**[پنج راهکار برای جلوگیری از حملات سایبری به رایانه‌ها](http://www.rajanews.com/news/253935/%D9%BE%D9%86%D8%AC-%D8%B1%D8%A7%D9%87%DA%A9%D8%A7%D8%B1-%D8%A8%D8%B1%D8%A7%DB%8C-%D8%AC%D9%84%D9%88%DA%AF%DB%8C%D8%B1%DB%8C-%D8%A7%D8%B2-%D8%AD%D9%85%D9%84%D8%A7%D8%AA-%D8%B3%D8%A7%DB%8C%D8%A8%D8%B1%DB%8C-%D8%A8%D9%87-%D8%B1%D8%A7%DB%8C%D8%A7%D9%86%D9%87%E2%80%8C%D9%87%D8%A7)**

شرکت آمریکایی سیمنتک، پیش‌بینی می‌کند که حملات سایبری در حال افزایش هستند و در این میان، شرکت‌های تجاری بیشتر هدف این حملات قرار خواهند گرفت.

شرکت آمریکایی سیمنتک (Symantec)، بزرگ‌ترین تولیدکننده نرم‌افزارهای امنیتی برای رایانه‌های شخصی در دنیا پیش‌بینی می‌کند که حملات سایبری در حال افزایش هستند و در این میان، شرکت‌های تجاری بیشتر هدف این حملات قرار خواهند گرفت.

این شرکت معروف آمریکایی در اولین نشست برگزار شده با موضوع امنیت سایبری در نیوزیلند اعلام داشت: نوع تجارت و کاری که انجام می‌دهید اهمیت ندارد؛ باید امنیت فناوری اطلاعات رایانه‌ها را در محل کار حفظ نمایید تا از هرگونه سرقت اطلاعات توسط هکرها جلوگیری شود.

سیمنتک همچنین با ارائه گزارشی بیان کرد که مجرمان اینترنتی، شرکت‌های تجاری را هدف قرار می‌دهند و پس از بدست آوردن اطلاعات سری از این شرکت‌ها، از آن‌ها باج‌گیری می‌کنند.

از همین رو، در میان شرکت‌های تجاری نیوزیلند دستور کاری منتشر شده است تا از حمله سایبری قریب‌الوقوع به آن‌ها جلوگیری شود.

راهکارهای ارائه شده در این دستور کاری برای حفاظت از رایانه‌ها در برابر حملات سایبری عبارتند از:

1) از ادمینی استراتور (Administrator) استفاده نکنید؛

2) نرم‌افزارها، پچ‌ها و آپدیت‌ها را به محض منتشر شدن به روز رسانی کنید؛

3) نرم‌افزارهایی که نیاز ندارید از رایانه پاک کنید؛

4) یک آنتی‌ویروس معروف نصب نمایید و آن را در حالت پیشرفته تنظیم کنید؛

5) بک‌آپ گرفتن.



از ادمینی استراتور (Administrator) استفاده نکنید: اولین دلیل برای اینکه از ادمین استراتور استفاده نکنید، کم کردن احتمال قرار گرفتن در معرض بدافزار و ویروس است. اگر با حالت ادمینی استراتور یک برنامه را اجرا نمایید، این برنامه دسترسی کامل و نامحدود به رایانه شما خواهد داشت. در نتیجه، اگر یکی از این برنامه‌ها حاوی یک بدافزار باشد، تمام بخش‌های رایانه، از جمله شبکه رایانه‌ای در معرض این ویروس قرار خواهد گرفت.

نرم‌افزارها، پچ‌ها و آپدیت‌ها را به محض منتشر شدن به روز رسانی کنید: نه تنها ویندوز، بلکه تمام نرم‌افزارهای دیگر هم باید به روز شوند. دقت داشته باشید، به محض اینکه یک پچ جدید برای نرم‌افزارها و ویندوز منتشر می‌شود، هکرها با استفاده از روش مهندسی معکوس نقاط ضعف پچ قدیمی را پیدا کرده و از طریق آن‌ها می‌توانند به رایانه‌هایی که به روز نشده‌اند آسیب وارد کنند.

هر چه زودتر پچ‌های منتشر شده را نصب کنید، احتمال در معرض حمله هکرها قرار گرفتن نیز کمتر می‌شود. همچنین در نظر داشته باشید که تنها پچ‌های میکروسافت نیست که باید نصب شوند، بلکه پچ تمام نرم‌افزارها را باید روی رایانه نصب نمایید.

نرم‌افزارهایی که نیاز ندارید از رایانه پاک کنید: تجربه نشان می‌دهد که اگر به چیزی نیاز ندارید، نباید آن را نصب نمایید. هر چه برنامه‌های بیشتری از رایانه شخصی‌تان پاک کنید، ردپای کمتری برای هکرها باقی گذاشته‌اید. همان‌طور که در بالا قید شد، تمام برنامه‌های غیرضروری در رایانه نیز باید به روز رسانی شوند تا امنیت رایانه حفظ شود، اما اگر نیازی به این نرم‌افزارها ندارید، آن‌ها را پاک کنید.

یک آنتی‌ویروس معروف نصب نمایید و آن را در حالت پیشرفته تنظیم کنید: ما معمولاً افرادی را می‌بینیم که هزینه بالایی برای خرید نرم‌افزار آنتی‌ویروس می‌پردازند، اما پس از نصب برای حفاظت کامل از رایانه آن را تنظیم نمی‌کنند. بنابراین، آنتی‌ویروسی خریداری کنید که در بازار شناخته شده و معروف باشد و مطمئن شوید که به درستی نصب و تنظیمات آن انجام شده باشد تا بهترین حفاظت ممکن را در مقابل بدافزارهای جدید به شما ارائه دهد.

بک‌آپ گرفتن: آخرین مرحله محافظت رایانه در برابر بدافزارها بک‌آپ گرفتن از اطلاعات و بازیابی آن‌ها در مواقع لزوم است. تجربه نشان می‌دهد تا زمانی که شما سه نسخه از اطلاعاتتان را کپی نکرده باشید، نمی‌شود آن را بک‌آپ نامید؛ دو نسخه از اطلاعات در رایانه نگه‌داری می‌شود و نسخه سوم باید خارج از رایانه ذخیره شود.

پس همین اکنون تهدید حملات سایبری را از رایانه‌هایتان دور نمایید.