10سد در برابر هکرهای رایانه

فعالیت مجرمان سایبری به تلفن‌های همراه هوشمند محدود نمی‌شود و آنها با هک اطلاعات رایانه‌های شخصی یا شرکت‌ها به دنبال اخاذی و اقدامات مجرمانه‌شان هستند. برای این‌که رایانه خود را از ورود مجرمان در امان نگه دارید به این توصیه‌های جدی توجه کرده و با ما همراه باشید.

سیستم عامل خود را به‌روز کنید

مهم‌ترین مسأله امنیت در کامپیوتر به روز رسانی سیستم عامل است. استفاده از سیستم عامل کرک شده باعث می‌شود کاربر برای استفاده امن و بدون دغدغه از کامپیوتر، آمادگی نداشته باشد. در کل کاربران کشورهای جهان سوم (ازجمله ایران) به دلیل استفاده از نرم‌افزارها و سیستم‌های عامل کرک شده، بیشتر در معرض خطر قرار دارند. همیشه به یاد داشته باشید، هر زمانی ناشر سیستم عامل اعلام کرد از یک نسخه خاص دیگر پشتیبانی نخواهد کرد، به معنای این خواهد بود که شما با استفاده از آن نسخه، امنیت نخواهید داشت.

اگر از نرم‌افزاری خاص استفاده می‌کنید که روی نسخه‌های قدیمی سیستم‌عامل‌ها اجرا می‌شود، ناشر آن نرم‌افزار ملزم است محصولات خود را به روز کند نه این‌که شما به عنوان استفاده‌کننده سیستم عامل رایانه‌تان را با نرم‌افزار هماهنگ کنید.

نصب و به‌روزرسانی نرم‌افزارهای امنیتی

آپدیت سیستم عامل به تنهایی نمی‌تواند از ورود ویروس یا هکر جلوگیری کند. به همین علت وجود یک نرم‌افزار امنیتی (ترجیحا اینترنت سکوریتی) نیز مورد نیاز است. نرم‌افزارهای امنیتی متعددی به بازار عرضه شده‌اند. کاربر باید تنها یک نرم‌افزار امنیتی (در یک حیطه کاری) را با مشورت یک کارشناس برای خود انتخاب و نصب کند تا دچار مشکلاتی از قبیل افت سرعت سیستم یا تداخل بین نرم‌افزارهای دیگر نشود. اگر کاربر مایل به خرید و صرف هزینه نباشد، نباید نسخه کرک نرم‌افزار امنیتی را نصب کند. مثل این است که یک راننده برای امنیت، کمربند ایمنی بی‌کیفیت در اتومبیل خود نصب کند.

پیشنهاد ما برای این نوع از کاربران، نصب آنتی‌ویروس یا اینترنت سکوریتی رایگان است. بهترین نرم‌افزارهای امنیتی _ که به صورت رایگان عرضه شده‌اند _را می‌توان ۳۶۰ Internet Security در حیطه آنتی ویروس و امنیت در اینترنت) و Avast Free Antivirus در حیطه آنتی ویروس) را نام برد.

این دو نرم‌افزار که به صورت رایگان منتشر شده‌اند، از حافظه رم بسیار پایین استفاده می‌کنند و می‌تواند از جمله بهترین انتخاب‌ها برای کاربران باشد. ما بیشتر نصب نرم‌افزار امنیتی Internet Security ۳۶۰ را به کاربران پیشنهاد می‌دهیم، چرا که این نرم‌افزار از امکانات کامل‌تری نسبت به نرم‌افزار Avast Free Antivirusبرخوردار است و از همه مهم‌تر، فاقد هرگونه تبلیغاتی است.

از کافی‌نت یا کامپیوترهای دیگران برای کارهای شخصی استفاده نکنید

هنگام استفاده از کامپیوترهای عمومی یا کامپیوتر دیگران، بدترین احتمال را در سرلوحه کارتان قرار دهید. این احتمال که صاحب کامپیوتر میزبان، دقت کافی در استفاده را به کار نبرده است، یعنی نه سیستم خود را به‌روزرسانی کرده و نه توجهی به نرم‌افزارهای امنیتی خود دارد. هر چند که بی دقتی‌های دیگری هم هستند که در ادامه این مقاله عنوان خواهیم کرد.

رمز خود را در اختیار دیگران قرار ندهید

بارها پیش آمده شخصی ـ به خاطر نداشتن دسترسی به اینترنت یا عواملی دیگر ـ رمز خود را در اختیار دیگران قرار می‌دهد تا برای مثال، ایمیلی را بررسی کنند.

این کار ممکن است باعث سوءاستفاده دیگران شود و از آنجایی که کل تنظیمات امنیتی شبکه‌های اجتماعی بر مبنای ایمیل شخص است، بسیار خطرناک و کاری بسیار پرریسک خواهد بود.

تاریخ سیستم خود را به روز نگه دارید

از آنجا که مرورگرهای اینترنتی و نرم‌افزارهای دیگر برای چک کردن مجوزهای امنیتی به تاریخ سیستم کاربر رجوع می‌کنند، کاربر باید هر از چند گاهی تاریخ سیستم و منطقه زمانی خود را بررسی نماید.

نکته: در صورتی که بعد از خاموش و روشن کردن کامپیوتر خود، متوجه تغییر تاریخ خود شدید، باید باتری Motherboardخود را تعویض کنید.

از نصب برنامه‌های غیرضروری پرهیز کنید

بسیاری از کاربران (البته بیشتر در کشورهای جهان سوم و ازجمله کشور ما (می‌پندارند هر چقدر نرم‌افزارهای مختلف نصب کنند، کامپیوتری کامل‌تر خواهند داشت. در حالی که با این کار امنیت کامپیوتر خود را به خطر می‌اندازند .مثالی ساده می‌زنیم: یخچال منزل کاربر را یک سیستم عامل، موتور آن را یک نرم‌افزار امنیتی و

همین‌طور محتویات آن را نرم‌افزارهای جانبی آن در نظر می‌گیریم. کاربر نمی‌تواند در داخل یخچال ـ سیستم‌عامل ـ خود (حتی در مواقعی که موتور آن بدون مشکل کار می‌کند) بیش از نیاز خود مواد غذایی ـ نرم‌افزار ـ انبار کند. مواد غذایی ـ نرم‌افزارها ـ دارای تاریخ انقضا هستند و خراب خواهند شد. حتی اگر موتور یخچال نیز بدون مشکل باشد، برای نگهداری از آنها، باید وقت و هزینه بیشتری را صرف کنید و اگر هم نگهداری نشود، خطر روز به روز بیشتر خواهد شد.

درایورهای سخت‌افزاری خود را به روزرسانی کنید

شاید از خودتان بپرسید به روزرسانی درایورهای سخت‌افزار چه ربطی به امنیت دارد، اما ما به شما اطمینان می‌دهیم این موضوع اهمیت بسیاری در تأمین امنیت کامپیوتر کاربر دارد.

سیستم عامل و آنتی ویروس بایستی در کامپیوتری بدون اشکال فنی کار کنند تا کارها به درستی پیش برود و در صورتی که درایور سخت افزاری معیوب باشد، دستگاه به درستی سیستم عامل را اجرا نخواهد کرد و علاوه بر کندی سرعت، باعث بد اجرا شدن نرم‌افزارهای دیگر (ازجمله نرم‌افزار امنیتی) خواهد شد. به همین علت شرکت‌های سازنده قطعات سخت افزاری، هر از چند گاهی (در صورت گزارش وجود مشکل در درایور) نرم‌افزارهای آنها را برای عملکرد بهتر، به‌روزرسانی و در سایت رسمی شرکت منتشر می‌کنند.

پیشنهاد می‌شود هنگام خرید کامپیوتر، نام شرکت سازنده و مدل‌های سخت افزارهای خود را روی کاغذی بنویسید و در اختیار داشته باشید تا بتوانید در صورت لزوم، برای به‌روزرسانی آنها اقدام کنید. تأکید می‌شود از سایت‌های رسمی شرکت‌های ارائه دهنده سخت‌افزار، درایورهای خود را با توجه به مدل سخت‌افزار دریافت کنید.

نرم‌افزارهای جانبی را به‌روزرسانی کنید

همان‌طور که پیش‌تر عنوان کردیم، برای حفظ امنیت کامپیوتر خود باید سیستم عامل و نرم‌افزارهای امنیتی خود را به‌روزرسانی کنید. نرم‌افزارهای جانبی نیز از این قاعده مستثنا نیستند و این کار باعث می‌شود ایرادات نرم‌افزارها (ایرادات امنیتی و اجرایی) برطرف شود.

از نرم‌افزارهای کرک شده استفاده نکنید

ما برای این توصیه، چهار دلیل داریم.

دلیل اول :همان‌طوری که در دلایل قبلی گفته شد، کامپیوتر برای حفظ امنیت نیاز به آپدیت دارد، چه سیستم‌عامل باشد، چه آنتی ویروس و چه نرم‌افزارهای جانبی... . حال استفاده از نرم‌افزارهای کرک شده، باعث می‌شود که هنگام آپدیت نرم‌افزار، سرور ناشر سازنده از کرک بودن ـ غیرقانونی بودن ـ نرم‌افزار مطلع شود و خدمات خود را برای کاربر قطع کند. این کار سبب می‌شود کاربر از دریافت به‌روزرسانی‌های امنیتی نرم‌افزار که گاهی اوقات خیلی ضروری است محروم شود.

دلیل دوم :کرک‌ها هیچ موقع قابل اطمینان نبوده و نخواهند بود. کسی بدون نیت قبلی، نرم‌افزاری را برای استفاده عمومی کرک نمی‌کند. انکار نمی‌کنیم که هستند در میان این افراد که با شعار «رایگان برای همه» در این عرصه فعالیت می‌کنند، ولی باز کاربر نمی‌تواند از نیت برنامه نویس آگاه باشد و به همین علت ما روی این دلیل پافشاری می‌کنیم.

دلیل سوم :این کار در کشورهای پیشرفته (چه برای کرک‌کننده و چه برای استفاده‌کننده نرم‌افزار) کاری غیرقانونی است. کسانی هستند که بدون نیت‌های سیاسی، خواهان رفع تحریم‌های نرم‌افزاری هستند. به همین دلیل برای این کار باید توسط خود کاربران زمینه‌سازی شود تا دولت بتواند با خیالی آسوده قانون کپی‌رایت را بپذیرد.

دلیل چهارم :همان‌طوری که حال یک نویسنده از انتشار کتاب یا مقاله خود در جایی دیگر بدون درج نامش دگرگون می‌شود، ناشر و برنامه‌نویسان نرم‌افزارها نیز به همین حال دچار می‌شوند. به همین علت، اگر تمامی مشکلات امنیتی را نیز نادیده بگیریم، از لحاظ وجدان و انسانیت نیز این کار صحیح نیست.

وارد سایت‌هایی که نمی‌شناسید نشوید

در صورتی که کاربری همه مسائل امنیتی را نیز رعایت کند، ولی بدون دقت به سایت‌های ناشناس وارد شود، باز دچار مشکل خواهد شد. ما می‌توانیم عنوان کنیم خطرناک‌ترین کار همین مورد است، چرا که اولین جایی که در آن ویروس جدیدی منتشر می‌شود، اینترنت است و بعد از انتشار آن شرکت‌های سازنده نرم‌افزارهای امنیتی به مقابله با ویروس می‌پردازند. پس حتماً به آدرس سایت‌ها دقت کنید.

مزایا و معایب این نرم‌افزار:

مزایا:

1ـ استفاده از ۳ موتور جست‌وجوگر ویروس و کرم‌های اینترنتی

2ـ اسکن سریع و دقیق فایل‌ها

3ـ نداشتن هیچ‌گونه تبلیغی برای نرم‌افزار

4ـ استفاده بسیار کم از حافظه رم و سرعت پردازنده

5ـ نرم‌افزار رایگان است (با تمامی امکانات)

6ـ نصب سریع و آسان نرم‌افزار

7ـ کنترل نرم‌افزار بر دستکاری فایل‌ها و رجیستری سیستم عامل توسط نرم‌افزارهای دیگر

معایب:

1ـ نداشتن تنظیمات پیشرفته برای فایروال

2ـ نداشتن کنترل برنامه‌ها برای اتصال به شبکه اینترنت

واگریک شاهوردیان - کارشناس امنیت شبکه

منتظر شما هستیم

Taradof.Blog.ir