چند نکته درباره حفظ امنیت رایانه‌های شخصی

روشن کردن دیوار آتش

مهندس سید کاظم بحرینی
رئیس اداره فناوری اطلاعات و ارتباطات معاونت بهداشتی
دانشگاه علوم پزشکی مشهد

مقدمه

هرچند رایانه‌های شخصی باعث راحتی انجام برخی از فعالیت‌های روزمره شده‌اند، ولی همیشه در معرض خطر و تهدیدهایی از جمله ویروس‌ها و بدافزارها، هکرها و حتی مفقود شدن اطلاعات شخصی هستند. بنابراین رعایت برخی توصیه‌ها برای حفظ امنیت رایانه‌های شخصی بسیار مهم است که در ادامه به برخی از آن‌ها اشاره می‌کنیم:

- استفاده از نرم افزارهای محافظتی/ ضد ویروس‌ها و به‌روز نگه داشتن آن‌ها
- باز نکردن نامه‌های دریافتی از منابع ناشناس
- وارد نشدن به سایت‌های ناامن
- استفاده از گذرواژه‌های مناسب و پیچیده
- محافظت از رایانه در برابر نفوذ با استفاده از «دیوار آتش»[1]
- قطع اتصال به اینترنت در مواقع عدم استفاده
- تهیه پشتیبان از داده های مهم و حیاتی سیستم
- بررسی منظم امنیت رایانه

1. firewall

امنیت در سیستم عامل ویندوز

حفظ امنیت در اینترنت و دنیای دیجیتال علاوه بر شباهت‌های آن با دنیای واقعی، تفاوت‌های بزرگی نیز دارد. بنابراین می‌بایست کلیه کاربران نسبت به سیستم‌ها و سرویس‌هایی که با آن‌ها در ارتباط هستند و خطرات محیط دیجیتال و راه‌های جلوگیری، آگاهی اولیه داشته باشند.

یکی از سیستم عامل‌های محبوب روی رایانه‌های رومیزی و لپ‌تاپ‌ها، سیستم عامل ویندوز [1] است. در ادامه موارد مرتبط با حفظ امنیت در سیستم عامل ویندوز را مورد بررسی قرار می‌دهیم.

نصب آنتی ویروس: بعد از نصب سیستم عامل ویندوز، گام بعدی نصب یک آنتی ویروس به‌روز و مطمئن روی سیستم مورد استفاده است.

نصب نرم افزارهای ضد برنامه‌های مخرب: حتی بهترین آنتی ویروس‌ها هم ممکن است برخی نرم افزارهای مخرب را تشخیص ندهند. بنابراین علاوه بر نصب آنتی ویروس که همیشه باید فعال باشد، یک نرم‌افزار برای تشخیص نرم‌افزارهای مخرب روی سیستم و فعال‌سازی آن در بازه‌های زمانی مشخص برای اسکن کامل سیستم، ضروری است.

فعال و تنظیم کردن دیوارآتش: برنامه دیوار آتش هم مانند آنتی ویروس از رایانه مورد استفاده محافظت می‌کند. در حالی‌که نرم‌افزارهای آنتی ویروس، برنامه‌ها و فایل‌های روی رایانه را اسکن می‌کنند، برنامه دیوارآتش ترافیک اینترنت بین رایانه و بقیه شبکه اینترنت را کنترل می‌کند. برای حفظ امنیت در سیستم عامل ویندوز، برنامه دیواره آتش را از طریق بخش Control Panel فعال کنید.

به‌روزکردن: آپدیت یا به‌روزرسانی ویندوز می‌تواند در حالت خودکار قرار گیرد، البته خیلی بهتر است که قبل از دانلود و به‌روزرسانی هر یک از موارد توضیحات آن را خوانده و سپس در صورتی که برای سیستم عامل مشکل ساز نیست آن‌را دانلود و نصب کنیم.

حساب کاربری جداگانه: برای ورود به محیط ویندوز، داشتن دو حساب کاربری مهم است. یک حساب کاربری با دسترسی مدیریت [2] برای نصب و حذف برنامه‌ها و دیگری برای کارهای روزانه.

امنیت و به‌روزرسانی مرورگر: مرورگر هم مانند ویندوز و نرم‌افزارهای نصب شده باید به‌روز رسانی شود. هر افزونه‌ای نباید روی مرورگر نصب شود.

رمزگذاری: اگر رایانه به سرقت رفت یا شخصی توانست به رایانه مورد نظر دسترسی پیدا کند، می‌تواند فایل‌ها و اطلاعات شخصی و مهم را در اختیار بگیرد، بنابراین می‌توان با رمزگذاری فایل‌های مهم یا رمزگذاری سیستم عامل ویندوز خطر دسترسی به اطلاعات مهم را کاهش داد.

رمزعبور: کاربر برای ورود به هر حساب کاربری باید یک رمزعبور پیچیده و منحصر بفرد داشته باشد. بهترین روش استفاده از نرم افزارها یا ابزار مدیریت رمزعبور است.

نکته پایانی

یک سیستم عامل مثل یک مرکز فرماندهی به کاربر اجازه افزایش یا کاهش امنیت و سطوح دسترسی رایانه را می‌دهد. سیستم عامل ویندوز به داشتن نقاط آسیب پذیر فراوان مشهور است، اما اگر کاربر قصد نصب سیستم عامل دیگری مانند لینوکس را نداشته باشد، تنظیمات امنیتی ویندوز تا زمانی که روی حالت پیش فرض هستند هیچ تأثیری در امنیت رایانه مورد استفاده ندارد و باید به شکل شخصی یا سفارشی فعال شوند، بنابراین داشتن آگاهی اولیه در مورد روش‌های بالا بردن امنیت رایانه مورد استفاده و حفاظت از اطلاعات حیاتی و ضروری است.

مرجع:

- چالش‌ها و چشم‌اندازهای امنیت درفضای مجازی، آرشیو SID
- امنیت در سیستم عامل، فرادرس

1. OS Windows
2. Administrator