رویداد

گوگل خبرهای قلابی و دروغ را لو می‌دهد

• **مهر:** به دنبال گسترش بی‌سابقه محتوا و اخبار دروغین در اینترنت، گوگل در تلاش است تا کنترل صحت محتوای ارائه‌شده از طریق این جست‌وجوگر را ممکن کند. براساس گزارش سرچ انجین لند، گوگل از اکتبر گذشته امکان کنترل صحت اخبار ارائه‌شده در بخش گوگل‌نیوز را در آمریکا و انگلیس ممکن کرده بود تا کاربران با مشاهده محتوای جعلی موجود در برخی اخبار فریب نخورند. از این پس این خدمات به طور جهانی ارائه می‌شود تا در صورتی که کاربران بخواهند از صحت‌وسقم خبری مطلع شوند، بتوانند این کار را به صورت ساده‌تری انجام دهند. به‌عنوان مثال اگر کاربری خبر فروش اورانیوم به روسیه از سوی هیلاری کلینتون را با واردکردن کلیدواژه‌های مرتبط در گوگل جست‌وجو کند، لینک‌های مرتبط با این خبر را در جست‌وجوگر مذکور مشاهده می‌کند. اما در زیر این لینک‌ها عبارت ادعاشده به وسیله اینترنت قابل مشاهده است و همچنین با توجه به اینکه یک سایت معتبر خبر دروغ‌بودن این خبر را اعلام کرده این موضوع نیز به کاربر اعلام می‌شود. گوگل قصد دارد سرعت ارائه این خدمات را افزایش دهد تا تولیدکنندگان اخبار جعلی نتوانند محتوای دروغین را در فضای مجازی به‌عنوان خبر واقعی بازنشر کنند. این جست‌وجوگر در مواردی برای بررسی صحت یک خبر از چند منبع استفاده می‌کند تا درست یا خطا بودن خبر ارائه‌شده برای جست‌وجوگر به طور دقیق مشخص شود.

بدافزار خطرناک سیا افشا شد

• **فارس:** هکرهای وابسته به سازمان جاسوسی سیا با استفاده از برخی کدهای بدافزار مالی Carberp که در سال ۲۰۱۳ افشا شده بود، به جاسوسی از اهداف خود می‌پردازند. براساس گزارش کامپیوترورلد، نکته جالب این است که بدافزار مالی یادشده در اصل به وسیله هکرهای روس طراحی شده است و آمریکا با وجود ضدیت ظاهری با روسیه تصمیم گرفت از کدهای مذکور استفاده کند. براساس اسنادی که روز جمعه از سوی ویکی‌لیکس افشا شده است، سیا از بدافزار مبتنی بر Carberp برای نفوذ به رایانه‌های مجهز به سیستم‌عامل ویندوز استفاده کرده است. طبق ۲۷ سند افشاشده از سوی ویکی‌لیکس، سیا از کدهای Carberp برای طراحی ابزار هکری خاص خود موسوم به Grasshopper استفاده کرد. Carberp در اصل یک تروجان است که قادر به سرقت اطلاعات مربوط به فعالیت‌های بانکی آنلاین و دیگر اطلاعات مالی از رایانه‌های قربانیان است. این بدافزار که به وسیله گروه‌های جنایتکار روس طراحی شده، در روسیه و دیگر کشورهای وابسته به اتحاد جماهیر شوروی سابق هم بسیار مشکل‌آفرین شد و پس از افشای کدهای منبع طراحی آن در سال ۲۰۱۳ این نگرانی به وجود آمد که جنایتکاران آنلاین در دیگر کشورهای جهان نیز از آن سوءاستفاده کنند. در اسناد تازه افشاشده ویکی‌لیکس دستورالعمل سیا درباره نحوه استفاده این سازمان جاسوسی از بدافزار یادشده درج شده است.

بومی‌شدن نرم‌افزارهای نظام بانکی

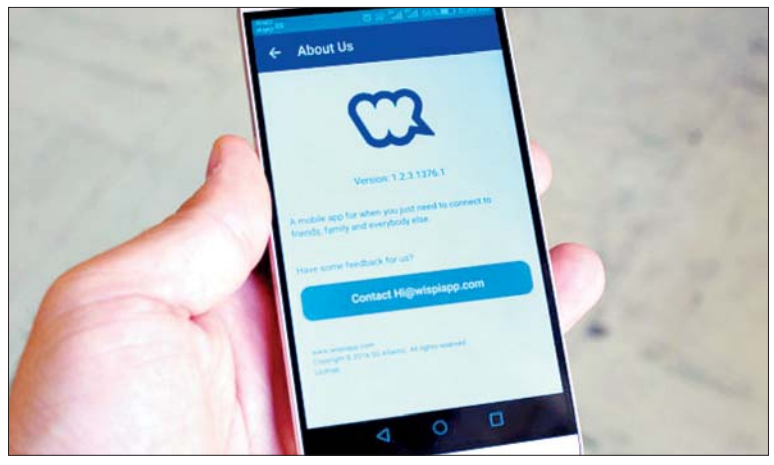
• **تماس‌نیوز:** به گفته معاون وزیر اقتصاد و دارایی هم‌اینک احتمال خطا در نقل و انتقالات الکترونیک به صفر رسیده و هزینه انجام مبادلات برای مردم به نحو درخورملاحظه‌ای کاهش پیدا کرده است. حسین قضاوی دراین‌باره بیان کرد: «در دولت یازدهم تعداد دستگاه‌های خودپرداز بانک‌ها در کشور ۱۵ هزار دستگاه افزایش یافته و به ۴۲ هزار دستگاه رسیده است». او مهم‌ترین رویکرد دولت در این عرصه را به‌حداقل‌رساندن فاصله بانکداری ایران با بانکداری عرصه جهانی در حوزه محصولات نوین بانکی دانست. به گفته او از نتایج مثبت این عرصه می‌توان به افزایش چشمگیر تعداد دستگاه‌های کارت‌خوان و خودپرداز، افزایش و تنوع هرچه‌بیشتر خدمات کارت‌های بانکی و در مجموع، رشد عرصه بانکداری الکترونیک کشور اشاره کرد. او افزود: «در حوزه گمرک نیز تلاش‌های بسیاری انجام شده که از جمله نتایج آن باید به این موضوع اشاره کرد که هم‌اکنون کلیه فرایند موردنیاز برای کالاهای صادراتی به خارج، از جمله اظهار کالا تا ارزیابی و سایر مراحل، همگی در بستر اینترنت قابل انجام است».

یوتیوب تی‌وی وارد میدان می‌شود

• **آی‌تی ایران:** یوتیوب تی‌وی (YouTube TV) بالاخره رسید. یوتیوب تی‌وی پتانسیل بالایی در تغییر گرایش‌های تلویزیونی خواهد داشت. یوتیوب تی‌وی عملکردی مشابه تلویزیون‌های کابلی دارد البته با این تفاوت که افراد می‌توانند شبکه‌های مورد علاقه خود را از طریق اینترنت و بدون نیاز به کابل و تلویزیون تماشا کنند. این سرویس که از امروز کار خود را در چندین شهر مختلف آغاز کرده، بیش از ۴۰ شبکه سرگرمی، اخبار و ورزش را با پرداخت ۳۵ دلار ماهانه در اختیار مخاطبان قرار می‌دهد. البته این سرویس فعلا کمی ضعیف به نظر می‌رسد اما احتمال می‌رود به‌زودی بینندگان تلویزیونی را شگفت‌زده کند و البته تبلیغ‌کنندگان هم علاقه خود را به تبلیغ در این سرویس نشان داده‌اند.

تنور تبلیغات انتخاباتی با شبکه‌های اجتماعی گرم می‌شود

«ویسپی» رقیب «تلگرام» در انتخابات؟!



پیش از شروع انتخابات مجلس شورای اسلامی و مجلس خبرگان رهبری در اسفندماه سال ۹۴ برای همه مسلم شده بود که در این انتخابات ابزارهای مجازی از جمله شبکه‌های پیام‌رسان موبایلی یک نقش عمده و تأثیرگذار را در تعیین نتایج انتخابات می‌توانند بر عهده داشته باشند؛ موضوعی که به نوبه خود می‌تواند تأثیر بسزایی در تغییر چهره انتخابات و فضای سیاسی در ایران بازی کند. به نحوی که رئیس پلیس فتا اعلام کرد ۷۹ درصد از کل فعالیت‌های انتخاباتی در فضای مجازی در تلگرام انجام شد و مابقی شبکه‌ها همچون فیس‌بوک، توییتر و... نقش جدی نداشتند. الجزیره در همین راستا گزارشی نیز منتشر کرد مبنی بر اینکه گروه‌ها و کانال‌های تلگرام منجر به آن شده است که کاربران و رأی‌دهندگان ایرانی به‌شدت به‌روز باشند و اخبار و آرایش‌های سیاسی انتخابات را به‌دقت و با جزئیات دنبال کنند. تاجایی‌که به نقل از یکی از مقامات وزارت ارتباطات بیان شده که تعداد افرادی که از تلگرام استفاده می‌کنند از تعداد بینندگان تلویزیون بیشتر است. در همین راستا مدیران شرکت تلگرام می‌گویند حدود ۲۰ درصد کاربران فعال آن ایرانی هستند. این‌گونه به نظر می‌رسد که تنها ایالات متحده تعداد کاربران بیشتری از ایران روی این برنامه پیام‌رسانی دارد. اما در کنار اهمیت شبکه اجتماعی تلگرام در فضای سیاسی ایران، مواردی نیز به وجود آمد که مسئولان را بر آن داشت که به فکر استفاده از ابزارهای جایگزین برای آن باشند. از طرفی راه‌اندازی ابزار صوتی رایگان برای تلگرام، مسئولان وزارت ارتباطات را بر آن داشته تا به طور جدی فکری برای این برنامه بی‌رقیب در ایران کنند. خبرگزاری فارس در این‌باره گزارش می‌دهد: «پس از انتشار شایعاتی درباره تلاش دولتی در آستانه انتخابات برای جایگزین‌کردن پیام‌رسان تلگرام با یک پیام‌رسان جدید چینی به نام ویسپی (Wispi) با مشارکت یک شرکت خصوصی ارائه‌دهنده اینترنت، چیزی نگذشت که عده‌هایی مبنی بر رزروشدن آدرس اشخاص و کانال‌های پرمخاطب، این شایعات را تقویت کرد. حتی گفته شده برای سرمایه‌گذاری و انتقال سرورهای این پیام‌رسان به ایران ۸۰ میلیارد تومان بودجه دولتی پیش‌بینی شده است». البته وزارت ارتباطات چنین موضوعی را تکذیب و در اطلاعیه‌ای بیان کرده است: «سیاست حمایتی دولت از پیام‌رسان‌های بومی شفاف و برای همه یکسان بوده و درخصوص تعامل با سرویس‌دهندگان بین‌المللی نیز تاکنون هیچ مذاکره‌ای از سوی وزارت ارتباطات با پیام‌رسان مذکور انجام نشده است». در پیگیری این موضوع خسرو سلجوقی، عضو هیئت عامل این سازمان در رأس موضوعات مهم در سازمان، فناوری اطلاعات گفته است: «طبق برنامه‌های حمایتی سازمان یا در مقام مشورت، در جریان موضوعات این‌چنینی قرار می‌گیریم که برای مثال شرکت ایرانی مطرح می‌کرد که برای خرید یک پیام‌رسان خارجی به مبلغ ۴۰ میلیارد تومان مذاکره کرده است؛ اما یقین دارم هیچ مذاکره‌ای درباره پیام‌رسان ویسپی یا حمایت دولتی از این پیام‌رسان از سوی سازمان فناوری انجام نشده است». او ادامه داده است: «نام پیام‌رسان ویسپی را از رسانه‌ها شنیده است».

پیام‌رسان Wispi یکی از تازه‌واردان قدرتمند این حوزه محسوب می‌شود؛ محصول یک توسعه‌دهنده نه‌چندان شناخته‌شده چینی که با امکاناتی ایده‌آل همچون برقراری تماس‌های رایگان اینترنتی، با جدیت بازار نقاط مختلف دنیا به‌ویژه ایران را هدف قرار داده و برای کنارزدن رقبای قدرتمندی همچون تلگرام و واتس‌اپ تلاش می‌کند. این اپلیکیشن نه‌تنها امکان چت و گفت‌وگوی معمولی همچون تلگرام و واتس‌اپ را برای اعضای شبکه‌اش مهیا کرده، بلکه امکان برقراری تماس‌های اینترنتی و ارسال پیامک رایگان با بسیاری از کشورهای دنیا را در اختیارتان می‌گذارد. ویسپی ضمنا به طور کامل از زبان فارسی هم پشتیبانی می‌کند و در تنظیمات اپ می‌توانید نوشته‌های انگلیسی محیط اپ را تماما به زبان مادری‌مان تغییر دهید. این اپ به غیر از رابط کاربری گمراه‌کننده‌ای که دارد، فضای رم زیادی هم اشغال می‌کند. برای مثال حجم فایل نصب اپ در نسخه اندروید حدودا ۵۰ مگابایت است، پس از نصب به صد مگابایت می‌رسد و هنگام فعال‌بودن در پس‌زمینه چیزی در حدود ۲۰۰ مگابایت از رم را به خود اختصاص می‌دهد که همین می‌تواند عامل افزایش مصرف باتری و کندی سیستم‌عامل شود. اما با وجود این مشکلات، شکی نیست که امکانات خوب و رایگان ارتباطی ویسپی برگ برنده‌اش محسوب شده و می‌تواند عامل استقبال کاربران ایرانی از آن در آینده‌ای نزدیک باشد.

رشد چشمگیر ارزش سهام اپل در ۳ماهه نخست ۲۰۱۷

روزنامه وال‌استریت ژورنال از رشد ارزش اپل و رسیدن به ۱۴۴.۸ میلیارد دلار در سه‌ماهه نخست ۲۰۱۷ خبر داد. به این ترتیب، دارندگان سهام اپل بهترین فصل مالی این شرکت را در پنج سال گذشته تجربه کرده‌اند. مطابق این گزارش، این افزایش در ارزش بازار اپل در سه‌ماهه مالی نخست ۲۰۱۷ (منطبق بر سه‌ماهه مالی دوم این شرکت) به میزان ۲۴ درصد برآورد شده است. براساس گزارشی که در تاریخ ۳۱ ژانویه ۲۰۱۷ از سوی اپل منتشر شد، این شرکت رقم فروش محصول آیفون را به حدود ۷۸.۳ میلیون واحد رسانده است؛ امری که نشان‌دهنده پایان دوره رکود در فروش این گوشی محسوب می‌شود. هر واحد سهم اپل در پایان روز ۳۱ ژانویه ۲۰۱۷، با قیمت معمول ۱۲۱.۳۵ دلار بسته شد و گزارش درآمدها پس از اتمام ساعات معاملاتی منتشر شد. به همین دلیل، روز معاملاتی بعد، یعنی نخستین روز فوریه، قیمت هر سهم اپل با رشدی ۶.۱ درصدی به ۱۲۸.۷۵ دلار رسید. این افزایش قیمت نظر خریداران را به خود جلب کرد و روند صعودی اپل به نحوی ادامه یافت که در پایان روز جمعه ۳۱ مارس، سهم این شرکت با ارزش ۱۴۳.۶۶ دلار بسته شد. به اعتقاد کارشناسان، گزارش مالی ۳۱ ژانویه، به تنهایی توانست باعث رشد ۱۸.۴درصدی ارزش سهام اپل در طول دوماهه پایانی فصل گذشته شود. به گزارش وب‌سایت mo-bile، گفتنی است سه‌ماهه مالی نخست اپل هم‌زمان با تعطیلات سال نوی میلادی بوده است که به طور معمول بیشترین خرید آیفون در این بازه زمانی انجام می‌شود. گزارش مالی این شرکت در سه‌ماهه منتهی به دسامبر ۲۰۱۶ نیز این موضوع را تأیید می‌کند. البته با وجود اینکه سهام اپل در سه‌ماهه نخست ۲۰۱۷ رشد کرده است، اما عایدی هر سهم (P/E) این شرکت براساس فهرست S&P ۵۰۰ همچنان پایین است. حال باید دید ۱۰سالگی آیفون و معرفی گوشی جدید اپل با نام احتمالی آیفون ۸ - که در سپتامبر ۲۰۱۷ عرضه خواهد شد- چه تأثیری بر رکورد ۷۸.۳ میلیونی این گوشی‌ها خواهد گذاشت. ارزش بازار این شرکت (حاصل ضرب قیمت هر سهم در مجموع سهام در جریان شرکت) در روز جمعه ۳۱ مارس پس از بسته‌شدن بازار برابر با ۷۵۳.۷۲ میلیارد دلار گزارش شده است.

امنیت

فکر عبور به جای رمز عبور



هکرها تا جایی پیش رفته‌اند که متخصصان حتی نسبت به امن‌بودن اثر انگشت برای ورود به سیستم‌ها هم تردید دارند. دانشمندان راهکاری جدید ارائه کرده‌اند که در آن به جای «رمز عبور» می‌توان با «فکر عبور» وارد سیستم‌ها شد. رمز عبور هنوز رایج‌ترین راه ورود به سیستم‌های کامپیوتری است. متخصصان امنیت همواره در تلاش‌اند تا راه ورود به سیستم‌ها را دشوارتر کنند تا نفوذ به آنها فقط با واردکردن پسوردی که به راحتی ممکن است در اختیار هکرها قرار گیرد، ممکن نباشد. یکی از راه‌های ورود که با تاچ‌آی‌دی اپل فراگیر شد، استفاده از اثر انگشت کاربران برای احراز هویت است. اثر انگشت مانند دیگر داده‌های بیومتریک از داده‌های منحصربه‌فرد هرکسی است. اما یکتابودن اثر انگشت به معنی آن نیست که استفاده از آن برای احراز هویت لزوما امن‌تر است. در سال ۲۰۱۴ هکرهای تحت فرمان دولت چین با نفوذ به شبکه کامپیوتری دفتر مدیریت پرسنلی آمریکا، اطلاعات حساس و خصوصی بیش از ۲۲ میلیون شهروند آمریکایی را ربودند. از جمله این اطلاعات، اثر انگشت ۵.۶ میلیون شهروند آمریکا بود. این داده‌ها هنوز در بازار سیاه عرضه نشده‌اند، اما هکرها هر زمان که بخواهند می‌توانند از آنها علیه صاحبانشان استفاده کنند. به گزارش مجله آتلانتیک، سال گذشته گروهی از متخصصان در دانشگاه میشیگان با استفاده از چاپگرهای جوهرافشان و کاغذهای مخصوص توانستند از اثر انگشت‌هایی که با کیفیت بالا اسکن شده بودند، مدلی سه‌بعدی بسازند که به سادگی گوشی‌های هوشمند را فریب می‌دهد و بازشان می‌کند؛ همه اینها با تجهیزاتی است که با کمتر از ۵۰۰ دلار می‌توان تهیه کرد. پژوهشگران مؤسسه انفورماتیک توکیو هم توانستند با استفاده از عکس‌هایی از افراد که در آنها دستشان به وضوح پیداست، اثر انگشت آنها را بازسازی کنند. این کار را می‌توان با بسیاری از عکس‌هایی که کاربران داوطلبانه در شبکه‌های اجتماعی منتشر می‌کنند هم انجام داد. این یعنی امنیت داده‌های بیومتریک، از جمله اثر انگشت، در معرض تهدیدهای جدی است و باید برای ارتقای امنیت تدابیر بهتری اندیشید. برای غلبه بر ریسک‌های امنیتی داده‌های بیومتریک از جمله اثر انگشت یا شبکیه چشم، برخی متخصصان روی توسعه سیستم‌هایی کار می‌کنند که برای احراز هویت از داده‌های بیومتریک تغییرپذیر استفاده می‌کنند. به گزارش دویچه‌وله، در سال ۲۰۱۳ گروهی از پژوهشگران در دانشگاه برکلی پروژه‌ای آینده‌پژوهانه آغاز کردند که در آن برای ورود به سیستم‌ها به جای «رمزهای عبور» (Passwords) از «فکرهای عبور» (Passthoughts) استفاده می‌شود. در این روش شما برای ورود باید سه فاکتور را با هم تلفیق کنید: چیزی که می‌دانید (مثلا یک فکر خاص)، چیزی که بخشی از شماست (مثلا الگوهای مغزتان) و چیزی که در اختیار دارید (مثلا سنسورهایی که برای اندازه‌گیری موج‌های مغزتان نصب شده‌اند). برای ورود به سیستم با این تکنیک، شما درحالی‌که حسگرها را بر تن دارید، به چیزی که پیش‌تر تعیین کرده‌اید، فکر می‌کنید. این فکر می‌تواند هر چیزی باشد: صحنه‌ای از یک فیلم، قطعه‌ای موسیقایی، یا عکسی از چشم‌انداز اتاقتان. این فکر هرگز منتقل نمی‌شود، فقط معادل ریاضی سیگنال‌های الکتریکی‌ای که حین فکرکردن مغزتان به آن تولید می‌شود، برای احراز هویت بررسی خواهند شد. حتی اگر هکری، یا هرکس دیگری بداند که دقیقا به چه چیزی فکر می‌کنید، باز هم نخواهد توانست به جای شما وارد سیستم شود، چون شیوه اندیشیدن هرکسی کاملا متفاوت و یکتاست. تنها راه هک‌کردن این سیستم این است که با حمله فیشینگ فریبتان دهند و وادارتان کنند خودتان فکر عبورتان را به ذهن بیاورید تا آنها حاصل کار را ذخیره کنند و بعدها با فریب سیستم به جای شما وارد آن شوند، اما نکته اینجاست که فکر عبور شما مثل پسوردها برای همیشه بر باد نخواهد رفت و به‌سادگی می‌توانید آن را هر زمان که می‌خواهید، تغییر دهید.

دریچه

ابزاری برای جلوگیری از ردیابی ارائه‌دهنده اینترنت

• حریم شخصی یا حریم خصوصی به آن معناست که یک فرد یا گروه، بتواند اطلاعات مربوط به خود را مجزا کند و در نتیجه بتواند اطلاعاتش را با انتخاب خویش در برابر دیگران آشکار یا پنهان کند. مرزها و محتوای آنچه خصوصی قلمداد می‌شود، در میان فرهنگ‌ها و اشخاص متفاوت است، اما قالب اصلی آنها مشترک است. براساس گزارش پی‌سی‌ورلد، اولین نکته‌ای که در زمینه ابزارهای مخصوص حریم خصوصی، با آن روبه‌رو می‌شویم، این است که تا حدی که می‌توانید از اچ‌تی‌تی‌پی‌اس اوری‌ور استفاده کنید. این ابزار تمام مسیرهای شما را رمزگذاری می‌کند و باعث می‌شود ارائه‌دهنده خدمات اینترنتی شما، نتواند محتوای آنچه شما در حال مشاهده آن هستید را بررسی کند. ارائه‌دهنده اینترنت، تنها زمانی می‌تواند محتوای شما را ببیند که از پروتکل مورد بحث استفاده نکنید. گام دوم آن است که از شبکه خصوصی مجازی استفاده کنید البته نکته‌ای که باید به آن توجه کنید، آن است که از نوع رایگان این شبکه استفاده نکنید زیرا نوع رایگان، اطلاعات خصوصی شما را گردآوری می‌کند و برای تجزیه و تحلیل به تحلیلگران می‌فروشد. کارهای دیگری نظیر وی‌پی‌ان است.

وی‌پی‌ان مانند یک تونل رمزگذاری‌شده بین شما و اینترنت است. گام سوم این است که دی‌ان‌اس خود را تنظیم کنید. دی‌ان‌اس درواقع، سیستم نام دامنه است که باعث می‌شود کامپیوتر، نام وب‌سایت را با آدرس پروتکل اینترنتی، تطبیق دهد و مانند دفترچه تلفن اینترنتی عمل می‌کند. البته مشکل این است که کامپیوتر، معمولا به گونه‌ای پیکربندی شده است که از سیستم نام دامنه ارائه‌دهنده خدمات اینترنت شما استفاده کند، یعنی ارائه‌دهنده، می‌تواند درخواست‌های مرورگر شما را ببیند. به گزارش ایتنا، وی‌پی‌ان کاری می‌کند که بتوانید کامپیوتر خود را به‌گونه‌ای تنظیم کنید که از انتشار اطلاعات به وسیله دی‌ان‌اس جلوگیری کند.

اکنون با استفاده از این سه‌گامی که در زمینه حریم خصوصی بیان شد، می‌توانید از آشکارشدن اطلاعات خصوصی خود جلوگیری و از حریم خصوصی خود حفاظت کنید.

