

عادات نادرست کاربران کامپیوتر



۱- عدم نصب ابزارهای امنیتی

تصور داشتن یک زندگی مجازی آرام بدون استفاده از ابزارهای امنیتی به منظور شناسایی و حذف انواع بدافزارها عملاً دور از انتظار است. امنیت تنها در اطلاع دقیق از محتویات لینکها و باز نکردن ایمیل‌های ناشناس خلاصه نمی‌شود. این روزها در امان ماندن از انواع بدافزارها و تکنیک‌های پیشرفته نفوذ و دسترسی امن به اطلاعات، بدون استفاده از مجموعه‌ای حرفه‌ای از ابزارهای امنیتی عملاً غیرممکن است.

بعضی از کاربران با دلایلی غیرمنطقی مثل کند شدن سرعت کامپیوتر هنگام نصب ضدویروس و کندی سرعت اینترنت در صورت فعال بودن فایروال، باورهای اشتباه خود در زمینه عدم استفاده از ابزارهای امنیتی را توجیه کرده و حتی دیگران را هم به این کار تشویق می‌کنند.

در حالی که این دسته از کاربران باید عواقب عدم استفاده از ابزارهای امنیتی را تصور کرده و بعد تصمیم به نصب یا عدم نصب آنها بگیرند. برای مثال شاید نصب یک ضدویروس موجب کندی نامحسوس و قابل تحمل کامپیوتر شود، اما بهتر است ساعات مدیدی که صرف نصب مجدد ویندوز و درایورها به دلیل آسیب دیدن فایل‌های سیستم‌عامل از سوی بدافزارها می‌شود را هم در نظر داشت.

ضمناً بهتر است از نصب نسخه‌های مجانی ضدویروس یا فایروال شرکت‌های غیرمعتبر بپرهیزید؛ این گونه ابزارها به جای محافظت از اطلاعات اقدام به سرقت آنها می‌کنند!

۲- عدم پشتیبان‌گیری از اطلاعات

پشیمانی برای آن دسته از کاربران تنبل که از اطلاعات خود پشتیبان تهیه نمی‌کنند، سودی نخواهد داشت. این کاربران با بهانه‌های بی‌پایه

و اساس، اطلاعات را در معرض خطرهای جبران ناپذیر قرار می‌دهند. ضمناً از کار افتادگی‌های هارد دیسک امری اجتناب ناپذیر است! بهتر است با شیوه‌های گوناگون پشتیبان‌گیری آشنا شده و از نرم‌افزارهای حرفه‌ای این حوزه که نیازی به دخالت شما نداشته و کار را به صورت خودکار انجام می‌دهند، استفاده نمایید. همچنین بهتر است فایل‌های پشتیبان را روی هارد دیسک اکسترنال قرار دهید.

۳- عدم پشتیبان‌گیری آنلاین

یکی از بهترین و امن‌ترین روش‌های موجود برای ذخیره‌سازی کاملاً امن اطلاعات، ارسال آنها به فضای ابرهاست. سرویس Live شرکت مایکروسافت ۲۵ گیگابایت فضای کاملاً مجانی در اختیار کاربران قرار داده و امکان آپلود انواع فایل‌های حجیم را میسر کرده است. البته در Gmail گوگل هم تقریباً ۸ گیگابایت فضا در اختیار دارید. با استفاده از نرم‌افزارهایی مثل Gmail Drive یا SkyDrive Explorer می‌توان این فضاهای رایگان ابری را در قالب درایو به ویندوز اضافه کرد و با استفاده از قابلیت کشیدن و رها کردن (Drag & Drop) اقدام به پشتیبان‌گیری از داده‌های مهم نمود.

البته این راه حل فقط برای کاربران مرفه (از نوع بی‌درد) است که اینترنت پرسرعت دارند و می‌توانند به راحتی فایل‌ها را آپلود و دانلود کنند!

۴- پاسخ به هرزنامه‌های تبلیغاتی

یکی از دلایل مهمی که اسپمرها را تشویق به ادامه کار می‌کند، کلیک کاربران روی لینک‌های موجود در هرزنامه‌های تبلیغاتی و حتی پاسخ به این گونه ایمیل‌هاست. بله اسپمرها کلیک روی لینک‌های Remove me یا Unsubscribe me (به منظور حذف از لیست ارسال) را پاسخی از سوی کاربران محسوب کرده، از فعال بودن آن آدرس ایمیل مطمئن شده و سیل هرزنامه‌ها را با شدتی بیشتر به سوی کاربر هدایت می‌کنند.

در صورتی که پیام تبلیغاتی از سوی یک شرکت معتبر ارسال شده باشد، کلیک روی چنین گزینه‌هایی خطرناک نیست؛ البته فراموش نکنید که این روزها با حرفه‌ای‌تر شدن خرابکاران، جعل آدرس ایمیل شرکت‌های معتبر هم کار سختی نبوده و بهتر است در این گونه موارد نیز جوانب احتیاط را در نظر داشته باشید.

۵- حمل دستگاه‌های روشن

حمل نوت‌بوک روشن از اتاق خواب تا نشیمن ایرادی ندارد، اما جابه‌جایی آن مثلاً از اداره تا منزل، پیاده‌روی طولانی، هنگام بالارفتن از پله‌ها و ... بسیار خطرناک بوده و امکان وارد آمدن صدمات جدی به دستگاه وجود دارد. در چنین مواقعی که هارددیسک در حال چرخش است، امکان از کار افتادگی آن در هر لحظه وجود دارد.

از این رو توصیه می‌کنیم هنگام جابه‌جایی، نوت‌بوک یا نت‌بوک، آن را خاموش کنید، مگر اینکه مدل مورد استفاده از نمونه‌های مقاوم در برابر ضربه و تکان‌های شدید باشد. ضمناً ریسک افتادن دستگاه از دست را هم نباید فراموش کرد. در این گونه مواقع بهتر است از حالت Hibernate که در آن، محیط کار ذخیره می‌شود، استفاده نمود. دقت داشته باشید در حالت Sleep هر لحظه امکان روشن شدن اتفاقی وجود دارد.

۶- نوت‌بوک در رختخواب!

استفاده از نوت‌بوک در رختخواب اشکالی ندارد، اما پرز و کرک بالش و لحاف و ... موجب گرفتگی پورته‌ها یا بسته شدن منافذ تهویه دستگاه و در نتیجه گرم شدن و در نهایت خرابی دستگاه خواهد شد. برای رفع این مشکل بهتر است از میز نوت‌بوک به منظور حفظ جریان هوا بین نوت‌بوک و سطوح پرزدار و همچنین خنک‌سازی دستگاه توسط فن استفاده کنید. فراموش نکنید که استفاده از نوت‌بوک در حالت درازکش یا دیگر وضعیت‌های بدنی نامطلوب، اثرات سو روی سلامت شما خواهد داشت.

۷- چاپ همه چیز

در صورت وجود نسخه دیجیتال یک سند چه نیازی به چاپ نسخه کاغذی وجود دارد؟ گاهی اوقات مطالب یک وبسایت نظرتان را جلب کرده و برای مطالعه بهتر آن را در قالب Word تنظیم و چاپ می‌کنید. بهتر نیست چنین سندی را تبدیل به فایل PDF کنید و به راحتی آن را در کامپیوتر یا حتی گوشی همراه مطالعه کنید. ضمناً چاپ کمتر، برابر با قطع کمتر درختان و ایفای نقشی هر چند جزئی در نجات کره زمین است.



۸- اظهار نظرهای آنلاین

در آغاز یک روز کاری بعد از نشستن پشت میز در اداره، برگه اخراج را روبروی خود خواهید دید و متوجه از دست رفتن شغل محبوبتان خواهید شد. اگر چه باور این مسئله تا حدودی سخت است اما امکان چنین اتفاقی دور از ذهن نیست. شاید یکی از اظهارنظرهای (کامنت‌های) قدیمی‌ شما در مورد عملکرد یکی از همکاران که هم اکنون رئیس شرکت شده، علت اخراج شدن تان باشد.

البته بعید نیست در وب سایت یا وبلاگ شخصی خود، یا در نظرات شبکه‌های اجتماعی از شرکت به خاطر بی‌کفایتی مدیران و کارکنان هم گله کرده باشید. حال یکی از مسئولان یا کارکنان بانفوذ با مشاهده چنین اظهارنظرهایی که حتی آنها را با نام مستعار منتشر کرده‌اید، موجبات بیکار شدن تان را فراهم کرده است؛ پس حتی نام مستعار (نام کاربری در وب سایت‌ها) خود را نزد همکاران فاش نکنید.

امروزه مسئولان با یک جستجوی ساده نام و نام خانوادگی، آدرس ایمیل یا نام مستعار، قادر به مشاهده نظرات شما در اینترنت هستند. بهتر

است جوانب احتیاط را رعایت کرده و از اظهارنظرهای بی‌مورد در فضای وب خودداری نمایید.

۹- رها کردن نوت‌بوک در خودرو

سارقان زیادی منتظر سرک کشیدن به درون خودروهای پارک شده هستند تا در صورت وجود چیزی با ارزش، دست به کار شوند. اگر نوت‌بوک خود را اغلب در خودرو به همراه دارید، باید احتیاط زیادی به خرج دهید. بهتر است هنگام پیاده شدن از خودرو نوت‌بوک را نیز با خود بردارید.

ضمناً استفاده از ابزارهایی موسوم به قفل سفر یا Travel Lock هم بد نیست. قفل سفر که نمونه‌های مختلفی دارد، به نوت‌بوک متصل شده و در صورت جدا شدن صدایی ناهنجار و بسیار بلند پخش می‌کند. ضمناً در ویندوز ۷ و ویستا نیز با استفاده از ویژگی Bitlocker می‌توان کار رمزنگاری اطلاعات روی هارددیسک را به منظور عدم دسترسی دیگران به آنها انجام داد.

۱۰- عدم داشتن آدرس ایمیل اضافه

کاربران حرفه‌ای چندین آدرس ایمیل داشته و از هر کدام برای مقاصد خاص استفاده می‌کنند. برای مثال آدرس ایمیل شخصی، در اختیار دوستان درجه یک و افراد خانواده قرار گرفته و آدرس ایمیل کاری را برای مکاتبات کاری در نظر می‌گیرند.

بهتر است آدرس شخصی را در اختیار خبرنامه‌ها، سرویس‌های وب و ... قرار ندهید، چرا که پیام‌های تبلیغاتی یا اطلاع‌رسانی‌های این گونه سایت‌ها شما را کلافه خواهند کرد. برای ثبت‌نام در بعضی سایت‌ها و استفاده از امکاناتی مثل دسترسی به لینک دانلود مجبور به وارد کردن آدرس ایمیل هستید؛ چنین سایت‌ها و سرویس‌هایی ایمیل‌ها را نگه‌داری کرده و بعضاً تبلیغات خود را از این طریق به شما ارسال کرده و حتی گاهی اوقات آنها را به اسپمرها می‌فروشند.

علیرغم قول عدم استفاده تجاری از ایمیل‌ها از سوی این سایت‌ها، گاهی اوقات این اتفاق نیفتاده و به بازدیدکنندگان خیانت می‌شود. فراموش نکنید حتی در صورت متعهد بودن سایت، احتمال هک شدن پایگاه داده و دسترسی هکرها به ایمیل‌ها وجود دارد. یک ایمیل اضافی ساخته و در موارد ضروری آن را در اختیار وبسایت‌ها قرار دهید.

۱۱- عدم استفاده از کلیدهای میانبر

برخی از کاربران آشنایی بسیار کمی با میانبرهای کیبورد داشته و حتی نمی‌دانند فشار دادن کلیدهای Ctrl+C کار کپی و Ctrl+V کار Paste را انجام می‌دهد. البته یادگیری تمامی میانبرهای کیبورد و عادت به استفاده از آنها کار ساده‌ای نیست، اما هر چه میانبرهای بیشتری یاد بگیرید، سرعت شما در انجام کارها بیشتر خواهد شد. از هم‌اکنون ماوس را کنار گذاشته و استفاده از میانبرهای پرکاربرد را آغاز کنید.

۱۲- نصب نرم‌افزارهای غیرضروری

“چرا ویندوزم کند شده؟” این سوالی است که به شنیدن آن عادت داریم و عوامل گوناگونی در بروز آن نقش دارند؛ احتمالاً ۳ نرم‌افزار مجزای پیام‌رسان، ۴ مرورگر اینترنتی مطرح و به همراه ۷ نوارابزار روی هر یک نصب کرده‌اید و فایل‌های زیادی روی دسکتاپ یا پوشه Documents ذخیره نموده‌اید و ...

عده‌ای عادت به تست و بررسی انواع نرم‌افزارهای غیرضروری و ناشناخته مثل انواع و اقسام پخش‌کننده‌های چندرسانه‌ای، ابزارهای امنیتی، مرورگرهای مختلف، بازی، محافظ‌های صفحه نمایش و دیگر موارد مشابه دارند. صرف‌نظر از مسایل امنیتی، نصب انواع ابزارهای غیرضروری مشکلاتی از قبیل کند شدن یا قفل کردن سیستم را برای کاربر به ارمغان می‌آورد. بهتر است چند ابزار مطرح برای نیازهای گوناگون خود در نظر گرفته و تنها از آنها استفاده نمایید.

ضمناً بسیاری از برنامه‌های ناشناخته مثل نوارابزارها به ندرت رد پایی از خود به جا گذاشته و حذف کامل آنها گاهی اوقات غیرممکن است، به طوری که تنها راهکار موجود برای حذف آنها نصب مجدد ویندوز است.

۱۳- بی توجهی به خطرات اینترنت

هر روز اخبار جدیدی در مورد جرایم اینترنتی از قبیل فاش شدن اطلاعات شخصی و قرار گرفتن عکس و فیلم‌های خانوادگی روی اینترنت در رسانه‌ها پخش می‌شود. توصیه اول برای کاهش خطرات اینترنت پرهیز از دوست‌یابی اینترنتی یا حداقل عدم اعتماد به چنین افرادی است.

هیچ‌گاه از تصاویر واقعی در پروفایل خود استفاده نکرده یا آن را

به عنوان آواتار انتخاب نکنید. از قرار دادن فیلم‌ها و عکس‌های خانوادگی در اینترنت اجتناب کنید؛ اگر امکان خرابی چنین داده‌هایی وجود دارد، بهتر است آنها را روی حساب ایمیل یا فضا‌های ابری ذخیره نمایید.

ایمیل یا حساب بانکی خود را از کامپیوترهای عمومی چک نکنید، زیرا احتمال نصب Keylogger □ سخت‌افزاری یا نرم‌افزاری در این سیستم‌ها و در نتیجه فاش شدن اطلاعات حیاتی، بسیار بالاست.

۱۴- استفاده از رمز عبور واحد در کلیه حساب‌های کاربری

بعضی افراد برای تمام حساب‌های کاربری از جمله ایمیل، حساب بانکی، شبکه‌های اجتماعی و ... یک رمز عبور انتخاب می‌کنند. از این رو هکر با دستیابی به رمز عبور یکی از حساب‌های چنین شخصی امکان دسترسی به دیگر حساب‌ها را خواهد داشت.

از سوی دیگر انتخاب رمز عبورهای منحصر به فرد برای هر وبسایتی که در آن ثبت‌نام می‌کنید کار آسانی نیست؛ توصیه می‌کنیم از نرم‌افزارهای مدیریت رمز عبور مثل Roboform استفاده کنید.

ضمناً از قابلیت به خاطر سپاری خودکار رمز عبور در مرورگر نیز استفاده نکنید. امروزه مرورگرهای اینترنتی هدف اول خرابکاران بوده و هر لحظه احتمال نفوذ به آنها و لو رفتن رمز عبورها وجود دارد. در صورت استفاده از کامپیوتر مشترک، ریسک مشاهده رمز عبور توسط دیگران را هم باید به جان خرید.

منبع: computernews.ir