



دوستی از من خواست برایش اینترنتی دو بلیت هواپیمای تهران - مشهد بگیرم. با گشتن در چندین سایت فروش اینترنتی بلیت هواپیما و انتخاب روز و ساعت حرکت، نوع هواپیما و اطلاعات دیگر بلیت‌ها را گرفتم. می‌خواستم اطلاعات بلیت‌ها را برای دوستم ایمیل کنم که در تلگرام یک پیغام از فردی ناشناس دریافت کردم «سلام، شما تهران هستید یا مشهد؟» جا خوردم. اگر هر زمان دیگری این پیغام را دریافت کرده بودم، به حساب یکی از خواننده‌های ماهنامه شبکه می‌گذاشتم.

روزانه پیغام‌های زیادی از این دست دریافت می‌کنم که راهنمایی می‌خواهند یا سؤالی دارند، اما دریافت چنین پیغامی به فاصله فقط یک دقیقه بعد از خرید دو بلیت هواپیمای تهران - مشهد حتماً داستان دیگری دارد. روی آیکن کاربری پیغام‌دهنده کلیک کردم، اما جز یک عکس نامفهوم و یک آیدی تلگرام چیز دیگری نوشته نبود. عکس هم نام یک شرکت تجاری را نشان می‌داد، ولی آن‌قدر خوانا نبود که بشود دقیقاً نام شرکت را خواند و اطلاعات بیشتری کسب کرد. اصول امنیتی حریم شخصی می‌گوید در این موارد مشکوک پیغام را جواب ندهید، اما من کنجکاو شده بودم و حدس‌هایی می‌زدم. پس با کمی مکث جواب دادم که تهران هستم. جواب داد «ممنون» و تمام! گفت‌وگوی ما در تلگرام همین‌جا خاتمه یافت.

حتماً خوانندگان عزیز هم تاکنون تجربه‌های مشابهی داشته‌اند. به عنوان مثال، بیمه‌نامه خودروی خود را تمدید می‌کنید و چند دقیقه بعد یک پیامک تبلیغاتی برای بیمه عمر، بیمه شخص ثالث و بیمه آتش‌سوزی از یک بیمه‌گذار ثالث دریافت می‌کنید. یا در یک نمایشگاه ثبت‌نام می‌کنید و چند روز بعد، ده‌ها شرکت سازنده غرفه و غرفه‌آرایی با شما تماس می‌گیرند. برای دانلود یک کتاب الکترونیکی در سایتی ثبت‌نام می‌کنید و از فردا صبح ایمیل‌های تبلیغاتی به سوی میل‌باکس شما سرازیر می‌شوند. این‌ها نمونه‌های پیش پا افتاده و ساده‌ای از فروش یا سوء استفاده اطلاعاتی هستند؛ بهره‌برداری از اطلاعات خام کاربران و مشتریان یک شرکت یا سایت که شاید خطر چندانی هم برایشان ایجاد نکنند و استفاده صرفاً تبلیغاتی و درآمدزایی دارند. اما وقتی پای هکرها، گروه‌های خراب‌کاری و تروریستی، مراکز امنیتی یا سرفتهای مالی به ماجرا باز می‌شود، دیگر نمی‌توان تعبیر «استفاده صرفاً تبلیغاتی و درآمدزایی» را به کار برد. یک سایت یا شرکت با سوء استفاده از اعتماد مشتریان، اطلاعاتشان را برای تأمین منافع شخصی یا درآمدزایی مستقیم به بهایی کم یا زیاد می‌فروشد.



توسط شرکت Telstra اولین LTE گیگابیتی در استرالیا راه اندازی شد

در این یادداشت نمی‌خواهم درباره روش‌ها و ترفندهای بهره‌برداری از اطلاعات خام مشتریان صحبت کنم، بلکه می‌خواهم روی موضوع و اقدامی غیر قانونی و غیر شرعی دست بگذارم که متأسفانه در ایران به‌وفور مشاهده می‌شود و ظاهراً قانون مدون، منسجم و شفاف هم برای مقابله با این جرم یا مجازات عاملان وجود ندارد. حداقل این طور به نظر می‌رسد که مراکز تصمیم‌گیری و نهادهای بازرسی و قضایی روی آن زیاد تمرکز ندارند و جز در مواردی که به یک مشکل حاد تبدیل و رسانه‌ای شود، برنامه‌ای جدی برای مقابله و جلوگیری نمی‌بینیم. تقریباً هر سایت، اپلیکیشن، سامانه یا شرکتی می‌تواند به راحتی در ایران خرید و فروش اطلاعات داشته باشد. با جست‌وجوی ساده در اینترنت، می‌توانید بانک‌های اطلاعاتی چند صد هزار تایی یا چند میلیونی از شماره تلفن‌های همراه یک اپراتور، ایمیل‌های دانشجویان مهندسی کامپیوتر تهران یا یک دانشگاه خاص، کاربران اینترنتی یک ارائه‌دهنده خدمات اینترنت، شماره تلفن و نشانی اعضای یک صنف تجاری در تهران و سراسر شهرستان‌ها و ده‌ها نمونه مشابه پیدا کنید.

مشکل اینجا است که جنس برخورد با اطلاعات در ایران بسیار متفاوت از کشورهای دیگر است. اطلاعات کاربران همانند خانه، ماشین یا وسایل شخصی هر فردی است، مانند سندهای هویتی و مالکیتی هر فردی است، مانند دارایی‌های شخصی و خصوصی محرمانه هر فردی است و به همان اندازه یا بیشتر اهمیت دارد. همان طور که هیچ بانکی حق ندارد یا جرئت نمی‌کند اطلاعات یک حساب مشتری را به دیگران بدهد یا محتویات صندوق امانات مشتری را به دیگران نشان بدهد، سایت‌ها و شرکت‌های خدماتی نیز حق و اجازه ندارند شماره تلفن همراه یا ایمیل یا هر اطلاعات شخص دیگری هرچند ساده و برای ارسال فقط یک پیامک تبلیغاتی را در اختیار افراد ثالث قرار بدهند.

در آمریکا و کشورهای اروپایی، بهره‌برداری و درآمدزایی مستقیم از اطلاعات ممنوع و غیر قانونی است و به شدت با برخوردهای امنیتی و قضایی روبه‌رو می‌شود. سال‌های متمادی است مراکز مختلف حاکمیتی و استانداردسازی این کشورها دارند روی برطرف‌سازی موانع کسب و کار فروش مستقیم اطلاعات کار و تحقیق می‌کنند تا استانداردها، قوانین و روال‌های مربوط را مشخص و تبیین کنند. بسیاری از شرکت‌های بزرگ دنیا برای استفاده و فروش صدها ترابایت اطلاعات ذخیره شده روی مراکز داده و سرورهای خودشان، هم از بعد حقوقی و هم از بعد تجاری و فرآیندهای امنیتی و احراز هویتی با چالش‌ها و مشکلات متعددی روبه‌رو هستند. تازه، پس از چندین سال بررسی این موضوع، به نظر می‌رسد شاید در سال ۲۰۱۷ روزه‌های امیدی پیدا شود و برخی موانع پیش روی برداشته شود تا کسب و کارها بتوانند از داده‌های خام ذخیره شده روی سیستم‌های خودشان درآمدزایی مستقیم داشته باشند. این شرکت‌ها بی‌خبر هستند که اینجا خرید و فروش آزاد است و حتی نیازی به دادن کوچک‌ترین تعهد، تضمین و وثیقه اعتباری نیست!

تاریخ انتشار:

20 بهمن 1395