تا جهنم و باز گشت...

داستان هک شدن و بازیابی حساب‌های کاربری مت هونان

» منبع: وایرد » گردآوری و ترجمه: احمد شریف‌پور

در آن بعدازظهر جمعه که گوشی آی‌فون مت هونان (از ژورنالیست‌های سایت گیزمودو و مجله وایرد) هنگامی که با دخترش بازی می‌کرد خاموش شد، او هرگز فکر نمی‌کرد که این موضوع سرآغاز دردسری است که تا چندین هفته گریبان او را خواهد گرفت و به گفته خودش او را تا قعر جهنمی دیجیتال پیش خواهد برد. تمام حساب‌های کاربری او در اپل، گوگل، آمازون و توییتر در کمتر از ۲ ساعت مورد نفوذ واقع شده و تمام اطلاعات موجود روی سیستم‌های اپلی او پاک شدند. در پشت این هک بزرگ و در عین حال ساده، هیچ انگیزه مالی یا انتقام‌جویی وجود نداشت. در آن از ابزارهای معمول نظیر بدافزارها و حملات فیشینگ هم استفاده نشده بود. پاره‌ای از ضعف‌هایی که امکان چنین حمله‌ای را فراهم کردند، در بی‌توجهی هونان به ملاحظات امنیتی نهفته بود و بخشی دیگر به شرکت‌هایی مربوط می‌شد که با تمهیدات امنیتی ضعیف و متناقض، راه را برای چنین کاری باز گذاشته بودند. در این نوشتار خواهیم دید که چگونه ضعف در سیستم‌های امنیتی آمازون و اپل و کم توجهی یک کاربر (حتی حرفه‌ای) می‌تواند کل زندگی دیجیتال او را به تلی از ویرانی تبدیل کند.

زندگی دیجیتال ما روز به روز بیشتر به ابرها و محاسبات ابری وابسته می‌شود. اپل به شدت اصرار دارد که کاربرانش را تقریباً برای برآورده کردن تمام نیازهای ذخیره‌سازی، پشتیبان‌گیری و همسان‌سازی به استفاده از iCloud وادار کند. سیستم‌عامل گوگل از بدو پیدایش ریشه در ابرها داشته است و ویندوز تازه مایکروسافت هم ابری‌ترین سیستم‌عاملی است که تاکنون توسط این شرکت عرضه شده است. عجین شدن زندگی ما با محاسبات و ذخیره‌سازی ابری سرآغاز دورانی است که در آن تعیین هویت و تأمین مجوز دسترسی به اطلاعات و حساب‌های کاربری، دیگر با استفاده از گذرواژه‌ها و راهکارهای معمول دسکتاپ امن نخواهد بود. اگر مت هونان سیستم امنیتی دو فاکتوری جی‌میل را فعال کرده بود، یا اگر علاوه‌بر پشتیبان‌گیری روی سرورهای ابری اپل، نسخه‌هایی محلی از داده‌هایش در اختیار داشت، شاید لازم نبود برای به‌دست آوردن دوباره تمام عکس‌هایی که از زمان تولد تا یک سالگی دخترش گرفته بود، دو هفته تلاش کند و هزینه‌ای در حدود ۱۷۰۰ دلار بپردازد.

آغاز سفر

داستان از آنجا شروع می‌شود که آی‌فون مت در ساعت ۵ عصر روز جمعه، هنگامی که او مشغول بازی با دختر یک ساله‌اش بود، خاموش می‌شود. او که در انتظار یک تماس است، با تصور این‌که خاموش شدن گوشی نتیجه یک باگ نرم‌افزاری یا سخت‌افزاری است، گوشی را دوباره روشن می‌کند. اما در کمال تعجب با صفحه راه‌اندازی اولیه گوشی مواجه می‌شود. قضیه هنوز چندان جدی نیست، چراکه او می‌تواند اطلاعاتش را به کمک نسخه پشتیبانی که دیروز روی مک‌بوک‌اش ذخیره کرده است، بازیابی کند. با روشن کردن مک‌بوک، مت با پیغامی مبنی بر عدم امکان اتصال به حساب کاربری گوگل روبه‌رو می‌شود که آن را هم چندان جدی نمی‌گیرد. درنهایت، آن‌چه باعث بیدار شدن مت می‌شود، کدی چهار حرفی است که باید برای دسترسی به مک‌بوک‌اش وارد کند. کدی که مت حتی از وجود آن خبر ندارد. این شوک، او را وادار می کند که تمام تجهیزات کامپیوتری از مودم و روتر و کامپیوترهایش را خاموش کرده و از تلفن همسرش با پشتیبانی شرکت اپل تماس بگیرد و یک ساعت و نیم بعدی را صرف فهمیدن عمق فاجعه‌ای کند که گریبانش را گرفته است.

پشتیبانی

آن تماس، نخستین تماسی نبود که برای بازیابی دسترسی به حساب کاربری مت هونان با بخش پشتیبانی اپل گرفته می‌شد. درست نیم ساعت پیش از مت، یعنی در ساعت ۴ و ۳۳ دقیقه شخص دیگری با اپل تماس گرفته و خود را مت هونان معرفی کرده بود. او از عدم امکان دسترسی به حسابی که در سایت Me.com داشت، شکایت کرده بود. با این‌که او نتوانسته بود پرسش‌های امنیتی تنظیم شده برای حساب کاربری مت هونان را پاسخ دهد، با فراهم کردن دو قطعه اطلاعاتی که به‌سادگی می‌توان از اینترنت جمع‌آوری کرد، به یک گذرواژه موقت و امکان دسترسی به حساب مت دست‌یافته بود.

در ساعت ۴:۵۰ گذرواژه حساب me.com عوض شده بود. در ۴:۵۲ گذرواژه حساب کاربری گوگل نیز عوض شده بود. ساعت ۵:۰۲ حساب کاربری توییتر هم از دست رفته بود. علاوه‌بر همه این‌ها، با فعال شدن امکان Find My . . . حساب کاربری اپل در ساعت ۵:۰۰ کل اطلاعات گوشی آی‌فون مت، در ساعت ۵:۰۱ دقیقه همه اطلاعات آی‌پد و در ساعت ۵:۰۵ دقیقه همه اطلاعات مک‌بوک او از راه دور پاک شدند. در همین دقایق، جی‌میل هم دیگر نابود شده و آرشیو ۸ ساله ایمیل‌های مت هونان از دست رفته بود. مت در ساعت ۵:۱۰ با اپل تماس گرفته بود و تقریباً دو دقیقه بعد از آن بود که هکر رسماً در اکانت توییتر مت اعلام وجود کرد!

جالب اینجا بود که کارمندان پشتیبانی اپل تا زمانی که به صورت مستقیم مورد پرسش قرار نگرفته بودند، از تماس قبلی (مربوط به هکر) چیزی به مت نگفته بودند! دلیل این موضوع شاید این بود که در تمام مدت یک و نیم ساعتی که مت نمی‌توانست به پرسش‌های امنیتی حساب کاربری‌اش جواب بدهد، کارمند اپل که نام هونان را اشتباه شنیده بود، در حال بازیابی امکان دسترسی به حساب فردی به نام هرمان بود!

با از دسترس خارج شدن و پاک شدن تمام اطلاعات مت روی سایت Me.com و جی‌میل، بازپس‌گیری این حساب‌های از دست رفته تقریباً دیگر غیرممکن بود. هدف استفاده از اطلاعات حساب‌های کاربری مت نبود، انگیزه مالی هم در کار نبود، حتی هدف نابود کردن کل آرشیو عکس‌های مت هم نبود. تنها نکته این بود که هکری ۱۹ ساله از نام کاربری سه‌حرفی مت هونان در توییتر خوشش آمده بود و تصمیم گرفته بود آن را در اختیار بگیرد و از آن برای انتشار پیام‌های نژادپرستانه و دیگر محتواهای خلاف عرف عمومی استفاده کند. پاک شدن اطلاعات شخصی و آرشیو ایمیل‌ها و... همه قربانی‌های جانبی داستان بودند و تنها به این دلیل انجام شده بودند که امکان بازپس‌گیری حساب‌های کاربری را از مت سلب کنند. برای تمام این کارها تنها به دست آوردن آدرس پستی مت و چهار رقم آخر شماره کارت اعتباری او کافی بود!

تا پایان آن هفته، کارمندان اپل دو بار تأکید کرده بودند که تنها اطلاعات لازم برای به‌دست آوردن امکان دسترسی به حساب‌های کاربری AppleID در اختیار داشتن آدرس ایمیل، آدرس پستی و چهار رقم آخر شماره کارت اعتباری متصل به آن حساب است و این به معنای فاجعه‌ای تمام عیار است.

شکل ۱ با استفاده از ضعف‌های امنیتی موجود در فرآیندهای مورد استفاده در آمازون و اپل، هکرها توانستند کنترل حساب‌های کاربری و دستگاه‌های مت هونان را در اختیار بگیرند.

مت هونان نباشید!

هونان اعتراف کرده است که بیشتر گناه این هک، به گردن اوست که ملاحظات امنیتی را چندان جدی نگرفته است. ۹ نکته کلیدی که در ادامه آورده شده است، به شما کمک می‌کنند که از بروز چنین اتفاقی برای خودتان جلوگیری کنید.

● از اعتبارسنجی‌های دوفاکتوری برای جی‌میل و سایر حساب‌ها استفاده کنید

با فعال‌کردن این سیستم، کدهای ثانویه اعتبارسنجی ازطریق تلفن به دست شما خواهد رسید. این قابلیت تماس تلفنی که حتی با شماره تلفن‌های کشور ما نیز امکان‌پذیر است، به رایگان در اختیار شما قرار می‌گیرد. علاوه براین، می‌توانید برنامکی را هم برای تولید این کدها از سایت گوگل دریافت کرده و با نصب آن روی گوشی هوشمندتان، کدهای ثانویه را خودتان تولید کنید. علاوه بر گوگل، تعدادی دیگر از شرکت‌ها نظیر آمازون نیز به تازگی از این سیستم استفاده می‌کنند.

● هنگام اتصال به وای‌فای‌های عمومی از VPN یا SSL استفاده کنید

هنگامی که با استفاده از شبکه‌های بی‌سیم یا سیستم‌های عمومی، قصد ورود به حساب‌های کاربری‌تان را دارید، حتماً از https یا از VPN استفاده کنید. این کار شنود اطلاعات ردوبدل شده میان دستگاه شما و شبکه را برای دیگران دشوار یا ناممکن می‌سازد.

● از گذرواژه‌های منحصر به فرد و متفاوت استفاده کنید

هیچ‌گاه از یک گذرواژه یکسان برای چندین حساب کاربری استفاده نکنید. برای هر یک از حساب‌ها گذرواژه‌ای جداگانه تعریف کنید و هر چند ماه یک بار آن‌ها را تعویض کنید.

● برای حساب‌های کاربری مهم از گذرواژه‌های پیچیده استفاده کنید

اگرچه حساب‌های کاربری مت به واسطه ضعف گذرواژه‌ها مورد نفوذ قرار نگرفتند، اما بدانید که گذرواژه‌های شما به عنوان بخشی از راهکار حفظ امنیت، باید از ۸ کاراکتر بیشتر بوده و شامل حروف، اعداد و کاراکترهای خاص باشند.

برنامه‌های فراوانی، برای تولید، نگه‌داری و مدیریت این گذرواژه‌ها موجود است که می‌توانید از آن‌ها استفاده کنید.

هرچند اپل بعدها اعلام کرده بود که کارمندان بخش پشتیبانی، دستورالعمل‌های داخلی مربوط به بازیابی حساب‌های کاربری را به درستی انجام نداده‌اند.

درنهایت و پس از تماس مستقیم مجله وایرد با اپل و پرسش درمورد تمهیدات امنیتی این شرکت، ناتالی کریس (Natalie Kerris) سخنگوی اپل گفته بود: «اپل حریم‌شخصی کاربرانش را جدی می‌گیرد و پیش از بازنشانی گذرواژه یک حساب‌کاربری AppleID از روش‌های گوناگون تشخیص هویت استفاده می‌کند. در این مورد خاص، اطلاعات مشتری ما توسط کسی مورد سرقت قرار گرفته است که توانسته بوده به اطلاعات شخصی آن مشتری دسترسی پیدا کند. علاوه بر این، ما دریافته‌ایم که در این روند، سیاست‌های داخلی ما تمام و کمال رعایت نشده‌اند. ما در حال بازبینی تمام فرآیندهای بازنشانی گذرواژه حساب‌هایمان هستیم تا اطمینان حاصل کنیم که اطلاعات مشتریان‌مان در امان است.»

داستان یک هک

شب آن روز جمعه، تمام حساب‌های کاربری از دست رفته بود. تلفن هم در وضعیت راه‌اندازی اولیه قرار داشت. مت تنها توانسته بود یک حساب کاربری جدید در توییتر باز کند و از حساب کاربری که در سایت تامبلر (thumblr.com) داشت، برای انتشار داستان این هک استفاده کند. دوستانش در کامنت‌ها احتمال استفاده از جاسوس‌افزارها را مطرح کرده بودند و او در تمام زندگی‌اش فکر می‌کرد که گذرواژه ۷ حرفی با ترکیبی از اعداد و ارقام مختلف، روشی مطمئن برای امن نگه‌داشتن حساب‌های کاربری است!

شکل ۲ آن‌چه آمازون آن‌قدر بی‌اهمیت می‌شمارد که به صورت متنی روی وب نمایش می‌دهد، از دید اپل آن‌قدر مهم است که آن را به‌عنوان ابزار هویت‌سنجی مورد استفاده قرارمی‌دهد.

در همین زمان، هکر که خود را فوبیا (Phobia) معرفی کرده بود، با مت تماس می‌گیرد. این تماس ابتدا از طریق توییتر انجام می‌شود و سپس به‌صورت چت و تماس‌های ایمیلی ادامه می‌یابد. با جزئیاتی که فوبیا آشکار می‌کند، مت مطمئن می‌شود که او واقعاً همان هکری است که مسبب تمام این دردسرهاست. فوبیا در همان ابتدای صحبتش تأکید می‌کند که «من گذرواژه تو را حدس نزدم. از تلاش کور (Brute Force) هم استفاده نکردم!» و هدفش را فقط در اختیار گرفتن حساب کاربری سه حرفی مت اعلام می‌کند و در ضمن ادعا می‌کند که به هر آدرس ایمیلی در اپل می‌توان نفوذ کرد. اندکی بعد و زمانی که مت به هکر اطمینان می‌دهد که او را مورد تعقیب قضایی قرار نخواهد داد، فوبیا داستان این هک را با تمام جزئیات برای او بازگو می‌کند.

داستان از آنجا آغاز می‌شود که هکر علاقه‌مند به حساب‌کاربری سه‌حرفی مت در توییتر، با بررسی دقیق این حساب به آدرس سایت شخصی مت پی می‌برد. با مراجعه به این سایت، فوبیا می‌تواند به آدرس ایمیل مت روی جی‌میل نیز دست یابد. فوبیا که حدس می‌زند همین آدرس جیمیل برای باز کردن حساب کاربری توییتر به کار رفته باشد، مستقیماً به صفحه بازیابی رمز عبور گوگل می‌رود. در این صفحه با این‌که گوگل آدرس ایمیل بازیابی گذرواژه را به صورت کامل نشان نمی‌دهد و بخش‌هایی از آن را با کاراکتر ستاره جایگزین می‌کند، اما فوبیا از روی حروفی که نشان داده شده‌اند و تعداد آن‌ها می‌تواند به آدرس ایمیل مت روی سایت Me.com نیز پی ببرد. یکسان بودن شناسه کاربری مت در گوگل و اپل این کار را به شدت برای فوبیا ساده می‌کند. اگر مت از ایمیل دیگری به عنوان پشتیبان استفاده کرده بود یا اعتبارسنجی دوفاکتوری گوگل را فعال کرده بود، فرآیند هک در همین جا با شکست روبه‌رو می‌شد. به هر حال با مشخص شدن آدرس ایمیل مرتبط با AppleID مت هونان، فوبیا متوجه می‌شود که برای دسترسی به این AppleID باید آدرس پستی و چهار رقم آخر شماره کارت اعتباری مت هونان را بیابد.

یافتن مورد اول یعنی آدرس پستی کار به نسبت ساده‌ای است. فوبیا با استفاده از سرویس WhoIs که برای یافتن صاحبان دامنه‌های ثبت شده به کار می‌رود و با جست‌وجوی آدرس سایت شخصی مت هونان، به‌سادگی به آدرس پستی او دست می‌یابد. حتی اگر کسی وب‌سایت شخصی هم نداشته باشد، با استفاده از اطلاعات موجود در سرویس‌هایی نظیر Spokeo، WhitePage یا PeopleSmart می‌توان به آدرس شخصی او دست یافت. اما یافتن شماره کارت اعتباری هرچند سختی چندانی ندارد، مستلزم طی کردن مراحل بیشتری است.

● حساب‌هایتان را به هم متصل نکنید

هکرهایی که توییتر هونان را هک کردند، می‌توانستند به حساب توییتر سایت گیزمودو هم نفوذ کنند، چرا که حساب کاربری مت (که قبلا با گیزمودو کار می‌کرد) به حساب توییتر گیزمودو هم لینک شده بود. تا حد ممکن از لینک کردن حساب‌ها به یکدیگر به خصوص از لینک کردن زنجیره‌ای آن‌ها پرهیز کنید.

● در انتخاب و پاسخ دادن به پرسش‌های امنیتی خلاقانه عمل کنید

از تنظیم پرسش‌های معمولی مانند مدل ماشین، نام مادربزرگ و نخستین مدرسه‌ای که رفته‌اید، به‌عنوان پرسش‌های امنیتی پشتیبان حساب کاربری‌تان خودداری کنید. یا در صورتی که امکان انتخاب ندارید، در پاسخ‌هایی که می‌دهید خلاقیت به خرج دهید. مثلاً پاسخ‌های دو پرسش را با هم عوض کنید یا در متن پاسخ از کاراکترهای خاص استفاده کنید.

● از سیستم‌هایتان پشتیبان بگیرید

بیشترین ناراحتی مت در جریان این هک، از دست رفتن عکس‌هایی بود که در یک سالی که از تولد دخترش می‌گذشت، گرفته بود. قیمت ابزارهای ذخیره‌سازی، این روزها به حدی پایین است که دیگر هیچ عذر و بهانه‌ای برای پشتیبان نگرفتن از داده‌های حساس‌تان پذیرفتنی نیست.

● دستگاه‌هایتان را رمزنگاری کرده و با گذرواژه محافظت کنید

برای جلوگیری از دسترسی دیگران به داده‌هایی که روی دستگاه‌هایتان دارید، آن‌ها را رمزگذاری کنید و در عین حال با گذرواژه‌های قدرتمند از آن‌ها محافظت کنید.

● از کارت‌های اعتباری تک منظوره استفاده کنید

تنها چهار رقم از شماره‌های کارت اعتباری مت، امکان دسترسی هکر به حساب اپل او را فراهم آورد. گرچه اپل نباید از چهار رقم آخر شماره کارت اعتباری برای تشخیص هویت استفاده کند، مت می‌توانست با استفاده از کارت‌های تک منظوره یا قابل دورانداختن در حساب کاربری آمازون، تعداد حساب‌هایی که شماره کارت واقعی او را دارند، محدود کند. با در اختیار داشتن شماره کارت واقعی شما، هیچ حایلی میان هکرها و پولی که در بانک دارید، وجود نخواهد داشت!

همکاری که از این‌جا به بعد در کنار فوبیا خواهد بود، با بخش پشتیبانی آمازون تماس می‌گیرد و اعلام می‌کند که قصد اضافه کردن یک کارت اعتباری جدید به حساب مت هونان را دارد. تنها چیزی که در این مرحله به آن احتیاج دارد نام صاحب حساب، آدرس ایمیل و آدرس پستی متصل به حساب است. این کار با موفقیت به انجام می‌رسد و کارت جدیدی به حساب کاربری مت در آمازون افزوده می‌شود. هکر ما اندکی بعد دوباره با آمازون تماس گرفته و اعلام می‌کند که امکان ورود به حسابش را ندارد و تقاضای اضافه کردن یک آدرس ایمیل جدید به حساب کاربری را مطرح می‌کند. به‌دلیل در اختیار داشتن نام کاربری، آدرس پستی و شماره کارت اعتباری (کارت جدیدی که به‌تازگی به حساب مت افزوده شده است)، آمازون امکان افزودن یک ایمیل جدید را نیز برای این حساب کاربری فراهم می‌کند. فوبیا و همکارش پس از این مرحله به سادگی به سایت آمازون برگشته و فرم بازنشانی گذرواژه را با استفاده از آدرس ایمیل جدیدی که خودشان به حساب کاربری مت در آمازون افزوده‌اند، پر کرده و از این طریق می‌توانند گذرواژه حساب آمازون را تغییر داده و کنترل این حساب را در دست بگیرند. پس از ورود به حساب کاربری مت در آمازون، آن‌ها می‌توانند اطلاعات مربوط به کارت اعتباری اصلی که به این حساب متصل بوده است را نیز بیابند. آمازون تمام ارقام شماره کارت‌های اعتباری را به صورت کامل نشان نمی‌دهد، بلکه تنها چهار رقم آخر را به نمایش در می‌آورد که همین چهار رقم برای مقصد بعدی هکرها یعنی نفوذ به AppleID مت کافی است. به عبارت دیگر، اطلاعاتی که آمازون آن‌ها را آنقدر بی‌اهمیت می‌داند که به صورت متنی و ساده در وب قابل دسترس است، از دید اپل آن‌قدر ایمن و خصوصی هستند که برای تأیید هویت و در اختیار گرفتن حساب‌های AppleID مورد استفاده قرار می‌گیرند. این فرآیند به قدری ساده و سرراست به انجام می‌رسد که به گفته مت اعضای وایرد توانسته‌اند ظرف چند دقیقه دوبار این کار را روی حساب‌هایشان به‌انجام برسانند!

در مرحله بعدی با تماس با بخش پشتیبانی اپل و اعلام آدرس پستی و چهار رقم آخر شماره کارت اعتباری مت، فوبیا و همکارش می‌توانند به حساب AppleID او دست یابند. از آنجا و با فعال کردن قابلیت ... Find My همکار فوبیا اقدام به نابود کردن داده‌های ذخیره شده در تلفن همراه، آی‌پد و مک‌بوک مت می‌کند. البته فوبیا گفته است که این کار توسط همکارش و تنها برای جلوگیری از بازپس‌گیری کنترل حساب کاربری توسط مت انجام شده است و او از آن بی‌اطلاع بوده است. او در جایی می‌گوید که اگر از پاک شدن اطلاعات و اهمیت عکس‌های کودک مت خبر می‌داشت، به یقین این فرآیند را متوقف می‌کرد.

به هر حال، پس از در اختیار گرفتن حساب AppleID، فوبیا به سراغ جی‌میل رفته و با پر کردن فرم بازنشانی گذرواژه، لینک انجام این کار را روی AppleID دریافت می‌کند. پس از در اختیار گرفتن جی‌میل و پاک کردن آرشیو هشت ساله ایمیل مت، همین روند بازنشانی گذرواژه روی توییتر نیز اجرا شده و در نهایت فوبیا به آن حساب کاربری سه حرفی توییتر دست یافته و شروع به انتشار مزخرفات نژادپرستانه می‌کند.

در جست‌وجوی مقصر

البته اوضاع می‌توانست از این هم بدتر باشد. اگر انگیزه‌های مالی در پس این هک نهفته بود، فوبیا می‌توانست از طریق این حساب‌های هک شده به اطلاعات مالی و بانکی مت دست یابد. از سوی دیگر چندین سال سابقه در زمینه ژورنالیسم در حوزه IT باعث شده است که مت اطلاعات تماس تعداد زیادی از افراد بانفوذ این حوزه را نیز در بخش مخاطبان ایمیل‌هایش داشته باشد که هکرها می‌توانستند برای طراحی حمله‌های فیشینگ و مهندسی اجتماعی به آن‌ها نیز از ایمیل‌های مت استفاده کنند. اما مت بیشتر تقصیرها را متوجه خودش می‌داند. اگر برای تمام حساب‌های کاربری‌اش نام‌های یکسانی در نظر نگرفته بود، اگر از یک ایمیل خاص و خصوصی جداگانه تنها برای بازیابی رمزهای عبور حساب‌هایش استفاده کرده بود، اگر حساب‌های کاربری‌اش به صورت زنجیری به هم متصل نبودند، اگر از اعتبارسنجی دومرحله‌ای گوگل استفاده کرده بود و درنهایت اگر سرویس ... Find My با

شکل ۳ عکسی از مت و دخترش درست بعداز تولد که تنها روی هارددیسک مک‌بوک او ذخیره شده بود.

آن پیاده‌سازی مبتنی‌بر PIN را حداقل برای لپ‌تاپش (دستگاهی که به سختی ممکن است گم شده یا در جایی فراموش شود) فعال نکرده بود، شاید اوضاع تا این حد وخیم نمی‌شد.

همان‌طور که پیش‌تر هم گفتیم، امنیت در دوره حساب‌های متعدد و رایانش ابری دیگر به ملاحظاتی فراتر از گذرواژه‌های پیچیده نیاز دارد. آن‌چه در کادر «مت هونان نباشید!» می‌بینید، خلاصه پیشنهادهایی است که پس از اتفاق افتادن این وقایع و برای پیش‌گیری از روی دادن دوباره آن، به صورت مقاله‌ای در دنباله مطالب مربوط به هک شدن حساب‌های کاربری مت هونان در وایرد منتشر شده است.

بازگشت از جهنم

گرچه تمام قضایایی که باعث هک شدن حساب‌های کاربری مت شد، به واسطه سرویس‌های ابری شرکت‌های مختلف بود، کلاود همان‌گونه که فرشته عذاب مت شده بود، تنها راه نجات او نیز بود. تلاش او برای نجات از این مخمصه درست بعد از گفت‌وگوی تلفنی با مرکز پشتیبانی اپل آغاز شده بود!

مت که در ابتدا فکر می‌کرد هکرها به شبکه بی‌سیم خانه‌اش نفوذ کرده‌اند، تمام تجهیزات اینترنتی را خاموش و اتصالش با دنیای بیرون را قطع کرده بود. اما برای بازیابی دسترسی به حساب‌هایش باید آنلاین می‌شد و به همین دلیل به خانه همسایه رفته و از کامپیوتر و اتصال اینترنتی آن‌ها استفاده کرد. پس از بازنشانی گذرواژه حساب کاربری iCloud و AppleID مت بازیابی اطلاعات داده‌هایش را از روی پشتیبان‌هایی که روی iCloud گرفته بود، آغاز کرد. بازگرداندن اطلاعات آیفون حدود ۷ ساعت زمان برد و زمان لازم برای بازگرداندن اطلاعات آی‌پد بیش از آن بود. در تمام این مدت، آن‌ها قابل استفاده نبودند. مت در همین زمان با بانک تماس گرفته و کل اطلاعات دسترسی به حساب‌های بانکی‌اش را تغییر داده بود. اکنون او که دیگر احساس امنیت نسبی داشت، دوباره تجهیزات خانگی‌اش را به راه انداخته و شروع به کنترل سایر حساب‌هایش کرد. اما مسئله این بود که او هیچ یک از گذرواژه‌هایش را به خاطر نداشت. او که به استفاده ازنرم‌افزار 1Password معتاد بود، تمام گذرواژه‌هایش را روی دستگاه‌های اپلی‌اش ذخیره کرده بود که به آن‌ها هم دسترسی نداشت.

۵ ساعت بعد از هک و در حالی که هنوز به هیچ حسابی دسترسی نداشت، مت به خاطر آورد که با کامپیوتر همسرش به DropBox، جایی که او اطلاعات تمام گذرواژه‌هایش و نسخه پشتیبانی از 1Password را نگه‌داری می‌کرد، متصل شده است. با آمیزه‌ای از بیم و امید به سراغ لپ‌تاپ همسرش رفت و در کمال ناباوری توانست به DropBox وارد شده و تمام گذرواژه‌هایش را بازیابی کند. با استفاده از آن گذرواژه‌ها به سایر حساب‌هایی که هک

شکل ۴ تیم Drive Savers که بازیابی اطلاعات مک‌بوک مت را برعهده گرفتند.

نشده بودند، وارد شد و تنظیمات امنیتی آن‌ها را تغییر داد. پس از آن در پستی که در تامبلر منتشر کرد، به شرح آن‌چه تاکنون رخ داده بود، پرداخت. مت باتوجه به سابقه طولانی در ژورنالیسم IT، دوستان فراوانی در میان مهندسان گوگل و توییتر داشت. مهم‌ترین گامی که این دوستان در جهت کمک به بازیابی اطلاعات او برداشتند، راهنمایی او به مسیرهای درست اداری برای بازیابی حساب‌های کاربری گوگل و توییتر بود.

شخص دیگری که این پست تامبلر را دیده و از این‌که مت فکر می‌کرد گذرواژه حساب کاربری‌اش با BruteForce لو رفته است به خشم آمده بود، خود شخص هکر بود! و این آغاز رابطه مت با هکر حساب‌هایش و مبنای تمام چیزهایی بود که تا این‌جا از نظر گذراندید.

با مراجعه به گوگل و پر کردن فرم‌های مربوطه و پاسخ دادن به پرسش‌هایی که به احتمال زیاد تنها خود او جواب آن‌ها را می‌دانست، او توانست تا پیش از ظهر روز شنبه، دوباره کنترل حساب کاربری جی‌میل‌اش را پس بگیرد. پس از بازپس‌گیری این حساب او نخست تنظیمات ایمیلش را کنترل می‌کند تا مبادا هکرها آن را برای ارسال خودکار نسخه‌ای از ایمیل‌های ورودی به آدرسی دیگر تنظیم کرده باشند! در بعد از ظهر روز شنبه او توانست کنترل حساب توییتر خود را نیز پس بگیرد. پس از تمام این مقدمات اولیه، زمان پرداختن به بزرگ‌ترین و مهم‌ترین دغدغه مت، یعنی بازگرداندن تصاویر نوزادی دخترش بود. در ظهر یک شنبه او به یکی از فروشگاه‌های اپل مراجعه کرد و به سراغ یکی از «نابغه‌های اپل» رفت. این کارمند اپل به او توضیح داد که آن‌ها نمی‌توانند اطلاعات از دست رفته را باز گردانند، اما می‌توانند روند پاک شدن اطلاعات را متوقف کنند. یافتن آن کد چهار حرفی PIN تا بعدازظهر روز دوشنبه به طول انجامید! آن‌ها روند پاک شدن داده را متوقف کرده بودند و مت اکنون باید به دنبال بازیابی اطلاعات از هارد دیسک مک‌بوک‌اش می‌رفت.

با توجه به استفاده از درایوهای SSD در مک‌بوک او، بازیابی داده چندان هم ساده نبود. شرکتی که در این جا به کمک مت آمد، DriveSavers بود. جمعه بعد، یعنی درست یک هفته بعد از هک، مت مک‌بوک‌اش را برای این شرکت ارسال کرد.

آرامش در خانه

کارکنان این شرکت ابتدا برای جلوگیری از وارد شدن صدمه به این هارددیسک از آن یک image تهیه کرده و کار را بر روی آن شروع کردند. در ۶ گیگابایت اول تنها یک نسخه سالم از Mac OS X یافته شد و بعد تا مدتی تنها صفرها بودند که بر صفحه نمایش ظاهر می‌شدند. اما درنهایت مت توانست دوشنبه هفته بعد اطلاعاتی را که DriveSavers توانسته بود بازیابی کند، روی یک هارد اکسترنال تحویل بگیرد. فایل‌هایی که بدون پوشه‌ها و تنها با توجه به نوع فایل و تاریخ ایجاد در این هارد ذخیره شده بودند، دوباره شادی و امید را به زندگی دیجیتال مت بازگرداندند. تمام آن خاطرات، عکس‌های کودکی، عکس‌های خویشاوندانی که دیگر در این دنیا نبودند، همه و همه هر چند بدون هیچ نظم و ترتیبی، بازگشته بودند. او همه اطلاعاتش را پس نگرفت. DriveSavers تنها چیزهایی را بازیابی کرده بود که مت به راستی آن‌ها را می‌خواست و برای همین مقدار نیز هزینه‌ای برابر ۱۶۹۰ دلار دریافت کرده بود! داستان هک شدن مت پایان به نسبت خوشی داشت، اما همیشه این گونه نخواهد بود و بهایی که برخی از ما در صورت از دست رفتن اطلاعات‌مان باید بپردازیم، بسیار بیش از دو هفته زمان و ۱۷۰۰ دلار پول خواهد بود. نگاهی دوباره به کادر«مت هونان نباشید!» به هیچ وجه خالی از فایده نخواهد بود!