رویداد

برگزاری نمایشگاه بومی امنیت سایبری

● **شرق:** نمایشگاه بومی امنیت سایبری توسط مرکز ملی فضای مجازی و با همکاری سازمان پدافند غیرعامل برگزار می‌شود. نخستین نمایشگاه بومی امنیت سایبری با هدف شناسایی و همراهی با شرکت‌های فناور در حوزه امنیت سایبر، یکشنبه سوم خرداد برگزار می‌شود. این نمایشگاه که با عنوان «بهره‌برداری از محصولات بومی تضمین امنیت پایدار» برپا می‌شود تا ششم خرداد در مرکز ملی فضای مجازی دایر خواهد بود.

درخواست شرکت‌های فناوری از اوباما

با رمزگذاری داده‌ها مخالفت نکنید

● **فارس:** برخی شرکت‌های بزرگ فناوری، سازمان‌های مدافع حقوق مدنی و متخصصان امنیتی نامه‌ای برای اوباما، رئیس‌جمهور آمریکا ارسال کرده و خواستار مخالفت وی با قوانین ضدرمزگذاری داده‌های کاربران شدند. براساس گزارش نیویورک‌تایمز، در این نامه که مدیران شرکت‌های بزرگی همچون گوگل، فیس‌بوک، اپل و مایکروسافت آن را امضا کرده‌اند در مورد پیامدهای ناخواسته سیاست‌هایی که به‌منظور تضعیف فناوری‌های رمزگذاری وضع می‌شوند، هشدار داده شده است. در دو سال اخیر و به خصوص پس از افشاگری‌های ادوارد اسنودن

در مورد همکاری شرکت‌های فناوری آمریکا با کاخ سفید برای جاسوسی از کاربران اینترنت و تلفن همراه، این شرکت‌ها که اعتبار و درآمد خود را در خطر دیده‌اند، تلاش کرده‌اند فناوری‌های رمزگذاری اطلاعات را بر روی تولیداتشان تقویت کنند تا حریم شخصی کاربران در برابر جاسوسی‌های دولتی محفوظ بمانند. به‌عنوان مثال، اپل مدعی است داده‌های کاربران آیفون۶ را به‌گونه‌ای رمزگذاری می‌کند که به جز خود کاربر گوشی، هیچ کس و از جمله اپل نمی‌تواند به این داده‌ها دسترسی یابد. اما اقداماتی از این دست با اعتراض اف‌بی‌آی و آژانس امنیت ملی آمریکا مواجه شده که می‌گویند نتیجه این کار به خطر افتادن امنیت ملی آمریکاست؛ زیرا تروریست‌ها، جاسوسان خارجی، هکرها و جانیان هم می‌توانند از فناوری‌های یاد شده سوءاستفاده کنند. کاخ سفید فعلا در حال بررسی موضوع است، اما ممکن است از وضع قوانینی حمایت کند که بر اساس آن شرکت‌های فناوری مجبور به استفاده از شیوه‌های خاصی از رمزگذاری اطلاعات شوند که توسط پلیس و نهادهای جاسوسی ایالات‌متحده قابل رمزگشایی باشد. شرکت‌های فناوری این روش را خطرناک دانسته و معتقدند اگر قرار باشد شیوه‌های رمزگذاری داده‌ها به طور عمدی دچار نقاط ضعف و ابزاری برای نفوذ باشند، علاوه بر مأموران دولتی، هر کسی می‌تواند از آنها سوءاستفاده کند بنابراین این روش هم به نتیجه نمی‌رسد. در بخشی از این نامه آمده است: ما هرگونه پیشنهاد به شرکت‌های آمریکایی برای تضعیف عمدی امنیت محصولاتمان را رد می‌کنیم و از کاخ سفید می‌خواهیم به جای این کار بر سیاست‌گذاری‌هایی متمرکز شود که به جای کاهش استفاده گسترده از فناوری‌های قدرتمند رمزگذاری موجب افزایش این کار شود.

۹۴ میلیون آیفون در آمریکا

● **فارس:** تازه‌ترین آمار منتشرشده از استفاده ۹۴ میلیون آمریکایی از گوشی آیفون حکایت دارد و نکته جالب این است که ۴۰ درصد از این افراد از آیفون۶ و ۶ پلاس استفاده می‌کنند. بر اساس گزارش هافینگتون‌پست، مؤسسه Consumer Intelligence Research Partners گزارشی را منتشر کرده که نشان می‌دهد تا پایان مارس سال ۲۰۱۵ حدود ۹۴ میلیون آمریکایی مالک آیفون بوده و از این رقم ۲۵ میلیون‌نفر از آیفون ۶ و ۱۳ میلیون نفر از آیفون۶ پلاس استفاده می‌کنند. همچنین ۵۶ میلیون نفر دیگر از کاربران آمریکایی از مدل‌های قدیمی‌تر آیفون استفاده می‌کنند. مقایسه میزان استقبال از مدل‌های تازه عرضه‌شده آیفون در سال‌های مختلف نشان می‌دهد اقبال به آیفون۶ و ۶پلاس بیش از مدل‌های دیگر بوده و از سپتامبر سال ۲۰۱۴ تا ۳۱ مارس سال ۲۰۱۵، ۳۸ میلیون گوشی از این نوع در آمریکا به فروش رفته است. اما میزان فروش آیفون۵ اس در مدت مشابه در سال ۲۰۱۳ تنها ۱۸ میلیون واحد بوده است. هم‌اکنون ۲۶ میلیون آیفون۵ اس در حال استفاده است که انتظار می‌رود مالکان آنها در ماه‌های آینده از آیفون ۶ استفاده کنند. علاوه بر این، هنوز حدود هشت میلیون نفر آمریکایی از گوشی قدیمی‌تر آیفون۴ اس استفاده می‌کنند که در سال ۲۰۱۱ تولید شده بود.

هشدار در مورد جدیدترین روش‌های کلاهبرداری اینترنتی در ایران

به نرم‌افزارها اعتماد نکنید

استفاده از تلفن همراه برای اخاذی و کلاهبرداری شیوه‌ای است که در تمام دنیا موردتوجه قرار می‌گیرد و بر همین اساس در کشور ما نیز اپراتورهای تلفن همراه به طور متناوب هشدارهایی در این‌باره منتشر کرده و از مشترکان خود می‌خواهند در این زمینه دقت‌عمل لازم و کافی به خرج دهند. اما نکته جالب اینکه کلاهبرداران در موارد متعدد برای دستیابی به اطلاعات بانکی یا مواردی مانند ورود به رایانه‌ها هم در حال استفاده از تلفن هستند. در یکی از شیوه‌هایی که برای این منظور در دنیا مورداستفاده قرار می‌گیرد، کلاهبرداران با افراد تماس می‌گیرند و ادعا می‌کنند پشتیبان فنی رایانه و از یک شرکت معتبر هستند. این افراد با ادعای اینکه ویروس‌ها یا بدافزارهایی را در رایانه شما شناخته‌اند، تلاش می‌کنند شما را مجاب کنند تا دسترسی از راه دور به آنها بدهید یا هزینه‌ای برای نرم‌افزارهایی که نیاز ندارید پرداخت کنید. بنا بر گزارش‌های منتشرشده از سوی مرکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه‌ای (ماهر) این کلاهبرداران از برخی نگرانی‌های شما در قبال ویروس‌ها و تهدیدات دیگر آگاه هستند و با استفاده از همین مورد سعی در نصب نرم‌افزارهای امنیتی می‌کنند. اما هدف اصلی این کار، محافظت از رایانه شما نیست بلکه هدف کسب پول است.

کلاهبرداری از نوع پشتیبان فنی چگونه کار می‌کنند؟

به گزارش ایسنا، سال‌هاست کلاهبرداران نرم‌افزارهای امنیتی جعلی را به فروش می‌رسانند. آنها وب‌سایت‌های جعلی ایجاد می‌کنند که پیشنهاد پویش‌های امنیتی رایگان در رایانه شما را می‌دهند؛ به همین دلیل، برای اینکه شما را متقاعد به آلوده‌بودن رایانه‌تان کنند، پیام‌های هشدارآمیزی نشان می‌دهند. سپس، تلاش می‌کنند نرم‌افزاری را برای حل این مشکل به شما بفروشند. در بهترین حالت، این نوع نرم‌افزارها، یا نرم‌افزارهای بی‌اهمیتی هستند یا در جای دیگر به صورت رایگان در دسترس هستند. در بدترین حالت نیز این نرم‌افزارها، بدافزار هستند و برای فراهم‌کردن امکان دسترسی مجرمان به رایانه و اطلاعات شخصی شما طراحی شده‌اند. جدیدترین نوع کلاهبرداری با تماس تلفنی شروع می‌شود. کلاهبرداران نام و اطلاعات اولیه افراد را از طریق کتب راهنمای عمومی به‌دست می‌آورند؛ حتی ممکن است نرم‌افزاری را که شما در حال استفاده از آن هستید، حدس بزنند. هنگامی که با شما از پشت تلفن صحبت می‌کنند، اغلب وانمود می‌کنند از یک شرکت شناخته‌شده هستند تا بتوانند اعتماد شما را جلب یا شما را با حجم زیادی از اصطلاحات فنی گیج کنند. ممکن است از شما بخواهند وارد رایانه خود شده و یک‌سری فعالیت پیچیده انجام دهید. گاهی اوقات، فایل‌های صحیح رایانه را موردهدف قرار می‌دهند و ادعا می‌کنند این فایل‌ها ویروسی هستند. کلاهبرداران فعالیت خود را به‌گونه‌ای انجام می‌دهند تا باور کنید آنها می‌توانند در حل مشکل به شما کمک کنند. اما هنگامی که کلاهبرداران اعتماد شما را جلب کردند، ممکن است کارهایی از قبیل اینکه از شما امکان دسترسی از راه دور به رایانه را بخواهند و سپس تغییراتی را در تنظیمات آن انجام دهند به‌طوری‌که رایانه در معرض آسیب قرار گیرد. همچنین برای ثبت‌نام‌کردن شما در برنامه warranty یا نگهداری رایانه تلاش کنند. یا اینکه درباره اطلاعات کارت بانکی بپرسند؛ در نتیجه بتوانند برای خدمات تلفنی صورت‌حساب بدهند. با حیله و نیرنگ بدافزاری را نصب کنند تا داده‌های حساس مانند کلمه عبور و نام کاربری را به سرقت ببرند و حتی شما را به وب‌سایتی رهنمون کنند که از شما بخواهد شماره کارت بانکی و دیگر اطلاعات شخصی خود را وارد کنید. صرف‌نظر از روش‌های مورداستفاده توسط کلاهبرداران، آنها یک هدف دارند: کسب درآمد مالی.

اگر تماس تلفنی دریافت کردید، چه کار باید بکنید؟

اگر تماس تلفنی از کسی که ادعا می‌کند پشتیبان فنی شرکت معتبری است دریافت کردید، خودتان به شماره‌ای که از آن شرکت دارید و از صحت آن شماره مطمئن هستید، زنگ بزنید. تماس‌گیرنده‌ای که حس اضطرار برای شما ایجاد می‌کند یا از روش‌های پرفشار استفاده می‌کند احتمالا کلاهبردار هنرمندی است. بر همین اساس لازم است کنترل رایانه خود را به طرف سومی که به‌صورت غیرمنتظره و هماهنگ‌نشده تماس‌گرفته است ندهید. برای احراز هویت تماس‌گیرنده، فقط به شناسه (شماره) تماس‌گیرنده اعتماد نکنید. مجرمان شماره‌های تماس گیرنده را جعل می‌کنند؛ ممکن است به‌نظر برسد از شرکتی قانونی یا شماره محلی در حال تماس هستند اما حتی از داخل کشور نباشند. نتایج جست‌وجوی آنلاین، بهترین راه برای پیداکردن پشتیبان فنی یا گرفتن اطلاعات تماس شرکت موردنظر نیست. کلاهبرداران گاهی اوقات برای متقاعدکردن شما به تماس با آنها، تبلیغات آنلاینی در اینترنت قرار می‌دهند. حتی با استفاده از روش‌هایی، رده سایت مربوط به خود را در نتایج جست‌وجو بالا می‌برند. اگر به پشتیبانی فنی احتیاج دارید، به‌دنبال اطلاعات تماس شرکت مربوط در بسته نرم‌افزاری یا در برگه رسید باشید. هرگز اطلاعات مالی یا شماره کارت خود را به کسی که تماس می‌گیرد و ادعا می‌کند از طرف پشتیبانی فنی است ندهید. اگر تماس‌گیرنده برای خرید یک محصول امنیت رایانه پافشاری کرد تلفن را قطع کنید. اگر در مورد رایانه خود نگران هستید، با پشتیبانی نرم‌افزار امنیتی نصب‌شده در رایانه خود تماس بگیرید و از آنها کمک بخواهید. هرگز کلمه عبور خود را از طریق تلفن به کسی ندهید. هیچ سازمان قانونی‌ای با شما تماس نمی‌گیرد و کلمه عبور شما را نخواهد پرسید.

اگر به یک کلاهبردار پاسخ دادید، چه کار باید بکنید؟

اگر فکر می‌کنید بدافزاری را از سایتی کلاهبردار، دانلود کرده‌اید یا به مجرم فضای مجازی اجازه دسترسی به رایانه خود را داده‌اید، نترسید و از بدافزار خلاص شوید. نرم‌افزار امنیتی را به‌روز کنید یا آن را دانلود و رایانه را پایش کنید. هر آنچه این نرم‌افزار به‌عنوان مشکل می‌شناسد حذف کنید. کلمات عبور افشاشده را تغییر دهید. اگر شما از این کلمات عبور برای حساب‌های دیگر خود نیز استفاده کرده‌اید، کلمات عبور آن حساب‌ها را نیز تغییر دهید.

امنیت

تلگرام و مشکل فنی

● استقبال چشمگیر کاربران موبایل از پیام‌رسان موبایلی تلگرام بعد از اختلالات وایبر، این برنامه موبایلی را دچار شوک کرده که ریشه آن هنوز مشخص نیست. پیام‌رسان‌ها نیز باتوجه به اقبال مردم دنیا از نسل‌های نوین ارتباطی نظیر 3G و 4G و درک نیاز مردم به برقراری ارتباطات ساده و کم‌هزینه، نهایت استفاده را کرده‌اند و روزبه‌روز توسعه یافته‌اند. اما قریب به یک ماه می‌شود که دسترسی به برخی شبکه‌های رایج نظیر تلگرام که بعد از اختلالات وایبر، مورد استقبال بسیاری از کاربران ایرانی قرار گرفت، مختل شده است. به گزارش تسنیم، کاربران بسیاری در شبکه‌های اجتماعی از این موضوع گلایه می‌کنند و اخیرا مدیر یکی از شرکت‌های اینترنتی، بیشترین حجم ترافیک صوتی مربوط به بخش پشتیبانی شرکت خود در یک هفته اخیر را مربوط به این موضوع دانست. درحالی این دغدغه، یکی از بیشترین موضوعات مورد دغدغه کاربران اینترنت است که مراکز پشتیبانی حرفی برای گفتن ندارند زیرا در شبکه شرکت‌های اینترنتی تغییری صورت نگرفته است. درحالی‌که دستوری هم برای محدودسازی رِنج آدرس‌های برخی اپلیکیشن‌ها وجود ندارد، اما پشتیبانان شرکت‌های اینترنتی می‌گویند که این اختلال در شبکه تمامی شرکت‌های ISP مشاهده می‌شود، اما موضوع در دست پیگیری است. بااین‌حال عده‌ای هم مشکل ایجادشده را مربوط به میزبان می‌دانند و می‌گویند که سرورهای وایبر و تلگرام مختل است، اما دراین‌بین برخی کارشناسان مراکز پشتیبانی هم احتمال تست الگوریتمی خاص در ارتباط با پالایش محتوا که در دومین فاز خود از سمت وزارت ارتباطات است را می‌دهند. با توجه به اظهارات محمود واعظی، وزیر ارتباطات و فناوری اطلاعات، مبنی بر اینکه جای هیچ نگرانی برای مردم نیست زیرا تصمیم مشخص وزارت ارتباطات آن است که فعلا برنامه‌ای برای محدودیت فعالیت شبکه‌های اجتماعی موبایلی ندارد و قطعا زمانی این موضوع اعلام می‌شود که جایگزین‌های مناسبی برای این شبکه‌ها در داخل کشور ایجاد شده باشد. نکته دیگر این است که دسترسی تمامی مشترکان موبایل به وایبر و تلگرام محدود نشده و ممکن است امروز در منطقه‌ای نتوانید به تلگرام وصل شوید که فردا این مشکل وجود نداشته باشد و این رویه برای دیگر مناطق اتفاق بیفتد. تاکنون دلیل مشخصی در ارتباط با این موضوع عنوان نشده است.

بازار

گوشی‌های هوشمند دارای ۲ سیم‌کارت

بهزاد ایزدی: یکی از قابلیت‌هایی که خریداران گوشی هوشمند به آن اهمیت می‌دهند، دو سیم‌کارته‌بودن دستگاه است. ازاین‌رو سعی شده تا بهترین گوشی‌های دارای دو سیم‌کارت موجود معرفی شوند. در ابتدای امر، این نکته را باید در نظر داشت که فهرست قیمت‌ها براساس چندین منبع تهیه شده و ممکن است با بازار شهری که شما در آن ساکن هستید، کمی اختلاف داشته باشد.

Sony Xperia Z3 Dual

این گوشی هم‌اکنون در بازار با حدود رنج قیمت از یک‌میلیون‌و ۴۸۹ تا دومیلیون‌و ۹۹ هزار تومان به فروش می‌رسد. به گزارش فارنت، لبه‌های این گوشی نسبت به Z2 گردتر شده. این انحنا به خوش‌دست‌بودن آن‌هم کمک شایانی کرده است.

Galaxy Note4 Duos

این نسل از سری نوت به پردازنده‌ای بسیار قدرتمند و دوربینی با وضوح بالا تجهیز شده است. درحال‌حاضر این گوشی در بازار با حدود رنج قیمت

دومیلیون‌و ۱۶۰ هزار تا دومیلیون‌و ۵۰۰ هزار تومان، بسته به میزان فضای ذخیره‌سازی داخلی، به فروش می‌رسد.

G3 Dual

قیمت این گوشی در بازار بین یک‌میلیون‌و ۳۵۰ تا یک‌میلیون‌و ۴۸۰ هزار تومان است. ال‌جی در این گوشی همانند جی۲، در نهایت رعایت سادگی، از طراحی هوشمندانه‌ای بهره برده و آخرین فناوری‌های خود را در یک قاب زیبا و طراحی نازک با صفحه نمایش ۵.۵ اینچی درخشان جای داده است.

HTC One M8 Dual Sim

اچ‌تی‌سی وان‌ام۸ هم‌اکنون با حدود رنج قیمت یک‌میلیون‌و ۵۴۵ تا یک‌میلیون‌و ۹۵۰ هزار تومان به فروش می‌رسد. این گوشی از یک بدنه آلومینیومی خوش‌ساخت و زیبا ساخته شده است. در ساخت بدنه این دستگاه، از پلاستیک کمتری استفاده شده و حتی اطراف و جداره‌ها نیز فلزی طراحی شده‌اند به‌طوری‌که مقدار کلی فلز در بدنه از ۷۰ درصد به ۹۰ درصد افزایش یافته است.

Galaxy S5 Duos

با اینکه بدنه گوشی کاملا پلاستیکی است، اما ویژگی‌های خوبی نظیر ضدآب‌بودن و امکانات سخت‌افزاری بالا دارد. قیمت این گوشی در بازار بین یک‌میلیون‌و ۳۰۰ تا یک‌میلیون‌و ۶۵۰ هزار تومان تعیین شده است.

Ascend Mate7

این گوشی نه‌تنها دارای نمایشگر کوچک‌تری نسبت به مدل‌های پیشین خود بوده، بلکه دارای ضخامت و حاشیه نمایشگر کمتری نسبت به آنهاست. این گوشی تنها ۷.۹ میلی‌متر ضخامت دارد. برای این گوشی قیمتی معادل یک‌میلیون‌و ۲۵۲ هزار تا یک‌میلیون‌و ۷۸۰ هزار تومان در بازار در نظر گرفته شده است.

Lumia 640 XL Dual SIM

خریداران این محصول از ۵۰ گیگابایت حافظه ذخیره‌سازی ابری سرویس وان درایو و اکانت یک‌ساله آفیس ۳۶۵ مستفیض خواهند شد. برای خرید، قیمتی معادل ۷۹۰ تا ۹۵۰ هزار تومان را باید هزینه کرد.

Galaxy A7

قیمت این گوشی هم‌اکنون در بازار با حدود رنج قیمت یک‌میلیون‌و ۲۰۰ تا یک‌میلیون‌و ۴۰۰ هزار تومان است. ضخامت این گوشی ۵.۵ اینچی، بدون احتساب دوربین بیرون زده، ۶.۳ میلی‌متر است که ۰.۴ میلی‌متر از گلکسی A5 و گلکسی A3 نازک‌تر است.

Honor6

این محصول دارای سخت‌افزار سطح بالا، اما بدنه‌ای با کیفیت و طراحی سطح پایین است. قیمت آن در بازار بین ۹۲۰ تا یک‌میلیون‌و ۳۰ هزار تومان است.

G3 Stylus

جی ۳ استایلوس را می‌توان نسخه ارزان‌تر و البته ضعیف‌تر، ال‌جی، نامید که به قلم استایلوس تجهیز شده است. صفحه‌نمایش ۵.۵ اینچی در کنار سخت‌افزار قدرتمند می‌تواند کاربران را راضی نگاه دارد. قیمت آن بین ۷۴۹ تا ۸۸۵ هزار تومان است.

Nokia-Lumia-730

برای خرید این گوشی باید ۶۲۰ تا ۶۷۰ هزار تومان هزینه کرد. این گوشی مقرون‌به‌صرفه، به نمایشگر ۴.۷ اینچی AMOLED 720p به همراه تراشه چهارهسته‌ای اسنپ‌دراگون ۴۰۰ مجهز شده است. چیزی که این دستگاه را از همتایانش متمایز می‌کند، وجود دوربین جلو پنج مگاپیکسلی برای تصویربرداری سلفی است.