The Daily Signal

Strategic Signal

Practical, adversarial security - without the fluff

Windows Cyber Bunker Playbook

A practical, end-user manual to debloat and harden Windows 10/11 against modern e-crime tactics.

- Default-deny execution: stop most malware families at launch
- Harden Defender (ASR, CFA, reputation): block common attack behaviors
- Resilience: offline backups + system image so you recover fast

Audience: Home/personal users. Usability is secondary to hardening.

Version 1.0 | 16 Dec 2025

Read this first

This playbook is designed to help a typical Windows 10/11 home user harden a PC for web browsing, email, and social media. It prioritizes security over convenience and uses mostly built-in Windows controls plus free/open tools.

Reality check: no Windows system is 100% unhackable. The goal is to remove the easy paths that mass cybercrime relies on, raise the attacker cost, and ensure you can recover quickly if something gets through.

Assumptions

- **Device:** Windows 10 or Windows 11 PC used for home/personal work.
- **User:** general user (internet, email, social media).
- **Priority:** usability is secondary to hardening.
- **Tools:** 99% free/open solutions; paid options are optional.
- **Threats:** phishing, malicious attachments, infostealers, ransomware droppers, and living-off-the-land abuse (PowerShell, wmic, mshta).

What you need

- A USB drive (8GB+) for a recovery drive.
- An external drive for offline backups (recommended).
- Admin access to the PC.
- 30-90 minutes for the initial hardening, plus time for testing/allowlisting.

Table of contents

0. Pre-flight safety (do this first)

These steps reduce the chance of getting locked out or losing data while hardening.

0.1 Create a Windows Recovery Drive (USB)

- Insert a USB drive (8GB+).
- Start menu -> type: **Recovery Drive** -> open it.
- Follow the wizard and create the recovery drive.

0.2 Create a restore point

- Start menu -> type: **Create a restore point**.
- Select drive C: -> click **Create** -> name it **Pre-Hardening**.

0.3 Patch everything

- Settings -> Windows Update -> install all updates.
- Reboot until no more updates are offered.
- Update your browser and any critical apps you keep.

Tip: Hardening changes are safest when applied in phases. After each phase, reboot and verify core functions (Wi-Fi, browser, email).

1. Optional clean base (recommended for maximum confidence)

If this PC is new, used, or you suspect previous compromise, start from a clean base. Hardening a dirty system is like installing locks after someone already lives in your attic.

1.1 Reset this PC

- Settings -> System -> Recovery -> **Reset this PC**.
- Choose **Remove everything** for the cleanest result (back up first).
- After reset, run Windows Update again until fully patched.

1.2 Smart App Control (Windows 11 - optional)

Smart App Control can block unknown/untrusted apps, but it typically requires a clean install/reset to enable. If your priority is strict privacy, you may choose to skip it.

1.3 BIOS/UEFI quick checks (optional but strong)

- Enable **Secure Boot** (usually on by default for Windows 11).
- Ensure **TPM** is enabled (Windows 11 requires TPM 2.0).
- If you are comfortable, set a BIOS/UEFI admin password to prevent unauthorized boot changes.

2. Debloat (reduce attack surface)

Bloat is not just annoying. Extra apps and background services are extra code and extra permissions. Debloating reduces what can be exploited and what can spy on you.

2.1 Uninstall obvious junk (manual)

- Settings -> Apps -> Installed apps.
- Remove OEM trialware, games you do not use, and any unknown toolbars/helpers.
- Reboot.

2.2 Debloat tools (choose one)

Rule: download tools only from their official GitHub repositories. Avoid re-hosted copies.

Option A - BloatyNosy (GUI)

- Run as Administrator.
- Apply a conservative preset first (telemetry + ads off, remove common bloat).
- Reboot, then test Wi-Fi, printing, and your browser.

Option B - Win11Debloat (PowerShell)

- Read the README first and use the default preset.
- Reboot, then test core features.

If something breaks, revert using the tool's restore option or Windows System Restore.

3. Identity and privilege (stop malware at the permission boundary)

Most attacks succeed because the user session has too much power. Your goal is to make 'running code' not equal 'owning the system'.

3.1 Create two accounts: one admin, one daily user

- Keep one Admin account for system changes (used rarely).
- Create a **Standard** account for daily use (browser, email, social).
- Use the Standard account by default.

Why this matters: if malware runs under a Standard account, it has fewer privileges to install services, tamper with security settings, or persist system-wide.

3.2 Set UAC to the strictest setting

- Start menu -> type **UAC** -> open **Change User Account Control settings**.
- Set to **Always notify**.

3.3 Disable or rename the built-in Administrator account (advanced)

- Windows Pro: Local Users and Groups (lusrmgr.msc) -> Users -> Administrator -> disable or rename.
- Windows Home: use Computer Management alternatives or PowerShell; if unsure, leave it disabled by default and protect your admin account with a strong password.

3.4 Authentication hygiene

- Use a password manager (e.g., KeePassXC) and unique passwords everywhere.
- Enable 2FA on email first, then social networks and financial services.
- Never type passwords after clicking a link in email - navigate manually instead.

4. Built-in protections (turn the strong stuff ON)

Windows includes serious defenses. The difference between 'default' and 'armored' is configuration.

4.1 Microsoft Defender - verify core protections

- Open **Windows Security** -> Virus & threat protection -> Manage settings.
- Ensure these are ON: Real-time protection, Cloud-delivered protection, Automatic sample submission, Tamper Protection.

4.2 Reputation and SmartScreen

- Windows Security -> App & browser control -> Reputation-based protection settings.
- Turn ON: Check apps and files, SmartScreen for Microsoft Edge, and potentially unwanted app (PUA) blocking.

4.3 Enable PUA blocking (PowerShell - optional but strong)

```
Set-MpPreference -PUAProtection Enabled
```

4.4 Core isolation: Memory integrity (if supported)

- Windows Security -> Device security -> Core isolation details.
- Turn ON **Memory integrity** and reboot.
- If incompatible drivers are listed, update or uninstall them and try again.

4.5 LSA protection (credential hardening)

- Windows Security -> Device security (or Local Security Authority protection, if shown).
- Enable Local Security Authority (LSA) protection when available and reboot.

4.6 Controlled Folder Access (anti-ransomware)

- Windows Security -> Virus & threat protection -> Ransomware protection -> Manage ransomware protection.
- Turn ON **Controlled folder access** (Block mode).
- If legitimate apps are blocked from saving, add them under **Allow an app through Controlled folder access**.

```
# Alternative method
Set-MpPreference -EnableControlledFolderAccess Enabled
```

4.7 Drive encryption (data protection if device is stolen)

- Windows Pro: enable **BitLocker** on the system drive.

- Windows Home: if 'Device encryption' is available, enable it; otherwise consider VeraCrypt for sensitive folders.

5. Attack Surface Reduction (ASR): break common attack chains

ASR rules are behavior controls in Microsoft Defender that block techniques used by modern malware (especially phishing -> script -> payload chains).

Recommended rollout: start in **Audit** mode for 24-48 hours, then switch to **Block**. Audit shows what would have been blocked so you can fix false positives first.

5.1 Recommended core ASR rules

ASR rule (recommended core set)	GUID
Block abuse of exploited vulnerable signed drivers	56a863a9-875e-4185-98a7-b882c64b5ce5
Block all Office apps from creating child processes	d4f940ab-401b-4efc-aadc-ad5f3c50688a
Block credential stealing from LSASS	9e6c4e1f-7d60-472f-ba1a-a39ef669e4b2
Block executable content from email client and webmail	be9ba2d9-53ea-4cdc-84e5-9b1eeee46550
Block execution of potentially obfuscated scripts	5beb7efe-fd9a-4556-801d-275e5ffc04cc
Block JavaScript or VBScript from launching downloaded executables	d3e037e1-3eb8-44c8-a917-57927947596d
Block Office apps from creating executable content	3b576869-a4ec-4529-8536-b80a7769e899
Block Office apps from injecting code into other processes	75668c1f-73b5-4cf0-bb93-3ecf5cb7cc84
Block persistence through WMI event subscription	e6db77e5-3df2-4cf1-b95a-636979351e5b

5.2 Enable the rules (PowerShell - Block mode)

```
$rules = @(
"56a863a9-875e-4185-98a7-b882c64b5ce5",
"d4f940ab-401b-4efc-aadc-ad5f3c50688a",
"9e6c4e1f-7d60-472f-ba1a-a39ef669e4b2",
"be9ba2d9-53ea-4cdc-84e5-9b1eeee46550",
"5beb7efe-fd9a-4556-801d-275e5ffc04cc",
"d3e037e1-3eb8-44c8-a917-57927947596d",
"3b576869-a4ec-4529-8536-b80a7769e899",
"75668c1f-73b5-4cf0-bb93-3ecf5cb7cc84",
"e6db77e5-3df2-4cf1-b95a-636979351e5b"
)
$actions = @(1) * $rules.Count   # 1 = Block

Add-MpPreference `
  -AttackSurfaceReductionRules_Ids $rules `
  -AttackSurfaceReductionRules_Actions $actions
```

5.3 Switch to Audit mode (if you want to test first)

```
# 2 = Audit
$actions = @(2) * $rules.Count

Add-MpPreference `
  -AttackSurfaceReductionRules_Ids $rules `
  -AttackSurfaceReductionRules_Actions $actions
```

5.4 If something breaks

- First try Audit mode to identify what rule is involved.
- If a legitimate app is blocked, update it or add an exception only when you fully trust the app.
- Avoid broad exclusions like excluding your entire Downloads folder.

6. Execution blocking (default-deny): stop malware at launch

Most commodity malware executes from user-writable locations (Downloads, Temp, email attachment caches, USB). Default-deny execution blocks these paths so malware cannot start.

6.1 Recommended: Hard_Configurator (SRP-based)

- Download Hard_Configurator from its official GitHub.
- Run as Administrator.
- Apply the **Recommended** profile first, then reboot.
- Test your normal workflow (browser, email, office apps).

Expect friction: installers and portable tools launched from Downloads may be blocked. This is a feature.

6.2 Create a trusted install/work folder

- Create a folder such as **C:\Tools\Trusted** (or another folder you control).
- Move installers/tools you intentionally want to run into this folder before running them.
- Keep this folder small and tidy: only software you trust.

6.3 Windows Pro alternatives (advanced)

- **AppLocker** or **WDAC** can enforce allowlisting more strictly than SRP, but they require careful design.
- If you are not comfortable managing allowlists, stick with SRP + Defender ASR.

6.4 Disable high-risk remote features (quick win)

- Turn off Remote Desktop unless you truly need it (Settings -> System -> Remote Desktop -> Off).
- Avoid enabling SMB file sharing on a home PC unless required.

7. Browser hardening (the most abused attack surface)

Most compromises start in the browser. The goal is to reduce what the browser can run, reduce what it can reach, and contain it when things go wrong.

7.1 Install a strong content blocker

- Install **uBlock Origin** (official store listing).
- Keep filter lists updated (default lists are fine for most users).

7.2 Use safer browsing defaults

- Enable the browser's phishing/malware protection (Safe Browsing / SmartScreen).
- Turn on HTTPS-only mode where available.
- Disable or remove unnecessary extensions. Fewer extensions = fewer risks.

7.3 Separate profiles for risky vs sensitive activity

- Create a dedicated browser profile for email + social media.
- Use a separate profile (or separate browser) for banking/financial logins.
- Do not store passwords in the browser - use a password manager instead.

7.4 Isolation options

- **Windows Sandbox** (if available): use it to open unknown links/files and discard the environment after.
- **Sandboxie Plus**: run your browser inside a sandbox and wipe it periodically.

Rule: treat unexpected downloads as hostile. Save, scan, and only run from your trusted folder.

8. Network hardening (block bad infrastructure early)

Network controls can stop threats before they ever reach the device, and can cut off command-and-control (C2) if something slips through.

8.1 Use DNS filtering (router-level preferred)

- Set a security-focused DNS resolver on your router so all devices benefit.
- If you cannot change the router, set DNS on the Windows network adapter instead.

8.2 Windows: set DNS on the adapter (generic steps)

- Settings -> Network & internet -> select your connection -> DNS server assignment -> Edit.
- Choose Manual -> enable IPv4 -> enter your chosen DNS servers -> Save.

8.3 Firewall discipline

- Keep Windows Defender Firewall enabled on all profiles (Public/Private).
- Do not allow inbound rules unless you understand why they exist.
- If you want outbound alerts and are comfortable with prompts, consider a firewall controller (advanced).

8.4 Defender Network Protection (optional)

Defender can block access to known malicious domains/IPs as an additional layer.

```
Set-MpPreference -EnableNetworkProtection Enabled
```

8.5 Router quick wins (if you control the router)

- Change the router admin password and disable remote management.
- Disable UPnP if you do not need it.
- Keep router firmware updated.
- Use WPA2/WPA3 with a strong Wi-Fi password.

9. Backups and recovery (assume breach, survive anyway)

Ransomware groups target backups. If your backups are always connected and writable, they can be encrypted too. The goal is survivable backups and fast recovery.

9.1 Follow the 3-2-1 rule

- 3 copies of important data
- 2 different media types (e.g., internal drive + external drive)
- 1 copy offline (disconnected) or immutable

9.2 Offline backup routine (recommended)

- Use an external drive for backups.
- Connect it only during backup, then safely eject and disconnect.
- Keep it physically separate when not backing up.

9.3 Create a system image after hardening

- After your system is stable, create a full system image so you can restore the hardened baseline quickly.
- Store the image on an external drive that is not always connected.

9.4 Test your restores

- Restore a few files as a test.
- Verify you can boot from your recovery USB.

Mindset: recovery speed beats perfection. A system that can be rebuilt fast is far safer than a system that hopes nothing ever goes wrong.

10. Verification checklist (confirm your armor is actually on)

10.1 Quick visual checks

- Windows Security: no warnings, Defender active.
- Controlled Folder Access: ON (Block).
- Core isolation Memory integrity: ON (if supported).
- SmartScreen / reputation protection: ON.

10.2 PowerShell checks

Open PowerShell and run:

```
Get-MpPreference
```

Look for: PUAProtection enabled, ControlledFolderAccess enabled, ASR rules populated, NetworkProtection enabled (if configured).

10.3 Test default-deny behavior (safe test)

- Download a harmless portable tool to Downloads.
- Attempt to run it. It should be blocked by SRP/Hard_Configurator if configured.
- Move it into your trusted folder and run again (only if you trust it).

11. Daily operating rules (non-negotiable habits)

Hardening buys you safety, but habits keep it. These rules prevent the most common e-crime tactics from succeeding.

- **Email:** never open unexpected attachments directly. Save -> scan -> open (preferably in a sandbox).
- **Links:** never sign in after clicking an email link. Navigate manually (bookmark or type the site).
- **Documents:** never enable macros unless you completely trust the source and you asked for the file.
- **Software:** do not install cracked/pirated software - it defeats your defenses.
- **Passwords:** use a password manager + 2FA; change reused passwords immediately.
- **Updates:** apply Windows/browser updates promptly.
- **Backups:** keep the offline backup routine. Disconnect backup drives when done.

Appendix A. Troubleshooting common friction

A1. An app cannot save files (Controlled Folder Access)

- Windows Security -> Virus & threat protection -> Ransomware protection -> Manage ransomware protection.
- Select **Allow an app through Controlled folder access** and add the specific application.
- Prefer allowlisting the exact app, not disabling Controlled Folder Access.

A2. A legitimate tool is blocked from running (SRP/default-deny)

- Move the tool/installer into your trusted folder (e.g., C:\Tools\Trusted) and run from there.
- If you must run from Downloads, you are weakening the model - avoid it.

A3. Something breaks after enabling ASR rules

- Switch ASR rules to **Audit** temporarily and reproduce the issue.
- Identify the offending rule and update the blocked application.
- Only add exceptions if you fully trust the application and understand the impact.

A4. Memory integrity will not enable

- Windows will list incompatible drivers. Update the drivers from the device vendor.
- If the device is optional, uninstall the driver/software and retry.

A5. You get locked out / something goes seriously wrong

- Use Windows System Restore to roll back to **Pre-Hardening**.
- Boot from your recovery USB if Windows will not start.
- If needed, restore from your system image.

Appendix B. One-page hardening checklist

Use this page to track progress. Apply changes in phases and test after each reboot.

	Item
[ ]	Recovery USB created
[ ]	Restore point created (Pre-Hardening)
[ ]	Windows fully updated (rebooted until clean)
[ ]	Debloat performed (manual + tool)
[ ]	Daily Standard account created and used
[ ]	UAC set to Always notify
[ ]	Defender: cloud + tamper protection enabled
[ ]	SmartScreen/reputation enabled, PUA blocking enabled
[ ]	Memory integrity enabled (if supported)
[ ]	Controlled Folder Access enabled and tested
[ ]	ASR rules enabled (Audit then Block)
[ ]	Execution blocking enabled (SRP/Hard_Configurator)
[ ]	Browser hardened (uBlock, fewer extensions, isolation)
[ ]	DNS filtering set (router or PC)
[ ]	Offline backups established (3-2-1) + system image created

Legal disclaimer

Educational use only. This document is provided for informational and educational purposes and does not constitute professional security, legal, or compliance advice.

Applying system-hardening changes can cause software incompatibilities, reduced functionality, loss of access, or data loss. You are responsible for testing changes in your own environment, maintaining backups, and verifying that your configuration meets your needs.

No security guidance can guarantee that a system will be free of compromise. Threats evolve, software changes, and the effectiveness of any configuration depends on correct implementation, ongoing patching, and safe user behavior.

To the maximum extent permitted by law, the author and publisher disclaim any liability for damages, losses, or claims arising from the use of this document.

Do not use this material to harm others. The techniques described are defensive in nature and should be used only to protect systems you own or are authorized to administer.

Brand: The Daily Signal - Strategic Signal