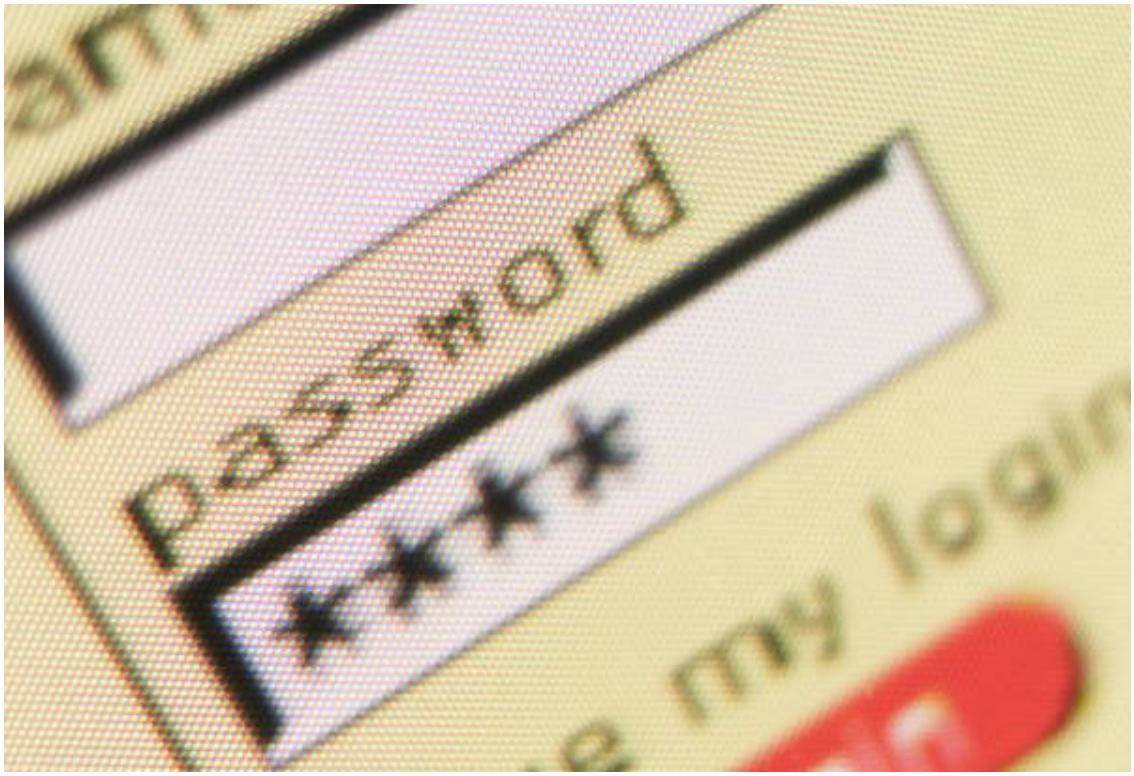
10ترفند برای بالا بردن امنیت رایانه و کاربر



اکثرمشکلاتی که امنیت سیستم کاربران و همچنین حریم شخصی آنان را به خطر می اندازد بر اثر ناآگاهی از الزامات و اصول اولیه به وقوع می پیوندد. در این ترفند قصد داریم به معرفی ۱۰ توصیه برای بالا بردن امنیت رایانه و کاربر بپردازیم. با رعایت این نکات می توانید امنیت حریم شخصی خود و رایانه ی خود را به حداکثر برسانید.

۱-استفاده از سیستم عامل به روز و اصل :

می توان گفت مهم ترین مسأله ی امنیت در کامپیوتر، به روزرسانی سیستم عامل است. با تنظیم سیستم عامل بر روی به روزرسانی خودکار می توانید از به روز شدن خودکار و به موقع سیستم عامل اطمینان حاصل کنید. بسیاری از تهدیدات امنیتی که کاربران را تهدید می کند در صورت به روز بودن سیستم عامل خنثی خواهند شد.
از طرفی استفاده از سیستم عامل کرک شده و غیراصل باعث می شود که کاربر برای استفاده ی امن و بدون دغدغه از کامپیوتر آمادگی نداشته باشد. به عنوان مثال نصب به روزرسانی ها در سیستم عامل های کرک شده به آسانی انجام نمی گیرد.

۲-استفاده از نرم افزارهای امنیتی و به روزرسانی مداوم آن ها :

به روزرسانی سیستم عامل به تنهایی نمی تواند از ورود ویروس و یا نفوذ هکر به سیستم شما جلوگیری کند. به همین علت وجود یک نرم افزار امنیتی (ترجیحاً Internet Security) نیز موردنیاز است.
نرم افزارهای امنیتی متعددی تاکنون منتشر شده اند که هر کدام علاقه مندان خاص خود را دارا هستند. کاربر باید تنها یک نرم افزار امنیتی (در یک حیطه کاری) را برای خود انتخاب کرده (با مشورت با یک کارشناس و یا مطالعه ی نقدهای مختلفی که در خصوص این نرم افزارها

وجود دارد) و نصب نماید تا دچار مشکلاتی از قبیل افت سرعت سیستم و یا تداخل بین نرم افزارهای دیگر نشود.
اگر کاربر مایل به خرید و صرف هزینه نباشد، نبایستی نسخه ی کرک شده ی نرم افزار امنیتی را نصب نماید. چرا که گویی یک راننده برای امنیت خود، کمربند ایمنی بی کیفیت در اتومبیل خود نصب نماید!
پیشنهادی که برای این نوع از کاربران وجود دارد، نصب Anti Virus یا Internet Security رایگان است. از میان بهترین نرم افزارهای امنیتی که به صورت رایگان عرضه شده اند میتوان به ۳۶۰ Internet Securityدر حیطه ی آنتی ویروس و امنیت در اینترنت) و Avast Free Antivirusدر حیطه ی آنتی ویروس) اشاره کرد. این ۲ نرم افزار که به صورت رایگان منتشر شده اند، مقدار بسیار پایینی از فضای رم را مصرف می کنند و می توانند از جمله بهترین انتخاب ها برای کاربران باشند.

از میان این دو نرم افزار نیز نصب نرم افزار امنیتی ۳۶۰ Internet Securityبیشتر پیشنهاد می شود، چرا که این نرم افزار از امکانات کامل تری نسبت به نرم افزار Avast Free Antivirus برخوردار است و از همه مهم تر، فاقد هر گونه تبلیغاتی است. از مزایای این نرم افزار می توان به استفاده از ۳ موتور جستجوگر ویروس و کرم های اینترنتی، اسکن سریع و دقیق فایل ها، نبود هیچ گونه تبلیغ در محیط نرم افزار، استفاده بسیار کم از فضای حافظه و اشغال بسیار کم فضای پردازنده، ۱۰۰% رایگان بودن کلیه ی امکانات نرم افزار، نصب سریع و آسان نرم افزار و نهایتاً کنترل نرم افزار بر دستکاری فایل ها و رجیستری ویندوز توسط دیگر نرم افزارها اشاره کرد. البته از معایب این نرم افزار می توان به عدم امکان تنظیمات پیشرفته برای فایروال و عدم کنترل برنامه ها برای اتصال به اینترنت اشاره نمود.

این نرم افزار را می توانید از سایت سازنده دریافت نمایید:
http://www.۳۶۰safe.com

۳-عدم استفاده از رایانه ی دیگران و یا رایانه های عمومی برای کارهای شخصی:

حتی الامکان از کافی نت و یا کامپیوترهای دیگران برای کارهای شخصی خود استفاده نکنید. در هنگام استفاده از از این کامپیوترها، بایستی بدترین احتمال را سرلوحه ی کارتان قرار دهید: این احتمال که صاحب کامپیوتر میزبان، دقت کافی در استفاده از کامپیوتر را به کار نبرده است. یعنی نه سیستم خود را به روزرسانی کرده است و نه توجهی به نرم افزارهای امنیتی خود داشته است!

٤-عدم به اشتراک گذاری رمز عبور:

بارها پیش آمده است که شخصی به خاطر نداشتن دسترسی به اینترنت یا دلایلی دیگر رمز خود را در اختیار دیگری قرار می دهد تا برای مثال او ایمیلی را بررسی کند. این کار به هیچ عنوان عملی صحیح نیست و از آنجایی که کل تنظیمات امنیتی شبکه های اجتماعی بر مبنای ایمیل شخص است، بسیار خطرناک و کاری بسیار پرریسک خواهد بود. چرا که علاوه بر اینکه ممکن است توسط فرد مورد نظر سوء استفاده صورت گیرد، ممکن است به دلیل عدم رعایت نکات امنیتی در سیستم شخص، رمز عبور شما به صورت ناخواسته لو رود.

٥-اطمینان از صحیح بودن تاریخ سیستم:

از آنجایی که مرورگرهای اینترنتی و نرم افزارهای دیگر برای چک کردن مجوزهای امنیتی به تاریخ سیستم کاربر رجوع می کنند، کاربر بایستی هر از گاهی تاریخ سیستم و منطقه زمانی خود را بررسی نماید و از صحت آن اطمینان حاصل کند.

٦-پرهیز از نصب نرم افزارهای غیرضروری:

بسیاری از کاربران می پندارند که هر چقدر نرم افزارهای مختلف نصب کنند، کامپیوتری کامل تر خواهند داشت؛ در صورتی که این گونه نیست و با این کار امنیت کامپیوتر خود را به خطر می اندازند.

به عنوان یک مثال، یخچال منزل کاربر را یک سیستم عامل، موتور آن را یک نرم افزار امنیتی و همین طور محتویات آن را نیز نرم افزارهای جانبی آن در نظر می گیریم. کاربر نمی تواند در داخل یخچال (سیستم عامل) حتی در مواقعی که موتور آن بدون مشکل کار می کند بیش از نیاز خود مواد غذایی (نرم افزار) انبار کند. مواد غذایی (نرم افزارها) دارای تاریخ انقضا هستند و خراب خواهند شد. حتی اگر موتور یخچال نیز بدون مشکل باشد! برای نگهداری از آن ها، باید وقت و هزینه بیشتری را صرف کنید و اگر هم نگهداری نشود، خطر روز به روز بیشتر خواهد شد.

٧-به روزرسانی دائمی درایورهای سخت افزاری:

شاید از خودتان بپرسید این موضوع چه ارتباطی به امنیت دارد! اما بایستی بدانید که 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. 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 نرم افزارهای دیگر (از جمله نرم افزار امنیتی) خواهد شد. به همین علت شرکت های سازنده قطعات سخت افزاری، هر از چند گاهی (در صورت گزارش وجود مشکل در درایور) نرم افزارهای آن ها را برای عملکرد بهتر، به روز رسانی و در سایت رسمی شرکت منتشر می کنند.

پیشنهاد می شود در هنگام خرید کامپیوتر، نام شرکت سازنده و مدل های سخت افزارهای خود را یادداشت کرده و در اختیار داشته باشید تا بتوانید در صورت لزوم، برای به روز رسانی آن ها اقدام نمایید. تأکید می شود که حتماً از سایت های رسمی شرکت های ارائه دهنده سخت افزار، درایورهای خود را با توجه به مدل سخت افزار دریافت کنید.

٨-به روزرسانی نر م افزارهای جانبی:

همان طور که پیش تر عنوان کردیم، برای حفظ امنیت کامپیوتر خود، بایستی سیستم عامل و نرم افزارهای امنیتی خود را به روز رسانی کنید. نرم افزارهای جانبی نیز از این قائده مستثنا نیستند. این کار باعث می شود که ایرادات نرم افزارها (ایرادات امنیتی و اجرایی) برطرف شود.

٩-عدم بهره گیری از نرم افزارهای کرک شده:

برای این موضوع ٤ دلیل وجود دارد:

•همان طور که پیش تر توضیح داده شد، کامپیوتر برای حفظ امنیت، نیاز به به روزرسانی دارد. خواه چه سیستم عامل باشد، چه آنتی ویروس و چه نرم افزارهای جانبی. استفاده از نرم افزارهای کرک شده در اکثر مواقع باعث می شود امکان به روزرسانی برنامه از کاربر سلب شود. همچنین ممکن است که در هنگام به روز نمودن نرم افزار، سرور ناشر سازنده از غیرقانونی بودن نرم افزار مطلع شود و خدمات خود را برای کاربر قطع کند. این کار سبب می شود که کاربر از دریافت به روزرسانی های امنیتی نرم افزار که گاهی اوقات خیلی ضروری است محروم شود.

•کرک ها هیچ موقع قابل اطمینان نبودند و نخواهند بود. بسیاری از کرک ها با وجود کارکرد صحیح آلوده به بدافزار هستند. در کنار کرک کننده هایی که با شعار «رایگان برای همه» در این عرصه فعالیت می کنند، افرادی نیز وجود دارند که با اهداف شخصی و تهدید امنیت کاربران فعالیت می کنند.
•این کار در کشورهای پیشرفته (چه برای کرک کننده و چه برای کاربر) کاری غیرقانونی است. کسانی هستند که بدون نیت های سیاسی خواهان رفع تحریم های نرم افزاری هستند. به خاطر همین مسأله برای این کار باید توسط خود کاربران زمینه سازی شود تا دولت بتواند با خیالی آسوده قانون کپی رایت را اجرا کند.
•همانطور که حال یک نویسنده از انتشار کتاب یا مقاله خود در جایی دیگر بدون درج نامش دگرگون می شود، ناشر و برنامه نویسان نرم افزارها نیز به همین حال دچار می شوند. به همین علت، اگر تمامی مشکلات امنیتی را نیز نادیده بگیریم، از لحاظ اخلاقی نیز این کار صحیح نیست.

۱۰-عدم ورود به سایت های ناشناس:

در صورتی که کاربری همه ی مسائل امنیتی را نیز رعایت کند ولی بدون دقت به سایت های ناشناس وارد شود، باز دچار مشکل خواهد شد. می توان عنوان کرد که خطرناک ترین کار، همین مورد است. چرا که اولین جایی که در آن ویروس جدیدی منتشر می شود، اینترنت است و بعد از انتشار آن است که شرکت های سازنده نرم افزارهای امنیتی به مقابله با ویروس می پردازند. پس حتماً به آدرس سایت ها دقت کنید.