The Grumpy Sysadmin

Windows Security Quick-Start Checklist

Lock down basic Windows security settings before one bad click turns into a really expensive lesson.

Before you trust your Windows PC, slow down. Windows may include solid security tools, but that doesn't mean they're configured, updated, or being used correctly. This quick-start checklist covers the first things to verify before malware, scams, bad downloads, or account problems turn into a much bigger mess.

> ***Grumpy Rule: Windows security isn't one magic button. If you never check updates, Defender, firewall, accounts, encryption, browsers, and remote access tools, you're not protected. You're just hoping the next bad click politely leaves you alone.***

1. Confirm Windows Security Is Actually On

Start with the built-in protection Windows already has. Don't assume it's working just because the icon's not screaming at you.

Security Check	Done
Windows Security opens without errors	☐
Virus & threat protection shows no action needed	☐
Real-time protection is turned on	☐
Cloud-delivered protection is turned on	☐
Tamper Protection is turned on	☐
Protection updates are current	☐
No expired trial antivirus or fake security tool is replacing Defender	☐

> ***Grumpy Rule: A security warning you ignore isn't a warning anymore. It's foreshadowing.***

2. Install Updates Without Letting Windows Ambush You

Security updates matter, but blindly clicking everything isn't a plan either. Update deliberately and restart when needed.

Update Check	Done
Windows Update has been checked recently	☐
Pending security updates are installed	☐
The PC has been restarted after updates, not just shut down	☐
Failed updates are not being ignored in a loop	☐
Active Hours are set to avoid surprise restarts	☐
Optional driver updates aren't installed blindly	☐
Browsers and important apps are updated too	☐

> ***Grumpy Rule: Ignoring updates forever isn't stability. It's leaving the front door open because the lock occasionally annoys you.***

3. Check Firewall and Network Profile

The firewall should be on, and Windows should know whether you are on a trusted home network or some other random network with questionable life choices.

Firewall / Network Check	Done
Windows Firewall is on for Domain, Private, and Public profiles	☐
Home network is set to Private only if you actually trust it	☐
Coffee shop, hotel, airport, and public Wi-Fi use Public profile	☐
Firewall allow-list doesn't include apps you don't recognize	☐
Remote Desktop is off unless you intentionally use it	☐
No random port forwarding was created to "fix" an app	☐

Grumpy Rule: Turning off the firewall to fix a problem is like removing the front door because the doorknob squeaked.

---

4. Stop Running Everything as Administrator

Using an administrator account for daily browsing, email, and downloads gives every bad decision a much bigger blast radius.

Account Check	Done
Your daily Windows account type has been checked	☐
A separate administrator account exists for maintenance	☐
The administrator account has a strong password	☐
Daily use is done from a standard account when possible	☐
User Account Control has not been disabled	☐
Family or guest accounts are not administrators by default	☐

Grumpy Rule: Running as admin all day's convenient in the same way driving without brakes is convenient. Right up until it's not.

---

5. Save Encryption and Recovery Details

BitLocker and Device Encryption can protect your data, but only if you know where the recovery key is before Windows asks for it.

Encryption / Recovery Check	Done
BitLocker or Device Encryption status has been checked	☐
Recovery key is saved somewhere safe	☐
Microsoft account password and recovery access are confirmed	☐
You know which device the recovery key belongs to	☐
A current backup exists before changing encryption settings	☐
Laptop is plugged in before encryption changes or major updates	☐

Grumpy Rule: Encryption without a recovery key isn't protection. It's a locked door with the key thrown into a volcano.

---

6. Clean Up Browsers, Downloads, and Remote Access Tools

A lot of real-world infections and scams start in the browser, the Downloads folder, or a remote access tool someone forgot was installed.

Browser / Remote Access Check	Done
Primary browser is fully updated	☐
Unneeded or suspicious browser extensions are removed	☐
Password manager or saved password access is confirmed	☐
Downloads folder has been reviewed for installers and junk	☐
AnyDesk, TeamViewer, Chrome Remote Desktop, and similar tools are checked	☐
Remote access tools you don't use are removed	☐
You know never to let a stranger remote into your PC from a pop-up or phone call	☐

> ***Grumpy Rule: If a stranger on the phone wants remote access to your PC, the correct technical response is absolutely not.***

Final "Don't Ignore This" Check

Final Check	Done
Windows Security shows no action needed	☐
Windows Update is current and the PC has been restarted	☐
Firewall is on and the network profile makes sense	☐
Admin account setup has been reviewed	☐
BitLocker/device encryption recovery key is saved if encryption is enabled	☐
Browsers and extensions have been reviewed	☐
Remote access tools have been checked	☐
Important files are backed up before major changes	☐

If any critical box is unchecked, stop. Fix the basics before you pretend your PC is "secure enough."

> ***Grumpy Rule: Security isn't about doing one dramatic thing. It's about not leaving seven obvious things broken at the same time.***

After You Tighten Security: Verify Before You Celebrate

Security changes should reduce risk, not break the computer. After making changes, confirm the things you rely on still work.

After-Security Check	Done
Internet and Wi-Fi still work normally	☐
Printer, scanner, VPN, and network access still work if used	☐
Important apps still open correctly	☐
Browser bookmarks and password manager still work	☐
Backups still run and can be opened	☐
Windows Security still shows no action needed	☐

> ***Grumpy Rule: The job isn't done when you flip a setting. It's done when the PC's safer and still usable. Revolutionary concept, I know.***

Want the Full Windows Security Hardening Playbook?

This free quick-start checklist covers the first security checks every Windows user should make. The full playbook goes deeper and walks through the settings, decisions, recovery details, and maintenance routine that are easiest to miss.

Full Playbook Includes	Covered
Step-by-step Windows Security and Microsoft Defender walkthrough	☐
Windows Update, restart, and optional update guidance	☐
Firewall and network profile explanations	☐
Administrator vs standard account setup guidance	☐
BitLocker/device encryption recovery key instructions	☐
Browser, download, and extension cleanup steps	☐
Remote access tool audit and scam prevention guidance	☐
Monthly security maintenance checklist	☐
Emergency “I think I clicked something bad” checklist	☐
Companion video walkthrough showing where the settings are	☐

Grumpy Rule: The free checklist is enough to point you at the obvious problems. The full playbook is the better plan when you want to actually understand what you are changing and why.

Get the full Windows Security Hardening Playbook
or the Ultimate Windows Survival System
https://thegrumpysysadmin.com/fixmypc

Final Word

You don’t need to turn your home computer into a government bunker. You do need the basics checked, the obvious holes closed, and a simple routine so things don’t drift back into chaos.

Windows security doesn’t stay fixed on its own.
Check it now.
Review it monthly.
Stay grumpy.