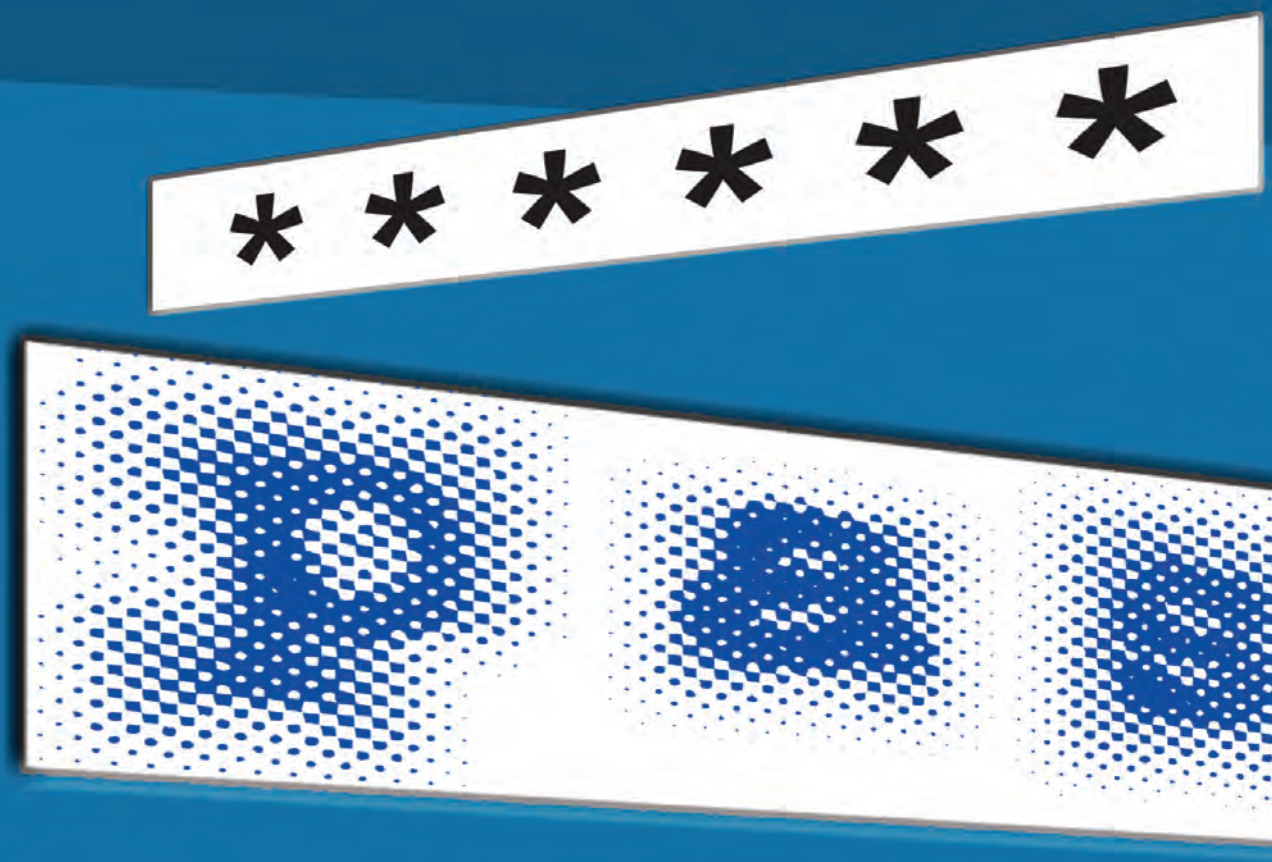
گذرواژه‌ها را فراموش کنیم

» منبع: وایرد
» گردآوری و ترجمه: احمد شریف‌پور

چرا دیگر رشته‌ای از کاراکترها نمی‌تواند امنیت ما را تأمین کند



شـــما هم بی‌شـــک رازی دارید که می‌تواند زندگی شما را زیر و رو کند و از این راز به‌خوبی نگه‌داری نمی‌کنید! تنها رشته‌ای از کاراکترها (اگر بی‌مبالات باشید حدود ۶ کاراکتر و اگر خیلی محتاط باشید ۱۶ کاراکتر) می‌تواند همه چیز را درباره شما آشکار کند!

آدرس ایمیل تان، حســـاب بانکی تان، آدرس پستی و شماره کارت اعتباری، عکس‌های شما یا بســـتگان تان، موقعیت دقیق محلی که هم‌اکنون در آن نشســـته‌اید، همه از جمله مواردی هستند که با یک رشته کاراکتر ساده قابل کشف هستند! از آغاز عصر اطلاعات تاکنون، ما همواره با این ایده روبه‌رو بوده‌ایم که یک گذرواژه با طول مناســـب، ابزاری مناســـب برای محافظت از تمام این داده‌های ارزشمند است. اما این روزها، این موضوع دیگر صحت ندارد، بلکه یک فانتزی و ایده‌ای تمام‌شده است و هر کس که هنوز چنین ادعایی دارد یا نادان است یا شما را نادان می‌پندارد.

گذرواژه‌های شما، هرچقدر پیچیده و هرچقدر یکتا باشند، دیگر نمی‌توانند از شما محافظت کنند.

مت هونان یکی از نویســـندگان ارشد وایرد می‌گوید: «تابستان گذشـــته هکرها در کمتـــر از یک ســـاعت، تمام زندگـــی دیجیتال من را ویران کردند.»

به اطرافتان نگاه کنید. نفوذها و درز کردن اطلاعات، هکرهایی که به سیستم‌های کامپیوتری نفوذ کرده و فهرستی از نام‌های کاربری و گذرواژه‌های افراد را روی وب منتشر می‌کنند، اکنون به اتفاقی معمول تبدیل شده‌اند. با سیستمی که ما حساب‌های کاربری‌مان را به هم متصل می‌کنیم و از آدرس ایمیل‌مان به‌عنوان یک نام کاربری جهانی در همه‌جا استفاده می‌کنیم، تنها یک نقطه ضعف اساسی به‌وجود آورده‌ایم که شکست آن می‌تواند نتایج هولناکی را برای ما به‌همراه داشته باشد. به‌لطف ذخیره‌سازی بیش‌ازپیش اطلاعات شخصی در ابرها، گول زدن کارمندان بخش خدمات شرکت‌ها برای تعویض گذرواژه‌ها هیچ‌گاه از این ساده‌تر نبوده است. تنها کاری که هکر باید انجام دهد این است که از اطلاعات شخصی شما که به‌صورت عمومی در یک سرویس خاص اینترنتی وجود دارد، برای نفوذ به حساب شما در سرویس‌های دیگر استفاده کند.

تابستان امسال، هکرها تمام زندگی دیجیتال من را در کمتر از یک ساعت نابود کردند. گذرواژه‌های من در سایت‌های اپل، توییتر و جی‌میل به اندازه کافی قدرتمند و طولانی (۷، ۱۰ و ۱۹ کاراکتر!) و همه آن‌ها ترکیبی از اعداد و حروف بودند. حتی در آن‌ها از نشانه‌های خاص هم استفاده کرده بودم. اما این سه حساب به هم مرتبط بودند و بنابراین زمانی که هکرها راهشان را به یکی از آن‌ها باز کردند، به هر سه دسترسی داشتند. آن‌ها تنها حساب توییتر من را با آدرس سرراست @mat می‌خواستند. یک نام کاربری سه حرفی که بسیار با پرستیژ به‌نظر می‌رسید. پس از آن برای ایجاد تأخیر در مراحل بازپس‌گیری این حساب کاربری، از حساب کاربری که در اپل داشتم برای پاک‌کردن اطلاعات تمام دستگاه‌های من یعنی آی‌فون، آی‌پد و مک‌بوک استفاده کردند. به این ترتیب همه پیام‌ها، اسناد و تمام عکس‌هایی که از دختر ۱۸ ماهه‌ام داشتم، از میان رفتند.

دوران گذرواژه‌ها گذشته است. مسئله این است که ما هنوز متوجه این قضیه نشده‌ایم.

از آن روز هولناک به بعد، من خودم را وقف تحقیق و بررسی در دنیای امنیت آنلاین کرده‌ام. چیزی که من یافته‌ام، بسیار وحشتناک است: نابود کردن زندگی دیجیتال ما بسیار ساده است! فرض کنید که من می‌خواهم به ایمیل شما نفوذ کنم و فرض کنید شما از خدمات AOL استفاده می‌کنید. تنها کاری که کافی است من انجام دهم این است که به سایت AOL بروم و اطلاعاتی مانند نام شما و شهر محل تولدتان را وارد کنم. شما هم می‌دانید که در دوران گوگل و شبکه‌های اجتماعی یافتن چنین اطلاعاتی بسیار ساده است. با این اطلاعات AOL به‌سادگی امکان بازنشانی گذرواژه را برای من فراهم می‌کند و من می‌توانم به جای شما وارد آن ایمیل شوم.

نخستین کار من پس از ورود چیست؟ به دنبال کلمه بانک می‌گردم تا ببینم بانکداری آنلاین‌تان را به حساب‌های کدام بانک انجام می‌دهید. پس از آن به سایت آن بانک می‌روم و روی لینک فراموشی «کلمه عبور کلیک» می‌کنم. یک گذرواژه جدید می‌سازم و وارد حساب بانکی‌تان خواهم شد. اکنون علاوه‌بر ایمیل، حساب بانکی شما هم دراختیار من است.

تابستان امسال من یادگرفتم که چگونه می‌توان تقریباً به همه چیز نفوذ کرد! با دو دقیقه زمان و هزینه کردن ۴ دلار در یک سایت ابتدایی و سردستی خارجی، می‌توانم به‌سادگی شماره کارت اعتباری، شماره تلفن، آدرس منزل و حتی شماره تأمین اجتماعی شما را به دست بیاورم. پنج دقیقه دیگر به من فرصت بدهید و خواهید دید که به‌سادگی می‌توانم وارد حساب‌های آمازون، بست‌بای، مایکروسافت و نت‌فلیکس شما بشوم و با افزودن ۱۰ دقیقه دیگر به این زمان، می‌توانم حساب‌های شما در AT&T، کام‌کست و ورایزون را هم دراختیار بگیرم. با دراختیار داشتن حداکثر ۲۰ دقیقه زمان، PayPal شما هم دراختیار من خواهد بود. برخی از این حفره‌های امنیتی تاکنون بسته شده‌اند، اما نه همه آن‌ها و تازه حفره‌های جدید هم هر روز کشف می‌شوند.

ضعف اساسی که در همه این نفوذها مورد استفاده قرار می‌گیرد، گذرواژه است. گذرواژه محصول دوره‌ای بود که سیستم‌های کامپیوتری ما این‌چنین به هم متصل نبودند. امروزه، هر کاری که بکنید و هر اقدام پیشگیرنده‌ای که به انجام برسانید، هیچ رشته تصادفی از اعداد و حروف و نشانه‌ها نمی‌تواند جلوی نفوذ مجرمانی که خود را وقف نفوذ به حساب کاربری شما می‌کنند، بگیرد. دوران گذرواژه‌ها گذشته است. مسئله این است که ما هنوز متوجه این قضیه نشده‌ایم.

عمر گذرواژه‌ها به اندازه عمر تمدن بشری است و در تمام این مدت مردم آن‌ها را شکسته یا کشف می‌کردند.

در سال ۴۱۳ پیش از میلاد و در اوج جنگ‌های پلوپونز (Peloponnesian War) ژنرال یونانی دموستنس (Demosthenes) با ۵ هزار سرباز وارد سیسیل شد تا در حمله به سیراکوزا شرکت کند. همه چیز برای یونانی‌ها خوب به‌نظر می‌رسید. سیراکوزا، دروازه ورود به اسپارت فتح شده تصور می‌شد.

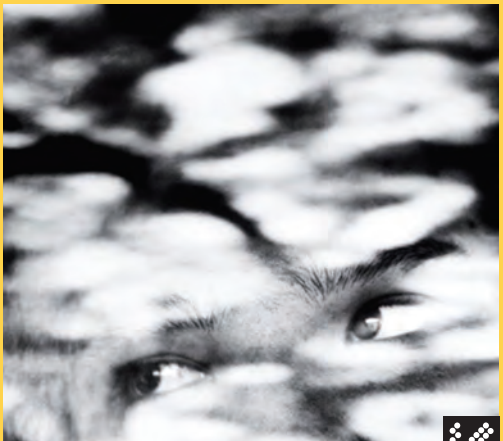
اما در یک درگیری شبانه در اپی‌پل (Epipole) نیروهای دموستنس متفرق شدند و در حالی که تلاش می‌کردند دوباره نظم و اتحاد خود را بازیابند شروع به فریاد زدن رمز شب کردند. کلمه‌ای از پیش تعیین شده که نشان می‌داد یک سرباز خودی است. سیراکوزایی‌ها این کلمه عبور را دریافته و به اطلاع تمام نیروهای خود رساندند. زمانی که یونانیان بسیار قدرتمند و یکپارچه به‌نظر می‌رسیدند، این رمز شب به دشمنان آن‌ها اجازه داد که نیروهای اندک‌شان را یونانی جا زده و با این حیله تلفات سنگینی را به ارتش یونان وارد کردند و زمانی که

تابستان امسال، هکرها تمام زندگی دیجیتال من را در کمتر از یک ساعت نابود کردند. گذرواژه‌های من در سایت‌های اپل، توییتر و جی‌میل به اندازه کافی قدرتمند و طولانی (۷، ۱۰ و ۱۹ کاراکتر!) و همه آن‌ها ترکیبی از اعداد و حروف بودند. دوران گذرواژه‌ها گذشته است. مسئله این است که ما هنوز متوجه این قضیه نشده‌ایم.

آفتاب برآمد، سواره‌نظام آن‌ها بقایای ارتش یونان را نیز نابود کرد و این نقطه عطفی در تاریخ این جنگ‌ها بود.

نخستین سیستم‌هایی که از گذرواژه‌ها استفاده کردند به‌احتمال زیاد ماشین‌های سیستم اشتراک زمانی MIT بودند که در سال ۱۹۶۱ توسعه یافته بودند. برای محدود کردن زمانی که هر کاربر می‌توانست از CTSS (سرنام Compatible Time Sharing System) استفاده کند، از یک سیستم لاگین استفاده شد. تنها یک سال طول کشید تا یک دانشجوی دکترا با نام آلان شر (Allan Scher) که به زمانی بیش از ۴ ساعت مقرر شده نیاز داشت، بتواند با حقه‌ای ساده این سیستم لاگین را دور بزند. او فایل حاوی گذرواژه‌ها را یافت و یک پرینت از آن تهیه کرد! از آن به بعد او هرچه قدر می‌خواست وقت دراختیار داشت.

در سال‌های شکل‌گیری وب، که ما کم‌کم به زندگی آنلاین روی می‌آوردیم، گذرواژه‌ها به‌خوبی کار می‌کردند. مهم‌ترین دلیل این امر این بود که داده‌های اندکی برای محافظت کردن وجود داشت. گذرواژه‌های ما تنها برای چند مورد خاص نظیر یک ایمیل و یک یا دو حساب تجارت الکترونیکی، کاربرد داشتند. چون در آن زمان تقریباً هیچ اطلاعات شخصی در ابرها ذخیره نشده بود (در واقع هنوز ابری وجود نداشت!)، نفوذ به حساب کاربری افراد تقریباً هیچ صرفه اقتصادی نداشت و هکرها هم بیشتر به‌دنبال نفوذ به سیستم‌های شرکت‌های بزرگ بودند. و ما کم‌کم مغرور شدیم. آدرس‌های ایمیل به‌نوعی لاگین جهانی تبدیل شدند و به‌عنوان نام کاربری تقریباً در همه سرویس‌ها مورد استفاده قرار گرفتند. این کار به‌رغم افزایش نمایی تعداد حساب‌های آنلاین، یا به عبارتی تعداد نقطه ضعف‌های ممکن، به همان شکل ادامه یافت. ایمیل‌های وب، دروازه‌های ورود به دوران کامپیوترهای لوحی و برنامک‌های ابری شدند. ما استفاده از خدمات بانکی روی کلاود را آغاز کردیم، اعتبارها و کارهای مالی‌مان را در کلاود انجام دادیم و مالیات‌هایمان را هم



شکل ۱ «کازمو» هکر نوجوانی از اهالی لانگ‌بیچ کالیفرنیا است که توانسته است با مهندسی اجتماعی، به حساب‌هایی در سایت‌های آمازون، AT&T، AOL، مایکروسافت، نت‌فلیکس و... نفوذ کند.

نحوه کار یک هکر گذرواژه

متن زیر از گفت‌وگوی آنلاین کارمند پشتیبانی اپل و هکری که خود را برایان (یک مشتری واقعی اپل) جا زده است نقل می‌شود. این گفت‌وگو در ژانویه ۲۰۱۲ صورت گرفته است. هدف هکر بازنشانی گذرواژه و دراختیار گرفتن حساب کاربری است.

اپل: آیا می‌توانید به یک پرسش درباره حساب کاربری‌تان پاسخ دهید؟ نام بهترین دوست‌تان چیست؟

هکر: فکر کنم کوین، آستین یا مکس باشد.

اپل: هیچ کدام از این پاسخ‌ها درست نبودند. فکر نمی‌کنید در پاسخ به این پرسش‌ها نام خانوادگی را تنظیم کرده باشید؟

هکر: فکر نمی‌کنم البته غیرممکن هم نیست. من که ۴ رقم آخر کارت اعتباری را گفتم. این کافی نیست؟

اپل: آن ۴ رقم هم اشتباه بودند. کارت اعتباری دیگری ندارید؟

هکر: ممکن است دوباره چک کنید؟ من یک کارت Visa دارم که همین حالا جلوی چشمم است و ۴ رقم آخرش ۵۵۵۵ است.

اپل: من دوباره کنترل کردم. ۵۵۵۵ شماره‌ای نیست که در حساب شما ثبت شده است. آیا سیستم آنلاین و تأیید صلاحیت با استفاده از ایمیل را امتحان کرده‌اید؟

هکر: بله اما ایمیل من هک شده است. من فکر می‌کنم که هکر یک کارت اعتباری جدید به حساب من اضافه کرده باشد. این اتفاق تقریباً برای تمام حساب‌های من افتاده است.

اپل: می‌خواهید گزینه نام و نام‌خانوادگی بهترین دوست‌تان را امتحان کنید؟

هکر: الآن برمی‌گردم. غذایم دارد می‌سوزد. ببخشید یک لحظه.

اپل: باشد. مشکلی نیست.

هکر: خوب. من برگشتم. فکر می‌کنم جواب ممکن است کریس باشد. او دوست خوبی است.

اپل: متأسفم برایان. این جواب هم اشتباه است.

هکر: نام کاملش کریستوفر ... است. گزینه دیگر هم ممکن است ریموند ..... باشد.

اپل: هر دوی این‌ها متأسفانه غلط هستند.

هکر: من می‌توانم یک فهرست از این دوستان احتمالی برایت ردیف کنم. برایان ....، استیون ....، بریین ....

اپل: نظرتان راجع به یک گزینه دیگر چیست؟ نام یکی از پوشه‌هایی را که خودتان در سیستم ایمیل ایجاد کرده‌اید بگویید.

هکر: فکر کنم Google، Gmail یا Apple باشد. من به عنوان برنامه‌نویس در گوگل کار می‌کنم.

اپل: خوب. اپل درست است. می‌توانم آدرس پشتیبان شما را داشته باشم؟

هکر: آدرس ایمیل جایگزینی که هنگام ساختن حساب کاربری وارد کرده‌ام؟

اپل: من فقط به یک آدرس ایمیل نیاز دارم تا لینک بازنشانی گذرواژه را برای شما ارسال کنم.

هکر: ممکن است از آدرس toe@aol.com استفاده کنید؟

اپل: ایمیل برای شما ارسال شد.

هکر: ممنون!

تابستان امسال من یادگرفتم که چگونه می‌توان تقریباً به همه چیز نفوذ کرد! با دو دقیقه زمان و هزینه کردن ۴ دلار در یک سایت ابتدایی و سردستی خارجی، می‌توانم به‌سادگی شماره کارت اعتباری، شماره تلفن، آدرس منزل و حتی شماره تأمین اجتماعی شما را به دست بیاورم. پنج دقیقه دیگر به من فرصت بدهید و خواهید دید که به‌سادگی می‌توانم وارد حساب‌های آمازون، بست‌بای، مایکروسافت و نت‌فلیکس شما بشوم.

داده‌های‌مان را هم در فضای ابری ذخیره کردیم.

درواقع هرچه تعداد هک‌های قابل توجه بیشتر شد، ما بیشتر و بیشتر به یک فلسفه نگه‌دارنده روانی تکیه کردیم و آن نظریه «گذرواژه‌های قوی» بود. این مصالحه‌ای بود که شرکت‌های وبی در حال رشد، برای نگه‌داشتن افراد و جلب اعتماد آن‌ها برای ذخیره اطلاعات‌شان در سایت‌هایشان به آن روی آوردند. این یک چسب زخم معمولی بود که اکنون در رودی از خون در حال شسته شدن است.

هر چهارچوب امنیتی برای استفاده در شرایط دنیای واقعی باید در دو چیز با کاربران مصالحه کند. نخستین موضوع راحتی کاربران است. امن‌ترین سیستم، در صورتی که استفاده از آن بسیار دشوار باشد، هیچ فایده‌ای نخواهد داشت. الزام کاربر به وارد کردن یک گذرواژه ۲۵۶ حرفی مبنای ۱۶ می‌تواند داده‌های شما را امن نگه دارد، اما هیچ کاربری حاضر به لاگین یا استفاده از این سیستم نخواهد بود. دستیابی به امنیت بیشتر در صورتی که بخواهید کاربران را آزار داده و تحت فشار قرار دهید، به‌سادگی امکان‌پذیر خواهد بود. اما چنین شیوه‌ای کار نخواهد کرد.

مصالحه دوم، حریم خصوصی است. اگر تمام سیستم طراحی شده باشد که داده‌ها را امن نگه‌دارد، کاربران به سختی با روشی کنار خواهند آمد که حریم خصوصی آن‌ها را مورد تعرض قرار دهد. یک گاوصندوق جادویی را برای منزل‌تان در نظر بگیرید که به هیچ گذرواژه یا کلیدی احتیاج نداشته باشد. چرا که کارشناسان امنیت ۲۴ ساعت روز و ۷ روز هفته در خانه شما حضور دارند و گاوصندوق را زمانی که مطمئن شوند خود شما به محتویاتش نیاز دارید، برای تان باز می‌کنند. بدون حریم خصوصی، می‌توانیم امنیت کامل را برقرار کنیم، اما هیچ‌کس چنین سیستمی را نخواهد پذیرفت.

دهه‌ها است که این مصالحه‌ها شرکت‌های وبی را می‌ترسانند. آن‌ها می‌خواستند که فرآیند وارد شدن به حساب کاربری و استفاده از خدمات‌شان، هم کاملاً خصوصی و امن و هم بسیار ساده به نظر برسند. درست همان‌چیزی که امنیت کامل را تقریباً غیرممکن می‌کند. درنتیجه آن‌ها به راه‌کار گذرواژه‌های قدرتمند روی آوردند. آن را به حد کافی طولانی کنید، چند حرف بزرگ و عدد در آن وارد کنید و در آخر آن علامت تعجب بگذارید و همه چیز خوب پیش خواهد رفت.

اما سال‌ها است که این روش مناسب و کارآمد نبوده است. در دوران الگوریتم‌ها، زمانی که لپ‌تاپ ما توان پردازشی بیش از ایستگاه‌های کاری یک دهه قبل دارند، شکستن یک گذرواژه با تلاش کور، تنها به چند میلیون چرخه اضافی از پردازنده احتیاج دارد. این تازه بدون در نظر گرفتن روش‌های جدید هک برای سرقت گذرواژه‌ها یا دور زدن کامل آن‌ها است. این‌ها روش‌هایی هستند که طول زیاد یا پیچیدگی گذرواژه نمی‌تواند در برابر آن مقاومت کند. میزان نفوذ به اطلاعات در ایالات‌متحده در سال ۲۰۱۱ حدود ۶۷ درصد بیشتر شده است و هر نفوذ اطلاعاتی مهم، بسیار گران تمام می‌شود: پس از آن‌که پایگاه داده حساب‌های پلی‌استیشن سونی هک شد، شرکت مجبور شد ۱۷۱ میلیون دلار را صرف بازسازی شبکه‌اش و حفاظت از کاربران در برابر سرقت هویت کند. اگر هزینه کل را در نظر بگیریم که شامل کسب‌وکارهای نابود شده هم می‌شود، می‌بینیم که یک هک واحد می‌تواند به یک مصیبت چند میلیارد دلاری تبدیل شود.

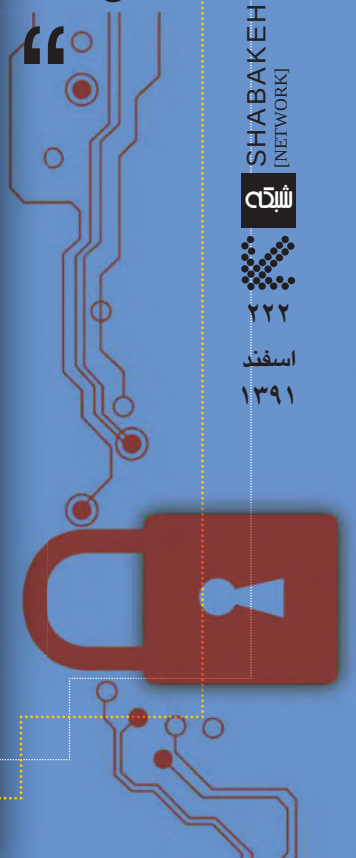
گذرواژه‌های آنلاین ما چگونه لو می‌روند؟ این کار به هر طریقی که فکر کنید ممکن است رخ دهد. گذرواژه‌های ما حدس زده می‌شوند، از فایل dump گذرواژه‌ها استخراج می‌شوند، با تلاش کور شکسته می‌شوند، توسط یک keylogger سرقت می‌شوند یا با گول زدن دپارتمان خدمات مشتریان یک شرکت بزرگ بازنشانی می‌شوند.

بیایید با یک هک ساده یعنی حدس زدن شروع کنیم. مشخص است که بی‌احتیاطی بزرگ‌ترین ریسک امنیتی است. به‌رغم این که سال‌ها است به مردم گفته می‌شود که از گذرواژه‌های ساده و قابل حدس زدن استفاده نکنند، آن‌ها این کار را می‌کنند. وقتی که مارک برنت (Mark Burnett) با استفاده از منابع در دسترس (نظیر جست‌وجو در گوگل یا فایل dump گذرواژه‌ها که هکرها در اینترنت منتشر می‌کنند) فهرستی از ۱۰ هزار گذرواژه پرکاربرد را تهیه کرد، متوجه شد که رتبه نخست این فهرست به کلمه password تعلق دارد! دومین گذرواژه پرکاربرد؟ رشته اعداد ۱۲۳۴۵۶! اگر شما از گذرواژه ساده‌ای مانند این‌ها استفاده می‌کنید، به‌دست‌آوردن حساب کاربری شما هیچ کاری نخواهد داشت. ابزارهای نرم‌افزاری رایگانی نظیر Cain & Abel یا John the Ripper فرآیند شکستن گذرواژه‌ها را تا حدی ساده می‌کنند که حتی یک کودک هم از پس آن برمی‌آید. تنها چیزی که لازم است یک اتصال اینترنتی و فهرستی از گذرواژه‌های پرکاربرد است؛ که چنین فهرست‌هایی هم به سادگی و در قالب‌های معمول پایگاه‌های داده، در اینترنت یافت می‌شوند.

نکته تکان‌دهنده این نیست که مردم هنوز از این گذرواژه‌ها استفاده می‌کنند، بلکه این است که برخی شرکت‌ها هنوز اجازه استفاده از چنین گذرواژه‌هایی را می‌دهند. همان فهرست گذرواژه‌های پرکاربردی که برای شکستن گذرواژه‌ها استفاده می‌شود، را می‌توان برای حفظ امنیت کاربران به کار برد و از همان ابتدا اجازه نداد که کاربران چنین گذرواژه‌هایی را مورد استفاده قرار دهند. اما ترک دادن عادات بد ما برای پذیرفتن گذرواژه به عنوان یک مکانیسم امنیتی کافی نیست.

دیگر اشتباه رایج استفاده دوباره از گذرواژه‌ها است. در دو سال گذشته بیش از ۲۸۰ میلیون هش (hash فهرستی

هرچه تعداد هک‌های قابل توجه بیشتر شد، ما بیشتر و بیشتر به یک فلسفه نگه‌دارنده روانی تکیه کردیم و آن نظریه «گذرواژه‌های قوی» بود. این مصالحه‌ای بود که شرکت‌های وبی در حال رشد، برای نگه‌داشتن افراد و جلب اعتماد آن‌ها برای ذخیره اطلاعات‌شان در سایت‌هایشان به آن روی آوردند. این یک چسب زخم معمولی بود که اکنون در رودی از خون در حال شسته شدن است.



رمزنگاری شده اما آماده شکستن از گذرواژه‌ها) به‌صورت آنلاین منتشر شده‌اند که هر کسی می‌تواند آن‌ها را ببیند. سایت‌های Gawker، Yahoo، LinkedIn و eHarmony همه شاهد نفوذهای امنیتی بوده‌اند که باعث به سرقت رفتن نام‌های کاربری و گذرواژه‌های میلیون‌ها نفر و انتشار آن‌ها در فضای وب شده است. مقایسه‌ای که میان دو مورد از فایل‌های dump این سایت‌ها انجام گرفت، نشان داد که ۴۹ درصد مردم از نام کاربری و گذرواژه‌های یکسانی در این سایت‌ها استفاده کرده‌اند.

دیانا اسمترز (Diana Smetters) یکی از مهندسان نرم‌افزار گوگل که روی سیستم‌های تشخیص هویت کار می‌کند، می‌گوید: «استفاده دوباره از گذرواژه‌ها چیزی است که شما را به ورطه نابودی می‌برد. اقتصاد کارآمدی وجود دارد که در آن این اطلاعات را خرید و فروش می‌کنند.» غالب هکرهایی که dump گذرواژه‌ها را روی وب منتشر می‌کنند، آدم‌های به‌نسبت خوبی هستند. آدم‌های بد گذرواژه‌ها را دزدیده و به سرعت آن را در بازار سیاه به فروش می‌رسانند. اطلاعات لاگین شما، ممکن است خیلی وقت پیش لو رفته باشد، و شما از آن بی‌خبر باشید تا زمانی که همان حساب کاربری یا حساب‌هایی با اطلاع مشابه را از دست بدهید.

هکرها از طریق گول زدن ما نیز ممکن است به گذرواژه‌ها دست پیدا کنند. شناخته‌شده‌ترین روش در این زمینه فیشینگ است. در این روش هکر ظاهر سایت‌های مشهور را شبیه‌سازی کرده و کاربر را وادار می‌کند اطلاعات لاگین را وارد کند. استیون داونی (Steven Downey) مدیر ارشد اطلاعات شرکت Shipley Energy در پنسیلوانیا توضیح می‌دهد که چگونه این روش باعث لو رفتن حساب‌های آنلاین یکی از اعضای هیئت مدیره شرکت در بهار گذشته شده است. این عضو هیئت مدیره از گذرواژه‌ای طولانی با حروف بزرگ و کوچک و اعداد برای حفاظت از ایمیلش در سایت AOL استفاده می‌کرد. اما اگر بتوانید صاحب گذرواژه را وادار کنید آن را برای شما تایپ کند، نیازی نیست آن را با تلاش کور بشکنید.

این هکر کار خود را به این صورت پیش برد: او ایمیلی را برای این عضو هیئت مدیره فرستاد. این ایمیل محتوی لینکی به یک صفحه AOL شبیه‌سازی شده بود که از او می‌خواست اطلاعات لاگین‌اش را وارد کند و او این کار را کرد! اما پس از آن هکر اقدام دیگری انجام نداد. تنها وارد حساب ایمیل او شده و همه ایمیل‌های او را برای شناختن بیشتر قربانی‌اش مطالعه کرد. او فهمید که این عضو هیئت مدیره از خدمات کدام بانکداری آنلاین استفاده می‌کند و همین‌طور فهمید که او حسابداری دارد که کارهای مالی‌اش را ردیف می‌کند. او حتی شیوه نگارش و رفتار دیجیتال او را یاد گرفت و فهمید ایمیل‌ها و چت‌هایش را چگونه شروع یا تمام می‌کند. تازه اینجا بود که او وارد

چگونه از فاجعه گذرواژه‌ها جان سالم به در ببریم

تا زمانی که راه بهتری برای محافظت از داده‌های آنلاین‌مان پیدا کنیم، در اینجا ۴ اشتباه را که نباید در مورد گذرواژه‌ها انجام دهید به شما یادآوری می‌کنیم و همین‌طور از ۴ راه‌کاری صحبت می‌کنیم که باعث می‌شوند نفوذ به حساب‌های شما سخت‌تر (اما نه غیرممکن) شوند.

نبایدها

هیچ‌گاه از گذرواژه‌های‌تان دوباره استفاده نکنید. اگر این کار را بکنید، هکری که به یکی از حساب‌های شما دست پیدا کند، تمام آن‌ها را دراختیار خواهد داشت.

هیچ‌گاه از کلمات معمول که در فرهنگ لغات یافت می‌شوند استفاده نکنید. اگر مجبور شدید چند لغت را به هم بچسبانید تا یک عبارت طولانی‌تر ساخته شود.

از جایگذاری معمول اعداد به‌جای حروف خودداری کنید. فکر می‌کنید P455wOrd گذرواژه مناسبی است؟ نه!

ابزارهای نفوذ این قابلیت‌های جایگذاری را به‌صورت توکار دارند.

از گذرواژه‌های کوتاه استفاده نکنید. مهم نیست که چقدر دشوار باشد، سرعت پردازشی کنونی به این معنا است که حتی گذرواژه‌هایی مانند h6!r$q هم به‌سادگی قابل شکستن هستند. بهترین دفاع شما طولانی‌ترین گذرواژه ممکن است.

بایدها

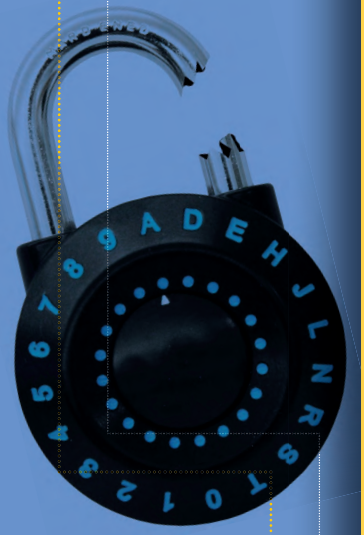
در هرجایی که ممکن است از اعتبارسنجی دو مرحله‌ای استفاده کنید. وقتی که از مکان‌های ناشناس به حساب‌تان لاگین می‌کنید، سیستم‌های اعتبارسنجی دو مرحله‌ای کد تأییدی را به‌صورت پیامک به دست شما می‌رسانند تا فرآیند لاگین را کامل کنید. بله، به این سیستم‌ها هم می‌توان نفوذ کرد، اما به هر حال از هیچ بهتر است.

برای پرسش‌های امنیتی جواب‌های عجیب و غریب تعیین کنید. به آن‌ها به دید یک گذرواژه ثانویه نگاه کنید. فقط جواب‌هایتان باید قابل حفظ کردن باشند. نخستین ماشین‌تان؟ جواب مثلاً باید این باشد:

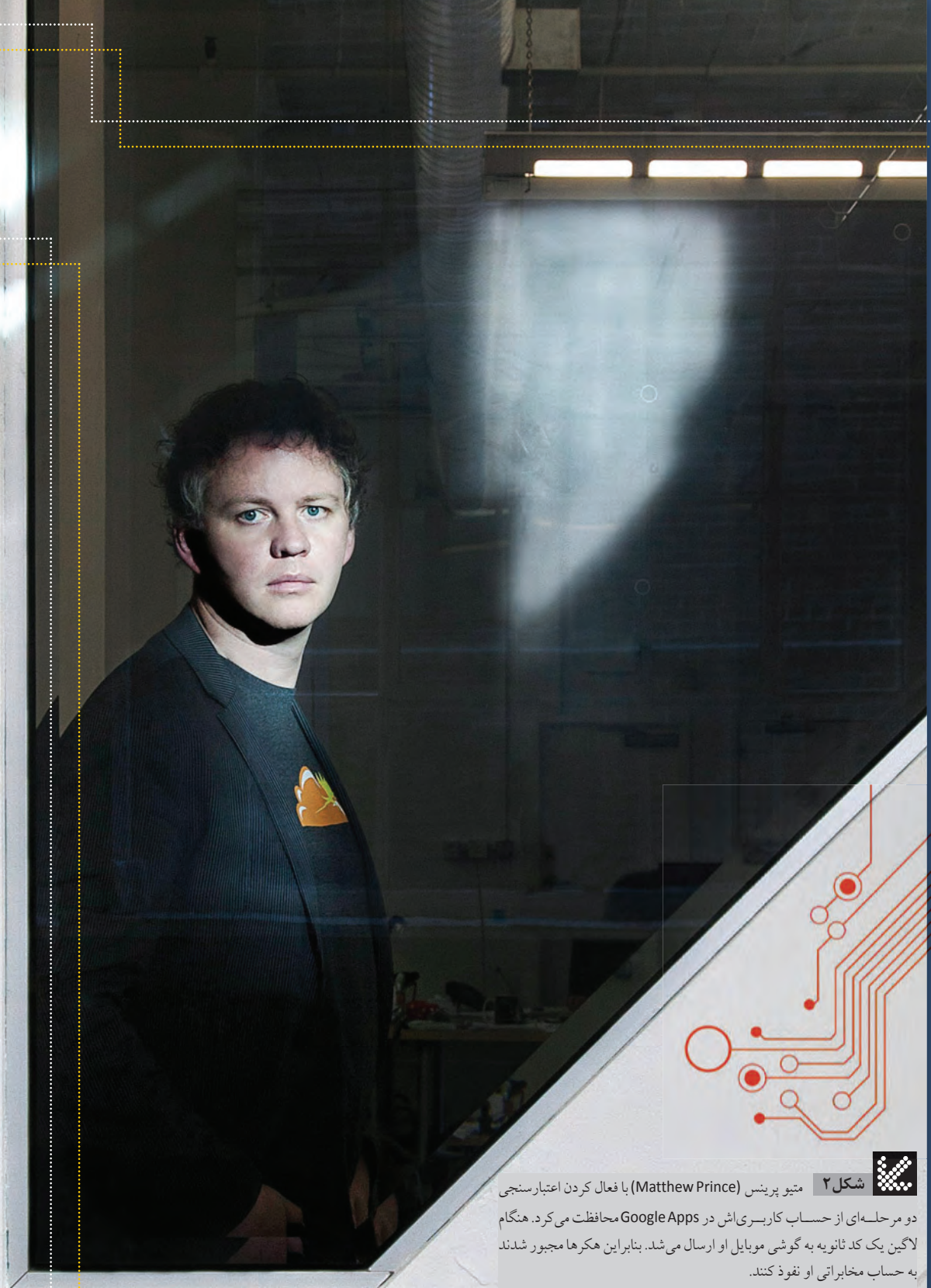
Camper Van Beethoven Freaking Rules

همه اطلاعات‌تان را در فضای مجازی آشکار نکنید. ساده‌ترین راه نفوذ به یک حساب کاربری، از طریق ایمیل و آدرس پرداخت صورت‌حساب‌های‌تان است. سایت‌هایی مانند Spokeo یا WhitePage روش‌هایی برای حذف اطلاعات شما از پایگاه‌های داده‌شان فراهم آورده‌اند.

از یک ایمیل یکتا و امن برای بازیابی گذرواژه‌های‌تان استفاده کنید. اگر هکر بداند که لینک‌های بازیابی گذرواژه شما به کدام آدرس می‌رسند، این آدرس به خط مقدم حمله تبدیل خواهد شد. پس یک حساب کاربری باز کنید و از آن برای هیچ یک از تماس‌های‌تان استفاده نکنید. همچنین مطمئن شوید که از یک نام کاربری استفاده کرده‌اید که هیچ ربطی به نام واقعی‌تان ندارد. به این ترتیب، این حساب به‌سادگی قابل حدس زدن نخواهد بود.



گذرواژه‌های آنلاین ما چگونه لو می‌روند؟ این کار به هر طریقی که فکر کنید ممکن است رخ دهد. گذرواژه‌های ما حدس زده می‌شوند، از فایل dump گذرواژه‌ها استخراج می‌شوند، با تلاش کور شکسته می‌شوند، توسط یک keylogger سرقت می‌شوند یا با گول زدن دپارتمان خدمات مشتریان یک شرکت بزرگ بازنشانی می‌شوند.



شکل ۲ متیو پرینس (Matthew Prince) با فعال کردن اعتبارسنجی دو مرحله‌ای از حساب کاربری‌اش در Google Apps محافظت می‌کرد. هنگام لاگین یک کد ثانویه به گوشی موبایل او ارسال می‌شد. بنابراین هکرها مجبور شدند به حساب مخابراتی او نفوذ کنند.

ما با ضعیف‌ترین حلقه این زنجیر روبه‌رو هستیم؛ حافظه انسان. گذرواژه‌ها باید دشوار باشند تا حدس زدن یا شکستن آن‌ها دشوار باشد. به همین دلیل اگر گذرواژه شما به اندازه کافی خوب باشد، به‌احتمال زیاد خودتان هم آن را فراموش خواهید کرد، به‌خصوص اگر به آن توصیه ایمنی قدیمی پایبند باشید و آن را جایی یادداشت نکنید.

عمل شد و از طرف قربانی ایمیلی برای حسابدارش فرستاد و تقاضای انجام سه انتقال آنلاین پول به یکی از بانک‌های استرالیا را کرد که جمع مبلغ آن‌ها ۱۲۰هزار دلار بود. پیش از آشکار شدن این نفوذ، حسابدار او ۸۹هزار دلار را واریز کرده بود!

یکی دیگر از راه‌های سرقت گذرواژه‌ها استفاده از انواع بدافزار است. برنامه‌هایی مخفی که به کامپیوتر شما نفوذ کرده و مخفیانه اطلاعات شما را برای دیگران ارسال می‌کنند. بنا به گزارش ورایزون، حمله‌های بدافزاری منشاء ۶۹ درصد از موارد لو رفتن داده‌ها در سال ۲۰۱۱ بوده‌اند. آن‌ها در ویندوز و آندروئید به اپیدمی تبدیل شده‌اند. بیشتر این بدافزارها کارشان را با نصب یک keylogger یا نوعی جاسوس‌افزار (spyware) انجام می‌دهند که آن‌چه شما تایپ می‌کنید یا بر صفحه نمایش می‌بینید را تحت‌نظر می‌گیرند. هدف این حمله‌ها اغلب شرکت‌های بزرگ هستند و هدف آن‌ها دزدیدن یک گذرواژه نیست، بلکه به دست آوردن هزاران گذرواژه و دراختیار گرفتن کل سیستم را مدنظر دارند.

یکی از مخرب‌ترین نمونه‌ها ZeuS است، بدافزاری که نخستین‌بار در سال ۲۰۰۷ مشاهده شد. کلیک یک لینک

آلوده که اغلب از طریق یک ایمیل فیشینگ به دست قربانی می‌رسد، آن را روی کامپیوتر نصب می‌کند. پس از آن این برنامه همانند یک هکر انسانی منتظر می‌ماند تا قربانی به یکی از سایت‌های بانکداری آنلاین وارد شود. به محض انجام این کار، ZeuS نام کاربری و گذرواژه قربانی را برای سروری که در اختیار هکر قرار دارد، ارسال می‌کند. تنها در یک مورد در سال ۲۰۱۰ اف‌بی‌آی به دستگیری ۵ نفر در اوکراین کمک کرد که از ZeuS برای سرقت ۷۰ میلیون دلار از ۳۹۰ قربانی استفاده کرده بودند که اغلب آن‌ها کسب‌وکارهای کوچکی در ایالات متحده بودند.

هدف گرفتن چنین شرکت‌هایی درواقع بسیار طبیعی است. جرمی گرانت (Jeremy Grant) که مدیر دپارتمان راهبردی ملی تجارت برای هویت‌های مطمئن در فضای سایبری (National Strategy for Commerce's Trusted Identities in Cyberspace) است می‌گوید: «هکرها به‌طرز فزآینده‌ای به‌دنبال کسب‌وکارهای کوچک می‌روند. آن‌ها پول بیشتری نسبت به افراد حقیقی دارند، اما از حفاظت کمتری نسبت به شرکت‌های بزرگ برخوردار هستند.» او درواقع کسی است که وظیفه عبور دادن ما از شیوه کنونی مبتنی‌بر گذرواژه را بر عهده دارد.

اگر مشکلات ما با گذرواژه‌ها در همین‌جا خاتمه می‌یافتند، می‌توانستیم سیستم را نجات دهیم. می‌توانستیم گذرواژه‌های ساده را ممنوع کنیم و درباره استفاده دوباره از گذرواژه‌ها به همه هشدار بدهیم. می‌توانستیم مردم را آموزش دهیم که از هکرهایی که حقه‌های فیشینگ را سرهم می‌کنند، زرنگ‌تر باشند. یعنی با دقت بیشتری به URL سایتی که گذرواژه‌شان را می‌پرسد نگاه کنند. می‌توانستیم از ضدویروس‌ها برای نابود کردن بدافزارها استفاده کنیم.

اما ما با ضعیف‌ترین حلقه این زنجیر روبه‌رو هستیم؛ حافظه انسان. گذرواژه‌ها باید دشوار باشند تا حدس زدن یا شکستن آن‌ها دشوار باشد. به همین دلیل اگر گذرواژه شما به اندازه کافی خوب باشد، به‌احتمال زیاد خودتان هم آن را فراموش خواهید کرد، به‌خصوص اگر به آن توصیه ایمنی قدیمی پایبند باشید و آن را جایی یادداشت نکنید. به همین دلیل تمام سیستم‌های مبتنی بر گذرواژه احتیاج به مکانیسمی برای بازنشانی گذرواژه‌ها خواهند داشت. آن مصالحه‌های اجتناب‌ناپذیر (امنیت در مقابل راحتی و حریم خصوصی) نیز به این معنا خواهند بود که بازیابی گذرواژه‌های فراموش‌شده هم نمی‌تواند چندان سخت باشد. این درست همان چیزی است که حساب‌های کاربری را در برابر مهندسی اجتماعی نفوذپذیر می‌کند. اگرچه نفوذ اجتماعی یا socialing تنها مسبب ۷ درصد از هک‌هایی بوده است که در سال گذشته توسط آژانس‌های دولتی ردگیری شده‌اند، اما ۳۷ درصد داده‌های به سرقت رفته از این طریق دزدیده شده‌اند.

نفوذ اجتماعی علت هک شدن Apple ID من در تابستان گذشته است. هکرها اپل را ترغیب کردند که گذرواژه من را در سیستم اپل تغییر دهد و این کار را با فراهم آوردن جزئیات آدرس و چهار رقم آخر شماره کارت اعتباری من انجام دادند. و چون من آدرس اپل را به عنوان آدرس پشتیبان حساب کاربری جی‌میل تنظیم کرده بودم، هکرها توانستند آن را هم هک کنند و در جریان این کار تمام اطلاعات آن (یعنی سابقه ۸ ساله ایمیل‌ها و اسناد آنلاین) را پاک کردند. آن‌ها همچنین خودشان را در توییتر به جای من جا زدند و مطالب نژادپرستانه‌ای را با نام من منتشر کردند.

زمانی که داستان من به رسانه‌ها راه یافت و عمومی شد، اپل روش کارش را عوض کرد: به‌صورت موقت امکان بازنشانی گذرواژه از طریق تلفن را غیرفعال کرد. اما هنوز می‌توانید این کار را به‌صورت آنلاین انجام دهید. به این ترتیب، تنها یک ماه بعد هکرها یک حفره امنیتی دیگر را برعلیه دیوید پوگو (David Pogue) نویسنده ستون فناوری نیویورک تایمز به کار گرفتند. این بار هکرها توانستند با عبور از پرسش‌های امنیتی که برای حسابش تنظیم کرده بود، گذرواژه او را بازنشانی کنند.

شاید شما هم روش کار را می‌دانید. برای بازنشانی گذرواژه‌های فراموش شده، کاربر باید به پرسش‌هایی پاسخ دهد که قرار است پاسخ آن‌ها را تنها خود او بداند. دیوید پوگو سه پرسش را برای تأمین امنیت حسابش انتخاب کرده بود. نخستین پرسش این بود: «نخستین ماشین شما چه بود؟» پرسش دوم این بود که «چه مدلی از ماشین‌ها را می‌پسندید؟» و بالاخره پرسش آخر این بود که «شما در اول ژانویه ۲۰۰۰ کجا بوده‌اید؟» پاسخ دو پرسش نخست از طریق گوگل مشخص می‌شود! او جایی نوشته بود که نخستین ماشین‌اش یک تویوتا کرولا بوده است و به تازگی هم نوشته‌هایی در تعریف از ماشین جدیدش (یک تویوتا پایروس) منتشر کرده بود. هکرها پاسخ پرسش آخر را با یک حدس عمومی به دست آوردند و مشخص شد که دیوید هم مانند بسیاری دیگر در سپیده‌دم هزاره سوم، در یک «مهمانی» بوده است!

با این اطلاعات هکرها توانستند به حساب کاربری او وارد شوند. آن‌ها به سراغ فهرست مخاطبان او رفتند و به آی‌مک او نیز دسترسی پیدا کردند.

شما ممکن است فکر کنید که این اتفاق برای شما رخ نخواهد داد و دلیل شما ممکن است این باشد: دیوید پوگو در دنیای اینترنت بسیار شناخته شده است؛ او یک نویسنده پرکار است که تمام امواج مغزی او روی اینترنت منتشر می‌شوند. اما اطلاعات چندانی از شما در اینترنت وجود ندارد. اشتباه می‌کنید. آیا به اطلاعات حساب کاربری LinkedIn خود فکر کرده‌اید؟ به صفحه فیس‌بوک‌تان چطور؟ به صفحات فرزندان، دوستان یا همکاران‌تان چطور؟ اگر حضوری فعال در اینترنت داشته باشید، پاسخ شما به پرسش‌های استاندارد (که تنها گزینه‌های موجود در تنظیمات امنیتی سایت‌ها هستند) به‌راحتی قابل کشف خواهد بود. نام دوشیزگی مادر شما ممکن است در سایت Ancestry.com موجود باشد، اسباب‌بازی مورد علاقه

"نفوذ اجتماعی علت هک شدن Apple ID من در تابستان گذشته است. هکرها اپل را ترغیب کردند که گذرواژه من را در سیستم اپل تغییر دهد و این کار را با فراهم آوردن جزئیات آدرس و چهار رقم آخر شماره کارت اعتباری من انجام دادند. و چون من آدرس اپل را به عنوان آدرس پشتیبان حساب کاربری جی‌میل تنظیم کرده بودم، هکرها توانستند آن را هم هک کنند و در جریان این کار تمام اطلاعات آن را پاک کردند."

دوران مدرسه‌تان در سایت Classmates در دسترس است، تاریخ تولدتان از طریق فیس‌بوک قابل کشف است و حتی نام بهترین دوست‌تان هم حداکثر با چندبار تلاش به دست خواهد آمد.

مشکل نهایی گذرواژه‌ها این است که تنها یک نقطه ضعف در سیستم، راه‌های زیادی را برای حمله هکرها باز می‌کند. به احتمال زیاد نمی‌توان یک سیستم امنیتی مبتنی بر گذرواژه طراحی کرد که آن‌قدر قابل حفظ کردن باشد که بتوان در تجهیزات قابل حمل از آن استفاده کرد، آن‌قدر انعطاف‌پذیر باشد که بتوان در سایت‌های مختلف از گذرواژه‌های مختلف استفاده کرد، بازنشانی آن به‌نسبت راحت باشد و در عین حال در مقابل تلاش‌های کور امنیت کافی را داشته باشد. اما این دقیقا همان سیستمی است که اکنون ما به آن تکیه کرده‌ایم!

اما این هک‌ها را چه کسانی انجام می‌دهند؟ چه کسی حاضر است با این جدیت هک کردن حساب کاربری شما را دنبال کند؟ پاسخ به این پرسش دو گروه را به ما معرفی می‌کند که هر دوی آن‌ها به یک اندازه خطرناک هستند: سندیکاهای بین‌المللی و نوجوانان بی‌کار!

سندیکاها به این دلیل خطرناک هستند که بسیار کارآمد و در همه زمینه‌ها توانا هستند. نوشتن ویروس و بدافزار کاری بود که هکرها برای سرگرمی و تفریح انجام می‌دادند، مدرکی برای اثبات یک ادعا بود! اما دیگر این‌چنین نیست. در اواسط دهه اول قرن جاری، ظهور جرایم سازمان‌یافته آغاز شد. امروزه نویسندگان ویروس‌ها به‌احتمال زیاد عضوی از یک گروه تبهکار حرفه‌ای هستند که در یکی از بقایای اتحاد جماهیر شوروی فعالیت می‌کند، نه دانشجویانی در یک خوابگاه دانشگاهی در بوستون. آن‌ها دلیل خوبی برای کارهای‌شان دارند؛ پول!

آمار نشان می‌دهد که هکرهای روس زبان در سال ۲۰۱۱ به تنهایی حدود ۴/۵ میلیارد دلار از طریق جرائم سایبری به جیب زده‌اند. به همین دلیل اصلا عجیب نخواهد بود که چنین فعالیت‌هایی سازمان‌دهی شده، به یک صنعت تبدیل شوند و حتی به اعمال خشونت نیز کشیده شوند. همچنین آن‌ها تنها کسب‌وکارها و مؤسسه‌های مالی را هدف نمی‌گیرند، بلکه به سراغ افراد عادی نیز می‌روند. تبهکاران سایبری روسیه، که بسیاری از آن‌ها به مافیای سنتی روسیه وابسته هستند، در سال گذشته ده‌ها میلیون دلار را از هک حساب‌های افراد عادی به دست آورده‌اند. غالب این درآمد با جمع‌آوری گذرواژه حساب‌های بانکداری آنلاین از طریق فیشینگ و حمله‌های بدافزاری کسب شده است. به عبارت دیگر، زمانی که گذرواژه حساب شما در Citibank سرقت می‌شود، به احتمال زیاد کار یکی از این تبهکاران است.

اما گروه نوجوانان خطرناک‌تر هستند، چراکه آن‌ها خلاقیت بیشتری به خرج می‌دهند. گروه‌هایی که حساب کاربری من و دیوید پوگو را هک کردند یک عضو مشترک داشتند. نوجوانی ۱۴ ساله که با نام مستعار Dictate فعالیت می‌کند. او براساس تعاریف سنتی یک هکر محسوب نمی‌شود، او تنها به بخش پشتیبانی شرکت‌ها زنگ زده یا به‌صورت آنلاین چت کرده و از آن‌ها می‌خواهد که گذرواژه‌ها را بازنشانی کنند. اما این امر نقش او را کم اهمیت نمی‌کند. افرادی مثل او کار را با جست‌وجوی وب برای یافتن اطلاعاتی از شما که به صورت عمومی در دسترس هستند، آغاز می‌کنند. اطلاعاتی عمومی مانند اسم، آدرس ایمیل و آدرس منزل که از طریق Spokeo و Whitepages.com به‌سادگی در دسترس هستند. آن‌ها در ادامه با استفاده از این اطلاعات گذرواژه‌های سایت‌هایی نظیر Hulu و Netflix را بازنشانی می‌کنند. این سایت‌ها جاهایی هستند که اطلاعات پرداخت شما از جمله چهار رقم آخر کارت اعتباری‌تان به سادگی قابل مشاهده است. زمانی که آن‌ها این چهار رقم را به دست آوردند، می‌توانند به حساب کاربری شما در AOL، مایکروسافت و سایر سایت‌های مشابه وارد شوند. به زودی با صبر و تحمل و انجام تلاش‌های آزمایش و خطا، او و دوستانش می‌توانند به ایمیل، عکس‌ها و فایل‌های شما دسترسی پیدا کنند، درست همان‌طور که به اطلاعات من دسترسی پیدا کردند.

چرا نوجوانانی مثل Dictate دست به چنین کارهایی می‌زنند؟ بیشتر اوقات برای تفریح، برای خرابکاری و لذت بردن از آن. یکی از اهدافی که زیاد دنبال می‌شود، خراب کردن وجهه اجتماعی افراد با انتشار مطالب نژادپرستانه و مستهجن از طریق حساب‌های کاربری و شخصی آن‌ها در شبکه‌های اجتماعی است. Dictate توضیح می‌دهد که «مطالب نژادپرستانه معمولاً واکنش‌های جالب‌تری را در میان مخاطبان ایجاد می‌کند. افراد به فعالیت‌های هکری توجهی نشان نمی‌دهند. زمانی که ما حساب کاربری @jennarose3x0 (یک خواننده نوجوان به نام جنا رز) را هک کردیم، اعلام این موضوع از طریق حساب کاربری توییتر او واکنش چندانی را برنیانگیخت. اما زمانی که ما یک ویدیو از تعدادی افراد سیاه‌پوست را آپلود کردیم و ادعا کردیم که ما این افراد سیاه‌پوست هستیم، بازخوردهای زیادی دریافت کردیم.» به‌نظر می‌رسد که جامعه‌ستیزی این گونه کار می‌کند.

بسیاری از این نوجوانان با اتکا به پس‌زمینه‌ای در شبکه‌های هک اکس‌باکس به اینجا می‌رسند. در این شبکه‌های رقابت آنلاین میان بازی‌کنان، بچه‌ها را ترغیب می‌کند که برای به‌دست آوردن ملزومات بازی (اسلحه و جان و...) به کدهای تقلب رو بیاورند. این نوجوانان گاهی روش‌هایی را توسعه می‌دهند که به کمک آن‌ها می‌توانند برچسب‌های نام به اصطلاح OG (سرنام Original Gamer) را از کاربران قدیمی‌تر بدزدند. مثلاً به‌جای Dictate27098 بتوانند از نام کاربری Dictate استفاده کنند. یکی از کسانی که با چنین پیش‌زمینه‌ای به کارهای هکری روی آورده است، Cosmo نام دارد. او از نخستین

> **این هک‌ها را چه کسانی انجام می‌دهند؟ چه کسی حاضر است با این جدیت هک کردن حساب کاربری شما را دنبال کند؟ پاسخ به این پرسش دو گروه را به ما معرفی می‌کند که هر دوی آن‌ها به یک اندازه خطرناک هستند: سندیکاهای بین‌المللی و نوجوانان بی‌کار!**

کسانی است که بسیاری از درخشان‌ترین روش‌های نفوذ اجتماعی یا socialing را کشف کرده است. از جمله این روش‌ها می‌توان به شیوه‌های نفوذ به آمازون و PayPal اشاره کرد. در ملاقاتی که چند ماه پیش در خانه مادربزرگش در کالیفرنیا با او داشتم، با غرور به من گفت: «من همین‌طوری به این کار روی آوردم.» در اوایل سال ۲۰۱۲ گروه Cosmo یعنی UGNazi به سایت‌های مختلفی از جمله Nasdaq و 4chan نفوذ کرد. این گروه اطلاعات شخصی مایکل بلومبرگ، اپرا وینفری و یک مقام دولتی را به دست آورد. زمانی که پلیس فدرال در ژوئن امسال این شخصیت مرموز را دستگیر کرد، متوجه شد که او تنها پانزده سال دارد. چند ماه بعد که ما با هم ملاقات داشتیم، من مجبور بودم رانندگی کنم!

دقیقاً به دلیل فعالیت‌های خستگی‌ناپذیر نوجوانانی مانند Dictate و Cosmo است که نمی‌توان سیستم‌های مبتنی‌بر گذرواژه را نجات داد. نمی‌توان تمام آن‌ها را دستگیر کرد و حتی اگر این کار انجام شود، دیگرانی در حال بزرگ شدن و پر کردن جای آن‌ها هستند. این معمای پیچیده را به این شکل ببینید: هر سیستم مبتنی‌بر گذرواژه که به اندازه کافی برای یک فرد شصت و پنج ساله راحت و قابل استفاده باشد، ظرف چند ثانیه توسط یک نوجوان چهارده ساله شکسته خواهد شد!

درست به همین دلیل بسیاری از راه‌های نجاتی که مردم فکر می‌کنند باعث نجات گذرواژه‌ها خواهند شد، محکوم به شکست هستند. به‌عنوان مثال، هکرها در سال ۲۰۱۱ به شرکت امنیتی RSA نفوذ کرده و داده‌هایی مرتبط با توکن‌های SecureID آن را به سرقت بردند. این توکن‌ها قرار بود ابزارهایی مقاوم در برابر هک باشند که کدهای ثانویه مورد نیاز برای لاگین با گذرواژه را فراهم کنند. شرکت RSA فاش نکرد که دقیقاً چه چیزهایی به سرقت رفته‌اند، اما بسیاری معتقدند که هکرها توانسته‌اند اطلاعات کافی برای شبیه‌سازی توکن‌ها و تولید کدهای ثانویه را به دست بیاورند. اگر آن‌ها به شناسه‌های اختصاصی (ID) دستگاه‌های توکن نیز دسترسی پیدا کرده باشند، قادر خواهند بود به امن‌ترین سیستم‌های حفاظتی در ایالات متحده نفوذ کنند.

از دید مشتریان نیز تبلیغات زیادی پیرامون سیستم اعتبارسنجی دو مرحله‌ای گوگل انجام گرفته است. سیستم کار به این شکل است که شما در ابتدا یک شماره تلفن به گوگل معرفی می‌کنید. پس از آن هرگاه که شما قصد لاگین کردن از یک آدرس IP ناشناس را داشته باشید، شرکت گوگل کد ثانویه‌ای را برای گوشی شما ارسال می‌کند. این همان فاکتور دوم اعتبارسنجی است. آیا این کار حساب کاربری شما را امن‌تر می‌کند؟ به یقین بله و

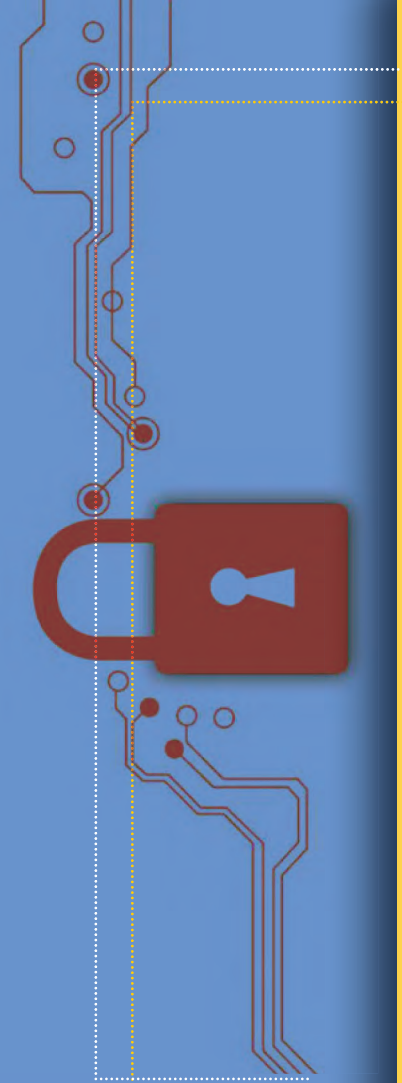
> **هکرهای روس زبان در سال ۲۰۱۱ به تنهایی حدود ۴/۵ میلیارد دلار از طریق جرائم سایبری به جیب زده‌اند. به همین دلیل اصلا عجیب نخواهد بود که چنین فعالیت‌هایی سازمان‌دهی شده، به یک صنعت تبدیل شوند و حتی به اعمال خشونت نیز کشیده شوند.**

دوران گذرواژه‌ها گذشته است. مسئله این است که ما هنوز متوجه این قضیه نشده‌ایم و هنوز هیچ کس نمی‌داند که چه چیزی جایگزین آن خواهد شد. آن‌چه می‌توانیم با یقین بگوییم این است که دسترسی به اطلاعات ما نمی‌تواند بیش از این به مجموعه‌ای از اطلاعات سری (یک رشته از کاراکترها، ۱۰ رشته از کاراکترها و حتی پاسخ ۵۰ پرسش امنیتی) که قرار است تنها ما بدانیم، متکی باشد. اینترنت جای اطلاعات سری نیست. همه ما تنها چند کلیک با فهمیدن همه چیز فاصله داریم.

اگر شما کاربر جی‌میل هستید باید آن را همین حالا فعال کنید. اما آیا فکر می‌کنید این شیوه دو قسمتی گذرواژه‌ها را از نابودی نجات خواهد داد؟ پس بگذارید داستان متیو پرینس را برای‌تان تعریف کنم.

تابستان گذشته، UGNazi تصمیم گرفت به سراغ متیو پرینس، مدیرعامل شرکت امنیت وبی CloudFlare برود. آن‌ها می‌خواستند به حساب کاربری او در Google Apps نفوذ کنند، اما او این حساب را با اعتبارسنجی دو مرحله‌ای گوگل محافظت می‌کرد. به همین دلیل هکرها حساب کاربری او در AT&T را هدف گرفتند! مشخص شد که AT&T از شماره تأمین اجتماعی به عنوان گذرواژه ورود به سیستم از طریق تلفن همراه استفاده می‌کند. این شماره ۹ رقمی (یا شاید ۴ رقم آخر آن) را به همراه نام، شماره تلفن و آدرس پرداخت صورت‌حساب، به سیستم بدهید و سیستم به‌سادگی به هر کسی اجازه می‌دهد یک شماره جدید را معرفی کند که تمام تماس‌های شماره موردنظر به آن forward می‌شوند. یافتن شماره تأمین اجتماعی هم اصلاً دشوار نیست، چرا که این شماره‌ها آزادانه از طریق وب و به صورت پایگاه‌های داده کامل فروخته می‌شوند.

هکرهای پرینس با استفاده از شماره تأمین اجتماعی، یک خط جدید را به حساب AT&T پرینس افزودند که همه تماس‌های شماره پرینس به آن forward می‌شد. پس از آن از گوگل تقاضای بازنشانی رمز عبور کردند. به این صورت زمانی که گوگل برای اطلاع دادن کد ثانویه با خط پرینس تماس گرفت، این تماس به طور مستقیم به شماره هکرها منتقل شد. به همین سادگی آن‌ها حساب کاربری او را دراختیار گرفتند. اعتبارسنجی دو مرحله‌ای تنها یک قدم اضافی و اندکی هزینه به هکرها تحمیل کرد. هرچه بیشتر با این سیستم از رده خارج کار کنیم، هرچه شماره‌های تأمین اجتماعی بیشتری به صورت پایگاه‌های داده دست به دست شوند، هرچه اطلاعات لاگین بیشتری لو برود و هرچه بیشتر ما اطلاعات زندگی‌مان را به‌صورت آنلاین



منتشر می‌کنیم، این هک‌ها ساده‌تر می‌شوند.

دوران گذرواژه‌ها گذشته است. مسئله این است که ما هنوز متوجه این قضیه نشده‌ایم و هنوز هیچ‌کس نمی‌داند که چه چیزی جایگزین آن خواهد شد. آن‌چه می‌توانیم با یقین بگوییم این است که دسترسی به اطلاعات ما نمی‌تواند بیش از این به مجموعه‌ای از اطلاعات سری (یک رشته از کاراکترها، ۱۰ رشته از کاراکترها و حتی پاسخ ۵۰ پرسش امنیتی) که قرار است تنها ما بدانیم، متکی باشد. اینترنت جای اطلاعات سری نیست. همه ما تنها چند کلیک با فهمیدن همه چیز فاصله داریم.

سیستم جدی در عوض باید به این موضوع متکی باشد که ما کیستیم و چه می‌کنیم. به کجا می‌رویم و در چه زمانی این کار را می‌کنیم، با خودمان چه داریم و وقتی به مقصد رسیدیم چه خواهیم کرد. هر حساب کاربری حیاتی ما باید به حداکثر تعداد ممکن از این نشانه‌ها متکی باشد؛ نه تنها دو مورد و به یقین نه یک عدد.

این نکته آخر از اهمیت زیادی برخوردار است. این همان چیزی است که ایده اعتبارسنجی دو مرحله‌ای گوگل را تا این حد درخشان می‌کند، البته آن‌ها این ایده را تا حد ممکن پیش نبرده‌اند. دو فاکتور حداقل تعداد ممکن است. به قضیه طور دیگری نگاه کنیم. زمانی که شما شخصی را در خیابان می‌بینید و فکر می‌کنید ممکن است از دوستان شما باشد، کارت شناسایی‌اش را نگاه نمی‌کنید. در عوض به مجموعه‌ای از نشانه‌ها توجه می‌کنید. شاید مدل موهایش را عوض کرده باشد، اما آیا این همان ژاکت اوست؟ آیا تن صدایش همان است؟ آیا جایی او را دیده‌اید که انتظار حضورش در آن می‌رود؟ اگر تعداد زیادی از مشخصات صحیح نباشند، شما به کارت شناسایی او اهمیتی نخواهید داد! حتی به‌عکس کارتش هم اعتماد نخواهید کرد، چراکه ممکن است جعلی باشد.

این شیوه در واقع جوهره سیستم‌های تشخیص هویت آنلاین آینده خواهد بود. این شیوه ممکن است شامل گذرواژه‌ها هم باشد، درست مانند کارت شناسایی در مثال قبلی. اما همان‌طور که ما افراد را از روی کارت شناسایی عکس‌دارشان نمی‌شناسیم، به‌یقین دیگر با یک سیستم مبتنی‌بر گذرواژه روبه‌رو نخواهیم بود. گذرواژه تنها یکی از توکن‌های مورد استفاده در یک سیستم چندوجهی خواهد بود. جرمی گرانت از دپارتمان تجارت، آن را یک اکوسیستم هویت می‌نامد.

اما نقش بیومتریک در این میان چیست؟ با دیدن فیلم‌های علمی‌تخیلی ممکن است بسیاری از ما به این فکر بیفتیم که شاید سیستم‌های تشخیص اثر انگشت یا تصویربرداری عنبیه وظیفه‌ای را که بر دوش گذرواژه‌ها بود، برعهده خواهند گرفت؛ سیستمی تک‌وجهی با اعتبارسنجی آنی. اما این شیوه‌ها دو مشکل اساسی دارند.

نخست این‌که زیرساختی که از آن‌ها پشتیبانی کند هنوز وجود ندارد. موضوع مرغ یا تخم‌مرغی که بسیاری از فناوری‌های نوین را تهدید می‌کند، اینجا هم خود را نشان می‌دهد. این سیستم‌ها گران و پر از ایراد هستند. به همین دلیل کسی از آن‌ها استفاده نمی‌کند و چون کسی از آن‌ها استفاده نمی‌کند، آن‌ها بهتر یا ارزان‌تر نخواهند شد.

مشکل مهم‌تر چیزی است که پاشنه آشیل تمام سیستم‌های تک فاکتوری است. اثر انگشت یا اسکن عنبیه تنها قطعه داده مورد نیاز است و بنابراین دزدیده خواهد شد. دیرک بالفانز (Dirk Balfanz) یکی از مهندسان نرم‌افزار گروه امنیت گوگل، اشاره می‌کند که کلیدها و کلمه‌های عبور می‌توانند تغییر داده شوند، اما عنبیه و اثر انگشت برای همیشه ثابت و بدون تغییر می‌مانند. او به شوخی می‌گوید: «وقتی اثر انگشت من از روی یک لیوان برداشته شود، برای من که بسیار سخت است انگشتم را عوض کنم.» اگرچه اسکن عنبیه در فیلم‌ها بسیار کارآمد ظاهر می‌شود، در دوران تصویرهای با کیفیت بالا استفاده از چهره، چشم یا حتی اثر انگشت به‌عنوان تنها فاکتور

دسترسی به حساب، به این معنا است که هر کس بتواند آن‌ها را کپی کند، می‌تواند به اطلاعات حساب‌ها هم دسترسی داشته باشد.

فکر می‌کنید زیاده‌روی کرده‌ایم؟ به هیچ‌وجه. کوین میتنیک، استاد مشهور مهندسی اجتماعی که پنج سال از عمرش را به‌واسطه فعالیت‌های هکری در زندان سپری کرده است، اکنون شرکت امنیتی خودش را رهبری می‌کند. کار شرکت او این است که به سیستم‌های شرکت‌های دیگر نفوذ می‌کند و سپس به صاحبان آن‌ها اطلاع می‌دهد که چگونه این کار را انجام داده است. در یکی از کارهای اخیرش، شرکت موردنظر از تشخیص هویت صوتی استفاده می‌کرد. برای وارد شدن به سیستم کاربر باید یک سری تصادفی از اعداد را بخواند. اگر هم اعداد و هم صدای کسی که آن‌ها را می‌خواند در سیستم وجود داشته باشد، عملیات لاگین انجام می‌شود. میتنیک به آن‌ها زنگ زد و مکالمه‌اش با آن‌ها را ضبط کرد. او مکالمه را طوری مدیریت کرد که مشتری مجبور شود کلمات صفر تا نه را به زبان آورد. او اعداد را از فایل صوتی استخراج کرد و با ترتیب مناسب برای سیستم تشخیص هویت پخش کرد و کار تمام بود.

گفتن این موضوعات به این معنی نبود که مشخصات بیومتریک نقشی اساسی در سیستم‌های امنیتی آینده بازی نخواهد کرد. دستگاه‌ها ممکن است برای کار کردن به یک مشخصه بیومتریک نیاز داشته باشند. سیستم‌های آندروئید پیش از این نیز از این شیوه‌ها استفاده می‌کردند و با خرید تازه اپل که شرکت بیومتریک موبایل AuthenTec را به تملک خود درآورد، بعید نیست که این شیوه‌ها به iOS هم راه پیدا کنند. آن‌وقت از این دستگاه‌ها نیز برای تشخیص هویت شما استفاده خواهد شد. کامپیوتر شما یا سایتی که می‌خواهید به آن وارد شوید، از این که شما یک دستگاه خاص را به‌همراه دارید مطمئن خواهد شد. در این صورت شما هم چیزی که هستید را ثابت کرده‌اید و هم چیزی را که به همراه دارید. اما اگر شما بخواهید از یک جای خیلی خاص مثلاً نیجریه یا لاگوس به حساب بانکی آنلاین‌تان وارد شوید، ممکن است لازم باشد که چند مرحله اضافی را طی کنید. ممکن است لازم شود که عبارت خاصی را در میکروفون گوشی بخوانید و هویت‌تان را با نمونه صوتی ذخیره شده تطبیق دهید. شاید دوربین گوشی عکسی از چهره شما تهیه کرده و برای سه نفر از دوستان‌تان ارسال کند تا پیش از ورود به سیستم آن‌ها هویت شما را تأیید کنند.

فراهم‌آورندگان خدمات داده‌ای در بسیاری موارد یاد خواهند گرفت که همانند شرکت‌های توزیع‌کننده کارت‌های اعتباری الگوهای رفتاری شما را اسکن کنند. با این کار آن‌ها نشانه‌های رفتار نامعمول را کشف کرده و فعالیت در حال انجام را در صورت شک به کلاه‌برداری متوقف می‌کنند. گرانت می‌گوید: «بسیاری از مواردی که در آینده خواهید دید نوعی از تحلیل‌های میزان ریسک است. فراهم‌کنندگان خدمات می‌توانند ببینند که شما از کجا به سیستم وارد شده‌اید و از چه سیستم‌عاملی استفاده می‌کنید.»

گوگل مدتی است که به همین سمت و سو می‌رود. این شرکت می‌خواهد از سیستم دو فاکتوری فراتر رود و اطلاعات هر لاگین را با لاگین‌های قبلی مقایسه کند تا ارتباط میان آن‌ها را در زمینه‌های موقعیت، دستگاه مورد استفاده و سایر نشانه‌هایی که شرکت اعلام نکرده است، بیابد. اگر مورد مشکوکی در این میان یافت شود، گوگل کاربر را مجبور می‌کند که به پرسش‌هایی درمورد حساب کاربری‌اش پاسخ دهد. اسمترز می‌گوید: «اگر کاربر نتواند به این پرسش‌ها پاسخ دهد، ما هشداری را برای صاحب حساب ارسال می‌کنیم که گذرواژه‌اش را تغییر دهد چراکه در معرض خطر لو رفتن قرار دارد.»

نکته دیگری که درباره سیستم‌های اعتبارسنجی آینده قطعی به‌نظر می‌رسد، این است که مجبور به پذیرفتن کدام مصالحه (راحتی یا حریم خصوصی) خواهیم بود. به‌یقین سیستم‌های چندفاکتوری اندکی از راحتی کار با سیستم کم می‌کنند، چراکه باید مراحل بیشتری را پشت سر بگذارید. اما قربانی اصلی حریم خصوصی شما خواهد بود. این سیستم بر موقعیت مکانی، عادت‌های شما، الگوهای صوتی و حتی دی ان ای شما متکی خواهد بود.

ما باید این مصالحه را بپذیریم و به‌احتمال زیاد این کار را خواهیم کرد. تنها راه پیش‌رو تأیید واقعی هویت است؛ به این صورت که حرکات و مشخصات فیزیکی ما از همه جهت و در همه زمینه‌ها ردگیری و ثبت شده و به هویت واقعی ما متصل شوند. ما از سیستم‌های کلاود دست نخواهیم کشید، چراکه آن‌ها را برای بازگرداندن عکس‌ها و ایمیل‌ها به هارددیسک‌مان احتیاج داریم. ما اکنون هم در ابرها زندگی می‌کنیم. پس به سیستمی احتیاج خواهیم داشت که از آن‌چه تاکنون در ابرها ذخیره کرده‌ایم استفاده کند: ما که هستیم، با که صحبت می‌کنیم، به کجا می‌رویم، در آنجا چه می‌کنیم، چه دستگاه‌هایی در اختیار داریم، چه شکلی هستیم، چه می‌گوییم و صدای‌مان چگونه است و حتی شاید این که چگونه فکر می‌کنیم.

این تغییر و تحول مستلزم سرمایه‌گذاری فراوان و تحمل سختی‌های زیاد است و همچنین مدافعان حریم خصوصی را بسیار نگران خواهد کرد. شاید وحشتناک به‌نظر برسد، اما گزینه دیگر آشوب و سرقت است و شکایت‌های بیشتری از دوستان خارجی که از آن‌ها سرقت شده است. زمانه عوض شده است. ما تا آنجا که توانسته‌ایم به یک سیستم شکست‌خورده اعتماد کرده‌ایم. نخستین گام این است که این حقیقت را بپذیریم. گام دوم این است که آن را اصلاح کنیم.

تنها راه پیش‌رو تأیید واقعی هویت است؛ به این صورت که حرکات و مشخصات فیزیکی ما از همه جهت و در همه زمینه‌ها ردگیری و ثبت شده و به هویت واقعی ما متصل شوند. ما اکنون هم در ابرها زندگی می‌کنیم. پس به سیستمی احتیاج خواهیم داشت که از آن‌چه تاکنون در ابرها ذخیره کرده‌ایم استفاده کند: ما که هستیم، با که صحبت می‌کنیم، به کجا می‌رویم، در آنجا چه می‌کنیم...