تحلیلی بر وضعیت امنیت در فضای مجازی*

* خبرگزاری مهر، شیوا سعیدی قوی‌اندام، کد خبر: ۴۴۳۱۰۵۲.

امنیت اطلاعات با گسترش روند دیجیتال شدن کاسته شده و هر روز حجم بیشتری از اطلاعات کاربران فاش می‌شود. این روند، در سال‌های اخیر نگران‌کننده‌تر شده است. طبق خبر گروه دانش و فناوری خبرگزاری مهر، چند هفته پیش، تیتر این خبر همه را شگفت‌زده کرد: «اطلاعات ۵۰ میلیون کاربر فیس‌بوک افشا شد.» هرچند این نخستین‌باری نیست که اطلاعات خصوصی افراد فاش می‌شود، اما حجم آن، نگران‌کننده است. پیش از این نیز اخبار مربوط به فاش‌شدن اطلاعات کاربران خبرساز شده بود؛ به عنوان مثال، در اوایل سال جاری رسوایی کمبریج آنالایتیکا در صدر اخبار قرار گرفت. این شرکت به وسیله اطلاعات کاربران فیس‌بوک، استراتژی تبلیغاتی دونالد ترامپ را طراحی کرده بود.

به هر حال، هم‌زمان با پیشرفت فناوری و دیجیتالیزه شدن سیستم‌های ذخیره اطلاعات و گسترش استفاده از اینترنت در گجت‌های مختلف، هر روز اخبار بیشتری درباره فاش شدن اطلاعات محرمانه کاربران منتشر می‌شود. افشای اطلاعات کاربران، در سال‌های اخیر وارد مرحله جدیدی شده است و دلایل مختلفی دارد.

دلایل افشای اطلاعات کاربران

افشای اطلاعات، در لغت به معنای انتشار عمدی یا غیرعمدی اطلاعات خصوصی و عمومی در محیطی غیر ایمن است. دلایل مختلفی به افشای اطلاعات منجر می‌شوند؛ مانند: هک اطلاعات توسط هکرهای زیرزمینی، افشای اطلاعات توسط فعالان سیاسی یا دولت‌های محلی یا حتی استفاده از تجهیزات رایانشی یا شبکه‌های ذخیره اطلاعات. در این میان، نباید نقش باگ‌های داخلی و بدافزارها را نیز نادیده گرفت.

روزانه حجم عظیمی از داده‌های تولیدی توسط شرکت‌های ارائه‌دهنده شبکه‌های اجتماعی و پیام‌رسان، مدیریت و تحلیل می‌شود و نتایج حاصل از تحلیل روی این داده‌های کلان (بیگ دیتا)، متقاضی بسیاری داشته و از بنگاه‌های تجاری که برای بهره‌مندی در تبلیغات هوشمند به این اطلاعات نیاز دارند، تا سازمان‌های امنیتی و حاکمیتی برای رصد وضعیت ملت‌ها در نقاط مختلف دنیا، متقاضی این داده‌ها هستند؛ حتی در این بین، شرکت‌های تحلیلی بسیاری، کلان‌داده‌ها را منبع اصلی درآمد خود قرار داده و با ارائه گزارش‌های هدفمند، می‌توانند نتیجه انتخابات مختلف را تغییر دهند. در این بین، نباید از سوء استفاده شرکت‌های تبلیغاتی و بازاریابی غافل ماند.

ناامنی روزافزون فضای مجازی

با روند رو به رشد ناامنی در فضای مجازی، در سال جاری میلادی، انبوهی از اخبار مربوط به افشای اطلاعات کاربران منتشر شد. پس از فاش شدن خبر مربوط به افشای اطلاعات ۵۰ میلیون کاربر فیس‌بوک، گزارش‌های دیگر نشان داد احتمالاً حساب کاربری اینستاگرام این افراد نیز هک شده است. همچنین، اگر یکی از این افراد از طریق اطلاعات حساب کاربری فیس‌بوک خود وارد اینستاگرام یا هر وب‌سایت دیگری شده بود، احتمالاً هکرها به اطلاعات حساب او دسترسی پیدا کرده بودند.

در آخرین نمونه این اخبار، مشخص شد که هکرها پیام‌های خصوصی ۸۱ هزار کاربر فیس‌بوک را منتشر کرده‌اند. آنها در یک آگهی تبلیغاتی اعلام نمودند دسترسی به حساب‌های کاربری را با قیمت ۱۰ سنت می‌فروشند.

همچنین، وب‌سایتی به نام Krebs on S – curity اعلام کرد که نرم افزار جاسوسی mSpy ، اطلاعات میلیون‌ها کاربر خود را فاش کرده است. جالب آنکه اطلاعات کاربران این نرم‌افزار، به‌راحتی قابل دسترسی است و حجم وسیعی را شامل می‌شود؛ از جمله نام، نشانی ایمیل، پیام‌های فیس‌بوک و واتساپ.

چندی پیش، محققان دانشگاه آکسفورد نیز هشدار دادند جمع‌آوری و اشتراک‌گذاری

هم‌اکنون با گسترش اینترنت اشیا و هوش مصنوعی، اطلاعات کاربران، نه تنها در وب‌سایت‌ها و مخازن اطلاعاتی شرکت‌ها، بلکه در گجت‌های ساده خانگی نیز ذخیره می‌شود. از آنجا که در بسیاری از این گجت‌ها، اقدامات امنیتی در نظر گرفته نشده، کارشناسان متعددی درباره سرقت از آنها هشدار داده‌اند

اطلاعات کاربران به وسیله اپلیکیشن‌های موبایل، از کنترل خارج شده است. آنها متوجه شدند ۹۰ درصد اپلیکیشن‌های رایگان در پلی‌استور، اطلاعات کاربران را با آلفابت (شرکت مادر گوگل) به اشتراک می‌گذارد. بیش از ۴۰ درصد این اپلیکیشن‌ها، اطلاعات کاربران را به کسب‌وکارهای متعلق به فیس‌بوک منتقل می‌کنند.

همچنین، گزارشی دیگر نشان داده اپلیکیشن‌هایی مانند Dr.Unarchiver و Dr.Cleaner که توسط شرکت Trens Micro عرضه شده‌اند، تاریخچه مرورگر کاربر را جمع‌آوری و آپلود می‌کنند. این برنامه‌ها همچنین، اطلاعات اپلیکیشن‌های دیگر نصب‌شده در دستگاه را جمع‌آوری می‌نمایند.

افشای اطلاعات با اهداف مختل تا به آنجا پیش رفته که یک شرکت هواپیمایی هنگ‌کنگی به نام Cathay Pasific نیز اعلام کرد اطلاعات ۹.۴ میلیون نفر از مشتریانش فاش شده است. در این نشتِ اطلاعات، اسامی، ملیت، تاریخ تولد، شماره تلفن، ایمیل، نشانی، شماره پاسپورت، شماره کارت شناسایی و تاریخچه سفر مشتریان فاش شده بود.

شاید یکی از تکان‌دهنده‌ترین اخبار نیز مربوط به وجود اطلاعات ۳۵ میلیون رأی‌دهنده امریکایی در وب تاریک بود. این اطلاعات، یک ماه قبل از شروع انتخابات مجلس نمایندگان، برای فروش در یک فروم آنلاین عرضه شده بود. البته کارشناسان ادعا می‌کنند عرضه اطلاعات، به معنای افشای اطلاعات نیست. این سوابق، احتمالاً از شرکت‌هایی سرقت شده که از اطلاعات رأی‌دهندگان برای استفاده در برنامه‌های انتخاباتی ایالت‌ها استفاده می‌کنند.

شبکه‌های اجتماعی نیز پلتفرم امنی برای اطلاعات به حساب نمی‌آیند. محققان امنیتی، به‌دفعات شکاف‌های امنیتی را در این زمینه کشف کرده‌اند. یکی از آن موارد، به سوءاستفاده از ویس‌میل واتساپ مربوط می‌شود. هکرها با استفاده از شماره تلفن کاربر سعی می‌کنند اپلیکیشن استاندارد واتساپ را در موبایل خود نصب کنند. در مرحله بعد، واتساپ با ارسال یک پیامک حاوی کد تأیید ۶ رقمی به موبایل کاربر، عملیات را احراز هویت می‌کند. به همین دلیل، هکرها سعی می‌کنند زمانی که کاربر موبایل خود را رصد نمی‌کنند (شب‌هنگام) این عملیات را انجام دهند. در مرحله بعد، واتساپ به کاربر اجازه می‌دهد که بین ارسال دوباره کد ۶ رقمی و تماس صوتی خودکار، یکی را انتخاب کند. از آنجا که کاربر موبایل خود را رصد نمی‌کند، پیام به ویس‌میل او ارسال می‌شود. در این مرحله، هکرها با استفاده از شکاف امنیتی در شبکه شرکت‌های مخابراتی، این ویس میل‌ها را دریافت می‌کنند.

حتی تلگرام نیز از این روند مستثنا نیست. یک محقق امنیتی کشف کرده که نسخه‌های قبلی اپلیکیشن دسکتاپ تلگرام، هنگام حین برقراری تماس صوتی، IP آدرس‌های عمومی و خصوصی (نشانی پروتکل اینترنت) را فاش کرده است. دلیل این امر، چارچوب کاری همتابه‌همتای تلگرام بوده است.

یکی دیگر از نمونه‌های جالب، اطلاعات مربوط به اپل است. بررسی‌های امنیتی نشان می‌دهد تعدادی از برنامه‌های محبوب آیفون، بی‌سروصدا اطلاعات موقعیت مکانی ده‌ها میلیون کاربر این گوشی را به اشتراک می‌گذارند. بسیاری از این برنامه‌ها، علاوه بر شناسایی موقعیت دقیق مکانی کاربران خود، اطلاعات حساس دیگری را نیز جمع‌آوری می‌کنند که دسترسی به آنها، توسط شرکت‌های ثالث می‌تواند امنیت افراد را به خطر بیندازد.

از سوی دیگر، صاحب خدمات ایمیل یاهو نیز اعلام کرده ایمیل‌های تجاری مشتریان خود را بررسی می‌کند و در اختیار شرکت‌های تبلیغاتی قرار می‌دهد. یاهو بیش از یک دهه قبل، رصد ایمیلی کاربران خود را آغاز کرده است. این شرکت، از الگوریتم‌های

مختلف برای بررسی ایمیل‌های تجاری در این باکس کاربر استفاده می‌کند.

راهی دیگر برای دسترسی به اطلاعات کاربران

شیوه‌های سرقت اطلاعات کاربران در سال‌های اخیر بسیار متنوع شده است. یکی از روش‌های کلاهبرداری از کاربران، مشکلات تقلبی رایانه‌هاست. طبق گزارش A - tion Fraud، (سازمان گزارش‌دهی جرایم سایبری در انگلیس) کلاهبرداران انگلیسی با ارائه خدمات مربوط به حل مشکلات تقلبی رایانه، بیش از ۲۱ میلیون پوند از ۲۲ هزار نفر کلاهبرداری کرده‌اند.

این نوع کلاهبرداری با یک تماس تلفنی، ایمیل یا یک پیام پاپ‌آپ در رایانه فرد آغاز می‌شود. این پیام به کاربر هشدار می‌دهد اختلالی در رایانه یا ارتباط اینترنتی او وجود دارد که باید حل شود. در مرحله بعد، کلاهبرداران از کاربر تقاضای مبلغی می‌کنند تا مشکل را حل کنند. در موارد دیگر، آنها قربانیان خود را فریب می‌دهند تا نرم‌افزاری روی دستگاهشان نصب کنند. با این وسیله، کلاهبرداران به اطلاعات شخصی و مالی کاربر دسترسی می‌یابند. در همین راستا، این سازمان برنامه‌ای برای آموزش مردم درباره «کلاهبرداری خدمات نرم‌افزار رایانه‌ای» را ارائه می‌کند.

تاریخچه سرقت اطلاعات

افشای اطلاعات، لزوماً فقط به شکل دیجیتالی نیست؛ اما به طور حتم، اوج‌گیری عصر دیجیتال، سبب افزایش رویدادهای مربوط به افشای اطلاعات شده است. کارشناسان و وب‌سایت‌های مختلف، در این باره نظریات متفاوتی دارند؛ اما با توجه به رویدادهای مهم، می‌توان گفت افشای اطلاعات در فضای دیجیتال، از ۲۰۰۵ میلادی آغاز شد. در همین راستا، یک سازمان غیرانتفاعی در امریکا به نام Pr - vacy Rights Clearinghouse آماری از میزان اطلاعاتِ فاش‌شده و تعداد رویدادهای افشای اطلاعات اعلام کرد.

طبق اطلاعات وب‌سایت این سازمان، از ۲۰۰۵ میلادی تاکنون ۱۱ میلیارد و ۲۳۷ میلیون و ۵۳۵ هزار و ۵۴۱ داده فاش شده است. همچنین، در این بازه زمانی، ۸۸۵۳ رویداد مربوط به افشای اطلاعات به طور عمومی اعلام شده‌اند.

یکی از بزرگ‌ترین نمونه‌های افشای اطلاعات در تاریخ، به شرکت Experian تعلق دارد. اکسپرین، یکی از سه سازمان اصلی گزارش‌دهی اعتباری در امریکاست که در سال ۲۰۱۲ میلادی، شرکتی به نام Court Ventures را خرید. این شرکت، اطلاعات مربوط به سوابق عمومی را جمع‌آوری می‌کرد. از سوی دیگر، در زمان ادغام Court Ventures نیز قراردادی با شرکتی به نام US Info Search داشت تا اطلاعات را در اختیار این شرکت قرار دهد. Court Ventures اطلاعات را به شرکت‌های طرف سوم، از جمله یک مؤسسه خدمات کلاهبرداری ویتنامی می‌فروخت و به آنها اجازه می‌داد تا اطلاعات خصوصی مشتریان امریکایی، از جمله آمار مالی و شماره‌های تأمین اجتماعی را بررسی کنند. در بسیاری از موارد، از این اطلاعات برای سرقت هویت استفاده می‌شد.

بزرگ‌ترین رخدادهای افشای اطلاعات کاربران

نام شرکت	تاریخ افشای اطلاعات	میزان اطلاعات فاش‌شده	شیوه فاش‌شدن اطلاعات
فیس‌بوک	۲۰۱۸	۵۰ میلیون کاربر	هک/ امنیت ضعیف
گوگل پلاس	۲۰۱۸	۵۰۰ هزار کاربر	امنیت ضعیف
ادوب سیستمز	۲۰۱۳	۱۵۲ میلیون کاربر	هک
نرم‌افزار جاسوسی mSpy	۲۰۱۸	تعداد نامشخص	ضعف امنیتی
اوبر	۲۰۱۷	۵۷ میلیون کاربر	هک
اپل	۲۰۱۲	۱۲ میلیون کاربر	انتشار تصادفی اطلاعات
تلگرام	۲۰۱۸	تعداد نامشخص	ضعف امنیتی
پیتزاهات	۲۰۱۷	تعداد نامشخص	ضعف امنیتی
وب‌سایت‌های بازی رایانه‌ای چینی (Duowan۷ ،K۷K۱۷۸ ،. com)	۲۰۱۱	۱۰ میلیون کاربر	هک

مرکز یکپارچه اطلاعات دفاعی کره جنوبی	۲۰۱۷	۲۳۵ گیگابایت	هک
ای.بی	۲۰۱۴	۱۴۵ میلیون کاربر	هک
Equifax	۲۰۱۷	۱۴۳ میلیون کاربر	امنیت ضعیف
اورنوت	۲۰۱۳	۵۰ میلیون کاربر	هک
اکسپرین	۲۰۱۲	۱۴۵ میلیون کاربر	سوءاستفاده از اطلاعات
جی.میل	۲۰۱۴	۵ میلیون کاربر	هک
شرکت هواپیمایی Cathay Pasific	۲۰۱۸	۹.۴ میلیون کاربر	ضعف امنیتی
هوم دیپوت	۲۰۱۴	۵۶ میلیون کاربر	هک
بانک جی.پی مورگان چیس	۲۰۱۴	۷۶ میلیون کاربر	هک
هک عظیم کسب‌وکارهای امریکایی از جمله بورس نزدک	۲۰۱۲	۱۶۰ میلیون کاربر	هک
سونی آنلاین اینترنتینمنت	۲۰۱۱	۲۴۶ میلیون کاربر	هک
سونی پلی استیشن نتورک	۲۰۱۱	۷۷ میلیون کاربر	هک
توئیتر	۲۰۱۳	۲۵۰ هزار کاربر	هک
اوبر	۲۰۱۴	۵ هزار کاربر	امنیت ضعیف
آندرآرمور	۲۰۱۸	۱۵۰ میلوین کاربر	هک
یاهو	۲۰۱۳	۳ میلیارد کاربر	هک

کاهش ارزش سهام و محبوبیت

چنین رویدادهایی، ریسک برای دزدی هویت یا پیامدهای وخیم‌تر همراه دارند. پس از اعلام این رویدادها، کاربران مجبور می‌شوند تمام اطلاعات و پسوردهای خود را تغییر دهند. از سوی دیگر، چنین رویدادهایی پس از علنی‌شدن، هیاهوی بسیاری ایجاد می‌کند و به طور معمول، شرکت سعی می‌کند از خسارات بیشتر جلوگیری کند؛ به عنوان مثال، افشای اطلاعات مشتریان خرده‌فروشی تارگت در ۲۰۱۳ میلادی، به کاهش سودآوری شرکت منجر شد. در پایان ۲۰۱۵ میلادی، تارگت با انتشار گزارشی اعلام کرد هزینه‌های مرتبط با افشای اطلاعات مشتریان آن، بالغ بر ۲۹۰ میلیون دلار بوده است.

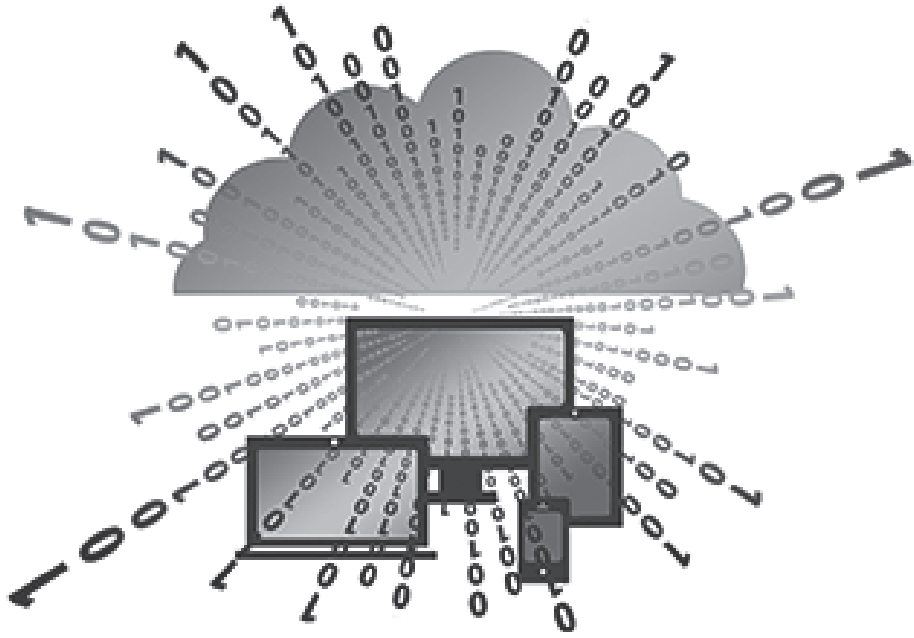
به نوشته رویترز، افشای اطلاعات ۳ میلیارد کاربر یاهو که در ۲۰۱۳ میلادی اتفاق افتاد، در ۲۰۱۶ میلادی فاش شد که یکی از پرهزینه‌ترین رویدادهای این‌چنینی در تاریخ بوده است. این رویداد، سبب شد شرکت وریزون قیمت پیشنهادی برای خرید یاهو را یک میلیارد دلار کاهش دهد.

البته به‌سختی می‌توان خسارت‌های مالی مستقیم و غیرمستقیم مربوط به افشای اطلاعات کاربران را به دست آورد. یکی از راه‌های معمول در این زمینه، ارزیابی واکنش بازار به چنین رویدادی است.

در نمونه افشای اطلاعات کاربران فیس‌بوک از طریق شرکت کمبریج آنالایتیکا، این امر، نه تنها به سقوط ارزش سهام شرکت و ورشکستگی آن منجر شد، در ایالات متحده امریکا از میزان محبوبیت دونالد ترامپ نیز کاسته شد. از سوی دیگر، مارک زاکربرگ مجبور شد برای شهادت در این باره، در برابر کنگره ظاهر شود. تمام این رویدادها، به کاهش محبوبیت و تعداد کاربران فیس‌بوک منجر شده است.

قوانین مربوط به اجباری شدن حفاظت از اطلاعات

به نوشته دیجیتال ورلد، با افزایش تعداد رویدادهای افشای اطلاعات، کشورها و مناطق مختلف قوانین متفاوتی را برای حفاظت از اطلاعات ارائه کرده‌اند. قوانینی مانند HIPAA (استانداردهای امنیتی برای حفاظت از سوابق بهداشتی افراد) یا PCI (استاندارد امنیت اطلاعات) در امریکا



ابداع شده‌اند تا راهنمایی برای شرکت‌ها و سازمان‌ها برای کنترل انواع خاصی از اطلاعات حساس مشتریان ابداع کنند. این قوانین، چارچوبی برای امنیت، ذخیره‌سازی و روش‌های استفاده از اطلاعات حساس را فراهم می‌نمایند؛ اما این قوانین در تمام صنایع وجود ندارند و لزوماً از افشای اطلاعات جلوگیری نمی‌کنند.

طبق قانون GDPR، شرکت‌ها در صورت افشای اطلاعات کاربران، ۲۰ میلیون یورو جریمه می‌شوند. از سوی دیگر، اتحادیه اروپا نیز چندی پیش، قانون GDPR را در راستای حفاظت از اطلاعات کاربران وضع کرد. به موجب این قانون، شرکت‌هایی که اطلاعات کاربران را فاش کنند، مشمول جریمه‌ای معادل ۲۰ میلیون یورو یا ۴ درصد از گردش مالی سالانه جهانی خود می‌شوند.

همچنین، ایالت کالیفرنیا در امریکا نیز با وضع قانونی جدید، انتخاب پسوردهای ضعیف برای دستگاه‌های الکترونیکی مانند رایانه و موبایل توسط شرکت تولیدکننده ممنوع است. در انگلیس نیز قانون‌گذاران در پی تصویب دستورعملی برای شرکت‌های تولیدکننده گجت‌های اینترنت اشیا هستند تا از انتخاب پسوردهای ضعیف برای آنها جلوگیری شود.

امنیت فضای مجازی؛ حال و آینده

پس از گذشت ۲۸ سال از تولد وب و گسترش اینترنت، «برنرز لی»، مخترع وب، طرح متن‌باز جدیدی به نام سولید را راه‌اندازی کرده که هدف از پیگیری آن، جلوگیری از جمع‌آوری انبوهی از اطلاعات خصوصی کاربران و انتقال این اطلاعات به شرکت‌های ثالث است.

او درباره این طرح می‌گوید: وب به موتوری برای نابرابری و تقسیم هم مبدل شده و نیروهای قدرتمند از آن برای پیشبرد دستور کار خود بهره می‌گیرند. ما امروز به نقطه حساسی رسیده‌ایم و تغییرات جدی ضروری است.

به گفته وی، با اجرای طرح سولید، مدل فعلی انتقال داده‌های خصوصی کاربران به شرکت‌های بزرگ فناوری تغییر می‌کند تا منافع آنها تأمین شود و اشخاص بتوانند بر روی داده‌های خود همچنان کنترل داشته باشند. در قالب این طرح، برخی تغییرات فنی به صورت ماژولار و چندبخشی بر روی فناوری‌های پُرکاربرد وب مانند: HTML، REST و HTTP اعمال می‌شود که استفاده از وب به صورت فعلی را مختل نمی‌کنند؛ اما کنترل داده‌های فردی و حفظ حریم شخصی را سهولت می‌بخشند.

یکی از دلایل فراگیرشدن افشای اطلاعات در سال‌های پس از ۲۰۰۵ میلادی، افزایش حجم اطلاعات است که به مجرمان سایبری فرصت‌های بیشتری می‌دهد تا حجم بیشتری از اطلاعات را در یک حمله سرقت کنند. در همین راستا، وب‌سایت‌ها و شرکت‌های مختلف، آمارهای مختلفی از آینده روند افشای اطلاعات منتشر می‌کنند. طبق گزارش CSC که در ۲۰۱۲ میلادی منتشر شده، تا ۲۰۲۰ میلادی بیش از یک‌سوم اطلاعات در خدمت ابر نگهداری می‌شود.

از سوی دیگر، وب‌سایت Statistica نیز در تحقیقی وضعیت واقعی امنیت اطلاعات در سراسر جهان از ۲۰۱۰ تا ۲۰۱۵ میلادی را نشان می‌دهد. از ۲۰۱۵ میلادی تاکنون، ۲۵ درصد اطلاعات جهان نیازمند اقدامات امنیتی بیشتری هستند؛ اما همچنان به طور غیر ایمن نگهداری می‌شوند. طبق تحقیق این وب‌سایتِ آماری، پیش‌بینی می‌شود که این شاخص در ۲۰۲۵ میلادی، به ۴۵ درصد می‌رسد.

هم‌اکنون با گسترش اینترنت اشیا و هوش مصنوعی، اطلاعات کاربران، نه تنها در وب‌سایت‌ها و مخازن اطلاعاتی شرکت‌ها، بلکه در گجت‌های ساده خانگی نیز ذخیره می‌شود. از آنجا که در بسیاری از این گجت‌ها، اقدامات امنیتی در نظر گرفته نشده، کارشناسان متعددی درباره سرقت از آنها هشدار داده‌اند. تمام این روندها، حاکی از آن است که حریم خصوصی برای افراد در حال از بین رفتن است و در صورتی که اقدامات امنیتی بیشتری انجام نشود، هر روز شاهد رویدادهای بیشتر افشای اطلاعات کاربران خواهیم بود.■