اخبار

کپی کردن ریلزها در اینستاگرام ممنوع شد

اینستاگرام ابزار جدیدی برای کمک به خالقان محتوا در محافظت از ویدئوهای اورجینال خود معرفی می‌کند. به گزارش مهر به نقل از تک کرانچ، این ویژگی که محافظت از محتوا نام دارد هم‌اکنون در فیس‌بوک ارایه می‌شود و هدف از طراحی آن ردیابی مواقعی است که ویدئوهای اورجینال خالقان محتوا بدون اجازه‌شان مورد استفاده قرار می‌گیرد. شرکت متا پلتفرمز نیز در حال گسترش این ابزار است تا نه‌فقط بازنشرهای سنتی محتوا بلکه محتوای هوش مصنوعی را نیز در بر گیرد. این خبر در واکنش به نگرانی‌های خالقان محتوا درباره سهولت کپی کردن و بازنشر محتوایشان در شبکه‌های اجتماعی مختلف است، به‌خصوص آنکه هوش مصنوعی دستکاری ویدئوهای موجود را بسیار ساده‌تر کرده است. اینستاگرام مدعی است ابزار حفاظت از محتوا به‌طور مداوم پلتفرم را برای موارد استفاده غیرمجاز از ویدئوهای محافظت شده کاربران اسکن می‌کند. هنگامی که محتوایی رصد می‌شود که با یکی از ریلزهای آپلودشده توسط کاربر دیگری مطابقت دارد، پلتفرم به سازنده اصلی محتوا هشدار می‌فرستد. خالقان محتوا می‌توانند در مرحله بعد نمایش ویدئو را مسدود کنند یا آنکه محتوای مذکور را در پلتفرم‌های اینستاگرام و فیس بوک پنهان کنند. آنها همچنین می‌توانند برچسب «منبع اصلی» روی محتوا که تماشاچیان را به سمت ویدئوی اصلی هدایت می‌کنند، برگزینند. در کنار این موارد خالقان محتوا می‌توانند ویدئو کپی شده را حفظ کنند و همزمان عملکرد آن را رصد کنند یا ادعای خود را درباره ریلز منتشر کنند و به این ترتیب محتوا در پلتفرم‌های شرکت متا قابل مشاهده خواهد بود. ابزار مذکور همچنین ویدئوهای تولیدشده با هوش مصنوعی از صوت‌های خالقان محتوای اصلی استفاده می‌کند را نیز ردیابی و به مالک اصلی هشدار می‌دهد. این به روز رسانی قرار است برای گروه کوچکی از خالقان محتوا در هفته‌های آینده آزمایش شود. اینستاگرام مدعی شده به‌دنبال روش‌های جدیدی برای محدودسازی گستره حساب‌ها و محتوایی است که به‌طور مرتب از ابزارهای هوش مصنوعی برای بازنشر آثار دیگران استفاده می‌کند.

مایکروسافت با ۷ مدل به جنگ اوپن‌ای‌آی و آنتروپیک رفت

مایکروسافت از هفت مدل هوش مصنوعی جدید با نام خانواده «مای» (MAI) رونمایی کرد که کدنویسی، امنیت سایبری، اصلاح عکس، گفتار، رونویسی و تصمیم‌گیری خودکار را هدف قرار داده‌اند. به گزارش خبرگزاری مهر به نقل از اینترستینگ انجینرینگ، به‌نظر می‌رسد این مدل‌ها از نظر عملکرد و هزینه با محصولات اوپن‌ای‌آی و آنتروپیک رقابت می‌کنند. مایکروسافت این محصولات را شامل مای سایبر ۲ فلش، مای کد ۲، مای کد ۲ فلش، مای ایمیج ۲.۷، مای ریل تایمز ۱، Dragon Copilot Transcribe و Decision ۱.۱ و در کنفرانس Ignite رونمایی کرد. این رونمایی نشان‌دهنده تلاش مایکروسافت برای ارزان‌تر کردن مدل‌های هوش مصنوعی پیشرفته برای کسب‌وکارهایی است که عامل‌های خودکار را به‌طور دایم فعال می‌کنند. این شرکت اعلام کرد بهای روزافزون توکن‌ها سبب می‌شود هزینه-عملکرد به‌شدت برای شرکت‌هایی که به‌دنبال گسترش این سیستم‌ها هستند، اهمیت یابد. مایکروسافت به‌جای اتکا به یک سیستم برای انجام همه فعالیت‌ها، هر مدل را برای انجام کاری خاص تعیین کرده است. این شرکت همچنین «مایا ۲۰۰»، دومین نسل شتاب‌دهنده هوش مصنوعی مولد که روی بزرگ‌ترین مدل‌های در حال تولید آن فعال می‌شود را برجسته کرد. «مای سایبر ۲ فلش» برای نظارت امنیت سایبری مداوم و فعالیت‌های دفاعی از جمله شناسایی و ترمیم شکاف‌ها در سیستم‌های تولید فعال ارایه شده است. مایکروسافت مدعی است کیفیت آن با کیفیت جی پی تی ۶ آسترا برابری می‌کند، آن هم در حالی که هزینه انجام هر وظیفه با آن کمتر از دو درصد هزینه استفاده از مدل اوپن‌ای‌آی است. این شرکت همچنین اعلام کرده مدل را بر اساس سیستم‌های «مای سایبر» پیشین ساخته است. مای کد ۲ توسعه‌دهندگان نرم‌افزار را هدف گرفته و فعالیت‌های کدنویسی روزمره شرکتی را انجام می‌دهد.

آمازون و گوگل مالک ۳۰ درصد سهام آنتروپیک پس از عرضه اولیه می‌شوند

آنتروپیک جزییات بیشتری درباره بزرگ‌ترین توافقنامه‌های سرمایه‌گذاری خود با آمازون و گوگل به اشتراک گذاشت. به گزارش مهر به نقل از تک کرانچ، قبلا اعلام شده بود آمازون از محل سرمایه‌گذاری‌های خود در شرکت آنتروپیک و عرضه اولیه سهام این شرکت سود هنگفتی به‌دست خواهد آورد، اما آنتروپیک اکنون فاش کرده که سهم کل آن از این شرکت به‌اندکی کمتر از ۱۵ درصد (دقیقا ۱۴.۷ درصد) خواهد رسید. نکته جالب‌تر اینکه آمازون در صورت تمایل می‌توانست سهم بزرگ‌تری از آنتروپیک را در اختیار داشته باشد. زمانی که آمازون در سال‌های ۲۰۲۳ و ۲۰۲۴ میلیاردها دلار در آنتروپیک سرمایه‌گذاری کرد این غول رایانش ابری، اسناد تعهد به پرداخت (Promissory Notes) دریافت کرد که قابلیت تبدیل شدن به سهام را داشتند. قیمت تبدیل این اسناد به سهام، بسته به سال سرمایه‌گذاری، حدود ۲.۰۹ یا ۵.۰۵ دلار به ازای هر سهم تعیین شده است. آمازون تصمیم گرفته بخشی از این اسناد را همزمان با عرضه اولیه سهام آنتروپیک به سهام تبدیل کند. این سهام از نوع ویژه و بدون حق رأی خواهند بود و در مجموع حدود ۱۵ درصد از مالکیت آنتروپیک را برای آمازون همراه خواهند داشت. بر اساس اسناد ارایه‌شده، این سهام از حق دریافت سود تقسیمی برخوردارند و هنگام فروش می‌توانند به سهام عادی کلاس A با حق رأی تبدیل شوند. با این حال، آمازون در حال حاضر تصمیم گرفته اسناد تعهد به پرداخت به ارزش میلیاردها دلار را نزد خود نگه دارد. اگر این شرکت همین حالا تمام این اسناد را به سهام تبدیل می‌کرد، مالک اندکی کمتر از ۲۴ درصد آنتروپیک (دقیقا ۲۳.۸ درصد) می‌شد. از سوی دیگر سهم گوگل از آنتروپیک به‌اندکی کمتر از ۱۴ درصد (۱۳.۷ درصد) خواهد رسید که آن هم در قالب سهام بدون حق رای است. این سهم از طریق تبدیل اسناد تعهد به پرداخت و همچنین خرید سهام در قالب فروش خصوصی همزمان با عرضه اولیه سهام به دست می‌آید. مجموعه‌ای از شرکت‌های بزرگ فناوری شامل AMD، بوردکام، گوگل، میکرون، مایکروسافت، انویدیا و TSMC Partners توافق کرده‌اند در مجموع ۲۶ میلیارد دلار از این سهام بدون حق رای را بخرند.

محدودیت ۴۰۰ یورویی، توقف رجیستری آیفون ۱۸ و افت ۵۷ درصدی واردات

بن‌بست در واردات گوشی‌های گرانقیمت

بازار تلفن همراه ایران در ماه‌های اخیر با مجموعه‌ای از تصمیم‌های محدودکننده و اختلاف‌نظرهای نهادی مواجه شده که آثار آن به تدریج در زنجیره واردات و عرضه نمایان شده است. در شرایطی که ثبت سفارش تجاری گوشی‌های بالای ۴۰۰ یورو با محدودیت روبرو شده، پرونده رجیستری آیفون ۱۸ نیز به نمونه‌ای تازه از ناهماهنگی میان دستگاه‌های مسوول تبدیل شده است. تعدادی از صاحبان این گوشی‌ها با وجود ثبت اطلاعات در گمرک و پرداخت هزینه‌های قانونی، همچنان امکان فعال‌سازی دستگاه خود را ندارند. این اتفاق در کنار کاهش ۵۷ درصدی ارزش واردات موبایل در نیمه نخست سال، پرسش‌هایی جدی درباره مبنای قانونی محدودیت‌ها، مسوولیت دستگاه‌های اجرایی و آینده تامین رسمی بازار ایجاد کرده است.

ماجرای محدودیت واردات گوشی‌های گران‌قیمت و توقف رجیستری آیفون ۱۸، اکنون فراتر از اختلاف بر سر یک برند یا مدل خاص رفته و به چالشی میان دستگاه‌های متولی تجارت، گمرک و مدیریت سامانه رجیستری تبدیل شده است. در حالی که محدودیت‌های جدید از ۲۰ مهرماه ابلاغ شده‌اند، ادامه ثبت گمرکی برخی گوشی‌ها پس از این تاریخ، شرایطی ایجاد کرده که مصرف‌کنندگان هزینه ورود قانونی دستگاه را پرداخت کرده‌اند، اما در مرحله نهایی امکان استفاده از آن را ندارند. این وضعیت در کنار کاهش چشمگیر واردات موبایل در نیمه نخست سال ۱۴۰۵، نگرانی‌ها درباره آینده تامین رسمی بازار را افزایش داده است. نکته مهم‌تر اینکه محدودیت تعیین‌شده به آیفون اختصاص ندارد و گوشی‌های گران‌قیمت سامسونگ، شیائومی و دیگر برندها را نیز در بر می‌گیرد. بنابراین، ادامه این سیاست می‌تواند دامنه اثرگذاری گسترده‌تری بر بازار تلفن همراه داشته باشد.

آیفون ۱۸؛ قربانی ناهماهنگی سامانه‌ها

از ۲۰ مهرماه محدودیت‌هایی برای ثبت و رجیستری آیفون ۱۸ و برخی گوشی‌های گران‌قیمت اعمال شد، اما ظاهرا اجرای این تصمیم در بخش‌های مختلف زنجیره واردات هم‌زمان نبوده است. در یک بازه زمانی حدود ۱۰ روزه پس از ابلاغ محدودیت، تعدادی از مسافران توانستند اطلاعات گوشی‌های خود را در گمرک ثبت کنند و هزینه‌های مربوط به ورود دستگاه را بپردازند؛ با این حال، هنگام تکمیل فرایند رجیستری با مانع مواجه شدند. نکته مهم در این پرونده، تفاوت میان ثبت گمرکی و فعال‌سازی گوشی است. ثبت اطلاعات در گمرک و پرداخت حقوق ورودی، به معنای امکان استفاده از دستگاه در شبکه تلفن همراه نیست و گوشی باید مراحل مربوط به ثبت و فعال‌سازی در سامانه همتا را نیز پشت سر بگذارد. در پرونده آیفون ۱۸، تعدادی از دستگاه‌ها مرحله نخست را طی کرده‌اند، اما در مرحله نهایی متوقف مانده‌اند. هنوز آماری از تعداد گوشی‌های گرفتار در این وضعیت و مجموع مبالغ دریافت‌شده از صاحبان آنها منتشر نشده است. همچنین مشخص نیست آیا امکان تکمیل رجیستری این دستگاه‌ها فراهم می‌شود یا خریداران باید برای بازپس‌گیری هزینه‌های پرداختی اقدام کنند. این اتفاق یک ابهام اجرایی مهم را مطرح می‌کند: اگر رجیستری یک مدل گوشی ممنوع یا متوقف شده بود، چرا سامانه گمرک همچنان امکان ثبت اطلاعات و دریافت هزینه را فراهم می‌کرد؟ به نظر می‌رسد نبود هماهنگی میان سامانه‌های مرتبط، موجب شده اجرای یک تصمیم در بخش‌های مختلف فرایند واردات با تاخیر و ناهماهنگی همراه شود.

گمرک در برابر محدودیت‌های وزارت صمت

اختلاف میان وزارت صمت و گمرک درباره واردات تلفن همراه، موضوع تازه‌ای نیست. رییس کل گمرک در مکاتبات خود با سازمان توسعه تجارت، توقف رجیستری گوشی‌های وارداتی را مغایر با حقوق مکتسبه واردکنندگان دانسته و بر ضرورت رعایت مقررات در پذیرش اظهارنامه‌های گمرکی تاکید کرده است. بر اساس موضع گمرک، این سازمان نمی‌تواند از پذیرش اظهارنامه کالاهایی که با مجوز معتبر ثبت سفارش وارد شده‌اند، خودداری کند. همچنین از نظر این سازمان، رجیستری پس از انجام تشریفات گمرکی و ترخیص کالا دنبال می‌شود و گمرک نمی‌تواند در حوزه مسوولیت سایر دستگاه‌ها مداخله کند. این اختلاف در واقع به مرزبندی اختیارات دستگاه‌های مسوول بازمی‌گردد. وزارت صمت سیاست‌گذاری تجاری و ثبت سفارش را بر عهده دارد، گمرک تشریفات ورود و ترخیص کالا را انجام می‌دهد و سامانه همتا مسوولیت ثبت و فعال‌سازی تلفن همراه را دنبال می‌کند. هرگونه تغییر در مقررات واردات باید به شکلی اجرا شود که سایر مراحل نیز متناسب با آن به‌روزرسانی شوند. گمرک همچنین درباره پیامدهای توقف رجیستری هشدار داده و از احتمال رسوب کالا، نارضایتی واردکنندگان و کاهش درآمدهای پیش‌بینی‌شده دولت سخن گفته است. با این حال، هنوز پاسخ روشنی درباره مبنای قانونی محدودیت فعلی و نحوه اجرای هماهنگ آن در سامانه‌های مختلف ارایه نشده است.

افت ۵۷ درصدی ارزش واردات موبایل

اختلاف دستگاه‌های اجرایی در شرایطی ادامه دارد که آمارهای گمرکی از کاهش چشمگیر واردات تلفن همراه حکایت می‌کنند. بر اساس اطلاعات اعلام‌شده در نامه رییس کل گمرک، ارزش واردات تجاری موبایل در شش‌ماهه نخست سال ۱۴۰۵ به ۲۸۵ میلیون دلار رسیده که در مقایسه با مدت مشابه سال گذشته ۶۸ درصد کاهش داشته است. در همین دوره، ارزش واردات مسافری نیز با افت ۲۱ درصدی به ۱۹۹ میلیون دلار رسیده است. به این ترتیب، مجموع ارزش واردات تجاری و مسافری تلفن همراه در نیمه نخست سال ۴۸۴ میلیون دلار بوده که کاهش ۵۷ درصدی را نشان می‌دهد. مقایسه این ارقام نشان می‌دهد واردات تجاری بیش از واردات مسافری تحت تاثیر شرایط موجود قرار گرفته است. سهم واردات مسافری از مجموع ارزش واردات موبایل نیز به حدود ۴۱ درصد رسیده است؛ موضوعی که اهمیت این مسیر را در تامین بازار افزایش می‌دهد. البته کاهش ارزش دلاری واردات لزوما به معنای افت تعداد گوشی‌های واردشده به همین میزان نیست و تغییر ترکیب مدل‌ها و سهم گوشی‌های گران‌قیمت نیز بر این شاخص اثر می‌گذارد. با این حال، افت قابل توجه واردات تجاری در کنار محدودیت ثبت سفارش، نگرانی‌ها درباره تامین رسمی بازار را افزایش داده است.



محدودیت ۴۰۰ یورویی؛ فراتر از آیفون

برخلاف تصوری که ممکن است درباره محدودیت‌های اخیر وجود داشته باشد، سیاست تعیین‌شده از سوی وزارت صمت تنها محصولات اپل را هدف قرار نداده است. بر اساس اظهارات فعالان صنفی، ثبت سفارش تجاری گوشی‌های بالای ۴۰۰ یورو برای تمام برندها محدود شده و مدل‌هایی از سامسونگ، شیائومی و سایر تولیدکنندگان نیز در این گروه قرار می‌گیرند. مجید پویان، رییس انجمن تلفن همراه ایران، پیش‌تر به پیوست گفته بود که واردات تجاری گوشی‌های بالای ۴۰۰ یورو متوقف شده و این محدودیت به آیفون اختصاص ندارد. او همچنین با اشاره به تفاوت وضعیت مدل‌های قدیمی و جدید توضیح داده بود که ممکن است برخی گوشی‌هایی که شناسه آنها پیش‌تر در سامانه ثبت شده، همچنان امکان رجیستری مسافری داشته باشند، اما مدل‌های تازه همان برند با محدودیت مواجه شوند. از سوی دیگر، افزایش قیمت جهانی قطعاتی مانند حافظه و رم می‌تواند دامنه این محدودیت را گسترش دهد. در صورت افزایش قیمت تمام‌شده، حتی برخی گوشی‌های میان‌رده نیز ممکن است از مرز ۴۰۰ یورو عبور کنند و مشمول محدودیت ثبت سفارش شوند. به این ترتیب، سیاست فعلی صرفا بازار گوشی‌های لوکس را تحت تاثیر قرار نمی‌دهد و ممکن است به‌تدریج بخشی از محصولات پرتقاضای بازار را نیز در بر بگیرد. در چنین شرایطی، واردکنندگان نمی‌توانند با اطمینان درباره تامین مدل‌های آینده برنامه‌ریزی کنند؛ به‌ویژه آنکه هنوز زمان مشخصی برای پایان محدودیت یا بازنگری در سقف تعیین‌شده اعلام نشده است.

محدودیت واردات بدون مصوبه هیات وزیران؟

یکی دیگر از ابهامات این پرونده، مبنای قانونی اعمال محدودیت ۴۰۰ یورویی است. این تصمیم در حالی اجرا شده که مصوبه‌ای از هیات وزیران برای ممنوعیت واردات گوشی‌های بالای این سقف ارایه نشده است. رییس کل گمرک نیز در نامه خود به رییس سازمان توسعه تجارت بر ضرورت طی مراحل قانونی برای ممنوعیت واردات کالا تاکید کرده است. از نگاه گمرک، نمی‌توان بدون رعایت ضوابط قانونی از پذیرش اظهارنامه کالاهایی که مجوز معتبر ثبت سفارش دارند، خودداری کرد. در کنار این موضوع، مقابله با سوءاستفاده از رویه مسافری نیز در دستور کار دستگاه‌های مسوول قرار گرفته است. رویه مسافری برای ورود گوشی همراه مسافر طراحی شده و نباید به مسیری جایگزین برای واردات تجاری تبدیل شود. تسنیم پیش‌تر از برنامه مشترک وزارت صمت و ستاد مبارزه با قاچاق کالا و ارز برای مقابله با سوءاستفاده از این رویه خبر داده بود. با این حال، برخورد با تخلفات احتمالی نباید به زیان مسافران واقعی تمام شود. در پرونده آیفون ۱۸ هنوز مشخص نیست چه تعداد از گوشی‌های ثبت‌شده متعلق به مسافران واقعی بوده و چه تعداد احتمالا از طریق سوءاستفاده از اطلاعات مسافران وارد کشور شده‌اند. بنابراین، تعیین تکلیف این دستگاه‌ها باید با تفکیک وضعیت قانونی هر پرونده انجام شود.

تجربه‌ای که همچنان تکرار می‌شود

بازار موبایل پیش از این نیز تجربه محدودیت واردات و رجیستری را پشت سر گذاشته است. در سال ۱۴۰۱، هم‌زمان با عرضه آیفون ۱۴، واردات و رجیستری نسل جدید گوشی‌های اپل با محدودیت مواجه شد؛ وضعیتی که تا سال ۱۴۰۳ ادامه یافت و در نهایت مسیر قانونی واردات این محصولات دوباره باز شد. تجربه آن دوره نشان داد محدودیت عرضه رسمی لزوما تقاضای بازار را از بین نمی‌برد و می‌تواند بخشی از خریدوفروش را به مسیرهای غیررسمی منتقل کند. مشکلات رجیستری نیز تنها به محدودیت واردات مربوط نبوده است. هشتم آبان امسال، قاسم نوده‌فراهانی، رییس اتاق اصناف ایران، از رفع مشکل رجیستری نزدیک به چهار هزار گوشی خبر داد که به دلیل کم‌اظهاری برخی واردکنندگان با مشکل مواجه شده بودند. این گوشی‌ها پیش از تعیین تکلیف تخلف واردکنندگان به مصرف‌کنندگان فروخته شده بودند و خریداران در ادامه با مشکل فعال‌سازی مواجه شدند. در نهایت، با پیگیری اتاق اصناف، وزارت صمت و ستاد مبارزه با قاچاق کالا و ارز، امکان رجیستری آنها فراهم شد. با وجود رفع مشکل مصرف‌کنندگان، هنوز جزییات روشنی درباره برخورد با واردکنندگان متخلف و دریافت مابه‌التفاوت حقوق گمرکی منتشر نشده است.

بازار در انتظار تعیین تکلیف

اکنون چند پرسش اساسی درباره آینده واردات تلفن همراه بی‌پاسخ مانده است: سرنوشت آیفون ۱۸هایی که پس از ابلاغ محدودیت در گمرک ثبت شده‌اند چه خواهد شد؟ هزینه‌های پرداختی صاحبان این گوشی‌ها چگونه تعیین تکلیف می‌شود؟ و وزارت صمت محدودیت ۴۰۰ یورویی را بر اساس چه مبنای قانونی و برای چه مدتی اعمال کرده است؟ در شرایطی که ارزش واردات موبایل در نیمه نخست سال ۵۷ درصد کاهش یافته، ادامه این وضعیت می‌تواند بر فعالیت واردکنندگان و دسترسی مصرف‌کنندگان به محصولات مختلف اثر بگذارد. تجربه پرونده آیفون ۱۴ و مشکلات تکرارشونده رجیستری نیز نشان می‌دهد تصمیم‌های مقطعی و ناهماهنگ، بدون حل ریشه‌ای اختلافات اجرایی، صرفا زمینه شکل‌گیری پرونده‌های مشابه را فراهم می‌کنند. بازار موبایل بیش از هر چیز به سیاستی شفاف و هماهنگ در حوزه واردات نیاز دارد؛ سیاستی که در آن محدودیت‌های تجاری، تشریفات گمرکی و مقررات رجیستری هم‌زمان و با اطلاع‌رسانی روشن اجرا شوند. در غیر این صورت، احتمال اینکه خریداران و واردکنندگان بار دیگر هزینه اختلاف میان دستگاه‌های مسوول را بپردازند، همچنان وجود دارد.

دنیای فناوری

اپل در فرانسه بر سر منسوخ‌سازی آیفون‌ها محاکمه می‌شود

شرکت فناوری امریکایی اپل در پی شکایت یک انجمن حمایت از مصرف‌کنندگان بر سر منسوخ‌سازی برنامه‌ریزی شده چندین مدل آیفون، در ژوئن ۲۰۲۷ در فرانسه محاکمه خواهد شد. به گزارش ایسنا، انجمن فرانسوی «توقف منسوخ‌سازی برنامه‌ریزی‌شده» (HOP) که علیه این رویه فعالیت می‌کند، اعلام کرد دادستانی پاریس تصمیم گرفته است اپل را به دلیل اقداماتی که مانع از تعمیر و بازسازی آیفون‌ها در خارج از شبکه خدمات مجاز این شرکت می‌شود، تحت پیگرد قرار دهد. این پرونده شامل ۲۴ مدل آیفون است و در پی شکایتی که هفتم دسامبر ۲۰۲۲ توسط انجمن HOP ثبت شده، به جریان افتاده است. این انجمن اعلام کرد که یک جلسه مقدماتی برای تعیین زمان‌بندی محاکمه در ۲۵ فوریه ۲۰۲۷ برگزار خواهد شد و انتظار می‌رود جلسات رسیدگی دادگاه نیز در ژوئن، طی چند روز برگزار شوند. محور اصلی این پرونده، رویه‌ای موسوم به «سری‌سازی» (serialization) است که در آن شماره سریال قطعات مختلف دستگاه - نظیر صفحه‌نمایش، باتری و دوربین - به خود گوشی متصل و در سیستم ثبت می‌شود. انجمن HOP مدعی است که این سیستم می‌تواند در صورتی که قطعات توسط تعمیرکارانی خارج از شبکه مجاز اپل تعویض شوند، باعث بروز اختلال در عملکرد دستگاه شود؛ حتی اگر از قطعات یدکی اصل استفاده شده باشد اما تاییدیه نرم‌افزاری اپل برای آنها صادر نشده باشد. بر اساس گزارش خبرگزاری آناتولی، انجمن HOP خاطرنشان کرد که اپل از سال ۲۰۲۲، اقداماتی را برای محدود کردن «سری‌سازی» در آیفون‌های جدیدتر و امکان‌پذیر ساختن تایید برخی تعمیرات انجام شده توسط تعمیرکاران ثالث، اعلام کرده است. با این حال، این انجمن افزود که میزان کارآمدی این تغییرات باید در گذر زمان مشخص و تایید شود.

ایالت اورگن جدیدترین شاکی اوپن‌ای‌آی شد

دن ریفیلد، دادستان کل ایالت اورگن، شکایتی علیه شرکت اوپن‌ای‌آی تنظیم کرده است. به گزارش خبرگزاری مهر به نقل از انگجت، این شرکت متهم شده کودکان ایالت مذکور را در معرض خطر قرار داده، افکار عمومی را درباره ایمنی محصولات خود گمراه و قانون حمایت از مصرف‌کنندگان و مقابله با رویه‌های تجاری غیرقانونی این ایالت را نقض کرده است. این شکایت تازه‌ترین مورد از مجموعه اقدامات حقوقی دادستان‌های کل ایالت‌های مختلف امریکا علیه اوپن‌ای‌آی است. بسیاری از این ایالت‌ها به نحوه طراحی چت جی‌پی‌تی، شیوه تبلیغ خدمات این شرکت و در مورد شکایت اخیر کالیفرنیا، نقش اوپن‌ای‌آی در ماجرای مربوط به پلتفرم هاگینگ فیس اعتراض دارند. در شکایت ایالت اورگن ادعا شده تلاش اوپن‌ای‌آی برای افزایش تعداد کاربران، باعث شده چت جی‌پی‌تی به گونه‌ای به درخواست‌ها پاسخ دهد که بیش از حد تأییدکننده و موافق باشد و به تعبیر شاکیان، طوری طراحی شده که دقیقا همان چیزی را به کاربران بگوید که دوست دارند بشنوند. براساس ادعای مقام‌های این ایالت، این مساله به‌ویژه زمانی خطرناک می‌شود که کودکان درباره موضوعات حساس با این چت‌بات گفت‌وگو می‌کنند. در شکایت مذکور همچنین ادعا شده اوپن‌ای‌آی با وجود آگاهی از خطراتی که محصولاتش برای کودکان دارند، به‌طور مستقیم به‌دنبال جذب این گروه سنی رفته و تجربه‌ای با عنوان «چت‌جی‌پی‌تی برای نوجوانان» راه‌اندازی کرده است. گروه‌های حامیان ایمنی کودکان نیز پیش‌تر درباره حساب‌های کاربری نوجوانان ابراز نگرانی کرده و گفته‌اند که دور زدن برخی از تدابیر حفاظتی این حساب‌ها بسیار آسان است. به گفته مقام‌های ایالت اورگن، این مسائل در کنار ضعف‌های رویکرد اوپن‌ای‌آی در تشخیص خودکار سن کاربران، نشان می‌دهد که این شرکت از ساکنان ایالت اورگن سود کسب می‌کند، در حالی که یک معضل عمومی تهدیدکننده امنیت آنان به‌وجود آورده است. این ایالت از دادگاه درخواست کرده با صدور حکمی قضایی، اوپن‌ای‌آی را وادار کند تا از ارایه اطلاعات گمراه‌کننده درباره ایمنی و مناسب‌بودن چت جی‌پی‌تی برای نوجوانان از نظر سنی دست بردارد و خطرات محصولات خود برای کودکان را به‌طور شفاف و کافی اعلام کند. این ایالت همچنین خواستار دریافت دست‌کم دو میلیارد دلار غرامت و جریمه‌های مدنی از اوپن‌ای‌آی شده است. دن ریفیلد در بیانیه‌ای گفت: اوپن‌ای‌آی می‌داند که چت‌جی‌پی‌تی به کودکان آسیب می‌رساند، اما برای اصلاح معنادار این پلتفرم خطرناک اقدامی نکرده است.

بی‌تفاوتی ترامپ به قطعی شبکه ارتباطات آژانس امنیت ملی امریکا

شبکه بسیار محرمانه‌ای که آژانس امنیت ملی امریکا از آن برای ارتباطات داخلی استفاده می‌کند طی فرایند نگهداری برنامه‌ریزی شده با اختلال روبرو شد. به گزارش مهر به نقل از رویترز، سازمان مذکور اعلام کرد: هرچند سیستم‌های داخلی تحت تاثیر این اختلال قرار گرفته‌اند اما قابلیت‌های مهم برای ماموریت همچنان قابل استفاده بودند و توانایی ما برای دفاع از امنیت ملی کشور ادامه می‌یابد. سی‌ان‌ان نخستین شبکه خبری بود که از این قطعی خبر داد و اعلام کرد شبکه مختل شده NSANet که به کارمندان این آژانس دولتی اجازه می‌دهد اطلاعات محرمانه را به اشتراک بگذارند، دچار مشکل شده است. این قطعی در حالی رخ داده که نگرانی‌ها درباره مجموعه‌ای از مشکلات به‌خصوص اختلالاتی که ترافیک هوایی امریکا را برهم زد و قطعی ایمیل مایکروسافت در هفته گذشته بیشتر شده است. از سوی دیگر دونالد ترامپ رییس جمهور امریکا این قطعی‌ها را کم‌اهمیت جلوه داد و گفت چنین مشکلاتی اجتناب‌ناپذیر هستند. در این میان سناتور جاش هاولی نماینده جمهوری‌خواه ایالت میسوری به خبرنگاران گفت: اگر این رویدادها یک تصادف باشد، باید آن را بزرگ‌ترین تصادف تاریخ جهان دانست. ترامپ پیش از این نیز چنین رویدادهایی را کم‌اهمیت جلوه داده بود و همین امر سوالاتی درباره آنکه آیا دولت و بخش خصوصی برای اخراج کارمندان بخش فناوری عجله کرده‌اند یا خیر، به‌وجود آورده است. ترامپ در مانیل پایتخت فیلیپین به خبرنگاران گفت: وقتی بزرگ و قدرتمند هستیم و پول در اختیار داریم چنین اتفاقاتی می‌افتد. مساله‌ای نیست. به گفته مارکو روبیو وزیر امور خارجه امریکا که به‌عنوان مشاور امنیت ملی نیز فعالیت می‌کند، این رویدادها ناراحت‌کننده هستند اما کاملا بی‌ارتباط هستند و هیچ شواهدی مبنی بر آنکه عاملان مخرب آنها را به‌وجود آورده‌اند، وجود ندارد.

۵ نشانه که از هک گوشی خبر می‌دهند

روش‌های بسیاری وجود دارد که افراد سودجو ممکن است از طریق آنها برای دسترسی به تلفن همراه شما تلاش کنند؛ از کلاهبرداری‌های فیشینگ گرفته تا نصب بدافزارهای مخرب، هکرها همواره به دنبال راهی برای نفوذ به اطلاعات شخصی و حساب‌های کاربری شما هستند. به گزارش ایسنا، زیر نظر داشتن عملکرد دستگاه - برای تشخیص موارد غیرعادی - و همچنین اطمینان از اینکه تماس‌ها یا پیامک‌های شما به دستگاه دیگری منتقل (دایورت) نشده باشند، راه‌کارهای بسیار خوبی برای حفظ امنیت و کنترل اوضاع هستند. اگر نگران هک شدن گوشی خود هستید، تنها نیستید. در عصر حاضر، امنیت سایبری به یکی از دغدغه‌های اصلی تبدیل شده است؛ به‌ویژه آنکه هکرها اکنون می‌توانند با استفاده از هوش مصنوعی، دست به اقدامات پیچیده‌ای مانند نفوذ به سیستم‌های «خانه هوشمند»، بزنند. متاسفانه، بسیاری از نشانه‌های هک شدن گوشی ممکن است با مشکلات معمولی که گوشی‌های قدیمی‌تر دچار آن می‌شوند - نظیر کاهش عمر باتری، افت عملکرد دستگاه یا مشکلات مربوط به حافظه - شباهت زیادی داشته باشند. با این حال، نشانه‌های مهمی وجود دارد که می‌تواند ثابت کند فردی به‌طور غیرمجاز به گوشی یا حساب‌های کاربری شما دسترسی پیدا کرده است؛ مواردی همچون شنیدن صداهای عجیب در پس‌زمینه هنگام مکالمه، وجود برنامه‌هایی که به یاد نمی‌آورید آنها را نصب کرده باشید، دریافت هشدارهای ورود به حساب کاربری که انتظارش را نداشتید و غیره. نسبت به این علائم هوشیار باشید و در صورت مشاهده آنها - به‌ویژه اگر چندین مورد را هم‌زمان تجربه کردید - اقدامات اصلاحی لازم را انجام دهید.

وجود برنامه‌ای روی گوشی که خودتان آن را نصب نکرده‌اید

معمولا تشخیص یک برنامه ناشناس روی گوشی آسان است، اما برخی بدافزارها به گونه‌ای طراحی شده‌اند که اصلا عجیب یا ناآشنا به نظر نرسند. «رت‌هت» (RatHat) که یک تهدید بدافزاری جدید برای کاربران گوشی‌های اندرویدی است، ظاهر برنامه‌هایی از جمله مرورگر «گوگل کروم» را تقلید می‌کند که اکثر افراد از قبل روی گوشی خود دارند. این بدافزار عمدتا از طریق پیامک‌ها و سایت‌های دانلود جعلی که شبیه به «گوگل پلی استور» هستند، منتشر می‌شود. اگر کاربر آن را باز کند و دسترسی مدیریتی (admin access) به آن بدهد، بدافزار یک عامل هوش مصنوعی را نصب می‌کند که در پس‌زمینه فعال شده و گذرواژه‌ها، کدهای تایید دومرحله‌ای و پیام‌های موجود در گوشی را سرقت می‌کند. اگر گوشی شما درخواست نصب برنامه‌ای را داد که همین حالا هم روی دستگاه دارید (مثلا یک نسخه دیگر از گوگل کروم)، این می‌تواند نشانه‌ای از حضور بدافزار «رت‌هت» باشد. در سیستم‌عامل اندروید، قابلیت «گوگل پلی پروتکت» (Google Play Protect) به‌صورت پیش‌فرض فعال است و در بیشتر موارد، برنامه‌های مخرب را به‌طور خودکار حذف می‌کند. با این حال، پاک‌سازی «رت‌هت» دشوارتر از سایر بدافزارهاست و تنها راه حذف کامل آن، بازگرداندن گوشی به تنظیمات کارخانه است. اگر از آیفون استفاده می‌کنید، بهتر است در برنامه «تنظیمات» (Settings) و در بخش «عمومی» (General)، به قسمت «مدیریت دستگاه و وی‌پی‌ان» بروید و بررسی کنید که آیا پروفایل‌های پیکربندی (configuration profiles) ناشناسی در آنجا وجود دارد یا خیر. بسیاری از مدارس و کسب‌وکارها از این پروفایل‌ها برای مدیریت آیفون‌هایی که در اختیار افراد قرار می‌دهند استفاده می‌کنند، اما اپل هشدار می‌دهد که این پروفایل‌ها ممکن است امکان دسترسی به اطلاعات یا موقعیت مکانی شما را فراهم کنند. اگر پروفایلی مربوط به محل کارتان باشد، جای نگرانی نیست، اما اگر نمی‌دانید منشأ یک پروفایل چیست، بهتر است آن را حذف کنید. البته به خاطر داشته باشید که با حذف یک پروفایل، تمام تنظیمات، برنامه‌ها و داده‌هایی که همراه آن نصب شده‌اند نیز پاک خواهند شد.

دریافت هشدارهای ورود به حساب (لاگین) که انتظارش را نداشتید

اگر کد تایید دومرحله‌ای برایتان ارسال شد، در حالی که خودتان قصد ورود به حساب کاربری‌تان را نداشتید، این می‌تواند نشانه‌ای از هک شدن یا نفوذ به حساب اپل شما باشد. موارد مشکوک دیگر شامل پیام‌هایی است که به یاد نمی‌آورید آنها را ارسال کرده باشید، یا خریدهایی که آنها را نمی‌شناسید. شرکت‌های دیگر، مانند گوگل نیز هشدارهای ورود ارسال می‌کنند و اگر فعالیت غیرمنتظره یا غیرعادی در ورود به حساب کاربری‌تان از طریق دستگاه مشاهده کنند، به شما اطلاع خواهند داد. در بسیاری از موارد، چنین هشدارهایی صرفا به این معناست که فرد دیگری در تلاش است به حساب کاربری شما دسترسی پیدا کند. این می‌تواند به این معنا باشد که آنها رمز عبور شما را به دست آورده‌اند و تلاش می‌کنند از طریق دستگاه خودشان به حساب شما دسترسی پیدا کنند. خوشبختانه، دور زدن «احراز هویت دو مرحله‌ای» بسیار دشوارتر است، اما همین موضوع باعث می‌شود برخی حملات، خود گوشی را هدف قرار دهند. برای مثال، در حمله موسوم به «پیکس‌نپینگ» (Pixnapping) به گوشی‌های اندرویدی، از یک برنامه مخرب استفاده می‌شود تا محتوای صفحه‌نمایش شما، پیکسل به پیکسل، بازسازی شود. پژوهشگران دریافته‌اند که این روش می‌تواند کد احراز هویت دو مرحله‌ای را تنها در ۱۴ ثانیه - خیلی پیش از آنکه کد منقضی شود - به دست آورد.

مشاهده پنجره‌های پاپ‌آپ (تبلیغاتی) در زمانی که مشغول وب‌گردی نیستید

تبلیغات پاپ‌آپ (Pop-up) آزاردهنده‌اند، اما بیشتر ما یاد گرفته‌ایم که به‌سادگی آنها را ببندیم و به کارمان ادامه دهیم. «کمیسیون تجارت فدرال» (FTC) امریکا وجود تعداد بیش از حد تبلیغات پاپ‌آپ را یکی از نشانه‌های بدافزار می‌داند؛ و اگر تبلیغات حتی زمانی که مرورگری باز ندارید همچنان ظاهر می‌شوند، این یک هشدار بسیار جدی‌تر است. در برخی گوشی‌های اندرویدی ارزان‌قیمت، حتی نیازی نیست چیزی دانلود کنید تا این اتفاق رخ دهد. پژوهشگران شرکت «بیت‌دیفندر» رد بدافزاری را که به‌صورت پیش‌فرض روی هزاران گوشی اندرویدی ارزان‌قیمت نصب شده بود، تا یک شبکه تبلیغاتی دنبال کردند. این بدافزار که پژوهشگران آن را «میدنایت میموسا» نامیده‌اند، در نرم‌افزار سیستمی گوشی پنهان می‌شود و برنامه‌هایی مانند هواشناسی یا سایر ابزارهای کوچک را نصب می‌کند. سپس از این برنامه‌ها برای نمایش تبلیغات استفاده می‌کند، حتی اگر شما هرگز آنها را باز نکنید. گوشی‌های آلوده عمدتا از تراشه‌های «مدیاتک» استفاده می‌کنند و تحت برندهایی مانند «کیوبوت» (Cubot) و «دوجی» (Doogee) فروخته می‌شوند. همچنین شامل نسخه‌های تقلبی سری «گلکسی اس» سامسونگ نیز می‌شوند. علاوه بر این، همیشه باید از نصب میان‌افزارهای (Firmware) غیررسمی یا استفاده از راهکارهای سریعی که به‌صورت آنلاین منتشر می‌شوند، خودداری کنید، زیرا این موارد اغلب می‌توانند مشکل را بدتر کنند.

داغ شدن گوشی در زمانی که از آن استفاده نمی‌کنید

اگر گوشی شما در حالی که صرفا روی میز قرار دارد داغ می‌شود، یا شارژ باتری‌اش به‌طور ناگهانی ساعت‌ها زودتر از یک ماه پیش تمام می‌شود، احتمالا برنامه‌ای در پس‌زمینه در حال اجراست که شما از آن بی‌خبرید. هر فعالیتی که بدافزار روی گوشی شما انجام می‌دهد، بخشی از توان پردازشی و شارژ باتری را مصرف می‌کند؛ به همین دلیل، داغ شدن دستگاه و تخلیه سریع‌تر باتری، از نشانه‌های رایج آلوده شدن گوشی اندرویدی شما به ویروس هستند. برای مثال، بدافزار «رت‌هت» یک عامل هوش مصنوعی را در پس‌زمینه فعال نگه می‌دارد تا فعالیت‌های شما را زیر نظر بگیرد. با این حال، پیش از آنکه به‌سراغ حذف برنامه‌ها بروید، ابتدا باید احتمال وجود دلایل عادی و معمول را بررسی و رد کنید. داغ شدن باتری باعث می‌شود شارژ آن بسیار سریع‌تر خالی شود، حتی زمانی که از گوشی استفاده نمی‌کنید. همچنین، پس از به‌روزرسانی نرم‌افزاری، ممکن است شارژ گوشی برای مدتی کوتاهی سریع‌تر از حالت معمول تمام شود، زیرا دستگاه در حال تکمیل برخی پردازش‌ها در پس‌زمینه است. این وضعیت در مورد گوشی‌های کاملا نو نیز ممکن است رخ دهد و شاید لازم باشد چند روز صبر کنید تا عملکرد دستگاه و وضعیت مصرف باتری به حالت پایدار و عادی برسند. اگر هیچ‌یک از این موارد دلیل مشکل شما نیستند، می‌توانید از طریق تنظیمات باتری گوشی بررسی کنید که کدام برنامه باعث بروز این مساله شده است. در اکثر دستگاه‌ها، با مراجعه به بخش «باتری» (یا گزینه‌ای مشابه)، می‌توانید ببینید دقیقا کدام برنامه‌ها از باتری شما استفاده کرده‌اند و میزان فشار آنها بر منابع سیستم چقدر بوده است.

گوشی شما بیش از حد معمول از اینترنت (داده) استفاده می‌کند

افزایش ناگهانی مصرف داده می‌تواند نشانه‌ای از وجود مشکل در گوشی شما باشد؛ زیرا هر عامل یا شخصی که اطلاعات را از گوشی شما سرقت می‌کند، باید آن داده‌ها را به مقصد دیگری ارسال نماید. در مورد بدافزار «رت‌هت»، اطلاعات سرقت شده از طریق یک پروکسی برای هکرهای پشت‌پرده ارسال می‌شود. بدافزار «میدنایت میموسا» نیز به شیوه متفاوتی باعث مصرف داده می‌شود. این بدافزار گوشی شما را به یک «پروکسی خانگی» تبدیل می‌کند تا از آن برای هدایت ترافیک اینترنتی دیگران استفاده شود. بر اساس گزارش وب سایت بی‌جی‌آر، هم در آیفون و هم در اندروید، می‌توانید میزان مصرف داده توسط هر برنامه را مشاهده کنید. این کار به شما کمک می‌کند تا بر فعالیت برنامه‌ها نظارت داشته باشید و بهتر است آن را به‌بخشی از بررسی‌های امنیتی همیشگی دستگاه خود تبدیل کنید. همچنین اگر مشکوک هستید که حجم داده‌های مصرفی بیش از حد انتظار است، اپل توصیه می‌کند با اپراتور تلفن همراه خود تماس بگیرید، زیرا آنها دقیق‌ترین اطلاعات را در این زمینه در اختیار دارند.