امنیت در سیستم عامل ویندوز

حفظ امنیت در اینترنت و دنیای دیجیتال علاوه بر شباهت‌های آن با دنیای واقعی، تفاوت‌های بزرگی نیز دارد. بنابراین 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 کامپیوترهای رومیزی و لپ‌تاپ ها، ویندوز (Windows OS) می‌باشد. در ادامه موارد مرتبط با حفظ امنیت در **سیستم عامل ویندوز** را مورد بررسی قرار می دهیم.

۱- **نصب نرم‌افزار آنتی‌ویروس:** بعد از نصب سیستم عامل ویندوز، گام بعدی نصب یک نرم‌افزار آنتی‌ویروس به‌روز و مطمئن روی سیستم مورد استفاده می باشد.

۲- **نصب نرم‌افزارهای ضد نرم‌افزارهای مخرب:** حتی بهترین آنتی‌ویروس‌ها هم ممکن است برخی نرم‌افزارهای مخرب را تشخیص ندهند. بنابراین علاوه بر نصب آنتی‌ویروس (که همیشه باید فعال باشد)، یک نرم‌افزار برای تشخیص نرم‌افزارهای مخرب بروی سیستم و فعال نمودن آن در بازه های زمانی مشخص برای اسکن کامل سیستم، ضروری است.

۳- **فعال و تنظیم کردن Firewall یا دیواره آتش:** برنامه Firewall هم مانند آنتی‌ویروس از کامپیوتر مورد استفاده محافظت می کند. در حالیکه نرم‌افزارهای آنتی‌ویروس، برنامه‌ها و فایل‌های روی کامپیوتر را اسکن می کنند، برنامه دیواره آتش ترافیک اینترنت بین کامپیوتر و بقیه شبکه (اینترنت) را کنترل می کند. برای حفظ امنیت در سیستم عامل ویندوز ، برنامه دیواره آتش را فعال نمایید. این برنامه را از طریق Control Panelفعال یا On کنید. در ویندوز ۱۰، از گزینه Advanced در پنجره به‌روز رسانی ویندوز و گزینهAutomatic را انتخاب نمایید .

٤- **به‌روز کردن:** آپدیت یا به‌روز رسانی ویندوز باید در حالت خودکار قرار گیرد، در قسمت جستجو برنامه‌های در سیستم عامل ویندوز عبارت Windows Update را جستجو و از پنل سمت چپ پنجره باز شده، روی Change settings کلیک و مطمئن شوید Install updates automatically انتخاب شده است.

٥- **حساب کاربری جداگانه:** برای ورود به محیط ویندوز، داشتن دو حساب کاربری مهم است. یک حساب کاربری با دسترسی مدیریت (Administrator) برای نصب و حذف برنامه‌ها و دیگری برای کارهای روزانه.

٦- **امنیت و به‌روز رسانی مرورگر:** مرورگر هم مانند ویندوز و نرم‌افزارهای نصب شده باید به‌روز رسانی گردد. هر اکستنشن یا افزونه‌ای نباید روی مرورگر نصب شود و همچنین جاوا اسکریپت روی مرورگر فقط برای وب‌سایت های مورد اطمینان، فعال شود.

۷- **رمزگذاری:** اگر کامپیوتر به سرقت رفت یا شخصی توانست به کامپیوتر مورد نظر دسترسی پیدا کند، می‌تواند فایل‌ها و اطلاعات شخصی و مهم را در اختیار بگیرد، بنابراین می توان با رمزگذاری فایل‌های مهم یا رمزگذاری سیستم‌عامل ویندوز خطر دسترسی به اطلاعات مهم را کاهش داد.

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

نکته پایانی:

یک سیستم عامل مثل یک مرکز فرماندهی به کاربر اجازه افزایش یا کاهش امنیت و سطوح دسترسی کامپیوتر را می دهد. 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 بر روی حالت پیش فرض هستند هیچ تاثیری در امنیت کامپیوتر مورد استفاده ندارد و باید به صورت شخصی فعال گردد، بنابراین داشتن آگاهی اولیه در مورد روش های بالا بردن امنیت کامپیوتر مورد استفاده و حفاظت از اطلاعات حیاتی و ضروری است.