌کند

برخلاف تصور رایج، فقط ابزارهای دیجیتال نیستند که امکان شنود و نظارت را فراهم می‌کنند. در برخی از پیشرفته‌ترین روش‌های تجسس، از عناصر کاملاً فیزیکی مانند شیشه‌ی پنجره، نور مانیتور و حتی ارتعاشات دیوار برای استخراج اطلاعات استفاده شده است. این موارد اگرچه بیشتر در سطح نظامی یا پژوهشی مورد استفاده قرار گرفته‌اند، اما آگاهی از آن‌ها برای درک گستره واقعی تهدیدات دیجیتال ضروری است.

الف) ضبط صدا از طریق ویبره‌ی شیشه‌ها

مطالعاتی که در دانشگاه MIT انجام شده، نشان داده‌اند که با استفاده از دوربین‌های با نرخ فریم بالا، می‌توان فیلم اجسام سبکی مانند کیسه نایلونی را که نزدیک شیشه قرار دارد، ضبط و سپس با تحلیل نوسانات آن، صدای محیط داخلی اتاق را بازسازی کرد. این روش که به میکروفون بصری معروف است، حتی قادر به تشخیص گفت‌وگوهای آرام و نجواگونه از پشت پنجره‌های بسته می‌باشد. استفاده عملی از این تکنیک‌ها، در محیط‌هایی چون سفارت‌خانه‌ها یا جلسات محرمانه، می‌تواند تهدید جدی تلقی شود. اما واقعیت این است که هر فضای دارای پنجره، به‌نوعی می‌تواند یک نقطه شنود بالقوه باشد.

ب) جاسوسی از طریق نور مانیتور

یکی از پیچیده‌ترین و کمترشناخته‌شده‌ترین روش‌های استخراج اطلاعات، استفاده از تغییرات نور ساطع‌شده از مانیتور است. این روش تحت عنوان Optical TEMPEST شناخته می‌شود و بر پایه این اصل استوار است که تغییرات بسیار ریز در نور یک صفحه‌نمایش، می‌تواند محتوای در حال نمایش را بازتاب دهد. مهاجم با قرار دادن یک دوربین بسیار حساس در فاصله‌ای نسبتاً دور (مثلاً در ساختمانی روبه‌روی دفتر هدف)، می‌تواند این تغییرات نوری را ثبت و با تحلیل آن‌ها، محتوای نمایش داده‌شده را بازسازی کند. در محیط‌های با سطح امنیتی بالا، این تهدید بسیار جدی تلقی می‌شود و به همین دلیل، استفاده از پرده‌های مخصوص جذب نور، فیلترهای فرکانس نوری، و موقعیت‌یابی دقیق مانیتورها از جمله اقداماتی است که در چنین فضاهایی توصیه می‌شود.

ج) شنود از طریق ارتعاش دیوار

شاید عجیب به‌نظر برسد، اما در برخی روش‌ها، از لرزش‌های دیوار یا میز ناشی از صدای صحبت‌کردن، برای بازسازی صدا استفاده می‌شود. دستگاه‌هایی خاص که ارتعاشات سطح را ثبت می‌کنند (نظیر سنسورهای لیزری یا میکروشتاب‌سنج‌ها)، قادرند با تحلیل این لرزش‌ها، حتی در فواصل زیاد، اطلاعات صوتی را استخراج کنند. گرچه این فناوری در حال حاضر بیشتر در حوزه نظامی و پلیسی کاربرد دارد، اما روند سریع پیشرفت تکنولوژی می‌تواند آن را به زودی در دسترس گروه‌های مخرب نیز قرار دهد.

04

شنود در جلسات آنلاین وقتی سکوت، سکوت نیست

افزایش چشمگیر استفاده از جلسات آنلاین در سال‌های اخیر، باعث شده تهدیدات جدیدی در این فضاها شکل بگیرد. بسیاری از کارمندان و مدیران، از پلتفرم‌هایی چون زوم، مایکروسافت تیمز، گوگل‌میت و سایر ابزارهای مشابه استفاده می‌کنند، اما کمتر کسی از خطرات نهفته در دل این ارتباطات دیجیتال آگاه است.

الف) ضبط خودکار بدون اطلاع

در برخی پلتفرم‌ها، گزینه‌ای برای ضبط خودکار جلسه فعال است. این ضبط می‌تواند بدون اطلاع کامل اعضای جلسه انجام شود. از سوی دیگر، کاربرانی که از طریق مرورگر و بدون بررسی کامل تنظیمات وارد جلسه می‌شوند، ممکن است اجازه دسترسی به دوربین و میکروفون را ناخواسته صادر کرده باشند. بدتر از آن، اگر سیستمی به بدافزار آلوده باشد، ممکن است تمامی مکالمات و تصاویر ضبط‌شده به‌صورت خودکار و در پس‌زمینه، به سرورهای مهاجم منتقل شوند.

ب) میکروفون‌های خاموش که همچنان گوش می‌دهند

در ظاهر، وقتی دکمه «Mute» در یک جلسه آنلاین را فشار می‌دهید، میکروفون خاموش می‌شود. اما تحقیقات نشان داده‌اند که در برخی موارد، تنها صدای ارسالی به جلسه قطع می‌شود، در حالی که اپلیکیشن مورد استفاده یا حتی سیستم‌عامل، همچنان صدا را ضبط و نگهداری می‌کند. برای مثال، بررسی‌هایی که روی اپلیکیشن‌هایی نظیر زوم صورت گرفته، نشان داده که در برخی نسخه‌ها، حتی زمانی که میکروفون خاموش است، داده‌های صوتی در حافظه موقت ثبت می‌شوند. اگر سیستم به هر دلیلی آلوده باشد، این اطلاعات قابل استخراج هستند.

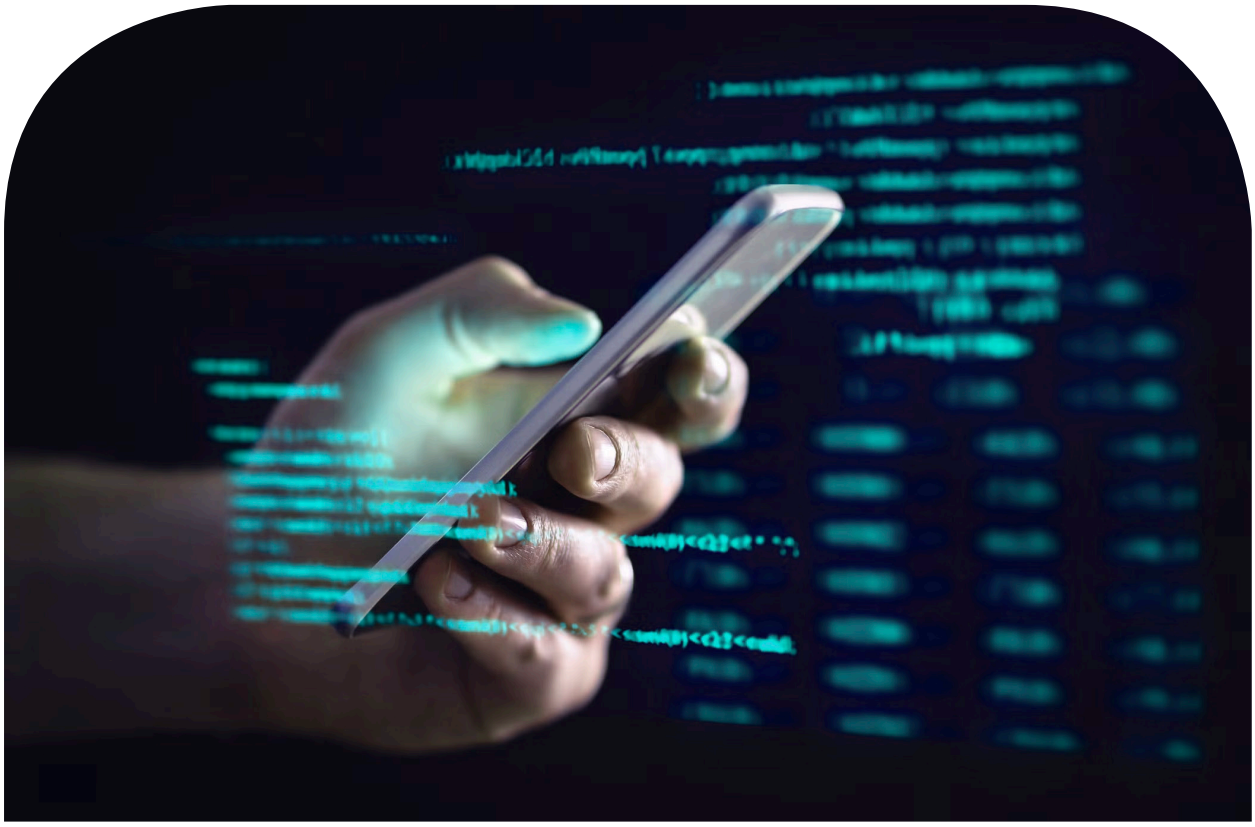
ج) اشتراک‌گذاری تصادفی

یکی از مشکلات رایج در جلسات آنلاین، اشتراک‌گذاری تصادفی فایل‌ها، پوشه‌ها یا حتی کل صفحه نمایش است. در محیط‌های سازمانی، چنین اشتباهی می‌تواند منجر به افشای اسناد محرمانه، تصاویر خصوصی یا حتی اطلاعات مالی شود. متأسفانه این موضوع معمولاً به دلیل عدم آشنایی کاربر با رابط کاربری رخ می‌دهد.

05

دستگاه‌های هوشمند خانگی؛ وقتی خانه‌تان با شما حرف می‌زند... و به دیگران هم می‌گوید

با گسترش روزافزون فناوری اینترنت اشیا، ابزارهایی که تا چند سال پیش صرفاً وسایل مکانیکی یا برقی ساده محسوب می‌شدند، حالا به گجت‌هایی متصل، شنوا، بینا و بعضاً تحلیل‌گر تبدیل شده‌اند. این تحول، هرچند رفاه کاربران را افزایش داده،



اما نگرانی‌های جدی امنیتی نیز به دنبال داشته است.

الف) دستیارهای صوتی؛ شنود قانونی یا نفوذ پنهان؟

دستیارهای صوتی مانند آمازون الکسا، دستیار گوگل و سیری اپل با هدف آسان‌سازی تعامل کاربر با فناوری طراحی شده‌اند. اما اساس عملکرد آن‌ها بر این است که به‌طور مداوم در حال «گوش‌دادن» به محیط هستند تا در لحظه‌ای که کاربر واژه بیداربخش را می‌گوید، فعال شوند. این یعنی، دستگاه عملاً همیشه در حال شنود است. اگرچه سازندگان ادعا می‌کنند که صدای محیط به‌صورت محلی تحلیل می‌شود و فقط پس از شنیدن واژه بیداربخش به سرور ارسال می‌گردد، اما چندین گزارش رسمی ثابت کرده‌اند که در موارد متعددی، این دستیارها به اشتباه فعال شده و مکالمات خصوصی را ضبط و حتی ارسال کرده‌اند. یکی از نمونه‌های مشهور، مربوط به کاربری بود که آمازون الکسا مکالمه‌ی خصوصی او و همسرش را شنیده، ضبط کرده و برای یکی از مخاطبین‌شان ایمیل کرده بود. چنین مواردی نشان می‌دهد که اطمینان مطلق به عملکرد بی‌نقص این ابزارها هنوز زود است.

ب) تلویزیون‌های هوشمند؛ تصویر، صدا و داده

تلویزیون‌های هوشمند جدید، اغلب به میکروفون و دوربین داخلی مجهز هستند؛ برای برقراری تماس تصویری، دستور صوتی یا کنترل هوشمند. اما برخی مدل‌ها، به‌صورت پیش‌فرض صدای محیط را برای تحلیل ترجیحات بیننده یا بهبود تبلیغات ضبط و پردازش می‌کنند. در سال‌های گذشته، شرکت‌هایی نظیر سامسونگ، ال‌جی و حتی برندهای ناشناس چینی، بارها به دلیل ارسال داده‌های کاربران بدون اطلاع آن‌ها، مورد انتقاد نهادهای حفاظت از داده قرار گرفته‌اند.

ج) جاروبرقی و یخچال؛ نقشه‌برداری از زندگی خصوصی

حتی وسایلی مانند جاروبرقی‌های رباتیک، با قابلیت نقشه‌برداری از خانه و اتصال به اینترنت، می‌توانند اطلاعات دقیقی از چیدمان منزل، مکان اشیاء، زمان‌بندی رفت‌وآمد افراد و نقاط پررفت‌وآمد ثبت کنند. این اطلاعات اگر به‌درستی رمزگذاری و محافظت نشوند، می‌توانند در دست افراد سودجو یا مهاجمان سایبری، به اطلاعاتی بسیار حساس تبدیل شوند.

› **نتیجه‌گیری:** امنیت دیجیتال، از خودآگاهی شروع می‌شود

ما در دورانی زندگی می‌کنیم که مرز بین ابزار و ناظر، بین رفاه و نظارت، به‌شدت باریک و گاه نامرئی شده است. هر ابزار دیجیتال ـ از تلفن همراه گرفته تا بلندگوهای هوشمند ـ نه‌تنها می‌تواند کار ما را ساده‌تر کند، بلکه در شرایط خاص، می‌تواند به ابزاری برای نفوذ، شنود، ردیابی و جمع‌آوری داده نیز تبدیل شود. اما در این میان، وحشت یا قطع کامل ارتباط با فناوری راه‌حل نیست. بلکه آنچه اهمیت دارد، آگاهی، دقت، و مدیریت هوشمندانه دسترسی‌ها و تنظیمات دستگاه‌هاست. کاربری که بداند چه دستگاهی در حال پردازش چه داده‌ای‌ست، یک کاربر آگاه و مقاوم در برابر تهدیدات است. به‌ویژه در محیط‌های سازمانی، داشتن رویه‌های مشخص برای استفاده از ابزارهای هوشمند، آموزش مستمر کارکنان، استفاده از ابزارهای نظارتی مطمئن، و پیاده‌سازی سیاست‌های شفاف در خصوص حفاظت از داده‌ها، همگی به کاهش ریسک کمک خواهند کرد.

A PRACTICAL GUIDE

راهنمای عملی ...

چگونه دسترسی دوربین، میکروفون و موقعیت مکانی را کنترل کنیم؟

در دنیای امروزی که بیشتر دستگاه‌های دیجیتال به ابزارهای شنوا، بینا و مکان‌یاب مجهز شده‌اند، یکی از مهم‌ترین گام‌ها در راستای حفظ حریم خصوصی و امنیت اطلاعات، مدیریت و کنترل دقیق مجوزهای مربوط به دوربین، میکروفون و موقعیت مکانی است. اگرچه این اجزا برای بسیاری از کاربردهای روزمره ضروری به‌نظر می‌رسند، اما سوءاستفاده از آن‌ها می‌تواند منجر به نقض گسترده حریم خصوصی، سرقت اطلاعات یا حتی جاسوسی هدفمند شود. در این راهنمای کاربردی، به‌صورت دقیق و مرحله‌به‌مرحله بررسی می‌کنیم که چگونه می‌توان با تنظیمات موجود در سیستم‌عامل‌های رایج (Android، iOS، Windows، macOS)، این دسترسی‌ها را تحت کنترل قرار داد. همچنین با مرور چند اصل عمومی، درک بهتری از مدیریت مجوزها و کاهش ریسک‌های امنیتی به‌دست خواهیم آورد.

بخش اول: اصول اولیه در مدیریت مجوزها

پیش از ورود به جزئیات فنی، درک چند اصل پایه برای حفاظت موثر از دوربین، میکروفون و موقعیت مکانی ضروری است:

۱. حداقل‌سازی دسترسی: فقط به نرم‌افزارهایی که عملکردشان واقعاً به این مجوزها وابسته است، اجازه دسترسی بدهید. مثلاً یک نرم‌افزار آب‌وهوا ممکن است نیاز به موقعیت مکانی داشته باشد، اما نیازی به میکروفون ندارد.

۲. بازبینی دوره‌ای مجوزها: به‌صورت ماهانه یا فصلی، لیست مجوزهای اعطا شده به اپلیکیشن‌ها را بررسی و در صورت عدم نیاز، لغو کنید.

۳. فعال‌سازی دسترسی موقتی: برخی سیستم‌عامل‌ها (مثل iOS) امکان اعطای دسترسی موقتی یا فقط برای استفاده فعلی را فراهم می‌کنند. این قابلیت‌ها را فعال کنید.

۴. اطلاع از دسترسی در حال اجرا: هرگاه یک نرم‌افزار در حال استفاده از دوربین یا میکروفون باشد، نماد یا هشدار خاصی روی صفحه نمایش ظاهر می‌شود. آشنایی با این هشدارها و واکنش سریع به آن‌ها ضروری است.

بخش دوم: کنترل دسترسی‌ها در دستگاه‌های اندروید (Android)

دوربین و میکروفون:

در نسخه‌های جدید اندروید (مخصوصاً Android ۱۲ به بعد)، گوگل امکانات کنترلی دقیقی را در اختیار کاربران قرار داده است:

- به بخش Settings > Privacy > Permission Manager بروید.
- در آنجا، دسته‌بندی‌هایی مثل Camera و Microphone را می‌بینید.
- با انتخاب هر کدام، لیستی از اپلیکیشن‌هایی که به آن قابلیت دسترسی دارند نمایش داده می‌شود.
- با لمس نام هر برنامه، می‌توانید دسترسی آن را به «اجازه در هنگام استفاده»، «همیشه مجاز» یا «هرگز مجاز» تغییر دهید.

همچنین در اندروید ۱۲ به بعد، با کشیدن نوار اعلان‌ها، دکمه‌های فعال/غیرفعال‌سازی سریع برای میکروفون و دوربین در دسترس هستند.

موقعیت مکانی (Location):

- مسیر Settings > Location > App permissions:
- دسترسی هر برنامه را به دقیق (Precise) یا تقریبی (Approximate) و یا غیرفعال تنظیم کنید.

نکتــه امنیتی: برخی اپ‌ها از طریق ترکیب داده‌های دیگر (مثل وای‌فای، بلوتوث یا شتاب‌ســنج) موقعیت نسبی شما را تخمین می‌زنند. بنابراین اگر **Location** را خاموش کرده‌اید ولی هنوز شک دارید، بهتر است بلوتوث و **Wi-Fi** را نیز در مواقع غیرضروری غیرفعال نگه دارید.

بخش سوم: مدیریت مجوزها در iOS (آیفون و آیپد)

در **iOS**، کنترل دسترســی‌ها نســبتاً دقیــق و قابل‌اعتماد طراحی شده است.

دسترسی به دوربین و میکروفون:

- مســیر :**Settings > Privacy & Security > Camera / Microphone**
- در این بخش می‌توانید مشــاهده کنید کدام اپلیکیشن‌ها به میکروفون یا دوربین دسترســی دارند و با یک کلید ساده، آن را غیرفعال نمایید.

هــرگاه اپی از میکروفون یا دوربین اســتفاده کند، نمادی نارنجی یا ســبز در گوشــه بالای صفحه ظاهر می‌شــود. این نشانه‌ها هشداری مستقیم از سیستم‌عامل هستند.

موقعیت مکانی:

- مســیر :**Settings > Privacy & Security > Location Services**
- هر برنامه را به‌صورت جداگانه بررسی کنید:
  - **Never**: هرگز مجاز نیست.
  - **Ask Next Time Or When I Share**: فقــط در صورت نیاز یا درخواست.
  - **While Using the App**: فقط هنگام استفاده از برنامه.
  - **Always**: همیشه مجاز است.

در صــورت فعال بــودن گزینــه **System Services**، می‌توانید خدمات سیستمی خاص مانند **Location-Based Alerts** یا **Share My Location** را نیز تنظیم کنید.

بخش چهارم: ویندوز (Windows 10 / 11)

ویــندوز نیز از طریق تنظیمات بخــش حریم خصوصی، کنترل نســبتاً خوبــی بر دسترســی‌های مربوط بــه دوربین، میکروفون و موقعیت مکانی ارائه می‌دهد.

دوربین و میکروفون:

- مســیر :**Settings > Privacy > Camera / Microphone**
- در ایــن صفحه، گزینه‌ای برای غیرفعال کردن کلی این قابلیت‌هــا و همچنین فهرســتی از برنامه‌هایی که دسترســی دارند وجود دارد.

نکتــه: اگر می‌خواهید دسترســی به میکروفــون را کاملاً مســدود کنیــد، می‌توانید آن را در ســطح ســخت‌افزاری از **Device Manager** غیرفعال نمایید.

موقعیت مکانی:

- مسیر **Settings > Privacy > Location**:
- در این بخش، می‌توانیــد تاریخچه مکان را پاک کنید، دسترســی کلی را غیرفعال کرده یا به‌صــورت برنامه‌به‌برنامه مجوز صادر نمایید.

بخش پنجم: macOS (مک‌اواس)

در مک، اپل سیاســت‌های ســخت‌گیرانه‌ای در خصوص دسترسی به سخت‌افزارهای حسی اعمال کرده است.

- مســیر :**System Preferences > Security & Privacy > Privacy**
- در پنجره سمت چپ، مواردی مانند **Microphone**، **Camera** و **Location Services** فهرست شده‌اند.
- با انتخاب هرکدام، می‌توانید مجوز دسترسی برنامه‌ها را بررسی و در صورت لزوم حذف کنید.

نکته امنیتی: برخی بدافزارها ممکن است با جعل امضا یا سوءاســتفاده از دسترسی‌های قدیمی، به این منابع دست پیدا کنند. بنابراین بررسی منظم این بخش اهمیت زیادی دارد.

بخش ششم: توصیه‌های تکمیلی برای امنیت بیشتر

- کاور فیزیکی برای دوربین لپ‌تاپ یا گوشی تهیه کنید. راه‌حلی ساده ولی بسیار مؤثر.
- از نرم‌افزارهایــی ماننــد **App Permissions Manager** یــا **Bouncer** (در اندروید) برای کنترل دقیق و لحظه‌ای دسترسی‌ها استفاده کنید.
- در صــورت اســتفاده از دســتیارهای صوتــی (**Siri**، **Google Assistant**)، تنظیمــات مربــوط به ضبط صدا و نگهداری داده‌ها را مرور و در صورت تمایل غیرفعال نمایید.
- در مرورگرها، اجازه دسترسی به موقعیت یا میکروفون را فقط به سایت‌های قابل‌اعتماد بدهید.
- هنگام نصــب برنامه‌های جدید، قبل از فشــردن دکمه «اجازه»، مجوزهای درخواست‌شده را دقیق مطالعه کنید.

جمع‌بندی

کنترل دسترســی به دوربین، میکروفون و موقعیت مکانی، نه‌تنهــا یک اقدام تکنیکی بلکه یک اصل بنیادین در حفاظت از حریم خصوصی و امنیت دیجیتال است. در عصری که فناوری به‌ســرعت در حال پیشروی است، داشتن دانش و آمادگی لازم بــرای مدیریت مجوزهــا، از کاربر عادی یک کاربر هوشــمند می‌ســازد. رعایت نکات ساده‌ای مانند بازبینی مجوزها، استفاده از ابزارهای کنترل دسترسی و تنظیم دقیق سیستم‌عامل، به میزان چشمگیری ریسک شنود، ردیابی یا تصویربرداری غیرمجاز را کاهش می‌دهد. در پایان این راهنما، توصیه می‌شود خوانندگان محترم، تنظیمات دستگاه‌های شــخصی و اداری خود را همین امروز مرور کرده و اطمینان حاصل نمایند که تنها کسانی اجازه شــنیدن، دیدن و دنبال‌کردن آن‌هــا را دارند که واقعاً باید چنین اجازه‌ای داشته باشند.

CASE STUDY

مطالعه موردی

همه‌چی از تماس تصویری با خواهرم شروع شد...

صدای زنگ تماس تصویری که در فضای خانه پیچید، مثل همیشه خوشحال‌کننده بود. «امیر» برادرم بود که از اروپا تماس می‌گرفت تا بعد از مدتی بی‌خبری، چند دقیقه‌ای حرف بزنیم. لپ‌تاپ رو باز کردم، روی مبل نشستم و تماس رو جواب دادم. اتاق پشت سرم مرتب بود، نور ملایم، اینترنت پایدار. همه‌چیز عادی به‌نظر می‌رسید. ولی هیچ‌وقت فکرش رو نمی‌کردم که این تماس تصویری، مقدمه‌ی یکی از جدی‌ترین نشت‌های اطلاعاتی زندگی کاری‌م باشه.

من کارمند واحد مالی یک شـرکت خصوصی هسـتم. اون روز بعدازظهر، بعد از یک جلسـه‌ی نیم‌ساعته‌ی آنلاین با مدیر مالـی که در مورد بودجه‌ی پروژه‌ی جدید صحبت کرده بودیم، سیسـتم رو به حالت Sleep گذاشـتم. لپ‌تاپ همچنان روشن بـود. نرم‌افزارهایی مثـل Teams، Excel و حتی یه مرورگر باز، بدون بسته‌شـدن در بک‌گراند باقـی موندن. من فکر کردم همه‌چیز امنه چون سیسـتمم پسورد داره و کسی بهش دسترسی فیزیکـی نداره. امـا واقعیت اینه که «فیزیکی» بـودن دیگه تنها خطر نیست.

تمـاس تصویری با بردارم حدود ٤٠ دقیقه طول کشـید. در حین تماس، صحبت‌هامون صرفاً خانوادگی بود، اما همون‌طور کـه می‌خندیدیم و گـپ می‌زدیم، من گاهی ناخـودآگاه روی صفحـه‌ی مانیتور نیم‌نگاهی به فایل‌هایـی که باز بودن انداختم: اکسـل‌های حقوق و مزایا، یه سـند محرمانه‌ی PDF درباره‌ی وضعیت مالی شـرکت، و یک ایمیل حاوی گزارش بدهی‌های بانکی پروژه.

فقط چنـد روز بعد، یـه اتفاق عجیب افتاد. مدیر سیسـتم شـرکت متوجه شد که آدرس IP ناشناسـی شب‌ها به VPN شـرکت وصل می‌شـه. بررسی دقیق‌تر نشـون داد که از همون دسـتگاه من، خارج از ساعت کاری، فعالیت‌هایی انجام شده که با سـبک کار من مطابقت نداشـت. موضوع امنیتی اعلام شد و بررسی‌های فنی شروع شد.

نتیجـه‌ی نهایی خیلی شـگفت‌انگیز نبود: بدافـزاری که از طریق یـک پلاگین آلـوده‌ی نصب‌شـده روی مرورگـر وارد سیسـتم شده بود، در پس‌زمینه فعال مونده بود و با دسترسی به دوربیـن و میکروفون، تماس تصویـری من رو ضبط کرده بود. در بازتاب صفحه‌نمایش روی عینک من، حتی بخشـی از فایل اکسـل مشخص شده بود. صداهای محیطی و کلیدواژه‌هایی که در طول تماس گفتم، ابزارهای هوشـمند تجزیه‌وتحلیل صدای نفوذگرها رو تغذیه کرده بود.

درس‌هایی که گرفتم:

۱. تماس تصویری در فضای کاری، حتی با افراد خانوادگی، می‌تونه پنجره‌ای باشـه بـرای لو رفتن اطلاعـات. گاهی حتی بازتاب مانیتور روی عینک، فنجان براق یا پنجره‌ی پشت‌سرتون اطلاعات حساس رو فاش می‌کنه.

۲. بعد از کار، فقط قفل‌کردن یا Sleep کردن لپ‌تاپ کافی نیست. باید نرم‌افزارها بسته بشن و از حساب‌های کاری خارج بشین.

۳. نصب هر نوع افزونه یا پلاگین مشـکوک روی مرورگر، ممکنه دروازه‌ی اصلی حمله باشـه. به‌خصوص پلاگین‌هایی که دسترسی به تب‌های باز و دوربین می‌گیرن.

٤. تنظیمـات پیش‌فـرض نرم‌افزارهـای تمـاس تصویری، معمولاً برای راحتی کار طراحی شدن، نه امنیت. باید مجوزهای دوربین و میکروفون بعد از استفاده غیرفعال بشن.

۵. درک نکردن نقش داده‌های محیطی مثل صدای پس‌زمینه، تصویر میز کار، یا حتی آیکون‌های دسکتاپ، یکی از اشتباهات متداول کاربرهاست.

در پایان:

بعد از بررسی کامل، سیستم من فرمت شد، همه رمزها تغییر داده شد، و روی اسـتفاده از دستگاه شخصی برای فعالیت‌های سـازمانی محدودیت‌هایی اعمال شـد. حالا قبـل از هر تماس تصویـری، صفحه‌نمایش رو خاموش می‌کنـم یا لپ‌تاپ رو به سمتی می‌چرخونم که پشت سـرم کاملاً خنثی باشه. یاد گرفتم که امنیت سـایبری، فقط درباره‌ی رمز عبور و فایروال نیسـت؛ گاهی همه‌چیز از یک تمـاس بی‌ضرر با عزیزترین فرد زندگی شروع می‌شه...

موضوع ویژه

دستیار صوتی، شنود خانگی؟

آیا Siri، Google Assistant و Alexa حریم خصوصی ما را تهدید می‌کنند؟

در سال‌های اخیر، دستیارهای صوتی هوشمند به‌سرعت جای خود را در خانه‌ها، محل کار و حتی خودروها باز کرده‌اند. کاربر تنها با گفتن عبارتی ساده مانند «Hey Google» یا «Hey Siri» می‌تواند موسیقی پخش کند، قرار ملاقات تنظیم کند یا پاسخ سؤالات روزمره‌اش را بگیرد. اما همان‌قدر که این ابزارها در ظاهر، زندگی را آسان‌تر کرده‌اند، نگرانی‌هایی جدی درباره‌ی حریم خصوصی نیز به همراه آورده‌اند؛ نگرانی‌هایی که دیگر صرفاً حدس و گمان نیستند، بلکه با شواهد و گزارش‌های رسمی نیز تقویت شده‌اند.

شنود فعال حتی بدون دستور مستقیم

بسیاری از کاربران تصور می‌کنند دستیارهای صوتی تنها زمانی شروع به شنود می‌کنند که با گفتن کلمه‌ی فعال‌ساز مانند «Hey Google» یا «Alexa» آن‌ها را فرا بخوانند. در حالی که واقعیت این است که این ابزارها به‌طور مداوم در حال گوش‌دادن هستند تا بتوانند فرمان را به‌موقع تشخیص دهند. این فرآیند نیاز به دسترسی دائمی به میکروفون دستگاه دارد.

طبق افشاگری‌ها و اسناد برخی سازمان‌های خبری، در مواردی حتی زمانی که کاربر تصور می‌کرد گفت‌وگویش خصوصی است، بخشی از مکالمات به سرورهای شرکت‌های سازنده منتقل شده‌اند. در چندین مورد، کارمندانی که وظیفه تحلیل داده‌های صوتی را داشتند، اذعان کرده‌اند که مکالمات خصوصی کاربران را شنیده‌اند.

پردازش صدا در سرورهای ابری

اگرچه بخشی از پردازش دستورات صوتی ممکن است به‌صورت محلی (روی خود دستگاه) انجام شود، اما بسیاری از عملیات‌های پیچیده‌تر نیاز به انتقال داده‌ها به سرورهای ابری دارند. این بدان معناست که صدای کاربر از دستگاه او به سرورهای شرکتی مانند گوگل، اپل یا آمازون منتقل می‌شود. در این مسیر، اگر ارتباط به‌درستی رمزگذاری نشده باشد، امکان شنود و دست‌کاری اطلاعات وجود دارد. علاوه بر آن، ذخیره‌سازی صداها روی سرورها، آن‌ها را در معرض خطر نفوذ سایبری یا حتی سوءاستفاده داخلی قرار می‌دهد.

سابقه‌ی گزارش‌های نقض حریم خصوصی

در سال‌های اخیر، چندین بار شاهد انتشار گزارش‌هایی مبنی بر سوءاستفاده از دستیارهای صوتی بوده‌ایم. به‌عنوان مثال:

- در سال ۲۰۱۹، افشا شد که آمازون فایل‌های صوتی ضبط‌شده توسط Alexa را برای تحلیل به پیمانکاران شخص ثالث داده است.
- گوگل نیز پذیرفت که بخشی از مکالمات ضبط‌شده توسط Google Assistant به‌صورت دستی توسط تحلیل‌گران انسانی بررسی می‌شوند.
- اپل پس از فشار رسانه‌ها، در سال ۲۰۱۹ اعلام کرد که سیاست‌های مربوط به دسترسی به داده‌های کاربران در Siri را اصلاح خواهد کرد.

حریم خصوصی در خانه و محل کار

نگرانی اصلی اینجاست که دستگاه‌های دارای دستیار صوتی نه فقط در خانه، بلکه در محیط‌های کاری نیز استفاده می‌شوند. در بسیاری از جلسات کاری، این ابزارها روی میز حضور دارند و به‌صورت ناخواسته ممکن است اطلاعات تجاری حساس، مذاکرات، یا حتی مکالمات مالی را ثبت کنند. حتی اگر این ثبت‌ها عمدی نباشند، وجود فایل صوتی روی حافظه دستگاه یا در سرور، خود یک ریسک امنیتی جدی است.

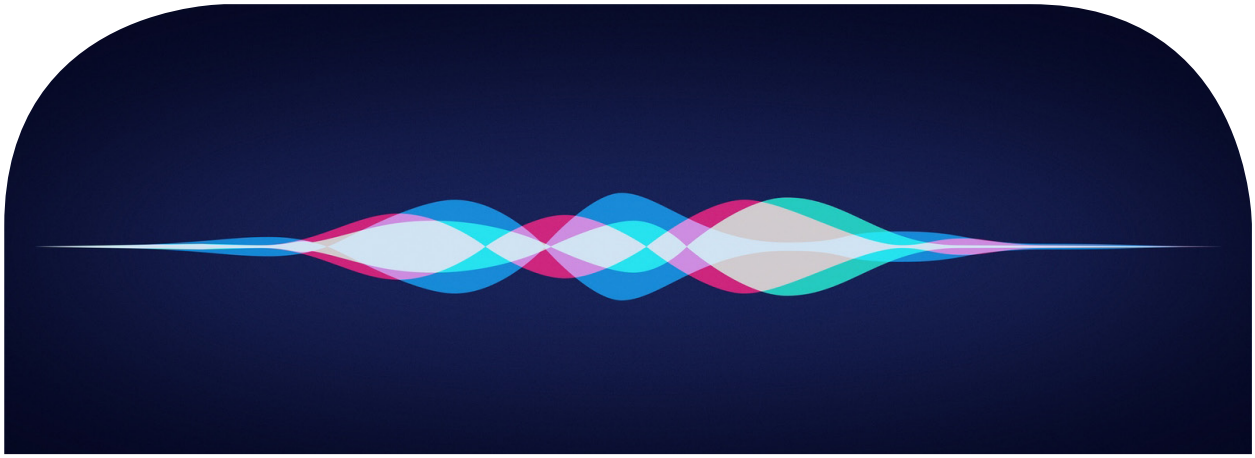
چگونه این ریسک را مدیریت کنیم؟

در کنار انتقادها، راهکارهایی هم برای افزایش ایمنی و حفظ حریم خصوصی هنگام استفاده از دستیارهای صوتی وجود دارد:

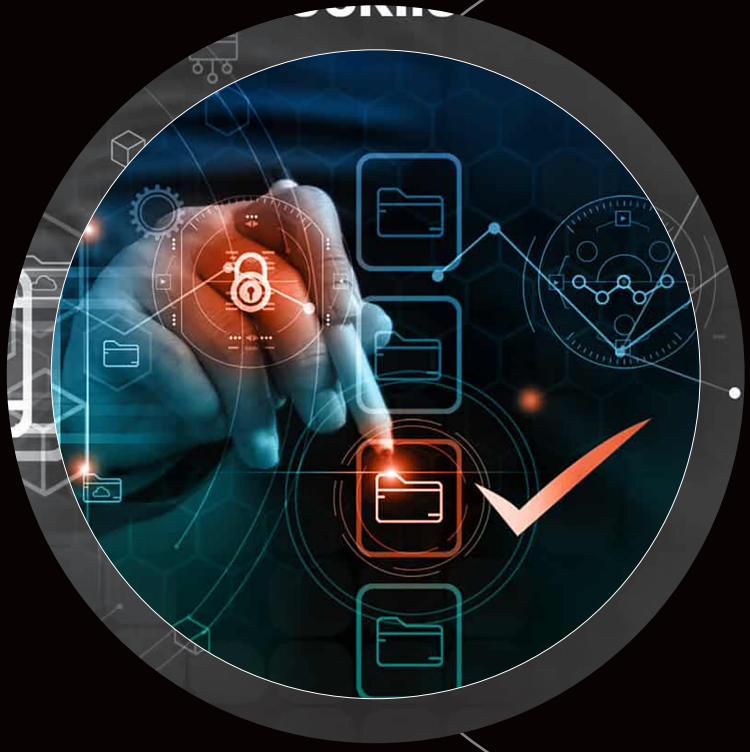
- بررسی و مدیریت دسترسی‌ها: تنظیمات دستگاه را مرور کرده و دسترسی‌های میکروفون و اینترنت را محدود کنید.
- غیرفعال‌سازی دائم یا موقت دستیار صوتی: اگر نیازی به آن ندارید، قابلیت دستیار صوتی را از تنظیمات دستگاه غیرفعال کنید.
- حذف تاریخچه صوتی: در تنظیمات حساب گوگل یا آمازون، امکان حذف دستورات صوتی ثبت‌شده وجود دارد.
- استفاده در مکان‌های کنترل‌شده: از قرار دادن دستگاه‌های دارای میکروفون فعال در جلسات مهم کاری یا اتاق‌هایی که مکالمات حساس در آن‌ها انجام می‌شود، خودداری کنید.

جمع‌بندی

دستیارهای صوتی هوشمند، بدون شک یکی از پیشرفت‌های چشم‌گیر در حوزه تکنولوژی هستند. اما نباید فراموش کرد که هرچه فناوری بیشتر با زندگی ما آمیخته شود، اهمیت مراقبت از حریم خصوصی نیز چند برابر می‌شود. همان‌طور که به راحتی به آن‌ها فرمان می‌دهیم، باید با همان دقت، دسترسی‌شان به اطلاعات‌مان را هم کنترل کنیم. تکنولوژی باید در خدمت ما باشد، نه در نقش نظاره‌گر پنهانی که لحظه‌به‌لحظه کنار ماست.



CHECKLIST



چک‌لیست ...

۸ کار ساده برای کاهش ریسک شنود دیجیتال در خانه و محل کار

چگونه با چند اقدام هوشمندانه، از میکروفون‌ها، دوربین‌ها و دستگاه‌های هوشمند خود محافظت کنیم؟ در دنیای امروزی، که در آن ابزارهای دیجیتال به بخشی جدایی‌ناپذیر از زندگی شخصی و کاری ما تبدیل شده‌اند، مراقبت از حریم خصوصی دیگر فقط یک انتخاب نیست؛ بلکه یک ضرورت است. با گسترش دستگاه‌هایی مانند گوشی‌های هوشمند، لپ‌تاپ‌ها، دستیارهای صوتی، دوربین‌های مداربسته متصل به اینترنت، و حتی ساعت‌های هوشمند، خطراتی مانند شنود دیجیتال و جمع‌آوری مخفیانه‌ی اطلاعات صوتی یا تصویری به طرز نگران‌کننده‌ای افزایش یافته‌اند.

این چک‌لیست، هشت اقدام ساده اما بسیار مؤثر را پیشنهاد می‌دهد که با اجرای آن‌ها می‌توانید به‌طور قابل توجهی خطر شنود ناخواسته را کاهش دهید – چه در محیط خانه و چه در فضای کاری. این اقدامات نیاز به تخصص فنی پیچیده ندارند و اغلب با چند تنظیم ساده قابل پیاده‌سازی‌اند.

غیرفعال‌سازی دستیارهای صوتی در دستگاه‌های هوشمند

اولین گام برای کاهش ریسک شنود، بررسی وضعیت دستیارهای صوتی مانند Google Assistant، Siri و Alexa است. این ابزارها به‌طور پیش‌فرض، همیشه در حال شنود کلمات بیدارباش (wake word) هستند. در بسیاری از موارد، این شنود منجر به ضبط و ارسال ناخواسته‌ی صداهای اطراف به سرورهای شرکت‌های سازنده می‌شود.

اقدامات پیشنهادی:

- اگر از دستیار صوتی استفاده نمی‌کنید، آن را به‌طور کامل از تنظیمات غیرفعال کنید.
- در گوشی‌های اندروید: به Settings > Google > Settings for Google Apps > Search, Assistant & Voice > Voice Match بروید و گزینه‌ی Hey Google را خاموش کنید.
- در دستگاه‌های اپل: در Settings، گزینه‌ی Siri & Search را یافته و «Listen for Hey Siri» را غیرفعال کنید.
- در دستگاه‌های Alexa، با مراجعه به اپلیکیشن Amazon Alexa می‌توانید میکروفون را غیرفعال کنید.

غیرفعال‌سازی این قابلیت‌ها نه‌تنها حریم خصوصی شما را بهبود می‌دهد، بلکه از ارسال‌های ناخواسته‌ی صوت به شرکت‌های ثالث نیز جلوگیری می‌کند.

استفاده از پوشش‌های فیزیکی برای دوربین و میکروفون

شاید ساده‌ترین و مؤثرترین اقدام، استفاده از پوشش‌های فیزیکی برای جلوگیری از شنود و تصویربرداری باشد. این پوشش‌ها می‌توانند قطعه‌ای کوچک از نوار چسب، یا ابزارهای مخصوصی باشند که به‌طور کشویی یا مغناطیسی روی دوربین قرار می‌گیرند.

چرا مهم است؟

در بسیاری از حملات سایبری، هکرها پس از دسترسی به سیستم قربانی، دوربین یا میکروفون را فعال کرده و بدون اطلاع کاربر، اقدام به ضبط اطلاعات می‌کنند. این نوع حملات خصوصاً در لپ‌تاپ‌ها و وب‌کم‌های خارجی بسیار رایج هستند.

اقدامات پیشنهادی:

- روی دوربین لپ‌تاپ و تبلت خود از پوشش‌های کشویی یا چسب مات استفاده کنید.
- در صورت عدم نیاز، میکروفون‌های خارجی را از دستگاه جدا یا غیرفعال کنید.
- برخی افراد حتی میکروفون موبایل خود را با ماده‌ای جذب‌کننده صدا می‌پوشانند — راه‌حلی افراطی ولی مؤثر در شرایط خاص.

محدود کردن دسترسی اپلیکیشن‌ها به میکروفون و دوربین

بسیاری از اپلیکیشن‌ها، به‌طور پیش‌فرض درخواست دسترسی به میکروفون و دوربین می‌کنند، حتی در زمانی که این دسترسی برای عملکرد اصلی آن‌ها ضروری نیست. با محدودسازی این دسترسی‌ها، از شنودهای ناخواسته جلوگیری می‌شود.

اقدامات پیشنهادی:

- در اندروید: Settings > Privacy > Permission Manager > Microphone و Camera
- در iOS: Settings > Privacy & Security > Microphone و Camera
- دسترسی‌هایی که ضرورتی ندارند را غیرفعال کنید.

به‌یاد داشته باشید که بسیاری از اپ‌ها حتی پس از بستن نیز می‌توانند در پس‌زمینه اجرا شوند و به این سخت‌افزارها دسترسی داشته باشند.

بررسی دستگاه‌های متصل به شبکه‌ی خانگی یا اداری

بسیاری از دستگاه‌هایی که به اینترنت متصل‌اند، مانند دوربین‌های مداربسته، اسپیکرهای هوشمند، چاپگرها، یا حتی تلویزیون‌های هوشمند، می‌توانند آسیب‌پذیر باشند یا اطلاعات حساس شما را منتقل کنند.

اقدامات پیشنهادی:

- از طریق پنل مدیریت مودم یا روتر، لیست دستگاه‌های متصل را بررسی کنید.
- دستگاه‌های مشکوک یا ناشناس را بلاک کنید.
- نام شبکه (SSID) خود را طوری انتخاب کنید که حاوی اطلاعات شخصی نباشد (مثلاً نام خانوادگی یا محل کار).
- رمز عبور شبکه را به‌طور دوره‌ای تغییر دهید و از رمزهای قوی استفاده کنید.

استفاده از نرم‌افزارهای امنیتی معتبر برای شناسایی شنود

نرم‌افزارهای امنیتی و ضدجاسوسی (Anti-Spyware) یکی از ابزارهای مهم برای بررسی و مقابله با شنود دیجیتال هستند. این برنامه‌ها می‌توانند دسترسی‌های پنهانی، فعالیت‌های غیرمعمول، و حتی اجرای سرویس‌هایی که در ظاهر خاموش‌اند را شناسایی کنند.

اقدامات پیشنهادی:

- استفاده از آنتی‌ویروس‌های معتبر با قابلیت real-time protection مانند Kaspersky، Bitdefender یا Norton
- نصب نرم‌افزارهایی مخصوص تشخیص جاسوس‌افزار مانند Malwarebytes یا Spybot
- انجام اسکن منظم از سیستم و موبایل
- بررسی لاگ‌های دسترسی در سیستم‌عامل‌هایی مثل اندروید یا ویندوز برای شناسایی رفتار مشکوک

توجه داشته باشید که برخی بدافزارها توانایی مخفی شدن از ابزارهای معمول را دارند، بنابراین انتخاب نرم‌افزارهای قدرتمند بسیار حیاتی است.

به‌روزرسانی منظم سیستم‌عامل‌ها و فریم‌ورک دستگاه‌های هوشمند

یکی از روش‌های رایج نفوذ به دستگاه‌ها، سوءاستفاده از آسیب‌پذیری‌های امنیتی در نسخه‌های قدیمی سیستم‌عامل‌هاست. به‌روزرسانی‌های امنیتی منتشرشده از سوی شرکت‌های سازنده، در اغلب موارد این آسیب‌پذیری‌ها را برطرف می‌کنند.

اقدامات پیشنهادی:

- به‌روزرسانی مرتب گوشی‌های موبایل، لپ‌تاپ، تبلت، و حتی ساعت‌های هوشمند
- در دستگاه‌های اندرویدی: Settings > Software Update
- در دستگاه‌های اپل: Settings > General > Software Update
- در سیستم‌های ویندوزی: Settings > Update & Security
- بررسی مرتب صفحه‌های پشتیبانی شرکت‌های سازنده برای اطلاع از آسیب‌پذیری‌های مهم

دستگاه‌هایی مثل دوربین‌های تحت شبکه، پرینترهای وایرلس و اسپیکرهای هوشمند هم باید به‌روزرسانی شوند.

تفکیک فضای کاری از فضای شخصی

ترکیب فضای کاری و شخصی در یک دستگاه یا شبکه، خطر نشت داده‌ها و شنود را افزایش می‌دهد. بسیاری از حملات شنود، از طریق اپلیکیشن‌های سرگرمی یا اجتماعی به سیستم‌های کاری راه پیدا می‌کنند.

اقدامات پیشنهادی:

- استفاده از دستگاه جداگانه برای کار و امور شخصی
- عدم نصب اپلیکیشن‌های غیرضروری بر روی دستگاه کاری
- استفاده از مرورگرهای جداگانه برای حساب‌های کاری و شخصی (مثلاً Chrome برای کار، فایرفاکس برای شخصی)
- تعریف پروفایل‌های مجزا در ویندوز یا اندروید برای تفکیک فعالیت‌ها

این تفکیک ساده، نه‌تنها خطر شنود را کاهش می‌دهد، بلکه مدیریت امنیت را نیز ساده‌تر می‌کند.

آموزش کاربران خانواده یا همکاران درباره شنود دیجیتال

تکنولوژی فقط توسط متخصصین استفاده نمی‌شود؛ اعضای خانواده، همکاران، و حتی کودکان نیز به دستگاه‌های متصل به اینترنت دسترسی دارند. در بسیاری از موارد، اقدامات ناآگاهانه‌ی یکی از اعضا می‌تواند باعث شنود یا نشت اطلاعات همه شود.

اقدامات پیشنهادی:

- برگزاری جلسه‌های آموزشی ساده برای خانواده یا تیم کاری درباره اهمیت امنیت صدا و تصویر
- اطلاع‌رسانی درباره خطرات نصب اپلیکیشن‌های مشکوک
- آموزش بررسی دسترسی‌ها و تنظیمات حریم خصوصی در گوشی یا لپ‌تاپ
- توصیه به عدم استفاده از وای‌فای عمومی برای جلسات آنلاین یا تماس‌های کاری

می‌توان در محیط‌های کاری، جزوه‌های ساده یا بروشورهای آموزشی منتشر کرد تا آگاهی عمومی بالا برود.

جمع‌بندی

شنود دیجیتال دیگر فقط تهدیدی در فیلم‌های جاسوسی نیست؛ بلکه واقعیتی است که هر روز به شکل پنهان‌تر و پیچیده‌تری در زندگی روزمره ما نفوذ می‌کند. اما خبر خوب این است که با رعایت چند اقدام ساده و کاملاً کاربردی، می‌توان ریسک این تهدید را به‌طور قابل توجهی کاهش داد. این چک‌لیست هشت‌گانه را می‌توان در هر خانه یا محیط کاری اجرا کرد، بدون نیاز به دانش فنی خاص یا سرمایه‌گذاری زیاد. از خاموش‌کردن یک دستیار صوتی تا استفاده از پوشش دوربین، همین کارهای کوچک هستند که از حریم خصوصی ما محافظت می‌کنند.

در پایان فراموش نکنیم: شنود دیجیتال فقط با نفوذ فنی اتفاق نمی‌افتد، بلکه اغلب از غفلت کاربران آغاز می‌شود. آگاهی، مهم‌ترین سپر ما در برابر این تهدید است.

اخبار امنیتی •••

افشای گزارش محرمانه‌ی نهادهای امنیتی در مورد شنود از طریق دستگاه‌های هوشمند

آیا خانه‌هایمان هنوز امن‌اند؟
در دنیای امروز، ابزارهای هوشمند به‌سرعت در حال نفوذ به خانه‌ها، دفاتر و حتی کیف‌های روزمره ما هستند. تلویزیون‌هایی که به اینترنت متصل‌اند، دستیارهای صوتی که همواره گوش می‌دهند، گوشی‌هایی که می‌توانند صدا و تصویر ما را ثبت کنند و حتی لامپ‌هایی که با اپلیکیشن کنترل می‌شوند. اما آیا تا به حال فکر کرده‌ایم که این ابزارها ممکن است «گوش‌های نامرئی» قدرت‌های بزرگ یا حتی مجرمان سایبری باشند؟

در هفته‌های اخیر، گزارشی محرمانه که از یک نهاد امنیتی فاش شده، بحث گسترده‌ای را در فضای عمومی و تخصصی به راه انداخته است. این گزارش نشان می‌دهد که برخی دولت‌ها، آژانس‌های اطلاعاتی و حتی بازیگران ناشناس از دستگاه‌های هوشمند برای شنود صوتی، تصویری و حتی موقعیت مکانی کاربران استفاده می‌کنند – آن هم بدون اطلاع یا رضایت آن‌ها.

افشای اطلاعات از درون NSA و GCHQ

ریشه اصلی این افشاگری، به اسناد منتشرشده توسط ادوارد اسنودن در سال‌های گذشته بازمی‌گردد؛ اما آنچه اخیراً توجه‌ها را جلب کرده، نسخه‌ی جدیدی از گزارش‌های داخلی NSA (آژانس امنیت ملی آمریکا) و GCHQ (آژانس ارتباطات دولت بریتانیا) است که به‌طور خاص بر شنود از طریق دستگاه‌های مصرفی تمرکز دارد.

طبق این گزارش، پروژه‌هایی با نام رمزهایی مانند Squeaky Dolphin، Optic Nerve و WALKING SHADOW وجود داشته‌اند که به کمک آن‌ها، صدها میلیون کاربر در سراسر جهان مورد شنود قرار گرفته‌اند – صرفاً از طریق ابزارهایی که خودشان خریداری و نصب کرده‌اند.

در یکی از بخش‌های این سند آمده است:

هدف ما دستیابی به صدای محیط، بدون نیاز به نفوذ فیزیکی، و تنها از طریق پروتکل‌های اینترنت اشیاء است. ابزارهای هدف شامل تلویزیون‌های هوشمند، دستگاه‌های پخش صوت، دوربین‌های نظارتی و دستیارهای صوتی است.

تلویزیون‌های هوشمند؛ چشم‌هایی همیشه باز

یکی از ابزارهایی که به‌طور خاص در این گزارش به آن اشاره شده، تلویزیون‌های هوشمند سامسونگ و LG است که در سال‌های اخیر قابلیت شنود صوتی در پس‌زمینه را فعال کرده‌اند. در بسیاری از این مدل‌ها، قابلیتی وجود دارد که به‌صورت دائم «کلمات کلیدی» مانند «Hi TV» را شنود می‌کند تا در صورت شنیدن آن، به فرمان صوتی پاسخ دهد.

اما این ویژگی بهانه‌ای شده برای استخراج اطلاعات شخصی. طبق گزارشات، اطلاعات ضبط‌شده از صدای اتاق نشیمن، از طریق سرورهای شرکت‌های واسطه به سرورهای ابری منتقل می‌شود. این داده‌ها می‌توانند شامل مکالمات خصوصی خانوادگی، اطلاعات مالی، و حتی صحبت‌های مربوط به محل کار باشند.

برخی از تولیدکنندگان، پس از اعتراض عمومی، گزینه‌ای برای غیرفعال‌سازی این قابلیت اضافه کرده‌اند – اما نکته مهم این است که بسیاری از کاربران حتی از وجود این تنظیمات اطلاعی ندارند.

دستیارهای صوتی؛ ابزار شنود داوطلبانه؟

Siri، Amazon Alexa، Google Assistant، و Cortana از جمله محبوب‌ترین دستیارهای صوتی جهان هستند. در ظاهر، آن‌ها ابزارهایی برای تسهیل زندگی دیجیتال‌اند: تنظیم آلارم، پخش موسیقی، یادآوری جلسات. اما در باطن، این دستیارها همواره در حال شنیدن‌اند – حتی وقتی کاربر حرفی نمی‌زند.

بررسی‌های انجام‌شده توسط محققان امنیتی نشان می‌دهد که این دستگاه‌ها گاهی بدون گفتن کلمه‌ی کلیدی نیز فعال می‌شوند و شروع به ضبط می‌کنند. در یکی از پرونده‌های داخلی شرکت آمازون، یک مکالمه خصوصی بین دو کاربر، بدون اطلاع آن‌ها ضبط و برای بازبینی به کارکنان این شرکت فرستاده شده بود.

علاوه بر این، گزارش فاش‌شده نشان می‌دهد که نهادهای اطلاعاتی برخی کشورها، با استفاده از آسیب‌پذیری‌های نرم‌افزاری در این دستیارها، می‌توانند آن‌ها را به ابزار شنود دائمی تبدیل کنند – بدون آن‌که حتی چراغ دستگاه روشن شود یا هشداری نمایش داده شود.

شنود از منابع غیرمنتظره
وقتی دیوارها هم گوش دارند

در حالی که اغلب مردم تصور می‌کنند فقط گوشی یا لپ‌تاپ ممکن است آن‌ها را شنود کند، یافته‌های جدیدتر نشان می‌دهد حتی منابعی مثل لامپ‌های هوشمند، پریزهای برق، و دستگاه‌های تهویه می‌توانند ابزار شنود شوند.

در یک پژوهش دانشگاهی در هلند، نشان داده شد که می‌توان با بررسی تغییرات شدت نور LED یک لامپ هوشمند در اتاق، صدای مکالمات را با دقت قابل‌توجهی بازسازی کرد. این پژوهش از الگوریتم‌های هوش مصنوعی برای تحلیل نوسانات نور استفاده کرده بود – بدون نیاز به هیچ میکروفونی.

در پرونده‌ای دیگر که در آلمان فاش شد، مشخص شد یک شرکت سازنده اسپیکرهای بلوتوث، بخشی از داده‌های صوتی کاربران را به سرورهای واقع در چین ارسال می‌کرده، و از طریق آن الگوریتم‌هایی برای شناسایی الگوهای گفتاری کاربران توسعه می‌داده است.

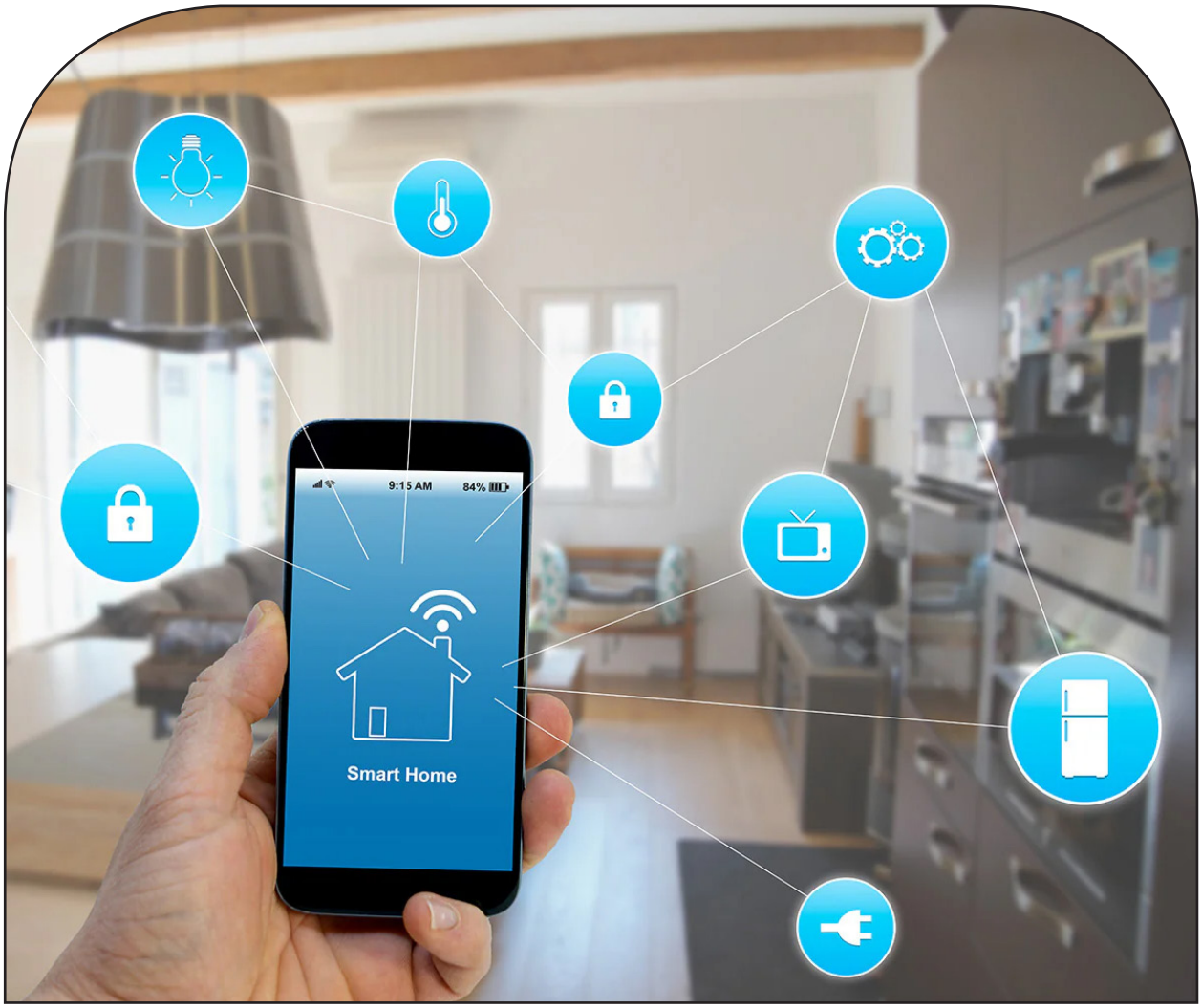
این‌ها تنها نمونه‌هایی از کاربردهای غیراخلاقی داده‌های محیطی در دستگاه‌هایی هستند که ظاهراً قرار است برای رفاه و آسایش ما کار کنند.

واکنش شرکت‌های فناوری؛ سکوت، بیانیه یا اصلاح؟

پس از افشای این اطلاعات، شرکت‌هایی مثل گوگل، آمازون، سامسونگ و اپل مجبور به پاسخ‌گویی شدند. برخی در بیانیه‌هایی اعلام کردند که داده‌های کاربران تنها برای بهبود خدمات جمع‌آوری می‌شود و هیچ سوءاستفاده‌ای در کار نیست. اما واقعیت این است که کاربران اغلب از حجم و نوع داده‌هایی که جمع‌آوری می‌شود، اطلاعی ندارند – و این همان چیزی است که نهادهای حقوق بشری به آن اعتراض دارند.

برای مثال، در یکی از قراردادهای کاربری دستیار صوتی Alexa آمده بود که «ممکن است برخی مکالمات برای بازبینی توسط انسان، از سرور استخراج شوند». این یعنی حتی بدون نیت تجسسی، داده‌های شما ممکن است توسط اشخاص ثالث بازشنوی و تحلیل شوند.

گوگل در واکنش به گزارش‌های اخیر، بخشی از تنظیمات



محرمانگی خود را به‌روز کرد و گزینه‌هایی برای حذف تاریخچه صوتی در اختیار کاربران گذاشت. اما این اقدامات بیشتر به‌نظر می‌رسد پاسخی به فشار رسانه‌ای باشد تا تغییر در فلسفه‌ی طراحی محصولات.

مسئولیت کاربران: غیرفعال‌سازی، محدودسازی، آگاهی

با وجود همه‌ی این تهدیدها، باید پذیرفت که بخشی از امنیت در دستان خود کاربران است. شما می‌توانید با اقداماتی ساده، ریسک شنود را به‌شدت کاهش دهید:

- بررسی مجوزهای اپلیکیشن‌ها: مطمئن شوید که فقط برنامه‌هایی که واقعاً به میکروفون یا دوربین نیاز دارند، دسترسی فعال دارند.
- استفاده از پوشش فیزیکی دوربین لپ‌تاپ: بسیاری از کارشناسان امنیتی توصیه می‌کنند حتی اگر مطمئنید دوربین غیرفعال است، با یک پوشش ساده جلوی آن را بگیرید.
- خاموش‌کردن دستگاه‌های شنود در زمان‌های حساس: هنگام جلسات کاری، تماس‌های خصوصی یا استراحت، دستگاه‌هایی مانند دستیار صوتی یا تلویزیون هوشمند را خاموش کنید.
- بروزرسانی مداوم نرم‌افزارها: بسیاری از حملات از طریق آسیب‌پذیری‌های نسخه‌های قدیمی صورت می‌گیرد.
- استفاده از شبکه‌های امن: در صورت استفاده از دستگاه‌های هوشمند در خانه یا محل کار، مطمئن شوید که رمز عبور شبکه وای‌فای قوی و غیرقابل‌پیش‌بینی است.

نتیجه‌گیری: خانه‌ی هوشمند یا خانه‌ی شیشه‌ای؟

اطلاعاتی که از طریق این گزارش فاش‌شده به‌دست آمده، تصویری نگران‌کننده از آینده‌ای نزدیک را نشان می‌دهد: جایی که خانه‌هایمان نه تنها مأمن و پناهگاه نیستند، بلکه شاید بزرگ‌ترین منبع نشت اطلاعات شخصی ما باشند.

درست است که نمی‌توان جلوی همه تهدیدات را گرفت، اما آگاهی از آن‌ها می‌تواند تفاوت بزرگی در امنیت اطلاعات ما ایجاد کند. اگر بدانیم که چه دستگاهی چه قابلیت‌هایی دارد و چگونه از آن استفاده کنیم، می‌توانیم از خانه‌های هوشمند لذت ببریم – بدون اینکه نگران گوش‌های نامرئی پشت هر دستگاه باشیم.

پس پیش از خرید، نصب و استفاده از هر ابزار هوشمند، از خود بپرسید: آیا این دستگاه واقعاً به این همه دسترسی نیاز دارد؟ و آیا من آماده‌ام برای این راحتی، بخشی از حریم شخصی‌ام را واگذار کنم؟

TOOLS

معرفی ابزار

اپلیکیشن‌ها و تنظیماتی برای محدود کردن دسترسی‌ها به دوربین، میکروفون، لوکیشن

در دنیای پر از فناوری امروز، ابزارهای دیجیتال مثل گوشی‌های هوشمند، لپ‌تاپ‌ها، تبلت‌ها و حتی ساعت‌های هوشمند، بخشی جدایی‌ناپذیر از زندگی ما شده‌اند. این ابزارها امکانات فراوانی در اختیار ما می‌گذارند، اما هم‌زمان به درگاه‌هایی برای دسترسی ناخواسته به اطلاعات شخصی ما تبدیل شده‌اند. دوربین، میکروفون، موقعیت جغرافیایی، فهرست مخاطبین، فایل‌ها و حتی تاریخچه‌ی مرورگر – همگی می‌توانند توسط اپلیکیشن‌ها و سرویس‌ها بدون اطلاع کامل کاربر جمع‌آوری یا شنود شوند.

برای مدیریت این دسترسی‌ها و جلوگیری از نقض حریم خصوصی، مجموعه‌ای از ابزارها و تنظیمات وجود دارد که در ادامه به معرفی کامل آن‌ها می‌پردازیم.

تنظیمات پیش‌فرض سیستم‌عامل: اولین گام دفاعی

در سیستم‌عامل Android:

نسخه‌های جدید اندروید، از جمله Android ۱۲ و ۱۳، امکان مدیریت بسیار دقیق‌تری برای مجوزهای اپلیکیشن فراهم کرده‌اند.

ویژگی‌های کلیدی:

- مشاهده‌ی لحظه‌ای دسترسی‌ها: اندروید در نوار وضعیت، آیکون میکروفون یا دوربین را نمایش می‌دهد اگر اپی در حال استفاده از آن‌ها باشد.
- دسترسی یک‌باره: می‌توانید به اپ‌ها فقط برای یک‌بار دسترسی به دوربین یا موقعیت بدهید.
- مدیریت از طریق Settings > Privacy > Permission Manager

در سیستم‌عامل iOS:

اپل هم در iOS ۱۵ و ۱۶ قابلیت‌های امنیتی خوبی ارائه کرده:

ویژگی‌های کلیدی:

- App Privacy Report: گزارشی دقیق از اینکه چه اپ‌هایی در چه زمان‌هایی به چه داده‌هایی دسترسی داشته‌اند.
- محدود کردن دسترسی به موقعیت دقیق (Approximate Location)
- کنترل میکروفون و دوربین از طریق Settings > Privacy & Security.

اپلیکیشن‌های مدیریت مجوزها (Permission Managers)

AppOps (برای اندروید – نیاز به روت یا ADB)

این اپلیکیشن کنترل عمیق‌تری روی مجوزها فراهم می‌کند، فراتر از تنظیمات پیش‌فرض اندروید.

قابلیت‌ها:

- امکان غیرفعال‌سازی دسترسی به دوربین یا میکروفون به‌صورت کامل.
- ثبت تاریخچه دسترسی اپ‌ها به موقعیت یا فایل‌ها.
- تنظیم مجوزها به‌صورت دائمی یا موقت.

Bouncer (برای اندروید)

Bouncer اجازه می‌دهد پس از استفاده از یک اپ خاص، مجوزهای داده‌شده به‌صورت خودکار لغو شوند.

مثال: فرض کنید اپلیکیشن تحویل غذا فقط وقتی باز است به لوکیشن دسترسی داشته باشد؛ Bouncer بلافاصله بعد از بستن اپ، آن را می‌بندد.

اپلیکیشن‌های محافظت از دوربین و میکروفون

Access Dots (برای اندروید)

این اپلیکیشن سبک و کم‌حجم مشابه عملکرد iOS، در زمان استفاده اپلیکیشن‌ها از میکروفون یا دوربین، هشدار تصویری نمایش می‌دهد.

MicLock (برای اندروید)

MicLock با ایجاد یک لایه حفاظتی، دسترسی دائمی اپلیکیشن‌ها به میکروفون را غیرفعال می‌کند و فقط در صورت تأیید کاربر فعال می‌شود.

OverSight (برای macOS)

یکی از بهترین ابزارهای رایگان برای نظارت بر فعال‌بودن میکروفون و دوربین در مک. هر زمان برنامه‌ای به میکروفون یا وب‌کم دسترسی پیدا کند، هشدار ارسال می‌کند.

ابزارهای مرورگر برای کنترل دسترسی‌ها

Privacy Badger (افزونه برای Chrome و Firefox)

این افزونه ساخته‌ی بنیاد Electronic Frontier Foundation است و رفتارهای ردیابی اپلیکیشن‌ها را در مرورگر مسدود می‌کند.

uBlock Origin

علاوه بر بلاک کردن تبلیغات، دسترسی به منابع مشکوک از

جمله کدهای شنود را نیز مسدود می‌کند.

DuckDuckGo Privacy Essentials

افزونه‌ای برای مرورگرهای دسکتاپ که نمره‌ی امنیتی هر سایت را نشان می‌دهد و مانع ردیابی کوکی‌ها و اسکریپت‌ها می‌شود.

غیرفعال‌سازی کامل سخت‌افزاری (راه‌کار پیشرفته)

در برخی موارد، امنیت واقعی فقط با حذف فیزیکی دسترسی ممکن است. مثلاً:

- استفاده از وب‌کم USB جداگانه و خارج‌کردن آن پس از استفاده.
- نصب کلید فیزیکی Kill Switch برای قطع میکروفون در لپ‌تاپ.
- استفاده از قاب گوشی‌هایی که اسلایدر فیزیکی برای بستن دوربین دارند.

در محصولات حرفه‌ای مثل Purism یا Fairphone، این امکانات به‌صورت کارخانه‌ای در نظر گرفته شده‌اند.

۶. مدیریت شبکه و جلوگیری از انتقال ناخواسته داده‌ها

NetGuard (برای اندروید)

یک فایروال قوی بدون نیاز به روت که به شما امکان می‌دهد دسترسی هر اپ به اینترنت (Wi-Fi یا دیتا) را کنترل کنید.

مثال: می‌توانید اپلیکیشن دوربین را از دسترسی به اینترنت محروم کنید تا اگر کدی در پس‌زمینه وجود داشت، نتواند اطلاعات را ارسال کند.

Little Snitch (برای macOS)

نرم‌افزار قدرتمند برای کنترل تمام اتصالات شبکه. هر بار که برنامه‌ای می‌خواهد به اینترنت وصل شود، هشدار می‌دهد و اجازه‌ی شما را می‌خواهد.

تنظیمات مکمل برای حفظ حریم خصوصی

در گوشی:

- خاموش‌کردن موقعیت جغرافیایی (GPS) به‌صورت پیش‌فرض
- حذف اپ‌هایی که مدت‌هاست استفاده نمی‌کنید
- فعال‌سازی حالت Guest (کاربر مهمان) برای مواقعی که گوشی را دست فرد دیگری می‌دهید

در لپ‌تاپ:

- فعال‌سازی فایروال داخلی (مثل Windows Defender Firewall)
- بررسی لیست برنامه‌های استارت‌آپ و حذف برنامه‌های غیرضروری
- استفاده از اکانت استاندارد (نه ادمین) برای کارهای روزمره

بررسی امنیتی جامع با اپلیکیشن‌های امنیتی

Exodus Privacy Scanner (برای اندروید)

این اپ با بررسی ساختار داخلی اپلیکیشن‌های نصب‌شده، گزارش می‌دهد که هر برنامه از چه ابزارهای ردیابی (Tracker) و چه مجوزهایی استفاده می‌کند.

Jumbo Privacy (برای iOS و Android)

یک دستیار امنیتی که تنظیمات حریم خصوصی شبکه‌های اجتماعی (مثل فیسبوک، توییتر و گوگل) را بررسی و پیشنهاداتی برای بهبود می‌دهد.

نتیجه‌گیری

در عصر ابزارهای هوشمند، حفظ حریم خصوصی بیش از هر زمان دیگری اهمیت دارد. هرچند سازندگان این دستگاه‌ها امکانات فراوانی ارائه می‌دهند، اما همین امکانات اگر بدون نظارت باشند، می‌توانند دروازه‌ای به دنیای ناامن شوند. آگاهی از ابزارهای موجود، استفاده صحیح از تنظیمات، و گاهی احتیاط فیزیکی، مجموعه‌ای از گام‌های ضروری برای حفظ امنیت دیجیتال در محیط کار و خانه است.

فراموش نکنید: هر اپلیکیشنی که نصب می‌کنید، مثل مهمانی است که به خانه‌تان دعوت کرده‌اید. قبل از دادن دسترسی، از خود بپرسید: آیا این اپ واقعاً به این اطلاعات نیاز دارد؟

KNOWLEDGE TEST

••• آزمون دانشی

قدر حواست به وسایل دور و برته؟

آیا شما هدف بعدی جاسوسی دیجیتال هستید؟

سؤال ۱
وقتی برای تماس تصویری از لپ‌تاپ استفاده می‌کنی، بعدش با دوربین لپ‌تاپ چکار می‌کنی؟
A. همیشه با چسب می‌پوشونم – حتی وقتی تماس ندارم. (۳ امتیاز)
B. گاهی اوقات یادم می‌ره، ولی وقتی حواسم باشه می‌پوشونم. (۲ امتیاز)
C. اصلاً اهمیتی نمی‌دم، نیازی نمی‌بینم. (۰ امتیاز)

سؤال ۲
تا حالا شده اپلیکیشنی نصب کنی که دسترسی دوربین و میکروفون می‌خواد ولی نمی‌دونی چرا؟
A. نه، همیشه مجوزها رو بررسی می‌کنم. (۳ امتیاز)
B. بعضی وقت‌ها شک می‌کنم ولی ادامه می‌دم. (۱ امتیاز)
C. اغلب بدون فکر تأیید می‌کنم. (۰ امتیاز)

سؤال ۳
موقعیت جغرافیایی گوشی‌ت همیشه فعاله؟
A. فقط وقتی نیاز دارم روشنش می‌کنم. (۳ امتیاز)
B. بیشتر وقتا فعاله ولی گاهی خاموشش می‌کنم. (۱ امتیاز)
C. همیشه فعاله؛ اصلاً خاموشش نمی‌کنم. (۰ امتیاز)

سؤال ۴
در خانه یا محل کار، چند دستگاه هوشمند با میکروفون فعال داری؟ (مثل دستیار صوتی، تلویزیون هوشمند، ساعت هوشمند)
A. هیچ‌کدوم – یا ندارم یا همه رو بی‌صدا کردم. (۳ امتیاز)
B. یکی دو مورد هست ولی نگران نیستم. (۱ امتیاز)
C. چندتا دارم و هیچ‌وقت بهش فکر نکردم. (۰ امتیاز)

سؤال ۵
وقتی لینک مشکوک در پیام یا ایمیل دریافت می‌کنی، چکار می‌کنی؟
A. فوراً حذف می‌کنم و گزارش می‌دم. (۳ امتیاز)
B. باز نمی‌کنم ولی همون‌جا رهاش می‌کنم. (۱ امتیاز)
C. گاهی کنجکاو می‌شم و روش کلیک می‌کنم. (۰ امتیاز)

سؤال ۶
بعد از اتمام جلسه مجازی، برنامه‌های جلسه رو کامل می‌بندی؟
A. بله، همیشه از برنامه خارج می‌شم. (۳ امتیاز)
B. فقط صفحه‌شو می‌بندم ولی برنامه باز می‌مونه. (۱ امتیاز)
C. اصلاً نمی‌دونم باید ببندم یا نه. (۰ امتیاز)

سؤال ۷
تا حالا بررسی کردی چه اپلیکیشن‌هایی به میکروفون یا دوربین دسترسی دارن؟
A. مرتب بررسی و محدود می‌کنم. (۳ امتیاز)
B. یکی دو بار بررسی کردم. (۱ امتیاز)
C. نه، اصلاً نمی‌دونم از کجا باید چک کنم. (۰ امتیاز)

سؤال ۸
روی گوشی‌ات آنتی‌ویروس یا نرم‌افزار امنیتی نصبه؟
A. بله، و مرتب هم آپدیتش می‌کنم. (۳ امتیاز)
B. نصب هست ولی زیاد بهش توجه نمی‌کنم. (۱ امتیاز)
C. نه، بهش نیازی نمی‌بینم. (۰ امتیاز)

سؤال ۹
وقتی دستگاهی رو به وای‌فای خونه‌ت وصل می‌کنی، چقدر به امنیتش فکر می‌کنی؟
A. مطمئنم دستگاه ناشناس نیست و فقط خودم اجازه می‌دم. (۳ امتیاز)
B. گاهی بررسی می‌کنم، ولی نه همیشه. (۱ امتیاز)
C. هر کسی رمز رو داشته باشه وصل می‌شه – اشکالی نداره. (۰ امتیاز)

سؤال ۱۰
تا حالا تنظیمات حریم خصوصی شبکه‌های اجتماعی‌ت رو بررسی کردی؟
A. بله، دقیق تنظیمشون کردم. (۳ امتیاز)
B. یه‌بار بررسی کردم ولی تغییر زیادی ندادم. (۱ امتیاز)
C. اصلاً نمی‌دونم چنین تنظیماتی هست. (۰ امتیاز)

جمع امتیاز:
امتیاز هر سؤال رو جمع بزنید.

تفسیر نتایج
۲۵ تا ۳۰ امتیاز: محافظ حرفه‌ای
آفرین! حواست کاملاً جمعه و به خوبی از خودت محافظت می‌کنی. آگاهی تو از تهدیدات دیجیتال نشون می‌ده که به امنیت خودت و اطرافیانت اهمیت می‌دی. این سبک زندگی دیجیتالِ آگاهانه باید الگویی برای دیگران باشه.

۱۵ تا ۲۴ امتیاز: خوب ولی جای بهترشدن هست
تو مسیر درستی هستی، ولی هنوز چند نقطه‌ی ضعف داری که ممکنه در موقعیت‌های خاص باعث خطر بشن. بهتره گاهی یه بازبینی کلی در تنظیماتت انجام بدی و اپلیکیشن‌های مشکوک رو زیر ذره‌بین ببری.

زیر ۱۵ امتیاز: خطر در کمینه!
شاید هنوز خطرات امنیتی دیجیتال رو جدی نگرفتی. دستگاه‌های اطرافت ممکنه بیشتر از اونچه فکر می‌کنی در حال ضبط، ذخیره یا ارسال اطلاعات باشن. پیشنهاد می‌کنیم از همین الان، آگاهی دیجیتال خودت رو افزایش بدی.

نکته پایانی:
این آزمون صرفاً یک ابزار سرگرم‌کننده برای خودارزیابی نیست؛ یک زنگ خطره. امنیت دیجیتال فقط با نصب آنتی‌ویروس حل نمی‌شه؛ آگاهی، عادت و توجه لازمه. آیا وقتشه یه بازبینی جدی توی رفتار دیجیتالت انجام بدی؟