کارشناسان امنیت سایبری در گفت‌وگو با «ایران» بیان کردند

انتشار گزارش هک مانع گسترش حملات سایبری

سوسن صادقی
خبرنگار

چندی پیش هک شدن سازمان صداوسیما و تلویبون خبرساز شد اما باز مانند دیگر هک‌هایی که در کشور اتفاق می‌افتد، هیچ گزارشی مبنی بر اینکه چرا هک اتفاق افتاده، مشکل چه بوده است و... از سوی این سازمان و مراکز امنیت سایبری منتشر نشد تا دیگر سازمان‌ها نیز از راه‌های نفوذ مطلع شده و دست به اقدام‌های عملی پیشگیرانه بزنند. این در حالی است که وب سایت «چک پوینت» که متعلق به رژیم صهیونیستی است، جزئیات این هک را منتشر کرده است. اما چرا در کشور ما هکی که صورت می‌گیرد گزارش آن منتشر نمی‌شود؟ انتشار گزارش هک چه پیامدهای مثبتی دارد و اینکه در انتشار گزارش‌ها چه موارد امنیتی نیز باید رعایت شود؟ کارشناسان امنیت سایبری اعتقاد دارند که منتشر نشدن گزارش هک به دلایلی مانند نبود آگاهی، دانش، تجربه کافی و در صورت تهیه گزارش به‌دلیل محرمانگی منتشر نمی‌شوند این در حالی است که با رعایت امنیت لازم در انتشار گزارش می‌توان دیگر سازمان‌ها را از نحوه حملات و... آگاه کرد و مانع هک‌های مشابه و حملات سایبری گسترده شد.

■ نبود فرهنگ نشر گزارش هک

کاظم فلاحی، کارشناس امنیت سایبری معتقد است بخشی از منتشر نشدن گزارش‌های هک به دلیل نبود فرهنگ آن در کشور است.

فلاحی با بیان اینکه البته به تازگی سازمان‌ها و نهادها در صورتی که سازمان آنها هک شوند، هک را تأیید می‌کنند و باز این یک گام رو به جلو است، به «ایران» گفت: کارشناسان و مدیران امنیت سایبری سازمان‌ها نمی‌دانند که انتشار گزارش‌ها و اشتراک‌گذاری آن با دیگر سازمان و نهادها می‌تواند به افزایش دانش آنها کمک کند.

وی افزود: وقتی گزارش هک منتشر می‌شود نشان می‌دهد که از چه بدافزاری استفاده شده، حمله‌کننده از کجا و چه کشوری بوده و به چه داده‌ها و چه آدرسی حمله شده است. بنابراین دیگر سازمان‌ها هم با استفاده از این اطلاعات متوجه عمق خطر می‌شوند و سریع می‌توانند جلوی خطرات احتمالی سازمان خود را بگیرند.

به گفته فلاحی، آمارهای جهانی نیز حکایت از آن دارد که ۷۵ درصد حملات در مدت ۲۴ ساعت اشتراک‌گذاری می‌شود به طوری که اگر جلوی حملات از نقطه اول گرفته نشود ۷۵ درصد اتفاق‌های مشابه می‌افتد و به صورت یکسان تکرار می‌شود. به‌عنوان مثال وقتی راه‌آهن هک شود در ۲۴ ساعت امکان اینکه دیگر حمل و نقل‌ها نیز هک شوند، وجود دارد.

این کارشناس امنیت سایبری در ادامه گفت: هر سازمانی که هک می‌شود می‌تواند با استفاده از کارشناسان امنیت سایبری سریع حمله را بررسی کرده و گزارش دهند و نیازی به ورود نهاد دومی و سومی برای ارائه گزارش حملات نیست. اگر خود کارشناسان امنیت سایبری سازمان هم نتوانستند می‌توانند با برون‌سپاری به افراد معتبر گزارش را تهیه و منتشر کنند.

فلاحی افزود: البته در انتشار گزارش نیز نباید صفر تا صد گزارش منتشر شود چون خود انتشار تمام جزئیات خود ناامنی ایجاد می‌کند. بنابراین انتشار گزارش هم دارای اصولی است و باید اصول امنیتی نیز در نوشتن گزارش‌ها رعایت شود. این گزارش منتشر شده از سوی چک پوینت که در کشور ما فعال نیست چگونه توانسته برای چندمین بار چنین گزارشی آن هم با جزئیات بنویسد؟ به نظر می‌رسد فردی هرچه مستندات بوده را تحویل این شرکت خارجی داده است.به گفته وی در دنیا پایگاه‌هایی وجود دارد که آنجا اطلاعات را به اشتراک می‌گذارند تا جلوی حملات بیشتر گرفته شود که البته این کار برای کسانی که کار دفاعی انجام می‌دهند مثبت است اما باید این را هم در نظر گرفت که مهاجمان هم بیکار نمی‌نشینند و از آن مطالب استفاده می‌کنند.

به اعتقاد این کارشناس امنیت سایبری، سایت‌هایی وجود دارند که با بررسی بدافزارها آنها را تحلیل می‌کنند. به نظر می‌رسد برخی به جای اینکه خود علت هک را بررسی کنند به این سایت‌ها داده‌اند و این نشان از کم دانشی و بی‌تجربگی فرد بوده است چون بررسی هک از سوی بیگانگان و دشمنان باعث می‌شود آنها به سازمان‌های ما اشراف کامل داشته باشند و راه‌های نفوذ دیگری را یافته و حمله کنند.

وی در ادامه گفت: درست است که کارشناس نمی‌تواند جلوی حملات سایبری را بگیرد، چراکه همیشه امنیت صددرصدی نیست و کارشناسان هر کاری کنند باز امکان حملات سایبری وجود دارد اما وقتی هکی از ساده‌ترین راه صورت بگیرد قابل اغماض نخواهد بود از این‌رو در دیگر کشورها اگر مشخص شود که کارشناسان امنیت سایبری سازمانی کوتاهی کرده با فرد خاطی به‌صورت کاهش حقوق یا اخراج برخورد می‌کنند و حتی با ارائه مستندات از افرادی که کوتاهی کرده‌اند، شکایت می‌کنند.

■ محرمانگی بی‌مورد

مرتضی نکویی دیگر کارشناس امنیت سایبری نیز معتقد است اگر گزارشی از سوی سازمان‌ها و نهادها منتشر نمی‌شود دلیل بر تدوین نکردن گزارش نیست چون اگر گزارشی هم تهیه شود، معمولاً محرمانه بوده و با جزئیات کامل قابل انتشار نیستند.

نکویی به «ایران» گفت: اما باید بعد از وقوع هک گزارش‌های جرم شناسی یا گزارش‌های ثبت رویدادها و... به هر طریقی انجام شده و در اختیار متخصصان فعال کشور قرار گیرد تا جزئیات کاملی از هک‌های داخلی از سوی شرکت‌های امنیتی خارجی گزارش نشود.

وی افزود: قبل از اینکه نفوذگر فایل‌های مموری دامپ و امثال آن از سوی افراد ناآگاه در واحدهای امنیت اطلاعات سازمان‌ها در سامانه‌های اینترنتی خارجی منتشر شود، باید خود سازمان‌ها با اعتماد به توانمندی‌های داخلی گزارش هک‌ها را منتشر کنند تا شاید دفعات حملات به حداقل برسد.

این کارشناس امنیت سایبری با بیان اینکه حداقل دستاورد ارائه گزارش‌ها می‌تواند شناسایی روش‌های حمله و اقدام‌های پیشگیرانه قبل از وقوع حوادث مهلک‌تر در دیگر زیرساخت‌های کشور باشد، گفت: هر چند با توجه به فیلترهای متعدد افتایی اکنون بسیاری از شرکت‌ها و نیروهای خبره در این حوزه قادر به دریافت چنین گزارشاتی نیستند و از ظرفیت‌ها و توانمندی‌های آنها استفاده‌ای نمی‌شود. بنابراین ناچار هستند گزارش‌های بسیار کامل‌تری که در VirusTotal و سندباکس‌های عمومی اینترنت عرضه می‌شود، دریافت کنند.

وی با ابراز تعجب از انتشار گزارشی با جزئیات از سوی CheckPoint گفت: معتقدم که هنوز جزئیات بسیار بیشتری نیز وجود دارد که این شرکت خارجی براساس مصلحت‌های احتمالی آنها را منتشر نکرده است، چرا که خروجی تحلیل شده از سوی این شرکت گویای جزئیات بیشتری است.

این کارشناس افزود: البته این سؤال‌ها نیز پیش می‌آید که آیا در تشکیل تیم‌های CERT (مرکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه‌ای) در سازمان‌های کشور، دستورالعملی در خصوص چگونگی دسته‌بندی و انتشار گزارش‌ها وجود ندارد؟ آیا نفوذگران تنها به سرویس دهنده‌ها دسترسی داشتند؟ اگر چنین است چگونه فایل‌ها و شواهد جرم شناسی از سرور استخراج شده؟

به گفته وی اگر دسترسی اینترنتی از سوی کارشناسان سازمان داده نشده یا نفوذگر به تجهیزات امنیتی و مسیریاب‌های موجود کنترل کاملی داشته که به بیرون ارسال شده پس احتمال می‌رود در بخش‌هایی به‌دلیل ناآگاهی و نبود آموزش مناسب، شواهد و فایل‌های مورد نیاز در virustotal و سندباکس‌ها و غیره بارگذاری شده‌اند.

نکویی در ادامه گفت: در دنیا گزارش‌ها با جزئیات منتشر می‌شود، چون همه حکومت‌ها و دولت‌ها و نهادهای جهان به این امر واقف هستند که احتمال وقوع چنین حوادثی برای دیگران هم محتمل است. بنابراین با انتشار چنین جزئیاتی درصدد به چالش کشیدن شرکت‌های نرم افزاری و سیستم عامل‌ها و به طور کلی سازنده‌هایی که محصولاتشان مورد نفوذ قرار گرفته است، هستند.

وی افزود: البته در کشورهای دیگر به‌دلیل تعاملات نزدیک با تولیدکنندگان نرم افزاری و شرکت‌های بزرگ فناوری اطلاعات، قبل از انتشار اخبار و گزارش‌ها، نسبت به شناسایی، مهار و ریشه کن کردن حمله اقدام و بعد از آن گزارش‌ها را منتشر می‌کنند که این اتفاق در کشور ما نمی‌افتد.

به اعتقاد این کارشناس، متأسفانه در کشور ما ارائه گزارش‌ها از سوی بخش خصوصی یا حتی نهادهای تصمیم گیرنده امنیت اطلاعات امری نکوهیده محسوب می‌شود و حتی شرکت‌های بخش خصوصی نه تنها دسترسی به شواهد جرم شناسی پیدا نمی‌کنند که بخواهند نظری در این خصوص بدهند و گزارش‌های تحلیلی خود را ارائه دهند، بلکه اگر اینچنین هم بود جرأت انتشار آن را نداشتند.

به گفته نکویی در دنیای امروز فناوری اطلاعات، نمی‌توان ادعا کرد که امکان نفوذ به زیرساخت‌های هیچ کشوری وجود ندارد، همان‌طور که نفوذ به زیرساخت‌های کازینوهای امریکا نیز در سال ۲۰۱۳ را شاهد بودیم. پس چه ابرقدرت‌ها و جهان اولی‌ها و چه کشورهای درحال توسعه، هیچ کدام از این قبیل حملات در امان نیستند، ولی روش برخورد و نگرش آنها به این قبیل مسائل متفاوت است.

وی افزود: حملات اخیر متأسفانه بر اساس گزارش‌های منتشر شده، شباهت‌هایی با حملات سایبری در زیرساخت‌های کشور سوریه و حملات گذشته در کشورمان داشته‌اند که جای بسی تأسف است که از این سوراخ چندین و چندبار گزیده شده‌ایم.

عکس: تک رادار

هوش مصنوعی مانع سوءتغذیه سالمندان می‌شود

ایده‌های نو

میترا جلیلی
خبرنگار

سالمندی، یکی از مراحل زندگی بشر است که اگر با تغذیه مناسب همراه نباشد دردسرهای جدی ایجاد می‌کند. این موضوع احتمالاً برای سالمندانی که در خانه سالمندان، بیمارستان‌ها و مراکز اقامتی مشابه سکونت دارند از اهمیت بیشتری برخوردار است، زیرا ممکن است به‌دلیل افسردگی، بی‌علاقگی به غذاها، تلاش برای جلب توجه و... همه غذایی که برای آنها تهیه شده است را نخورند و حتی گاه به سوءتغذیه دچار شوند. درنتیجه این سوءتغذیه ممکن است سالمندان با کم‌خونی یا کمبود مواد معدنی، کلسیم، پتاسیم، منیزیم و... مواجه شوند. این، مشکلی است که مورد توجه محققان حوزه فناوری قرار گرفته و برای کمک به این دسته از سالمندان، دست به دامان هوش مصنوعی شده‌اند.

دانشمندان در این روش از یک سیستم آزمایشی جدید مبتنی بر هوش مصنوعی کمک گرفته‌اند که می‌تواند به راحتی به تجزیه و تحلیل تصاویر بشقاب غذای این دسته از سالمندان بپردازد که به‌مدت طولانی در مراکز خاص، خانه سالمندان و... نگهداری می‌شوند. این فناوری در حال حاضر ازطریق مشارکت بین دانشگاه واترلو کانادا و مؤسسه تحقیقات سالمندی Schlegel-UW در حال توسعه است تا بتوان از سلامت جمعیت سالمند اطمینان حاصل کرد.

به بیان ساده، این سیستم مبتنی بر هوش مصنوعی، یک عکس قبل از سرو غذا می‌گیرد، درحالی که عکس دیگر پس از اتمام غذا توسط ساکنان گرفته می‌شود. حال با مقایسه عکس‌های بشقاب غذای سالمندان با یکدیگر می‌توان مشکلات را بررسی کرد. کارکنان می‌توانند این تصاویر را ازطریق تبلت دریافت کنند و سالمندانی را که به تغذیه خود اهمیت نمی‌دهند بیشتر مورد توجه قرار دهند.از آنجا که نرم‌افزار استفاده‌شده از سوی این سیستم نسبت به دستورالعمل‌ها و برنامه‌های غذایی خانه مراقبت مرتبط است، از قبل از نوع و ارزش‌غذایی غذاهای موجود در هر وعده غذایی خاص مطلع است بنابراین با تجزیه و تحلیل عواملی مانند میزان غذایی که در بشقاب باقی مانده است، می‌تواند تعیین کند که چه مقدار از هر نوع غذا مصرف شده است و با توجه به ارزش غذایی هربخش از مواد موجود در بشقاب، می‌تواند مشخص کند که بدن سالمند در زمینه دریافت کدامیک از ریزمغذی‌ها کمبود دارد.

اگر مشخص شود که ساکنین دارای رژیم غذایی ناکافی یا نامتعادل از نظر تغذیه‌ای هستند، به مراقبان اطلاع داده می‌شود و به‌دنبال این موضوع، کارکنان این مراکز کمبودهای غذایی را از طریق قرص یا افزایش غذاهای حاوی آهن، کلسیم و... برطرف می‌کنند. البته پیش از این نیز کارکنان خانه‌های مراقبت از سالمندان، با بررسی دستی میزان غذای باقیمانده در بشقاب‌ها، میزان مصرف غذا توسط آنها را تخمین می‌زدند تا سالمندانی را که به هر دلیلی تغذیه مناسبی ندارند شناسایی کنند. اما دانشمندان معتقدند که چنین روشی حداقل ۵۰ درصد احتمال خطا دارد. در مقابل، ادعا می‌شود که سیستم مبتنی بر هوش مصنوعی از دقت بالایی برخوردار است و می‌تواند به‌سرعت به سالمندان کمک کند تا این دوران را با سلامت بیشتری طی کنند و مبتلا به سوءتغذیه نشوند.

شبیه‌ساز پیانو برای دوستداران موسیقی

نرم‌افزار آنلاین

برخی افراد علاقه زیادی به آموختن ساز دارند اما به‌دلیل گران بودن کلاس‌های آموزشی و گاه نیز نبود استادان مطرح در محدوده زندگی‌شان با مشکل مواجه می‌شوند. خبر خوب برای این دسته افراد این است که می‌توان این مشکل را با کمک نرم‌افزارها حل کرد. یکی از سازهایی که ممکن است به‌دلیل قیمت بالا هرکسی نتواند به طور فیزیکی آن را در اختیار داشته باشد، پیانو است. فعالان حوزه نرم‌افزار برای کمک به افرادی که علاقه‌مند به آموزش و نواختن پیانو هستند اما این ساز را در اختیار ندارند یک نرم‌افزار ویژه ارائه داده است. Everyone Piano یک نرم‌افزار کاربردی شبیه‌سازی کیبورد پیانو است که شما را با دنیای موسیقی و پیانو بیش از پیش آشنا می‌کند. کاربران می‌توانند با کمک این نرم‌افزار در کامپیوتر خود پیانو بنوازند و از این موسیقی لذت ببرند. این نرم‌افزار به شما این امکان را می‌دهد تا بتوانید موسیقی‌های مشهور از موسیقیدانان مطرح جهان را بنوازید. همچنین باید گفت که طراحی نرم‌افزار به گونه‌ای است که صدای خارج شده از نواختن پیانو به گونه‌ای باشد که حس نواختن پیانو را به‌صورت واقعی حس کنید. شبیه ساز پیانو Everyone Piano به شما این امکان را می‌دهد تا بتوانید به‌راحتی موزیک‌های حرفه‌ای بنوازید و از آنها لذت ببرید. Everyone Piano امکان ذخیره‌سازی آهنگ‌های تولید شده را در فرمت EOP به شما می‌دهد، چراکه بعد از نواختن یک قطعه توسط شما می‌توانید آهنگ تولید شده را با موزیک پلیر باکیفیت این نرم‌افزار بشنوید و از موزیک نواخته شده توسط خودتان لذت ببرید. از ویژگی‌های شبیه ساز Everyone Piano می‌توان به قابلیت اتصال کیبوردهای اکسترنال برای نواختن موزیک اشاره کرد. پشتیبانی از نواختن ۲ دست و همچنین پشتیبانی از ریتم‌های اتوماتیک بخشی دیگر از پتانسیل این نرم‌افزار کاربردی برای دوستداران موسیقی محسوب می‌شود. با کمک این نرم‌افزار همچنین امکان اتصال کیبوردهای الکترونیکی وجود دارد و برای آن می‌توان قابلیت‌هایی همچون قالب‌پذیری پویا و همچنین به روزرسانی با نوت‌های بیشتر را ذکر کرد. این نرم‌افزار همچنین قابلیت پشتیبانی از کارت صداهای آنبورد را دارد و با کمک آن می‌توان پدال پیانو را شبیه‌سازی کرد. قابلیت شخصی‌سازی کیبورد پیانو و نیز امکان ذخیره، برگشت و نیز پخش موزیک بخشی دیگر از پتانسیل این نرم‌افزار پرطرفدار به شمار می‌رود. اگر شما هم علاقه مندید این نرم‌افزار را در اختیار داشته باشید می‌توانید به وب سایت پی سی ورلد مراجعه کنید. برای این کار تنها کافی است آدرس WWW.P۳۰world.com را در گوگل تایپ کنید تا بتوانید این نرم‌افزار را به‌صورت رایگان بارگذاری کنید و در اختیار داشته باشید.

تشخیص دمای دنیای مجازی با تهویه هوای شخصی

قاب فناوری

Pebble Feel دستگاهی برای «تهویه هوای شخصی» است که با هدف ارائه تجربه‌ای بی‌نظیر در متاورس ساخته و در CES2022 به‌نمایش گذاشته شده است Pebble Feel. دستگاه جدیدی است که احساسات منحصربه‌فردی به فضای دیجیتال می‌آورد. این فناوری پوشیدنی می‌تواند کاربران را گرم یا خنک کند و به آنها اجازه دهد حین کاوش در فضاهای دیجیتالی متاورس، تغییرات دما را احساس کنند.

به‌گزارش دیجیتال ترندز، این فناوری را شیفتال (Shiftall) توسعه داده است؛ شرکتی که رؤیای تسریع تجارت متاورس خود ازطریق همکاری با پاناسونیک را در سر می‌پروراند. این شرکت فناوری مجموعه‌ای از محصولات جدید VR را در CES2022 معرفی کرد که از آنها می‌توان به هدست بسیار سبک MeganeX اشاره کرد. Pebble Feel با آوردن کنترل دما به فضای دیجیتال، دنیای مجازی متاورس را به سطح بعدی می‌برد. این «تهویه هوای شخصی» دستگاهی ۶۰گرمی به‌اندازه کف دست است و می‌تواند دمای بدن را تنظیم کند. باید آن را با نوعی بند یا پیراهنی خاص به کاربر متصل کرد که به‌نظر نمی‌رسد همراه محصول ارائه شود. می‌توان از دستگاه مذکور همراه با اپ‌های SteamVR، ازجمله VRChat استفاده کرد. هدف کلی گجت مذکور این است که به کاربران اجازه دهد تغییرات دما را تجربه کنند.

حداقل سرمایش Pebble Feel به ۴۸درجه فارنهایت (۸،۸ درجه سانتیگراد) و حداکثر گرمای آن به ۱۰۷درجه فارنهایت (۴۱،۶ درجه سانتیگراد) می‌رسد. افزون‌براین، باتری آن با یک‌بار شارژ می‌تواند در حالت خنک‌کننده متوسط ۱۵ساعت و در حالت گرمایش متوسط ۲۵ساعت دوام بیاورد. شیفتال، استفاده از Pebble Feel را در محیط‌های بین ۴۱ تا ۱۰۴درجه فارنهایت توصیه می‌کند.

هنگام صحبت درباره دستگاه، شیفتال تأکید زیادی بر متاورس می‌کند؛ اما اگر کسی صرفاً تهویه هوای مطبوع شخصی بخواهد، می‌توان از آن خارج از فضای دیجیتال نیز استفاده کرد. درحالی‌که Pebble Feel با SteamVR سازگار است، می‌توان از آن همراه با دستگاه‌های iOS و اندروید نیز استفاده کرد؛ زیرا برای این کار فقط به اتصال بلوتوث نسخه ۵ نیاز دارید.

انتظار می‌رود Pebble Feel در بهار امسال با قیمت حدود ۲۰۰ دلار عرضه شود.

منبع:زومیت

ترفند

چگونه بدافزارهای گوشی اندرویدی را پاک کنیم؟

گوشی‌های هوشمند هم درست مانند رایانه، لپ تاپ و... می‌توانند قربانی بدافزار شوند؛ بدافزارهایی که می‌توانند مشکل ساز شوند و از سرعت سیستم شما بکاهند. درنتیجه، اشکالاتی ایجاد می‌شود که حتی گاه استفاده از گوشی را دشوار می‌کند بنابراین برای محافظت از گوشی خود باید هرچه سریع تر مشکل را حل کنید. به گزارش دیجیتال ترندز، اگر یک برنامه آلوده در گوشی‌تان دانلود شده یا از یک وب سایت مخرب بازدید کرده باشید، می‌توانید با طی کردن چند مرحله برای حذف بدافزار و محافظت از گوشی خود اقدام کنید.

■ ۱: با خاموش کردن گوشی، جزئیات را بررسی کنید.

هنگامی که مطمئن شدید گوشی شما مورد حمله یک بدافزار قرار گرفته است، دکمه پاور را پایین نگه دارید و گوشی را کاملاً خاموش کنید. ممکن است این کار از ایجاد آسیب توسط بدافزار جلوگیری نکند، اما می‌تواند از بدتر شدن مشکل جلوگیری کند و حتی تلاش‌های بدافزار برای دسترسی به شبکه‌های اطراف را نیز متوقف کند. درواقع خاموش شدن گوشی به شما فرصت می‌دهد تا تحقیق کنید که آیا برنامه آلوده خاصی را می‌شناسید که بدافزار را روی دستگاه شما آورده است؟ ممکن است بدانید چه نوع نرم‌افزارهایی ممکن است بدون رضایت شما دانلود شده باشد اما اگر اطلاعی در این زمینه ندارید، به رایانه دیگری بروید و تاریخچه خود و همچنین هر برنامه جدیدی را که امتحان کرده‌اید ، جست‌وجو کنید. اگر تحقیقات شما چیزی را نشان نداد، ممکن است بخواهید تلفن خود را دوباره روشن کنید اما این بار باید این کار را با ملاحظاتی خاص انجام دهید.

■ ۲: تغییر به حالت امن در حالی که گوشی شما کار می‌کند.

وقتی دستگاه خود را دوباره روشن می‌کنید و برای جداسازی برنامه مشکل‌ساز وارد آن می‌شوید، ابتدا به حالت امن (safe mode) بروید. این موضوع کمک می‌کند تا میزان آسیب برنامه آلوده کاهش یابد. می‌توانید با نگه داشتن دکمه پاور برای چند ثانیه زمانی که دستگاهتان روشن است، به

حالت ایمن بروید، سپس روی گزینه خاموش کردن ضربه بزنید و نگه دارید. اگر هم نمی‌توانید حالت ایمن را پیدا کنید، به جای آن حالت هواپیما را فعال کنید تا دستگاه خود را از هر شبکه‌ای قطع کنید. معمولاً می‌توانید آن گزینه را در بالای صفحه اعلانات خود پیدا کنید.

■ ۳: به تنظیمات بروید و برنامه را پیدا کنید.

به تنظیمات دستگاه اندرویدی خود مراجعه کنید. تنظیمات معمولاً یک نماد چرخ‌دنده دارد، اما این به تم‌ها و ترتیب شما بستگی دارد: اگر در یافتن مکان مناسب مشکل دارید، آن را جست‌وجو کنید.

■ ۴: در تنظیمات، اسکرول کنید تا قسمتی به نام Apps را ببینید و روی آن کلیک کنید.

به‌دنبال فهرستی از همه برنامه‌های فعلی خود بگردید. ممکن است برای یافتن فهرست کامل، لازم باشد App Manager را انتخاب کنید.

■ ۵: هنگامی که به آنجا رسیدید، پیمایش کنید تا برنامه آلوده را در مرکز مشکلات خود بیابید.

■ ۶: برنامه را انتخاب کنید؛

با این کار گزینه‌های Uninstall، Force Close یا Force Stop ظاهر می‌شود (اغلب نمی‌توانید برنامه‌های اصلی را حذف کنید، فقط آنها را غیرفعال کنید، اما بعید است که مشکل از این برنامه‌ها باشد.)

■ ۷: با انتخاب Uninstall، برنامه آلوده و هر چیز مشکوک دیگری را حذف کنید و دستگاه Android شما باید برنامه مورد نظر را حذف کند.

همچنین ایده خوبی است که لیست برنامه‌های خود را مرور و دانلودهای مشکوک دیگر را حذف نصب کنید.

منبع:انتخاب

درباره ویژگی‌های جدید واتس اپ بیشتر بدانید

شبکه‌های اجتماعی

واتس اپ ویژگی‌های جدیدی را برای تعاملی‌تر کردن چت به این پیام‌رسان افزوده است که این ویژگی‌های جدید بزودی در دسترس کاربران خواهند بود.

به گزارش ایسنا و به نقل از ایندین نیوز، موارد جدید شامل کاربران اندروید، IOS و نسخه دسکتاپ است که بزودی در دسترس کاربران قرار می گیرد .این شبکه اجتماعی برای کاربران IOS و اندروید، در حال توسعه یک گزینه جست‌وجوی جدید در صفحه اطلاعات تماس است. واتس اپ همچنین ویژگی واکنش را برای کاربران دسکتاپ اضافه می‌کند که مخصوصاً برای چت‌های گروهی طراحی شده است. به این ترتیب امکان مشاهده اینکه چه کسی به پیام‌های دریافتی و خروجی در یک گروه واکنش نشان داده است، وجود خواهد داشت. همچنین واتس اپ میانبر جست‌وجو را به صفحه اطلاعات تماس بازطراحی شده اضافه می‌کند. برخی از کاربران همچنین می‌توانند همین میانبر را در اطلاعات گروه نیز مشاهده کنند. متأسفانه، به نظر می‌رسد میانبر جست‌وجو چندان خوب کار نمی‌کند حتی اگر این ویژگی بدرستی در حساب واتس اپ شما ارائه شده باشد، ممکن است در شرایط خاصی ظاهر نشود، البته ناگفته نماند که این نسخه بتا است ، بنابراین ممکن است چنین اتفاقاتی بیفتد، احتمالاً در نسخه نهایی همه این مشکلات حل خواهد شد.

ازسوی دیگر باید گفت که واتس اپ یک رابط ایجاد کرده است که واکنش‌های مشترک را گروه‌بندی می‌کند، بنابراین می‌توانید فهرست همه افرادی را که با استفاده از همان واکنش به یک پیام عکس‌العمل نشان داده‌اند، مشاهده کنید؛ قبلاً اعلام شده بود که نسخه آزمایشی واتس اپ برای IOS و بتا برای اندروید در حال توسعه است و حالا به نظر می‌رسد این موضوع وارد فاز جدیدی شده است.