کرونا زمینه‌ساز بزرگ‌ترین هک های سال ۲۰۲۰

میترا جلیلی
خبرنگار

همزمان با شیوع کرونا بازار حمله‌های سایبری نیز داغ شد و کار به جایی کشید که پلیس اینترپل و یوروپل نسبت به افزایش تعداد این حملات هشدار دادند. به دنبال این هشدارها، گوگل هم در اواسط ماه آوریل سال‌جاری گزارش داد که تنها در یک هفته روزانه بیش از ۱۸ میلیون حمله بدافزاری اسکم یا فیشینگ ایمیل مرتبط با کووید ۱۹ را ثبت کرده که این، رقمی بسیار چشمگیر است و نشان از افزایشی ۳۰ درصدی نسبت به هفته‌های پیشین دارد. اکنون در میانه سال ۲۰۲۰ قرار داریم و در مدتی که از سال ۲۰۲۰ گذشته، شاهد هک‌ها و حمله‌های گسترده‌ای بوده‌ایم که البته برخی از آنها با شیوع کرونا بی‌ارتباط نیستند. اما بزرگ‌ترین هک‌های سال ۲۰۲۰ تاکنون، کدام حمله‌های سایبری بوده‌اند؟

گردشگری زیر تیغ هکرها

با وجودی که سفر و گردشگری در دوران کرونا رونق چندانی نداشت اما ماجرای هک ایرلاین Easyjet در ماه مه سال ۲۰۲۰ خبرساز شد. در قالب این هک، اطلاعات ایمیل آدرس و اطلاعات سفر ۹ میلیون مشتری این ایرلاین بریتانیایی به سرقت رفت. این اطلاعات شامل کدهای ۹ رقمی و همچنین CVV سه رقمی کارت‌ها و نیز تاریخ انقضای کارت و... بوده است. به‌دنبال اعلام این هک، ایرلاین Easyjet به مشتریانش هشدار داد تا رمز عبور خود برای ورود به سرویس‌های Easyjet را تغییر بدهند. همچنین این ایرلاین به پرداخت ۱۸ میلیارد پوند غرامت به‌دلیل سهل‌انگاری در محافظت از اطلاعات کاربران و مشتریان محکوم شد. یکی دیگر از هک‌های بزرگ سال ۲۰۲۰ در حوزه گردشگری را می‌توان حمله سایبری به یک هتل دانست. طی این هک در ماه مارس درمجموع اطلاعات ۵،۲ میلیون نفر از میهمانان هتل Marriott فاش شد. هکرها با دسترسی به اکانت دو نفر از کارمندان هتل Marriott موفق شدند به اطلاعات کاربران دسترسی پیدا کنند. این اطلاعات شامل نام، جنس، سن، شماره تلفن و اطلاعات سفر مسافر بوده است به همین دلیل هم نارضایتی بسیار مسافران را به‌دنبال داشت و در شرایط کرونا که این هتل عملاً غیرفعال بود، اعلام خبر هک ضربه‌ای سنگین‌تر به پیکر این هتل معروف وارد کرد. البته گفته می‌شود این هک از ژانویه ۲۰۲۰ آغاز شده بوده ولی تا فوریه از چشم محققان سایبری و تیم‌های امنیت سایبری پنهان مانده بود، این بدان معناست که هکرها به‌مدت ۶ هفته فرصت داشتند تا اطلاعات مشتریان هتل را دروکنند. این، دومین هک بزرگ اطلاعات مشتریان این هتل در سال‌جاری به شمار می‌رود چرا که در ماه فوریه نیز اطلاعات ۱۰،۶ میلیون نفر از مشتریان این هتل سرقت شد که در میان آنها نام «جاستین بیبر» خواننده معروف و همچنین «جک دورسی» مدیرعامل توئیتر دیده می‌شود.

هک گسترده ابزارهای ارتباطی دیجیتال

در دوران قرنطینه و دورکاری، کاربران از ابزارهای ارتباطی دیجیتال بیشترین بهره را گرفتند و در این میان شاید بتوان گفت محبوب‌ترین آنها اپلیکیشن‌های ارتباطی زوم (Zoom) ، Microsoft Teams و همچنین Google Meet بودند. اما همانقدر که این اپ‌ها مورد توجه کاربران قرار داشتند هکرها نیز نسبت به آن بی‌توجه نبودند و به‌دنبال فرصتی می‌گشتند تا حمله سایبری خود را عملی کنند. درنهایت مشخص شد در شرایطی که بیشتر کاربران به نوعی به اپلیکیشن زوم اعتماد پیدا کرده‌اند، اطلاعات بیش از ۵۰۰ هزار نفر از کاربران این اپلیکیشن در فضای وب تاریک (Dark Web) و تالارهای هکرها فاش شده است و عملاً هکرها در حال خرید و فروش این اطلاعات هستند. گفته می‌شود در این حمله سایبری اطلاعات کاربرانی افشا شده است که برای حساب‌های کاربری مختلف خود یک رمز عبور را مورد استفاده قرار داده‌اند. درواقع اکانت این کاربران در فضایی دیگر لو رفته و به‌دلیل مشابه بودن رمزهای عبور، اطلاعات آنها در اپلیکیشن زوم نیز به سرقت رفت. به همین دلیل هم محققان حوزه سایبری بلافاصله از کاربران زوم یا سایر اپلیکیشن‌های ارتباطی درخواست کردند برای استفاده از این راه‌های ارتباطی دیجیتال حتماً یک رمز انحصاری استفاده کنند تا احتمال هک شدن حساب کاربری آنها به حداقل ممکن برسد. Microsoft Teams نیز از حمله هکرها در امان نماند و مورد حمله بدافزاری قرار گرفت. به محض اینکه قربانیان روی آیکون Open Microsoft Teams کلیک می‌کردند، به یک آدرس جعلی وارد می‌شدند و کامپیوتر آنها در اختیار هکرها قرار می‌گرفت. Google Meets هم با دامنه‌های جعلی همچون .\Googelmeets com در آوریل ۲۰۲۰ مورد حمله سایبری قرار گرفت و کاربران به جای وب سایت اصلی به وب‌سایتی راهنمایی می‌شدند که در تصرف هکرها قرار داشت.

لو رفتن اطلاعات ۴۴۰ میلیون کاربر

یکی دیگر از هک‌های بزرگ سال ۲۰۲۰ به یکی از بزرگ‌ترین کمپانی‌های آرایشی جهان مربوط می‌شود. در سال‌جاری میلادی مشتریان کمپانی آرایشی Estée Lauder از هک در امان نماندند و اطلاعات ۴۴۰ میلیون مشتری مورد دستبرد هکرها قرار گرفت. حتی ایمیل‌های داخلی این کمپانی آرایشی نیز مورد حمله سایبری قرار گرفت و نام مشتریان، شماره تلفن، لیست خرید و.... فاش شد و نارضایتی این مشتریان را به‌دنبال داشت. محققان عرصه سایبری اعلام کردند که هکرها می‌توانند با استفاده از هک ایمیل مشتریان، اطلاعات کارت‌های بانکی آنها را به دست آورده و حساب را خالی کنند یا اینکه حملات فیشینگ انجام دهند. این کمپانی به‌دلیل این حمله سایبری بسیار مورد سرزنش قرار گرفت چرا که از اطلاعات دیتابیس این کمپانی بخوبی محافظت نکرده بود و رمزگذاری‌های پیشرفته‌ای در آن دیده نمی‌شد.

گیمرها در کانون توجه هکرها

یکی دیگر از هک‌های قابل تأمل سال ۲۰۲۰ مربوط به بازی نینتندو بود. با توجه به اینکه در دوران قرنطینه تعداد زیادی از کاربران جهان به گیم و بازی‌های ویدئویی علاقه‌مند شدند هکرها نیز از این ظرفیت بزرگ غافل نماندند و به کاربران این حوزه حمله کردند. در این حمله سایبری که در اوایل آوریل انجام شد، اطلاعات بیش از ۳۰۰ هزار نفر از کاربران نینتندو فاش شد. این اطلاعات شامل اطلاعات شخصی همچون تاریخ تولد، کشور، آدرس ایمیل، رمز ورود و... بود و حتی برخی از این اطلاعات به فروش هم رسید. به‌دنبال وقوع این هک، کمپانی نینتندو بلافاصله قربانیان را ازطریق ایمیل مطلع کرد و از همه کاربران خود در جهان خواست تا تأیید دومرحله‌ای را برای ورود به حساب کاربری خود فعال کنند؛ موضوعی که محققان بارها نسبت به آن هشدار داده‌اند و معتقدند کاربران باید آن را در همه اکانت‌های خود در شبکه‌های اجتماعی، اپلیکیشن‌ها و... رعایت کنند تا کمتر در معرض هک قرار بگیرند. همچنین رمزهای عبور اکانت‌هایی که مورد حمله سایبری قرار گرفته بودند بلافاصله توسط نینتندو عوض شد و راه دسترسی به اکانت‌های نینتندو از طریق NNID مسدود شد. NNID‌ها پیش از این برای وسایل Wii U مورد استفاده قرار می‌گرفت اما آخرین مدل‌های نینتندو از Nintendo Account system بهره می‌گیرند به همین دلیل هم کاربران این مدل از نینتندوها در برابر هکرها امنیت بیشتری دارند. با وجودی که تعداد قربانیان این حمله هکری چندان بالا نبود اما محققان حوزه سایبری معتقدند به‌دلیل افزایش تعداد گیمرها در جهان باید منتظر اخبار بیشتری از هک‌های گسترده در این حوزه باشیم.

این وام‌های پردردسر

یکی دیگر از هک‌های سال ۲۰۲۰ باز هم به شیوع کرونا مربوط می‌شود. کسب و کارهای کوچک در امریکا به‌دلیل کرونا آسیب فراوانی دیدند و به همین دلیل هم تلاش شد تا وام‌هایی مشخص به شاغلان این حوزه اختصاص یابد. تعداد زیادی از کاربران درخواست وام ۱۰ هزار دلاری داشتند اما اطلاعات حداقل ۸ هزار نفر از این افراد مورد دستبرد هکرها قرار گرفت. درواقع از طریق پرتالی که برای تقاضای وام ایجاد شده بود نام، شماره تلفن، آدرس پستی و ایمیل، تاریخ تولد، وضعیت شهروندی و اطلاعات بیمه کاربران مورد سرقت قرار گرفت. هرچند تعداد قربانیان این هک نیز چندان بالا نیست اما از نگاه محققان حوزه سایبری نمی‌توان نسبت به این موضوع بی‌توجه بود چرا که هکرها به سایر پرتال‌های مشابه هم همین نگاه را دارند و احتمال می‌رود پرتال‌های درخواست بیمه بیکاری، ثبت مشخصات افرادی که شغل خود را از دست داده‌اند و... نیز مورد حمله هکرها قرار بگیرد.

هک یک شرکت ارتباطی بزرگ

لو رفتن اطلاعات بیش از یک میلیون نفر از مشتریان کمپانی T-Mobile و برخی کارمندان، این کمپانی بزرگ ارتباطی جهان در ماه مارس بار دیگر شرکت‌های ارتباطی را در کانون توجه قرار داد. در شرایطی که به‌دلیل کرونا بیشتر مردم جهان تنها راه ارتباطی خود را اینترنت می‌دانستند، این خبر بازتاب گسترده‌ای داشت. این حمله هکری از طریق ارسال فایل‌های آلوده به بدافزار به مشتریان کمپانی T-Mobile صورت گرفت. این کمپانی اعلام کرد که اطلاعات حساب‌های بانکی مشتریان و برخی کارمندان این کمپانی و نیز شماره و کدهای امنیتی آنان وهمچنین شماره تلفن و تماس‌های داخلی و خارجی آنها به سرقت رفته اما هیچ یک از اطلاعات کارت‌های بانکی یا پرداخت‌های مالی در دسترس هکرها قرار نگرفته است. این کمپانی در سال ۲۰۱۸ هم شاهد یک حمله هکری دیگر بود که طی آن اطلاعات ۲ میلیون مشتری این کمپانی هک شد و عاملان این حمله سایبری هکرهای بین‌المللی عنوان شدند.

یک اتهام بزرگ برای مایکروسافت

همزمان با سال نو میلادی خبر انتشار اطلاعات ۲۵۰ میلیون کاربر مایکروسافت، همه را شگفت‌زده کرد. این اطلاعات مربوط به کاربران در طول ۱۴ سال گذشته بود و در طول دو روز هرکسی در مرورگر وب می‌توانست به این اطلاعات دسترسی داشته باشد. بسیاری آن را یک هک بزرگ نامیدند اما مایکروسافت عنوان کرد که آسیب‌پذیری و نقص در یکی از دیتابیس‌های خود سبب شد بخشی از سوابق مربوط به مشتریان و کاربرانی که با بخش پشتیبانی و خدمات این شرکت در ارتباط بودند، به‌طور موقت لو برود. مایکروسافت می‌گوید قسمت اعظم داده‌های لو رفته شامل اطلاعات اصلاح شده هستند که هکرها نمی‌توانند از آنها استفاده کنند. ولی شرکت Comparitech می‌گوید برخی اطلاعات شامل ایمیل و آدرس IP در فایل متنی ذخیره شده هستند و هکرها می‌توانند با استفاده از آنها خود را جای کارمندان مایکروسافت جا زده و کاربران را به سایت‌های فیشینگ منتقل کنند. به هرحال مایکروسافت این را هرگز به‌عنوان یک هک قبول نکرد و تنها آن را نشت داده‌ها و اطلاعات به‌دلیل یک آسیب‌پذیری دانست.

چگونه از کامپیوتر خود مراقبت کنیم؟

نرم افزار آنلاین | روی وب

این روزها بحث آموزش آنلاین کماکان داغ است و کم نیستند کسانی که از کامپیوتر و لپ‌تاپ برای انجام کارهای خود استفاده می‌کنند. دراستفاده ازاین دستگاه‌ها باید دقت کرد چرا که روشن ماندن طولانی مدت، به‌دستگاه صدمه می‌زند بنابراین دراین مطلب سعی داریم به‌شما بگوییم از کدام حالت دستگاه برای استفاده بهینه بهره ببریم.

به‌گزارش زومیت، دراین دستگاه‌ها چند گزینه مانند خاموش کردن دستگاه (Shut Down)، حالت خواب (Sleep) و خواب زمستانی (Hibernate) وجود دارد و می‌توان برای جلوگیری از صدمات وارده به دستگاه از یکی از گزینه‌ها استفاده کرد.

خاموش کردن (Shut Down): این همان حالت خاموش کردن کامل کامپیوتر است وقتی کامپیوتر خود را خاموش کنید، تمام برنامه‌های شما بسته خواهند شد بنابراین برای روشن کردن آن باید منتظر مراحل معمولی بوت شدن باشید.

حالت خواب (Sleep): در حالت خواب، دستگاه شخصی شما وارد حالت کم مصرف می‌شود. تمام وضعیت کامپیوتر در حافظه ذخیره خواهد شد، اما سایر قسمت‌های رایانه خاموش می‌شود و از هیچ انرژی استفاده نخواهد کرد. هنگامی که رایانه را روشن می‌کنید، سریعاً شاهد اجرا شدن سیستم‌عامل خواهید شد و نیازی نیست که منتظر بمانید؛ تمام فرآیندها و برنامه‌ها از جایی ادامه خواهند یافت که آنها را رها کردید.

خواب زمستانی (Hibernate): رایانه شما وضعیت فعلی خود را در هارد دیسک ذخیره خواهد کرد و در حالت کلی می‌تواند محتوای حافظه را روی یک فایل، قرار دهد. وقتی کامپیوتر را بوت می‌کنید، حالت قبلی را از دیسک سخت خود به حافظه وارد کرده‌اید. این کار به شما اجازه می‌دهد وضعیت رایانه خود همانند تمام برنامه‌ها و اطلاعات را ذخیره‌سازی کرده و سپس اجرا کنید.

اما چه زمان‌هایی برای استفاده ازهریک از آنها خوب است. در صورتی که برای مدت زمان کوتاهی قصد دور شدن از کامپیوتر را دارید، بهترین انتخاب شما می‌تواند حالت Sleep باشد. شما می‌توانید این کار را برای صرفه‌جویی در مصرف انرژی و باتری، انجام دهید. هنگامی که مجبور هستید مجدداً از رایانه‌های شخصی خود استفاده کنید، می‌توانید این کار را فقط برای چند ثانیه انجام دهید و در ادامه کار خود را از همان مرحله که قرار داشتید، ادامه دهید. با انتخاب حالت Sleep، کامپیوتر خود را همواره برای استفاده مجدد در حالت آماده به کار قرار خواهید داد.

انتخاب حالت Hibernate برای دور شدن از کامپیوتر، می‌تواند انرژی بیشتری را ذخیره‌سازی کند. به‌عنوان مثال اگر می‌خواهید در شب بخوابید، ممکن است سیستم خود را در حالت خواب زمستانی قرار دهید. همان‌طور که گفته شد، بازیابی مجدد سیستم در حالت خواب زمستانی، کندتر از سایر شرایط خواهد بود. در صورتی که از کامپیوتر خود برای چند بار در طول یک بازه زمانی کوتاه، دور شوید، انتخاب این گزینه برای شما مناسب نخواهد بود.

وقتی برای مدت طولانی نمی‌خواهید از دستگاه خود استفاده کنید بهتر است گزینه Shut Down را بزنید. البته اکثر سیستم‌ها در حالت Hibernate، می‌توانند سریع‌تر از حالت Shut Down بازیابی شوند. در صورتی که لپ‌تاپ دارید، بهتر است از گزینه hibernate استفاده کنید. البته این امکان وجود دارد که برخی کامپیوترها هنگام راه‌اندازی مجدد از حالت Hibernate، نتوانند عملکرد خوبی داشته باشند. ایده خوبی است که گاهی وقت‌ها، کامپیوتر خود را خاموش کرده و از گزینه Shut Down استفاده کنید.

عکستان را در سه گام ویرایش کنید

نرم افزار آنلاین

حتماً برای شما هم تا به‌حال پیش آمده که از یک عکس خاطره دارید و می‌خواهید آن را چاپ کنید اما به‌دلیل پس‌زمینه نامناسب در عکس، مجبور می‌شوید از آن صرفنظر کنید. اینجاست که فناوری به کمک شما می‌آید و با کمک نرم افزارهای مختلف می‌توانید این موارد ناخواسته را از عکس خود پاک کنید. یکی از این نرم افزارها Movavi Photo Editor است؛ یک نرم افزاری حرفه‌ای و کارآمد برای حذف کردن موارد ناخواسته درعکس‌ها و تصاویر که با استفاده از آن براحتی می‌توانید تصاویر را همان‌طور که دوست دارید ویرایش کنید. با کمک این نرم افزار همچنین می‌توانید مواردی مانند نورها یا اشخاص اضافی را پاک کنید حتماً شما هم در مکان‌های عمومی قصد عکسبرداری داشته اید که در تصاویر خصوصیتان افرادی دیده می‌شوند که آنها را نمی‌شناسید. با استفاده از این نرم افزار می‌توانید براحتی هر موردی مانند تصویر افراد غریبه را از تصاویرتان پاک کنید. کار با این نرم افزار بسیار آسان است و براحتی می‌توانید اشیا و موارد ناخواسته تصاویر را به ظریف‌ترین حالت ممکن پاک‌سازی کرده و تصاویر دلخواه را داشته باشید.

از ویژگی‌های نرم افزار Movavi Photo Editor می‌توان به وجود ابزارهای ویرایشی ضروری برای کاربر اشاره کرد. کاربر براحتی می‌تواند کارهایی از قبیل ادیت و روتوش تصاویر، حذف روشنایی‌های اضافی در تصاویر، ویرایش کنتراست‌های تصاویر و... را انجام دهد و از این قابلیت‌های ویرایشی بهره ببرد. همچنین این نرم افزار قابلیت افزایش کیفیت تصاویر را دارد و براحتی می‌توانید کیفیت تصاویر را بالا ببرید. همه این کارها تنها در ۳ مرحله انجام می‌شود. در گام نخست تصویر مورد نظرتان را باز و روی منطقه‌ای که موارد ناخواسته در آن وجود دارد کلیک کنید. حالا پاک‌سازی را استارت کرده و تصویر را ذخیره کنید. اگر شما هم به این نرم افزار علاقه مندید می‌توانید آن را به طور رایگان از وب سایت به آدرس www.P۳۰world.com بارگذاری کنید.

سلامت قلب خود را با گردنبند هوشمند رصد کنید

قلب فناوری

علیرضا احمدی
خبرنگار

یکی از مشکلات قلبی، فیبریلاسیون دهلیزی آریتمی قلب است که غالباً نشانه‌هایی واضح ندارد و به سختی شناسایی می‌شود اما می‌تواند سکته قلبی را به‌دنبال داشته باشد. در این بیماری، ریتم قلب به‌صورت غیرطبیعی تند، کند یا نامنظم می‌شود و گاه زمانی این بیماری تشخیص داده می‌شد که دیگر دیر شده است. اینجاست که فناوری پا به میدان گذاشته و گردنبند ECG-packin را ارائه داده است. با کمک این گردنبند می‌توان ضربان قلب را سریع و آسان اندازه‌گیری کرد. این گردنبند فناورانه با کمک تیم محققان یکی از دانشگاه‌های فنلاند طراحی شده و فردی که در معرض خطر آریتمی فیبریلاسیون دهلیزی قرار دارد می‌تواند همیشه آن را به گردن داشته باشد. گفتنی است این فرد می‌تواند در هر زمان و مکانی با فشردن این گردنبند در کف دست یا فشردن آن به قفسه سینه، عملکرد قلب خود را مورد بررسی قرار دهد که این کار تنها ۳۰ ثانیه طول می‌کشد. نتیجه این بررسی، ازطریق یک اپلیکیشن، الکتروکاردیوگراف (ECG) قلب را نمایش می‌دهد و آن را برای سرورهای ابری خاصی ارسال می‌کند. سپس اطلاعات در این سرور با کمک هوش مصنوعی مبتنی بر الگوریتم‌هایی مشخص مورد بررسی قرار می‌گیرد و تنها در چند ثانیه می‌تواند دیتا را آنالیز کند، آریتمی قلب را شناسایی و آن را به اطلاع بیمار و پزشک برساند. گفته می‌شود تاکنون ۱۴۵ داوطلب در آزمایش این گردنبند شرکت کرده‌اند که البته سلامت قلب آنها به طور همزمان با استفاده از روش‌های سنتی نیز مورد بررسی قرار گرفت. نتیجه این تحقیق نشان داد که هر دو روش کاملاً دقیق هستند اما تفاوت اینجاست که بیمار با کمک گردنبند می‌تواند در هر زمان و هر مکانی از وضعیت سلامت قلب خود مطلع شود که خود نکته‌ای بسیار مثبت به‌شمار می‌رود. ازسوی دیگر نحوه استفاده از این گردنبند بسیار ساده است و کاربر می‌تواند خیلی سریع از آریتمی قلب خود مطلع شود. مجمع اروپایی قلب و عروق (ESC) توصیه می‌کند افراد بالای ۶۵ سال و کسانی که در معرض خطر سکته قرار دارند باید دائم وضعیت قلب خود را مورد بررسی قرار دهند که احتمالاً دچار بیماری آریتمی فیبریلاسیون دهلیزی نباشند.

از سوی خبر

اخبار

در مراسمی با حضور وزیر ارتباطات

بیش از ۱۰۰۰ روستا به شبکه ارتباطی متصل می‌شوند

برای تحقق شعار «دسترسی همگانی» روز شنبه ۲۴ خردادماه در مراسمی با حضور وزیر ارتباطات بیش از یکهزار روستای دیگر به شبکه ملی اطلاعات و شبکه پهن باند ارتباطی متصل می‌شوند.

به‌گزارش «ایران»، محمدجواد آذری جهرمی وزیر ارتباطات و فناوری اطلاعات در حساب کاربری توئیتر خود نوشت: ۱۰۳۴ روستای دیگر تا شنبه از طریق اپراتور دوم به شبکه ملی اطلاعات متصل خواهند شد. این بار استان‌های کردستان، خراسان رضوی، فارس و هرمزگان سهم بیشتری دارند.

همه در تلاشیم تا با شروع مجدد فصل تحصیل، عدالت آموزش مجازی برای دانش‌آموزان و دانشجویان، هر چه بیشتر محقق گردد. در این مراسم در مجموع ۱۰۳۴ روستا با سرمایه ۳۰۴ میلیارد و ۱۵۰ میلیون تومان به شبکه ملی اطلاعات متصل می‌شوند.

بر اساس این گزارش، وزارت ارتباطات و فناوری اطلاعات برای تحقق شعار «دسترسی همگانی» و بر اساس برنامه‌ریزی‌های انجام‌گرفته تا پایان سال‌جاری تمامی روستاهای بالای ۲۰ خانوار کشور را به شبکه ارتباطی پهن باند کشور متصل می‌کند.

برنامه اختصاصی هوآوی برای ردیابی کرونا

بعد از قطع ارتباط کاری اپل و گوگل با هوآوی به علت فشارهای امریکا، این شرکت قصد دارد به طور مستقل برنامه‌ای طراحی کند که شناسایی افراد مبتلا به کرونا را تسهیل کند.

به گزارش مهر، صدها میلیون نفر از کاربران گوشی‌های هوآوی به علت قطع اجباری همکاری این شرکت با مؤسسات امریکایی قادر به استفاده از خدمات گوگل پلی و بارگذاری برنامه‌های آن نیستند. هوآوی برای مقابله با این مشکل دست به کار شده و هم یک فروشگاه آنلاین عرضه اپلیکیشن‌های خود به‌نام HMS Core را راه‌اندازی کرده و هم طراحی برنامه‌ای برای ردگیری افراد مبتلا به کرونا را در دستور کار قرار داده است.

این فروشگاه دارای امکاناتی برای حفظ امنیت و حریم شخصی کاربران نیز هست که آپلود ناشناس داده‌ها در فضای کلود، تضمین عدم ذخیره‌سازی اطلاعات شخصی و موقعیت مکانی، پاکسازی تاریخچه اطلاعات هر برنامه از گوشی بعد از پاک کردن آنها و غیره را در بر می‌گیرد. هنوز مشخص نیست برنامه ردیابی کرونای هوآوی از طریق بلوتوث عمل می‌کند یا خیر. این شرکت در مورد سازگاری یا عدم سازگاری برنامه یادشده با برنامه‌های ردیابی کرونای اپل و گوگل هم سکوت کرده است.

مشکل امنیتی واتس‌اپ رفع شد

واتس‌اپ با انتشار اطلاعیه‌ای جدید اعلام کرد که مشکل امنیتی مربوط به افشای شماره تماس ۳۰۰ هزار نفر از کاربران این پیام رسان برطرف شده است.

به گزارش ایسنا، محققان و پژوهشگران فعال در حوزه امنیت سایبری چند روز پیش اعلام کردند که مشکل و حفره امنیتی جدیدی در پلتفرم اپلیکیشن پیام رسان واتس اپ وجود دارد که موجب افشای شماره تماس خیل عظیمی از کاربران در نتایج جست‌وجوی گوگل می‌شود.

اما حالا واتس اپ با انتشار بیانیه و اطلاعیه‌ای رسمی و جدید اعلام کرده است که این ضعف امنیتی از پلتفرم این پیام رسان برطرف شده است و کاربران دیگر نگران افشای اطلاعات و حریم خصوصی خود در فضای وب نباشند.

چند روز پیش یکی از محققان امنیتی در صفحه کاربری خود در توئیتر عنوان کرده بود که جست‌وجوی عبارتی خاص در گوگل موجب می‌شود که شماره تماس برخی از کاربران واتس اپ در نتایج گوگل نمایان شود و از طریق لینک کوتاهی که برای آنها ایجاد می‌شود به راحتی می‌توانند با افراد موردنظر مکالمه و چت کنند.

سخنگوی واتس‌اپ ضمن تشکر از محققان امنیتی در این خصوص خاطرنشان کرده است: قابلیتی که در پلتفرم واتس‌اپ وجود دارد که click to chat نامیده می‌شود، برای کسب و کارهای کوچک فعال در سراسر جهان طراحی شده تا به لطف آن لینک کوتاه URL برای خود بسازند و بدین ترتیب با مشتریان خود از این طریق به سادگی در ارتباط باشند.

احتمال فعال شدن مجدد تأیید هویت در توئیتر

منابع مطلع می‌گویند توئیتر قصد دارد خدمات تأیید هویت واقعی اشخاص را که از سال ۲۰۱۷ غیرفعال کرده بود، دوباره فعال کند.

به‌گزارش مهر، این ابزار به کاربران امکان می‌دهد تا به‌طور مستقیم از توئیتر بخواهند تا هویت حساب کاربری آنها را تأیید کند و جلوی سوءاستفاده افراد دیگر از نام و هویت آنها را بگیرد.

در صورت تأیید هویت اشخاص یک علامت چک آبی رنگ در برابر شناسه کاربری فرد نمایش داده می‌شود. توئیتر در سال ۲۰۱۷ و بعد از آنکه فردی توانست از این قابلیت سوءاستفاده کند، آن را از دسترس خارج کرد. اما ظاهراً قرار است با افزودن برخی تمهیدات امنیتی قابلیت یادشده به‌طور مجدد فعال شود.

این خدمات در صورت فعال شدن از بخش اطلاعات شخصی در بخش تنظیمات حریم شخصی در دسترس کاربران قرار می‌گیرد. تنظیمات حریم شخصی در بخش نمایه کاربری یا پروفایل قرار دارد. توئیتر هنوز به طور رسمی در مورد صحت این خبر و زمان فعال شدن قطعی آن اظهارنظر نکرده است.