⏱ زمان تقریبی مطالعه متن: ۸ دقیقه

مقدمه: ویندوز مدرن، نیازمند مدیریت مدرن است

ویندوز 10 و 11 به‌عنوان سیستم‌عامل‌های اصلی میلیون‌ها کاربر در محیط‌های شخصی، کسب‌وکاری و صنعتی، از قابلیت‌های پیشرفته‌ای در حوزه امنیت، عملکرد و یکپارچه‌سازی با سرویس‌های ابری برخوردارند. اما بسیاری از این قابلیت‌ها به‌صورت پیش‌فرض فعال نیستند یا نیازمند تنظیمات دستی دقیق هستند.

در این مقاله، **هفت ترفند حرفه‌ای و اثبات‌شده** برای **افزایش امنیت، بهبود عملکرد و کاهش مصرف منابع** در ویندوز 10 و 11 ارائه می‌شود. این راهکارها برای **کاربران پیشرفته، مدیران شبکه و متخصصان فناوری اطلاعات** طراحی شده و با رعایت استانداردهای امنیتی سازمان‌های بین‌المللی (مانند NIST و Microsoft Security Baselines) تدوین شده‌اند.

---

۱. غیرفعال‌سازی خدمات غیرضروری با استفاده از Group Policy

بسیاری از خدمات پیش‌فرض ویندوز (مانند **Connected User Experiences and Telemetry** یا **Print Spooler**) در صورت عدم استفاده، نه‌تنها منابع سیستم را مصرف می‌کنند، بلکه **ریسک امنیتی** نیز ایجاد می‌کنند.

🔧 روش اجرایی:

1. کلیدهای `Win + R` را فشار دهید و `gpedit.msc` را وارد کنید (در ویندوز 10/11 Pro و بالاتر).
2. مسیر زیر را دنبال کنید:
   `Computer Configuration > Administrative Templates > System > Services`
3. سرویس مورد نظر را انتخاب و آن را روی **Disabled** تنظیم کنید.

🔧 سرویس‌های پیشنهادی برای غیرفعال‌سازی:

- **Connected User Experiences and Telemetry** (DiagTrack)
- **Windows Search** (در صورت عدم استفاده از جستجوی فایل)
- **Secondary Logon** (در محیط‌های ایزوله)
- **Remote Registry** (همیشه غیرفعال باشد)

⚠ **نکته امنیتی:** غیرفعال‌سازی سرویس‌ها باید با دقت انجام شود. برخی سرویس‌ها به سایر ویژگی‌های سیستم وابسته‌اند.

---

۲. فعال‌سازی VBS (Virtualization-Based Security) و Credential Guard

VBS و **Credential Guard** دو فناوری کلیدی در ویندوز 10/11 هستند که از **حملات مدرن مانند Pass-the-Hash** و **Lateral Movement** جلوگیری می‌کنند.

✅ نحوه فعال‌سازی:

1. به **Group Policy** بروید:

```
Computer Configuration > Administrative Templates > System > Device Guard
```

گزینه **Turn On Virtualization Based Security** را فعال کنید. 3. نوع محافظت را روی **Credential Guard** تنظیم کنید.

✅ چرا مهم است؟

این فناوری از یک لایه ایزوله (Hyper-V) برای محافظت از اطلاعات احراز هویت (مانند هش رمز عبور) استفاده می‌کند و حتی در صورت دسترسی هکر به حافظه سیستم، نمی‌تواند اعتبارها را استخراج کند.

---

۳. مدیریت پنجره‌های اعلان (Notifications) بدون نیاز به رجیستری

در ویندوز 10 و 11، اعلان‌ها (Notifications) به‌صورت هوشمند مدیریت می‌شوند و نیازی به تغییر دستی رجیستری نیست.

✅ روش صحیح:

1. به `Settings > System > Notifications` بروید.
2. گزینه **Get notifications from apps and other senders** را غیرفعال کنید.
3. برای برنامه‌های خاص، اعلان را به‌صورت انفرادی مدیریت کنید.

💡 نکته:

استفاده از **Focus Assist** (کمک تمرکز) به جای غیرفعال کردن کامل اعلان‌ها، امکان دریافت هشدارهای مهم را حفظ می‌کند.

---

۴. استفاده از Windows Sandbox برای اجرای فایل‌های ناشناس

Windows Sandbox یک محیط مجازی ایزوله و موقت است که به‌صورت پیش‌فرض در ویندوز 10/11 Pro و Enterprise موجود است.

✅ نحوه فعال‌سازی:

1. به `Turn Windows features on or off` بروید.
2. گزینه **Windows Sandbox** را فعال کنید.
3. سیستم را ریستارت کنید.

🧪 کاربردها:

- تست فایل‌های اجرایی ناشناخته
- بررسی نرم‌افزارهای فیشینگ
- اجرای اسکریپت‌های خطرناک بدون خطر آلوده شدن سیستم اصلی

🔒 محیط پس از بسته شدن به‌طور کامل پاک می‌شود.

---

۵. بهینه‌سازی عملکرد با مدیریت Startup و Background Apps

برخلاف ویندوز XP، در ویندوز 10/11 مدیریت برنامه‌های اتوماتیک از طریق **Task Manager** و **Settings** انجام می‌شود.

روش‌های مدیریت:

1. `Ctrl + Shift + Esc` → تب **Startup**
2. برنامه‌های غیرضروری (مانند Discord، Steam، OneDrive) را **Disable** کنید.
3. به `Settings > Apps > Startup` بروید و برنامه‌های پس‌زمینه را مدیریت کنید.

تأثیر:

کاهش ۳۰ تا ۵۰ درصدی زمان بوت و کاهش مصرف CPU و RAM.

---

۶. استفاده از BitLocker + TPM برای رمزگذاری دیسک

BitLocker یکی از قوی‌ترین ابزارهای رمزگذاری دیسک در ویندوز است که با ترکیب **TPM 2.0**، امنیت بسیار بالایی فراهم می‌کند.

شرایط فعال‌سازی:

- ویندوز 10/11 Pro یا Enterprise
- وجود تراستد پلتفرم ماژول (TPM 2.0)
- داشتن USB برای ذخیره بازیابی کلید

مزایا:

- جلوگیری از دسترسی فیزیکی به داده‌ها
- سازگاری با استانداردهای GDPR و HIPAA
- رمزگذاری خودکار در هنگام بوت

۷. مدیریت پروکسی و شبکه با استفاده از تنظیمات مدرن (Modern Proxy Settings)

در ویندوز 10 و 11، تنظیمات پروکسی از طریق **Settings > Network & Internet > Proxy** مدیریت می‌شود و دیگر نیازی به تنظیم دستی در Internet Options نیست.

✅ گزینه‌های پیشرفته:

- **Automatic proxy setup** با استفاده از PAC File
- **Manual proxy setup** برای شبکه‌های سازمانی
- **Use setup script** برای محیط‌های پیچیده

⚠️ نکته امنیتی:

استفاده از پروکسی‌های ناشناس (مانند Proxify.com) ممکن است حریم خصوصی را فریب دهد. برای امنیت واقعی، از **VPNهای معتبر با رمزنگاری قوی (مثل WireGuard یا OpenVPN)** استفاده کنید.

نکات کلیدی برای مدیریت ویندوز مدرن

- ✅ **از نسخه‌های Pro یا Enterprise استفاده کنید.** نسخه Home امکانات امنیتی و مدیریتی محدودی دارد.
- ✅ **به‌روزرسانی‌های امنیتی را هرگز نادیده نگیرید.** بیش از ۷۰٪ نفوذها از طریق آسیب‌پذیری‌های شناخته‌شده و قابل رفع انجام می‌شود.
- ✅ **از حساب کاربری با دسترسی محدود (Standard User) برای کارهای روزانه استفاده کنید.** فقط در صورت نیاز به حالت Administrator سوئیچ کنید.
- ✅ **فعال‌سازی Windows Defender Application Control (WDAC)** برای جلوگیری از اجرای نرم‌افزارهای غیرمجاز.

پرسش‌های متداول درباره مدیریت ویندوز 10 و 11

آیا Windows Sandbox برای همه کاربران مناسب است؟
بله، اما نیازمند حداقل ۴ گیگابایت RAM و پردازنده با پشتیبانی از Virtualization است. در ویندوز Home نیاز به فعال‌سازی دستی دارد.

تفاوت BitLocker و EFS (Encrypting File System) چیست؟
BitLocker کل دیسک را رمزگذاری می‌کند و با TPM یکپارچه است. EFS فقط فایل‌ها و پوشه‌ها را رمزگذاری می‌کند و برای کاربران شخصی مناسب‌تر است.

آیا غیرفعال کردن Telemetry تأثیری بر عملکرد ویندوز دارد؟
خیر. غیرفعال کردن Telemetry تنها بر ارسال داده‌های تشخیصی به مایکروسافت تأثیر می‌گذارد و بر عملکرد سیستم بی‌تأثیر است.

چگونه مطمئن شویم Credential Guard فعال شده است؟
با اجرای دستور `msinfo32`، بخش **Device Guard Virtualization Based Security** را بررسی کنید. وضعیت باید **Running** باشد.