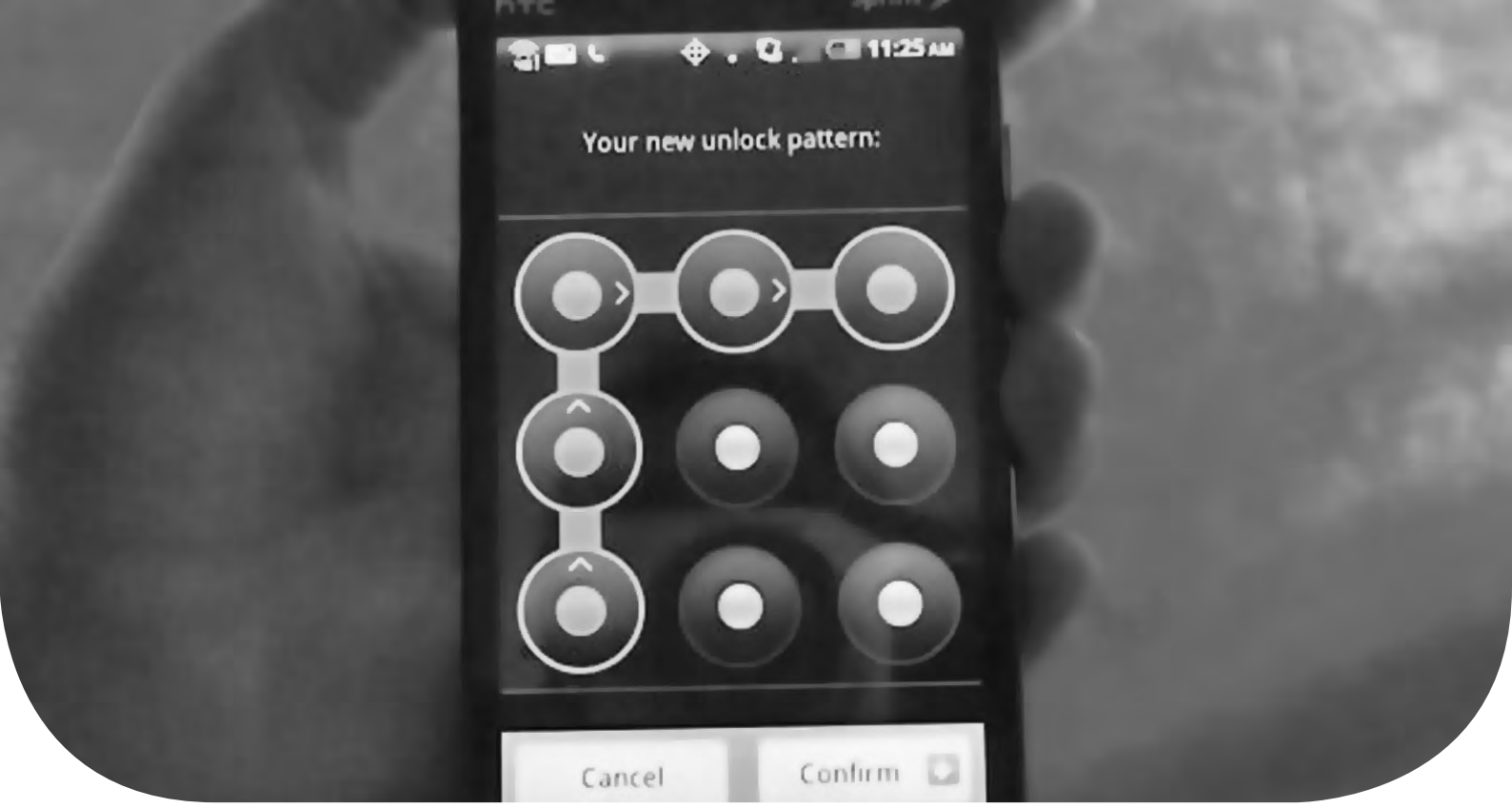

امنیت؛ ۲۰۱۲

به ۲۰۱۲ خوش آمدید! سالی که برخی پیش‌بینی کرده‌اند دنیا به پایان خواهد رسید! اما درباره این پیش‌بینی نیز مانند بسیاری موارد مشابه دیگر حرف و حدیث‌های بسیاری وجود دارد. تعیین درست و نادرست بودن پیش‌بینی‌ها به‌خصوص آنچه به ما و دنیای IT مربوط می‌شود، کاری بسیار دشوار است و بسته به این که کدام جامعه آماری را در نظر بگیرید و به آمار چه مؤسسه‌ای اعتماد کنید، یک پیش‌بینی برای شما کاملاً درست و برای دیگری کاملا نادرست جلوه خواهد کرد. در ادامه به بررسی خلاصه اتفاقات و پیش‌بینی‌های سال ۲۰۱۱ پرداخته و ملاحظات امنیتی را که باید برای سال جدید مدنظر قرار داد، بررسی می‌کنیم.

در میان پیش‌بینی‌هایی که برای سال ۲۰۱۱ انجام شدند، برخی به قطع یقین به حقیقت پیوستند. به عنوان نمونه می‌توان به افزایش شدید دستگاه‌های قابل حمل متصل به اینترنت (به پیش‌بینی Gens et al)، افزایش تقاضا برای خدمات ابری کاربرپسندتر (Gens et al)، افزایش ترافیک ویدیوهای زنده و غیر زنده در وب (Blue Coat System)، ثابت ماندن میزان ویدیوهای 3D و عدم افزایش آن‌ها (Blue Coat System)، و افزایش حساسیت درباره مسائل مرتبط با حریم خصوصی کاربران (William Winsborough) اشاره کرد.

دیگر پیش‌بینی مهمی که به نظر می‌رسد درست از آب درآمده باشد، افزایش فعالیت‌های هکتیویسم (Hacktivism) یا فعالیت‌های اجتماعی

درهم شکستن رمزنگاری وب

وقتی وارد یک سایت خرید و فروش اینترنتی یا حساب ایمیل‌تان می‌شوید، مرورگرتان با استفاده از فناوری به نام TLS (سرنام Transport Layer Security) ارتباطی رمزنگاری شده را با سرور برقرار می‌کند. این فناوری که در واقع نسخه بهبود یافته SSL 3.0 محسوب می‌شود بخشی از سیستم رمزنگاری HTTPS است و به نوعی یک استاندارد وب است. اما اکنون تای دوونگ (Thai Duong) و جولیانو ریزو (Juliano Rizzo) ادعا کرده‌اند که می‌توانند این سیستم رمزنگاری را درهم بشکنند.

اواسط سپتامبر سال گذشته؛ این دو در نمایشی زنده در بوئنوس آیرس، بدافزار مخربی با نام BEAST (Browser Exploit Against SSL/TLS) را به نمایش گذاشتند که می‌توانست به ارتباطات رمزنگاری شده TLS نفوذ کند. فارغ از جزئیات فنی؛ این بدافزار مرورگر کاربر را آلوده کرده و به پایش ارتباطات میان مرورگر و سروری که از TLS استفاده می‌کند می‌پردازد. همچنین بلوک‌هایی از متن ساده را در بسته‌های داده ارسالی جاسازی می‌کند و پس از آن سعی می‌کند با حدس‌های هوشمندانه، این بلوک‌ها را دوباره رمزگشایی کند. تقریباً پس از ۵ تا ۱۰ دقیقه BEAST موفق می‌شود و با مهندسی معکوس کد رمزنگاری را یافته و داده‌های آن نشست را که در کوکی‌های کامپیوتر قربانی ذخیره شده است رمزگشایی کند. این کار گرچه زمان‌بر است اما یکی از حفره‌های امنیتی شناخته شده SSL/TLS محسوب می‌شود و این دو محقق پیش از این نمایش، اطلاعات مربوط به این حفره‌امنیتی را برای توسعه‌دهندگان فایرفاکس و اینترنت اکسپلورر ارسال کرده بودند. آن‌ها امیدوارند که علنی شدن این موضوع باعث شود که مرورگرها وسرورهای بیشتری به پروتکل جدیدتر TLS 1.1 و 1.2 روی بیاورند. پروتکل‌هایی که هنوز به صورت تئوری دربرابر این حمله در امان هستند. مایکروسافت قول داده است که وصله‌ای را برای رفع این مشکل عرضه کند و به ادعای لابراتوارهای کاسپرسکی، کاربران کروم نباید نگرانی چندانی داشته باشند، چرا که کروم چند ماه پیش وصله امنیتی این حفره را دریافت کرده است. پروتکل TLS 1.1 تقریبا از سال ۲۰۰۶ در دسترس بوده است، اما هنوز بسیاری از سایت‌ها و مرورگرها از همان نسخه قدیمی استفاده می‌کنند.

تا پیش از این‌که تمام مرورگرها و سرورها به استاندارد جدید مهاجرت کنند، تنها راه تقویت عادت‌های مرور ایمن وب است. هرگز ایمیل‌های ناشناس و مشکوک را باز نکنید و روی لینک‌های نامطمئن کلیک نکنید. اطلاعاتتان را روی شبکه‌های اجتماعی به اشتراک نگذارید و کلمات عبورتان در فواصل زمانی کوتاه عوض کنید.

و به‌خصـــوص ضد دولتی هکرهای آنلاین اســت که بـــه عنوان مثال با دخالت‌های آنانیموس در اعتراضات سیاسی و اقتصادی امریکا و اروپا کم و بیش به واقعیت پیوست. همه این‌ها به سال گذشته مربوط می‌شد. اما برای ۲۰۱۲ چه می‌توان گفت؟

به یقین در سال پیش‌رو همانند همه سال‌های دیگر، با رشد بدافزارها و نفوذها و فعالیت‌های خرابکارانه روبه‌رو خواهیم بود. با افزایش حجم داده‌های تولید شـــده در دنیا و ظهور پدیـــده‌ای به نام Big Data، نه تنها لزوم یافتن متدهای جدید نگه‌داری داده و داده‌کاوی آشکار می‌شود بلکه به همین نسبت هم نگرانی‌ها درباره حریم‌خصوصی کاربران؛ داده‌هایی از آنان که نگه‌داری می‌شـــود و یا حتی مانند داســـتان PSN به دســـت سارقان می‌افتد، بیشتر خواهد شد.

رواج شدید و روزافزون شبکه‌های اجتماعی و واردشدن کاربرانی که تجربه چندانی در مســـائل مربوط به امنیت کامپیوترها ندارند، باعث رواج بیشـــتر هک‌های مبتنی بر مهندســـی اجتماعی خواهد شـــد. حتی در بهتریـــن حالت و با فرض عدم وجـــود چنین مزاحمت‌هایی داده‌های این شـــبکه‌ها برای تحلیل رفتار کاربران و اســـتخراج اطلاعاتی از آن‌ها بـــه کار خواهـــد رفت کـــه از دید بســـیاری، مصداق بـــارز نقض حریم شخصی است.

حتـــی گروهـــی رویدادهـــای ســـاده‌ای ماننـــد مشـــکلات ISPاها با «بی‌طرفی شـــبکه» و اختصاص پهنای باند بیشتر به کاربری‌های مورد نظر خودشـــان را به نوعی بخشـــی از نگرانی‌های امنیتی سال ۲۰۱۲ و سال‌های آینده می‌دانند. با همه این تفاصیل، دیگر هنگامی که صحبت از تأمین امنیت سیســـتم‌های کامپیوتری به میان می‌آید، موضوع فراتر از نصب یک آنتی‌ویروس یا استفاده از دیواره‌های آتش است. کلاهبرداران و مجرمان سایبری، در بیشتر موارد هدفی جز کسب درآمد ندارند و در این راه از انجام هیچ عملی فروگذار نخواهند بود.

هـــر فناوری نوین و هر پدیـــده پرطرفداری از دید این افراد به مثابه فرصتی جدید برای پیاده‌کردن ترفندها و حقه‌های جدید به شمار می‌آید. بـــه نظر می‌رســـد از میان تمام پدیده‌ها و فناوری‌های نوین، گســـترش اســـتفاده از شبکه‌های اجتماعی و رشد روزافزون تعداد ابزارهای قابل حمل متصل به اینترنت بیش از سایر موارد توجه هکرها را به خود جلب کرده و از دیگر سو بیش‌ترین ارتباط را با کاربران عادی دارد. در ادامه به اختصار این دو عرصه و پس از آن عرصه کامپیوترهای شـــخصی را بررسی خواهیم کرد.

موبایل‌ها و تبلت‌ها

در ســـال گذشته میزان گسترش بدافزارهای دستگاه‌های قابل حمل به شدت فزونی یافت؛ به گونه‌ای که به گزارش مک‌آفی میزان این حمله‌ها در شـــش ماهه نخست سال ۲۰۱۱ در حدود ۲۲ درصد بیش از کل سال ۲۰۱۰ بوده است.

آندروئیـــد به لحـــاظ تعداد حمله‌هـــای صورت گرفته؛ با جهشـــی ۷۶ درصدی از سه ماهه نخست ۲۰۱۱ تا ۳ ماهه دوم آن، از سیمبیان و جاوا پیش افتاده است. بسیاری این امر را نتیجه مستقیم ذات اپن‌سورس و ســـهم بزرگـــی که از بـــازار گجت‌های قابل حمـــل دارد (۴۳ درصد به گزارش نیلسن) می‌دانند.

به نظر می‌رسد با افزایش تعداد گجت‌های مبتنی بر آندروئید، میزان این حملات نیز در ســـال ۲۰۱۲ افزایش چشـــم‌گیری داشته باشد.(کادر دســـتگاه‌های موبایل و امنیت را ببینید) گســـترش بدافزارهای موبایل، معمولاً از طریق فروشـــگاه‌های آنلاین خریـــد برنامه صورت می‌گیرد.

دستگاه‌های موبایل و امنیت

کاربردهای ریسک‌پذیر دستگاه‌های قابل حمل در آینده

تأیید ســـن: دســـتگاه‌هایی که می‌توانند تأیید کنند که ســـن شـــما به ۲۱ (ســـن قانونی) رسیده است یا خیر. این دستگاه‌ها ممکن است برای عرضـــه تخفیف یـــا فراهم کـــردن اجازه دسترسی به تسهیلات خاصی به کار روند.

کنترل عضویـــت: دستگاه شما اطلاعات عضویت شـــما در کتابخانه، باشـــگاه و یا حتی داشتن شرایط استفاده از تخفیف دانشجویی را در خود نگاه خواهد داشت.

اثبـــات مقیـــم بـــودن: ایـــن دســـتگاه‌ها می‌توانند اطلاعات مربوط به اقامت شما در یک شـــهر یا منطقه خاص را نگه‌داری کنند و به این ترتیب دسترســـی به خدمات محلی و منطقه‌ای را فراهم کنند.

کنترل دسترســـی: تلفن‌های هوشـــمند جایگزیـــن کارت‌های امنیتی خواهند شـــد که اجازه دسترسی فیزیکی و ورود به ساختمان‌ها یا بخش‌های خاص را فراهم می‌کنند.

دســـتگاه‌های پرداخت: دستگاه‌های بانکی و پایانه‌های خرید به جای کارت‌های اعتباری از تلفن هوشمند شما استفاده خواهند کرد. دیگر لزومی به حفظ کردن اطلاعات حساب‌ها نخواهید داشت و تخفیف‌ها، خریدهای اعتباری و غیره همه به تلفن شما منتقل خواهند شد.

تشـــخیص هویت: زمانی که پلیس شما را به خاطر تخلف از سرعت مجاز متوقف می‌کند، به جای ارائه مدارک می‌توانید از تلفن هوشمند خود استفاده کنید. تلفنی که تمام اطلاعات مربوط به گواهی‌نامه، اسناد خودرو و بیمه شما را در خود دارد.

شیوه‌های حمله به موبایل‌ها

SMISHING/VISHING/PHISHING: استفاده از پیامک، صندوق پست صوتی یا ایمیل برای دسترسی به نام کاربری و کلمات عبور یک کاربر

آندروئید ۴ اکنون می‌تواند برای باز کردن قفل گوشی شما از فناوری تشخیص چهره استفاده کند.

دانلـــود برنامه‌ها: برنامه‌های ناشناخته می‌تواننـــد نرم‌افزارهـــای مخربـــی را به اجرا درآورنـــد، در عین حال مراقب نســـخه‌های مختلف و بـــه روزرســـانی‌های برنامه‌ها نیز باشید. بدافزار DroidDream دقیقاً به همین شـــکل کار می‌کند. ابتدا نســـخه‌ای ســـالم از برنامه را به کاربر می‌دهد و ســـپس از طریق به روزرسانی‌ها دستگاه را آلوده می‌کند.

جاسوســـی وای‌فـــای: هنگامـــی که بـــه یک شـــبکه وای-فـــای عمومـــی متصل می‌شـــوید، ســـایرین نیز می‌توانند به دستگاه شـــما نفوذ کرده و به داده‌های شما دسترسی یابند.

کرم‌ها/تروجان‌ها/جاسوس‌افزارها: نرم‌افزارهای آلوده را روی دستگاه شما نصب می‌کنند. ایـــن نرم‌افزارها می‌توانند اطلاعات شما را به سرقت برده، عملیات‌ها را لغو کنند یا برنامه آلوده کننده را برای تمام افراد فهرست مخاطبان شما ارسال کنند.

حفره‌ها و وصله‌ها

شـــرکت ادوبی به تازگی وصله جدیـــدی را برای اصلاح حفـــره‌ای امنیتی در محصولاتش منتشـــر کرده است. این حفره به نفوذگر اجازه می‌داد اعمالی را با مجوزهای کاربر به انجام برساند. این حفره در فلش پلیر نسخه 10.3.183.7 و قدیمی‌تر مخصوص ویندوز و مک و لینوکس و ســـولاریس و همین‌طور نســـخه 10.3.186.6 و قدیمی‌تر آندروئید گزارش شـــده بود. ادوبـــی همچنین وصله‌ها و به روزرســـانی‌هایی را برای Adobe Reader X (10.1) و Acrobat X (10.1) ویندوز و نســـخه‌های 9.4.2 یونیکسی منتشر کرد.

همان‌طور که گفته شـــد حفره فلش پلیر به نفوذگر اجازه می‌داد تا در هر ســـایت یا فراهم‌کننده خدمات ایمیل، کارهایی را به جـــای کاربر انجام دهد. حفره‌های مربوط بـــه آکروبات باعث کرش‌کردن نرم‌افزارها می‌شـــد و درســـت در همین زمان نفوذگر می‌توانست کنترل سیستم کاربر را به دست بگیرد. در آگوست ۲۰۱۱ میلادی، DigiNotar یکی از صادرکنندگان تأییدیه‌های دیجیتال هلندی، به اشتباه مجوزی جعلی را صادر کرد که باعث بروز حمله‌ای از نوع Man-in-the-Middle روی اتصالات SSL ســـرورهای گوگل می‌شـــد. موزیلا این تأییدیه را به فهرست تأییدیه‌های غیرقابل اعتماد اضافه کرده بـــود، اما نفوذکنندگان راهی برای دورزدن این محدودیت پیدا کرده بودند. موزیلا مجبور شد برای جلوگیری از حمله‌های آینده، تعداد بیشتری از تأییدیه‌ها را به فهرست غیرقابل اعتماد خود بیافزاید. اپل نیز همین تغییرات را در سافاری (نسخه‌های Mac OS X 10.6.8 و 10.7.1) اعمال کرده بود.

عـــلاوه بر همه این‌ها، موزیلا وصله‌هایی نیز برای رفـــع باگ‌های امنیتی حافظه و overflow جاوااسکریپت منتشر کرده بود. تمام این باگ‌ها باعث می‌شدند که یک نفوذگر بتواند کدهای مخرب را روی سیســـتم قربانی اجرا کرده و باعث از کار افتادن نرم‌افزارها شود. موزیلا همواره پیشنهاد می‌کند که از آخرین نسخه نرم‌افزارهایش استفاده کنید.

در ایـــن فروشـــگاه‌ها، به‌خصـــوص Android Market که در آن کنترل چندانی روی برنامه‌های جدید وجود ندارد، بدافزارها خود را به عنوان نرم‌افزاری جدید و یا نســـخه‌هایی شـــبیه نرم‌افزارهای شناخته‌شده جا می‌زنند. در این میان نســـبت بدافزارها در فروشـــگاه‌های غیررسمی به مراتب بیشـــتر اســـت. به همین دلیل باید تا حد ممکن از مراجعه به آن‌ها خـــودداری کرد. وجود برنامه‌های ضدویروس بر روی دســـتگاه‌های قابل حمل به امری اجتناب تبدیل شـــده اســـت. در پاسخ به همین نیاز نیز شرکت‌های بســـیاری نظیر Avast و LookOut نسخه‌های ضدویروس مخصوص سیستم‌عامل‌های موبایل را در محصولات خود گنجانیده‌اند.

از دیگر تهدیدات امنیتی دستگاه‌های موبایل، باید به مخاطرات امنیتی شـــبکه‌های وای‌فای اشـــاره کرد. این تهدیدات زمانی که از شـــبکه‌های عمومی مکان‌هایی نظیر رســـتوران‌ها و فرودگاه‌ها استفاده می‌کنید به شدت بیشـــتر خواهند شد. ابزارهای ساده و در دسترسی نظیر افزونه Firesheep مرورگر فایرفاکس، امکان سرک کشیدن در سیستم شما را برای دیگران فراهم می‌کند.

این افزونه به هکر یا حتی فرد کنجکاوی که از همان شـــبکه وای‌فای اســـتفاده می‌کند، اجازه می‌دهد تا نام کاربری و رمز عبور حســـاب‌های شـــما در سایت‌هایی نظیر توییتر و... را که به‌صورت پیش‌فرض از SSL استفاده نمی‌کنند، به‌دست آورد.

برای جلوگیری از این نفوذها، حداقل زمانی که از شبکه‌های عمومی اســـتفاده می‌کنید، به جای استفاده از برنامه‌ها به‌طور مستقیم از طریق مرورگرتان به سایت مورد نظر مراجعه کنید و مطمئن شوید که آدرس سایت به جای http با https شروع می‌شود و حتی در صورت لزوم این s را دســـتی وارد کنید. بهتر این اســـت که حسابتان را چک کنید و ببینید آیا تنظیمی برای فعال کردن اجباری این پروتکل دارد یا خیر. سعی کنید مرورگرتان را طوری تنظیم کنید که از آخرین نسخه این استانداردهای رمزگذاری استفاده کند (کادر در هم شکستن رمزنگاری وب را ببینید).

نکته آخر در مورد دستگاه‌های قابل حمل، حفظ امنیت فیزیکی آن‌ها اســـت. در مراقبت از آن‌ها بکوشـــید، از رمزهای عبور عددی و شـــکلی اســـتفاده کنیـــد و برنامه‌های محافظی را روی آن‌هـــا نصب کنید که در صورت گم شـــدن یا ورود کلمه عبور اشـــتباه داده‌های دستگاه شما را پاک کنند.

شبکه‌های اجتماعی

در ســـال ۲۰۱۱ شـــبکه‌های اجتماعـــی بـــا افزایـــش شـــدید تعـــداد کاربـــران و در نتیجـــه افزایـــش تعـــداد حمله‌هـــای بدافـــزاری مواجـــه شـــدند. هکرهـــا از طریـــق ســـایت‌های آلـــوده و فعالیت‌هـــای Phishing توانســـتند برخـــی از حســـاب‌ها را هک کـــرده و از طریق آن‌هـــا به توزیع بدافزارهایشـــان بپردازند. این بدافزارها از طریق پســـت‌ها و نظرات و حتی برنامه‌هـــای مختلف گســـترش یافتنـــد. در هنگام فعالیت در این شـــبکه‌ها احتیاط پیشه کنید.

از کلیک‌کردن لینک‌های مشـــکوک خودداری کنید، حتی اگر از ســـوی دوســـتی برای شـــما ارسال شـــده باشـــند. برخی از بدافزارهای اجتماعی حتی می‌توانند بدون اطلاع کاربران از حســـاب آن‌ها برای ارســـال پست‌ها و لینک‌های آلوده اســـتفاده کنند. از نصب و استفاده از برنامه‌های مشکوک نیـــز خودداری کنید و هـــر از چندگاهی، کل برنامه‌های نصب شـــده‌تان را بازبینی‌کرده و موارد اضافی را حذف کنید (برای اطلاعات بیشـــتر به مقاله شش تهدید امنیتی در حال رشد، در شماره ۱۲۹ ماهنامه مراجعه کنید).

پی‌سی‌ها و مک‌ها

اگرچـــه بدافزارهای موبایل توجه زیـــادی را به خود جلب کرده‌اند، امـــا بدافزارهـــا هنـــوز کامپیوترهای شـــخصی را رهـــا نکرده‌اند. تنها راه مقابلـــه ماننـــد همیشـــه نصب ضدویـــروس و به روز نگه‌داشـــتن آن اســـت. اگـــر در فکـــر کاهـــش هزینه‌هایتـــان هســـتید از نمونه‌های مجانی نظیـــر Avast یـــا Security Essential محصول مایکروســـافت استفاده کنید.

خرابـــکاران اینترنتـــی هـــر روز حفره‌هـــای امنیتی جدیـــدی را در محصـــولات ادوبی، برنامه‌های مایکروســـافت، جاوا و حتی مرورگرها مورد استفاده قرار می‌دهند. پس به روز کردن برنامه‌هایتان را نیز مدنظر داشـــته باشید. بیشـــتر این نرم‌افزارها گزینه‌هایی برای خودکارسازی فرآیند بروزرسانی دارد که پیشنهاد می‌شود حتماً از آن‌ها استفاده کنید (کادر حفره و وصله‌ها را ببینید).

در گذشته کاربران مک نگرانی زیادی درباره بدافزارها نداشتند، اما وضعیت در حال تغییر اســـت. سال ۲۰۱۱ اپل با افزایش بدافزارها برای سیســـتم‌عامل OS X روبه‌رو شد. بدافزارهایی نظیر ضدویروس جعلی Mac Defender کـــه تعدادی popup را به نمایش درمی‌آورد و ســـعی می‌کرد برای حذف آن‌ها از کاربران پول بگیرد.

بـــا افزایش ســـهم مک از بـــازار کامپیوترها، منتظـــر افزایش تعداد بدافزارهـــای آن هـــم باشـــید. اگرچه باز هم نســـبت بدافزارهای مک به ویندوز همچنان پایین خواهد ماند. همواره به یاد داشته باشید که بهترین راه در امان ماندن از این خطرات تکیه بر عقل سلیم و افزایش آگاهی در خصوص ملاحظات امنیتی دنیای سایبری است.