Window 10 Security
Hidden Feature

JUNE 15 **2024**

COMPUTER LEARNING CENTER
Authored by: ADNAN MAJEED

window 10 security hidden features

Windows 10 has several security features, some of which might not be immediately obvious. Here are some lesser-known security features you can take advantage of to enhance your system's security:

1. Windows Sandbox

- **Feature**: A lightweight, temporary virtual environment for running untrusted applications in isolation.
- **How to enable**:
    1. Go to Control Panel > Programs > Turn Windows features on or off.
    2. Check the box for Windows Sandbox.
    3. Restart your computer.

2. Windows Defender Exploit Guard

- **Feature**: Provides multiple layers of defense against malware, including attack surface reduction, network protection, controlled folder access, and exploit protection.
- **How to enable**:
    1. Go to Settings > Update & Security > Windows Security > App & browser control > Exploit protection settings.
    2. Configure settings according to your needs.

3. Controlled Folder Access

- **Feature**: Protects files and folders from unauthorized changes by ransomware and other malicious apps.
- **How to enable**:
    1. Go to Settings > Update & Security > Windows Security > Virus & threat protection.
    2. Click on Manage ransomware protection.
    3. Toggle on Controlled folder access.

4. Device Guard

- **Feature**: Ensures that only trusted applications run on your device by using hardware-based virtualization.
- **How to enable**: Requires Windows 10 Enterprise and Pro for Workstations.
    1. Configure via Group Policy Editor or Device Guard configuration packages.

5. Credential Guard

- **Feature**: Uses virtualization-based security to isolate and protect secrets so that only privileged system software can access them.
- **How to enable**: Requires Windows 10 Enterprise and Pro for Workstations.
    1. Enable via Group Policy Editor by configuring Computer Configuration > Administrative Templates > System > Device Guard > Turn On Virtualization Based Security.

6. BitLocker Encryption

- **Feature**: Encrypts your entire drive to protect your data from unauthorized access.
- **How to enable**:
    1. Go to Settings > Update & Security > Device encryption.
    2. Toggle on device encryption. (For Pro and Enterprise versions, use BitLocker directly from Control Panel > BitLocker Drive Encryption).

7. Windows Hello

- **Feature**: Provides biometric authentication options, including fingerprint, facial recognition, and PIN.
- **How to enable**:
    1. Go to Settings > Accounts > Sign-in options.
    2. Set up Windows Hello for the authentication method you prefer.

8. Dynamic Lock

- **Feature**: Automatically locks your device when you are away, using Bluetooth-paired devices.
- **How to enable**:
    1. Go to Settings > Accounts > Sign-in options.
    2. Scroll down to Dynamic lock and check the box for Allow Windows to automatically lock your device when you're away.

9. Tamper Protection

- **Feature**: Prevents unauthorized changes to Windows Defender Antivirus settings.
- **How to enable**:
    1. Go to Settings > Update & Security > Windows Security > Virus & threat protection.
    2. Under Virus & threat protection settings, click on Manage settings.
    3. Toggle on Tamper Protection.

10. Advanced Threat Protection (ATP)

- **Feature**: Provides advanced security analytics and endpoint detection and response capabilities.
- **How to enable**: Requires Windows 10 Enterprise E5.
    1. Configure via Microsoft Defender Security Center.

By utilizing these hidden security features, you can significantly enhance the security of your Windows 10 system.