

COMPLETE DIGITAL SECURITY SYSTEM

Secure Your Digital Life in 7 Days

Your START HERE guide and step-by-step roadmap

A practical home cybersecurity system for normal people

Seven focused security missions. Matching Quick-Start Checklists. Detailed Playbooks. One clear order of operations so you always know what to do next.

This guide is the roadmap for the entire Complete Digital Security System. Don't try to read every PDF before you begin. Start here, complete the days in order, and use the matching checklist and playbook when this guide tells you to.

Security should be useful, not theatrical. The goal isn't to become a security engineer, it's to make yourself substantially harder to compromise — and much easier to recover when something still goes wrong.

How to Use the Complete Digital Security System

You now have more than a single security guide. You have a complete set of focused checklists and playbooks covering the parts of your digital life that matter most. The purpose of this **START HERE** guide is to keep all the material from becoming one enormous pile of PDFs.

The system is organized into seven security missions. Complete them in order. You can do one mission per day, one per weekend, or spread them across seven sessions. The order matters more than the calendar.

Every day follows the same path

1. READ THE DAY'S MISSION in this guide. This gives you the goal, priorities, and the minimum work that should be completed.
2. OPEN THE QUICK-START CHECKLIST for that topic. Keep it beside you while you work and use it to track the important actions.
3. USE THE FULL PLAYBOOK for the detailed walkthrough, explanations, options, warnings, and maintenance guidance.
4. RETURN TO THIS GUIDE and complete the VERIFY IT section. Security isn't finished just because you changed a setting.
5. STOP WHEN THE DAY IS COMPLETE. Each mission ends with a clear definition of what "done" means so you're not left wondering whether you missed something.

Short on time?

Complete the Quick-Start Checklist first. That gives you the highest-priority work. Then return to the full Playbook when you have time to go deeper. Don't skip the verification steps.

The three layers of the system

- THE ROADMAP — this guide tells you what to do, in what order, and when a mission is complete.
- THE QUICK-START CHECKLISTS — the fastest path through the most important actions.
- THE PLAYBOOKS — the detailed "how and why" for each security area, including recovery and maintenance.

Don't turn security into a reading assignment. Use the material while you're actually securing your devices and accounts.

Before You Start

Don't begin by changing every password you own, turning on every security feature you can find, and then discovering you've locked yourself out of your email on three devices. Security changes can create their own problems when they're rushed.

Set aside these basics first

- ☐ A password manager you can access and understand.
- ☐ Access to your primary email account and its recovery options.
- ☐ Your smartphone, because many accounts use it for MFA, recovery, or identity verification.
- ☐ A safe place to store recovery codes and emergency instructions.
- ☐ Access to your router administration page or ISP app.
- ☐ Access to your important financial, cloud-storage, shopping, and phone-carrier accounts.
- ☐ A current backup of anything you can't replace.

IMPORTANT WARNING

Before changing passwords, MFA methods, encryption settings, recovery email addresses, or phone numbers, verify that you know how you'll get back in if the primary method fails.

A note about the seven "days"

A day is a security mission, not a stopwatch. Some people will complete a mission quickly. Others will need more time because they have more devices, more accounts, or more complicated setups. Finish the mission correctly instead of rushing to keep an arbitrary schedule.

"I know the password is around here somewhere" isn't a recovery plan. Neither is hoping your phone never breaks.

Your 7-Day Security Map

Day	Mission	Primary Materials	Goal
Day 1	Lock Down Windows	Windows Security + Browser Privacy	Close the obvious holes on the computer you use every day.
Day 2	Secure the Accounts That Control Everything	Account Lockdown	Protect email, passwords, MFA, recovery, financial accounts, cloud storage, and your phone carrier.
Day 3	Lock Down Your Home Network	Home Wi-Fi & Router Lockdown	Secure the router, Wi-Fi, guest access, firmware, and connected devices.
Day 4	Secure Your Smartphone	Smartphone Security	Protect the device that receives codes, resets passwords, stores personal data, and follows you everywhere.
Day 5	Build Your Scam & Identity Defenses	Scam & Phishing + Identity Theft & Fraud	Make fraud harder, recognize manipulation faster, and prepare before identity theft happens.
Day 6	Protect Your Files and Backups	Backup & Ransomware Recovery	Make sure ransomware, hardware failure, theft, or one bad click doesn't get the only copy of your files.
Day 7	Build Your Security Emergency Plan	Security Emergency Response	Know what to do first when an account is compromised, a device disappears, or something feels wrong.

When you finish Day 7, use the Security Checkup near the end of this guide as your final audit. Then keep the Maintenance Routine and Emergency Security Card somewhere you can actually find them later.

DAY 1 — Lock Down Windows

Your Windows PC is where email, banking, tax documents, photos, browser sessions, saved credentials, downloads, and years of accumulated digital clutter tend to meet. Start here because an insecure computer can undermine everything else you secure later.

TODAY'S MATERIALS

1. START WITH: Windows Security Hardening Quick-Start Checklist

Use this to identify and complete the highest-priority Windows protections.

2. GO DEEPER WITH: Windows Security Hardening Playbook

Use the full walkthrough for Windows Security, Defender, firewall, accounts, encryption, remote access, maintenance, and recovery considerations.

3. THEN REVIEW: Browser & Online Privacy Lockdown Quick-Start Checklist + Guide

Your browser is one of the most exposed applications on the PC. Use this companion module to review extensions, privacy, permissions, saved credentials, downloads, and tracking settings.

DO THIS TODAY

- ☐ Install current Windows security updates and restart the PC if required.
- ☐ Confirm Microsoft Defender Antivirus is active — or confirm your reputable third-party security product is installed, active, and fully updated.
- ☐ Confirm the Windows firewall is enabled.
- ☐ Review the current network profile and make sure public networks aren't treated as trusted private networks.
- ☐ Review administrator accounts and remove or investigate forgotten or mystery admin accounts.
- ☐ Confirm device encryption or BitLocker status and save the recovery key somewhere you can access without the PC.
- ☐ Review installed remote-access tools and remove old tools you no longer use.
- ☐ Remove obviously unwanted or abandoned software that increases attack surface.
- ☐ Review browser extensions, privacy settings, permissions, saved credentials, and download behavior using the Browser & Online Privacy materials.

VERIFY IT

- ☐ Windows Security shows no unresolved protection warnings you don't understand.
- ☐ You can locate the BitLocker/device-encryption recovery key without relying on memory.
- ☐ You know which user accounts are administrators and why.
- ☐ You can identify every remote-access application intentionally installed on the PC.
- ☐ Your normal browser still works, important sites open correctly, and you recognize the extensions that remain installed.

YOU'RE DONE FOR TODAY WHEN...

- ☐ Windows and its security tools are current.
- ☐ Firewall, network profile, administrator accounts, and encryption/recovery are understood.
- ☐ Remote-access tools and unnecessary software have been reviewed.
- ☐ Your browser and extensions have been deliberately reviewed instead of simply assumed to be safe.

Windows security isn't finished because the shield icon is green. The goal is a secure machine you can still use and recover.

SAMPLE
thegrumpysysadmin.com — full version has 21 guides, 239 pages

Windows Security Hardening Playbook

Step-by-step Windows security settings for regular users who want better protection without breaking their PC.

The free checklist shows you what to check. This playbook shows you how to actually check it, what the settings mean, what to change, what not to touch, and how to avoid turning a five-minute security check into a Whole Saturday.

Who this is for

Home Windows users, family tech helpers, small-office users, and anyone who wants better Windows security without needing an enterprise cybersecurity department or a panic room full of blinking lights.

Important warning

Security changes can affect how your PC behaves. Read each section before changing settings. Back up first. Save recovery keys before touching encryption. Don't blindly disable features because a random internet comment said it made Windows faster.

Contents

1. Start Here: How to Use This Playbook
2. Before You Change Anything
3. Windows Security and Microsoft Defender
4. Windows Update Security Settings
5. Firewall and Network Profile
6. Admin vs Standard Accounts
7. BitLocker, Device Encryption, and Recovery Keys
8. Browser Security and Download Safety
9. Remote Access Tools and Scam Risk
10. Installed Apps and Junk Security Tools
11. Microsoft Account Security Basics
12. Monthly Security Maintenance Routine
13. Emergency Plan: I Think I Clicked Something Bad
14. Final Windows Security Hardening Checklist
15. Worksheets and Printables

Grumpy Rule: Do not try to harden Windows by randomly clicking every scary-looking setting. That is not security. That is button mashing with consequences.

The Grumpy Sysadmin

Account Lockdown Playbook

Step-by-step account security, password manager, MFA, and recovery planning for regular users who want better protection without locking themselves out.

What this playbook helps you do

Lock down the accounts that control your email, passwords, MFA, recovery codes, banking, cloud storage, shopping, phone carrier, and emergency access plan.

Who this playbook is for

Home users, family tech helpers, creators, small-office users, and anyone who depends on email, banking, cloud storage, shopping accounts, or a password manager and doesn't want one bad password, lost phone, or missing recovery code to turn into a locked-out disaster.

You don't need to become a cybersecurity expert. You just need a sane order of operations, a recovery plan, and fewer accounts running on vibes.

Use this before something goes wrong

Use this playbook before you change phones, switch password managers, turn on MFA everywhere, clean up old passwords, help a family member secure accounts, or respond to a suspicious login alert.

The goal is simple: lock the important accounts down first, save the recovery options, and make sure you can still get back in.

Important warning

Account changes can lock you out if you move too fast. Confirm password manager access, recovery email, phone access, and backup MFA methods before changing critical accounts.

Lock it down now. Recover faster later. Stay grumpy.

Contents

1. Start Here: How to Use This Playbook
2. Before You Change Anything
3. Build Your Account Priority Map
4. Lock Down Your Main Email Account First
5. Set Up a Password Manager Without Creating a New Disaster
6. Create a Master Password and Emergency Access Plan
7. Replace Reused Passwords in the Right Order
8. Turn On MFA Without Locking Yourself Out
9. Use Passkeys and Security Keys When They Make Sense
10. Save Recovery Codes and Backup Access
11. Lock Down Your Phone Carrier Account
12. Secure Microsoft, Google, and Apple Accounts
13. Secure Banking, Credit Card, Shopping, and Cloud Accounts
14. Clean Up Browsers, Saved Passwords, and Extensions
15. Review Devices, Sessions, Login Activity, and Forwarding Rules
16. Recognize Phishing, Fake Logins, and MFA Prompt Attacks
17. Emergency Plan: Lost Phone, Stolen Password, or Suspicious Login
18. Family and Trusted-Person Emergency Access
19. Monthly Account Security Maintenance Routine
20. Final Account Lockdown Checklist
21. Worksheets and Printables

Grumpy Rule: Don't try to fix every account on the internet in one afternoon. Start with the accounts that can reset, empty, or lock up everything else.

Home Wi-Fi & Router Lockdown Guide

Lock down the router, Wi-Fi, smart devices, and internet-facing settings protecting your home.

What this guide helps you do

- Secure router admin access and cloud/app accounts.
- Choose safer Wi-Fi names, passwords, and WPA2/WPA3 settings.
- Separate guests and smart devices from your main network where practical.
- Review risky convenience features like WPS, UPnP, remote management, and port forwarding.
- Build a simple connected-device inventory and monthly review habit.

Grumpy Rule

The goal isn't to become a network engineer. The goal is to stop trusting a router nobody has checked since it came out of the box.

Lock it down now. Troubleshoot less later. Stay grumpy.

Home Wi-Fi & Router Lockdown Guide

A plain-English walkthrough for securing the home network that protects your laptops, phones, cameras, TVs, printers, and mystery gadgets.

Use this before something gets weird

Your router is the front door for almost every connected device in your house. This guide walks you through what to check, what to change, what to leave alone, and how to verify the house still has working internet when you are done.

How to use this guide

Do one section at a time, test the network, then move on. Don't change seven router settings at once unless you enjoy turning a ten-minute fix into a weekend archaeology project.

Who This Guide Is For

This guide is for home users who want a safer Wi-Fi network without becoming full-time network engineers. It's also useful for small home offices, remote workers, and families with a pile of phones, laptops, smart TVs, cameras, game consoles, printers, and mystery devices connected to the same router.

It assumes you are using a normal consumer router, ISP gateway, or mesh Wi-Fi system from companies like ASUS, TP-Link, Netgear, eero, Google/Nest, Linksys, Ubiquiti, or your internet provider. The exact screen names will vary, because router companies apparently enjoy hiding the same setting under twelve different labels.

The Lockdown Order

Do the work in this order. It keeps you from changing a risky setting first and then losing the ability to sign back in.

1. Identify your router, mesh system, modem, and provider equipment.
2. Save or screenshot current settings before changing anything important.
3. Secure router admin access and any cloud/app account.
4. Fix the main Wi-Fi name, password, and encryption.

The Grumpy Sysadmin

Scam & Phishing Defense Guide

Spot fake warnings, phishing emails, fake support calls, and account takeover tricks before they wreck your day.

What this guide helps you do

Recognize fake browser warnings, support scams, suspicious emails, fake login pages, MFA prompt attacks, remote-access tricks, money scams, and the first steps to take if you already clicked, called, installed, approved, or paid.

Who this guide is for

Home users, family tech helpers, creators, small-office users, and anyone who wants a simple scam-defense plan without turning every email into a courtroom investigation.

Important warning

If money has already moved, an account was accessed, or remote access was granted, stop following the scammer's instructions. Use a trusted phone number or official site to contact your bank, credit card company, or account provider. This guide is practical guidance, not legal, financial, or law-enforcement advice.

Slow down. Verify first. Stay grumpy.

Contents

1. Start Here: How to Use This Guide
2. The Scam Pattern: Panic, Pressure, Control
3. Fake Computer Warnings and Browser Popups
4. Fake Support Calls and Remote-Access Traps
5. Phishing Emails, Texts, and Fake Invoices
6. Fake Login Pages and Password Theft
7. MFA Prompts and Verification Code Scams
8. Remote Access Software: When It Is and Is Not Safe
9. Money Movement Scams: Gift Cards, Crypto, Wires, and Safe Accounts
10. Bank, Amazon, Microsoft, Google, and Shipping Impersonation
11. QR Code, Search Result, and Sponsored Link Scams
12. Social Media, Marketplace, and Family Emergency Scams
13. Phone Carrier, SIM Swap, and Account Recovery Scams
14. What to Do if You Clicked a Suspicious Link
15. What to Do if You Installed Remote Access Software
16. What to Do if You Shared a Code or Password
17. What to Do if Money or Payment Info Was Involved
18. Family Scam-Defense Plan
19. Monthly Scam-Defense Maintenance Routine
20. Final Scam Defense Checklist
21. Worksheets and Printables

Grumpy Rule: *Don't try to outsmart a scam while the scammer is still talking to you. End the interaction first. Think second. Act third.*

Backup & Ransomware Recovery Playbook

Build Backups That Survive Hardware Failure, Accidental Deletion, and Ransomware

Backups are not paperwork.

They're the difference between a bad day and losing years of photos, documents, financial records, family history, and everything else your computer was quietly holding hostage for you.

The Grumpy Sysadmin

Version: August 2026

SAMPLE
thegrumpysysadmin.com — full version has 21 guides, 239 pages

How to Use This Playbook

This playbook is designed for ordinary Windows users who need a backup system they can understand, maintain, and actually recover from. The goal isn't to turn your house into a data center. The goal is to keep one failed drive, one bad click, or one ransomware infection from becoming permanent.

Work through the design sections first, then the protection and testing sections, and finally the ransomware response plan. Fill out the worksheets and keep a copy somewhere other than the computer they describe.

Grumpy Rule: *The disaster isn't the day to discover what your backup software meant by "retention policy."*

The Five Questions Every Backup Plan Must Answer

- What data would hurt to lose?
- How many independent copies exist?
- Can the protected computer modify or destroy every backup?
- How far back can you restore?
- Have you successfully restored anything?

Table of Contents

- 1. Decide What Must Be Protected
- 2. Build a 3-2-1 Backup Design
- 3. Cloud Backup, Cloud Sync, Local Drives, and NAS
- 4. Add Ransomware-Resistant Protection
- 5. Protect Backup Accounts and Credentials
- 6. Set Retention and Recovery Points
- 7. Test Restores Before You Need Them
- 8. Ransomware: The First Hour
- 9. Decide Whether the Computer Can Be Trusted
- 10. Rebuild and Restore in the Right Order
- 11. Recovery Priorities
- 12. Backup Inventory and Emergency Worksheets
- 13. Maintenance Schedule
- 14. Final Verification

The Grumpy Sysadmin

Scam Warning Signs

Quick-Start Checklist

Spot fake warnings, fake support calls, phishing emails, and account takeover tricks before they wreck your day.

Before you trust a warning, call, email, or login page, slow down.

Scammers don't always hack their way in. A lot of the time, they scare you into opening the door. This quick-start checklist helps you spot the obvious red flags before you click a link, install remote access software, approve a login, read out a code, or move money.

Grumpy Rule: Scams work because they create panic. Your job is to slow the situation down before your mouse, phone, or wallet does something stupid on your behalf.

1. Watch for Fake Computer Warnings

Fake computer warnings usually try to scare you into calling a phone number, installing software, or paying for a problem that may not exist.

Fake Warning Check	Done
A browser page says your computer is infected and tells you to call a number	☐
A loud alarm, voice, or flashing screen is trying to panic you	☐
The warning claims to be Microsoft, Windows, Apple, Google, or your antivirus company	☐
The page says not to shut down or close the browser	☐
The warning appeared inside a web browser instead of the real security app	☐
The message says files, banking, or identity are at risk unless you act now	☐

Grumpy Rule: Real security software doesn't need a browser page screaming at you like a haunted slot machine.

2. Stop Fake Support Calls Before They Start

A real support person shouldn't need to scare you, control your computer, keep you on the phone, or walk you into your bank account.

Support Call Check	Done
Caller says they are from Microsoft, Amazon, your bank, antivirus company, or internet provider	☐
Caller asks you to install AnyDesk, TeamViewer, UltraViewer, Zoho Assist, RustDesk, or similar software	☐
Caller asks you to read out a login, verification, or MFA code	☐
Caller tells you to open banking, email, shopping, or password manager accounts	☐
Caller says to keep the call secret from family, your bank, or police	☐
Caller tells you to stay on the phone while they fix, refund, or secure something	☐

Grumpy Rule: Anyone telling you to keep a financial emergency secret is probably the emergency.

3. Treat Urgent Emails and Texts Like Suspicious Packages

Phishing messages usually try to create panic, curiosity, or urgency so you click before you think.

Message Check	Done
Message says your account will be closed, charged, locked, or suspended today	☐
Message claims you bought something expensive that you don't recognize	☐
Message includes an invoice, receipt, refund, shipping notice, or attachment you were not expecting	☐
Sender address looks almost right but not quite	☐
Message asks you to click a link to verify, cancel, refund, or secure an account	☐
The safer move is to open the official app or website yourself instead of clicking the link	☐

Grumpy Rule: A fake email doesn't need to be perfect. It only needs you to be rushed.

4. Check Login Pages Before Typing Passwords

Fake login pages can look professional. The logo may be real, the page may look familiar, and the trap may still be waiting.

Login Page Check	Done
You arrived from an email, text, ad, pop-up, or shortened link	☐
The web address looks misspelled, strange, shortened, or unrelated to the real company	☐
The page asks you to sign in again for no clear reason	☐
The page asks for more information than usual	☐
The page asks for a one-time code immediately after your password	☐
You closed the page and went to the official site yourself when something felt wrong	☐

Grumpy Rule: Scammers discovered logos. Truly groundbreaking. Check the address before you hand them the keys.

5. Never Share MFA or Verification Codes

One-time codes aren't customer-service trivia. They're often the key that lets someone into your account.

Code / MFA Check	Done
You never approve MFA prompts unless you personally started the login	☐
You never read one-time codes to someone on the phone, in chat, or by email	☐
You treat random MFA prompts as suspicious, not annoying background noise	☐
You know real support should not need your login code to cancel a charge or process a refund	☐
Family members understand not to share codes either	☐
You deny unexpected prompts and change passwords if suspicious activity continues	☐

Grumpy Rule: The code is the key. Stop handing the key to the person currently trying to rob the house.

6. Be Careful With Remote Access Software

Remote access tools can be legitimate, but they also give another person control of your computer. Treat that like a big deal, because it is.

Remote Access Check	Done
You contacted the company yourself using a trusted number or official website	☐
You know exactly who is connecting and why	☐
They are not asking you to open banking, email, password manager, or shopping accounts	☐
They are not asking you to disable security software	☐
They are not rushing you or telling you not to talk to anyone else	☐
Remote access software you do not use has been removed	☐

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

7. Money Requests Are the Giant Red Flag

Scammers love payment methods that are fast, hard to reverse, or embarrassing enough that people hesitate to ask for help.

Money Scam Check	Done
Someone asks for gift cards, cryptocurrency, wire transfers, or instant payments	☐
Someone says to move money to a safe account	☐
Someone asks for a test transaction or refund verification payment	☐
Someone wants payment to fix a warning that appeared on your screen	☐
Someone tells you to lie to the bank about why you are moving money	☐
Someone insists you must act immediately before asking anyone else	☐

Grumpy Rule: Microsoft doesn't want Apple gift cards. Your bank doesn't need Bitcoin. And the IRS isn't calling because they misplaced their Steam wallet.

Final "Do Not Ignore This" Check

Final Scam Check	Done
You do not call phone numbers shown in scary browser warnings	☐
You do not install remote access software because a stranger told you to	☐
You do not share passwords, MFA codes, verification codes, or recovery codes	☐
You do not approve MFA prompts you did not personally request	☐
You verify suspicious emails through the official website or app, not the message link	☐
You stop when someone rushes, scares, or tells you to keep secrets	☐
You ask a trusted person before moving money during a suspicious call or warning	☐
You know how to disconnect and get help if you already interacted with a scammer	☐

If several boxes are unchecked, stop pretending you can "just tell" when something is fake. Scammers count on confidence, panic, and nobody wanting to look foolish.

Grumpy Rule: The pause is the security control. Close the page. Hang up. Verify from somewhere you trust.

After a Scam Scare: Verify Before You Relax

If you clicked, called, typed credentials, approved a prompt, or allowed remote access, don't assume everything is fine just because the warning went away.

After-Scare Check	Done
End the call or chat and stop following the scammer's instructions	☐
Disconnect from the internet if remote access was involved	☐
Change affected passwords from a different trusted device	☐
Review email forwarding rules, recovery settings, and signed-in devices	☐
Check banking, credit card, shopping, and cloud account activity	☐
Remove unknown remote access software	☐
Run a security scan and ask for help before assuming the computer is clean	☐

Grumpy Rule: The browser tab closing doesn't mean the problem is over. That isn't a cleanup plan. That's a disappearance trick.

Want the Full Scam & Phishing Defense Guide?

This free quick-start checklist helps you recognize the obvious warning signs. The full guide goes deeper and walks through the scam patterns, safe response steps, recovery checks, and family rules that are easiest to miss when panic takes over.

Full Guide Will Include	Covered
Fake browser warning and tech-support scam walkthrough	☐
Phishing email, text message, and fake invoice examples	☐
Fake login page and suspicious link review checklist	☐
MFA prompt, verification code, and "read me the code" scam guidance	☐
Remote access software risk and removal checklist	☐
Bank, gift card, crypto, wire transfer, and refund scam warning signs	☐
Emergency response plan after clicking, calling, or allowing access	☐
Family scam-defense conversation guide	☐
Monthly scam-awareness review checklist	☐

Grumpy Rule: The free checklist is enough to make you stop and think. The full guide is for knowing what to do next when something already smells wrong.

**Get the full Scam & Phishing Defense Guide
or the future Home Cybersecurity Survival System**
<https://thegrumpysadmin.com>

Final Word

You don't need to become a cybersecurity expert to avoid most scams. You do need to slow down when something tries to scare you, rush you, isolate you, or make you share codes, install remote access tools, or move money.

Close the page. Hang up the phone. Open the official app or website yourself. Ask someone trusted before continuing.

Scams work fast. Your best defense is refusing to move at scammer speed.

Stay grumpy.

Emergency Security Card

Print this page or save a copy somewhere you can reach without your main computer or smartphone.

IF I THINK SOMETHING'S BEEN COMPROMISED

- ☐ STOP interacting with the suspicious caller, message, website, or software.
- ☐ Use a different trusted device if the affected device may be compromised.
- ☐ Secure my PRIMARY EMAIL account first if account takeover is possible.
- ☐ Secure my PASSWORD MANAGER and other critical identity accounts.
- ☐ Contact financial institutions directly if money or payment information may be involved.
- ☐ Contact my phone carrier directly if my number/SIM may be involved.
- ☐ Review active sessions, trusted devices, MFA methods, recovery methods, and forwarding rules.
- ☐ Preserve messages, emails, screenshots, transaction records, dates, and case numbers.
- ☐ Don't erase/reset/reinstall until I understand what I might destroy or lose.

Trusted contacts to fill in

Organization / Person	Trusted phone number / method
Primary bank	
Primary credit card	
Phone carrier	
Password manager	
Primary email provider	
Trusted family member	
Trusted technical contact	

Don't use contact information supplied by the suspicious person. That's how you end up calling the scammer's "fraud department," which is just the scammer with a different voice.

Security Checkup & Maintenance Routine

A practical audit and upkeep guide for your digital security system

Use this after completing the seven-day plan, then return to the maintenance routine to keep your protections current.

THE GRUMPY SYSADMIN SECURITY CHECKUP

You're finished with the seven-day plan when you can check these boxes honestly — not because you clicked through settings until everything looked reassuring.

Windows & Browser

- ☐ Windows/security tools, firewall, and network profile are current.
- ☐ Administrator accounts and encryption/recovery key are understood.
- ☐ Browsers, extensions, downloads, privacy settings, and remote-access tools were reviewed.

Accounts

- ☐ Critical accounts use unique passwords and MFA/passkeys where appropriate.
- ☐ Recovery methods and backup codes are current.
- ☐ Recent sessions/devices were reviewed.

Home Network

- ☐ Router admin access and firmware are secured.
- ☐ Wi-Fi uses modern encryption and WPS/remote management were reviewed.
- ☐ Connected devices and guest/IoT access were reviewed.

Smartphone

- ☐ Strong lock and Apple/Google account security are configured.
- ☐ Find/lock/erase plus backups/authenticator recovery are verified.
- ☐ Carrier/SIM protections and app permissions were reviewed.

Scams & Identity

- ☐ You verify unexpected requests independently and never share MFA codes.
- ☐ Financial alerts and identity-theft response steps are known.
- ☐ Family members know the urgent-money verification rule.

Backups

- ☐ Important files exist in multiple locations with at least one separated copy when practical.
- ☐ Backup jobs are current.
- ☐ A restore test succeeded and recovery keys are available.

Emergency Plan

- ☐ First-response order and critical-provider contacts are documented.
- ☐ Plan is accessible without the primary PC or phone.
- ☐ A trusted family member knows where the plan is.

If you can't honestly check a box, go back to that day, use the matching checklist and playbook, fix the gap, and verify it again.