



The
Grumpy
Sysadmin

**COMPLETE
BUNDLE**

THE COMPLETE DIGITAL SURVIVAL SYSTEM

SECURE IT. **FIX IT.** RECOVER IT.



2 FLAGSHIP SYSTEMS 1 COMPLETE SOLUTION.

SAMPLE PREVIEW

One System. Two Critical Jobs.

Keep Windows working - and protect the digital life built around it.

What you are getting

The Complete Digital Survival System combines both flagship Grumpy Sysadmin systems into one organized package. It is built for everyday Windows users who want practical help before something breaks, while it is breaking, and after the dust settles.

WINDOWS SURVIVAL

Maintain, troubleshoot, repair and recover your Windows PC without treating Reset This PC as the opening move.

DIGITAL SECURITY

Protect your accounts, home Wi-Fi, smartphone, files, backups and emergency recovery plan.

32

PDF RESOURCES

483

PAGES

2

FLAGSHIP SYSTEMS

Also included: the Windows Repair Toolkit

The bundle includes the Grumpy Sysadmin Windows Repair Toolkit alongside the guides, checklists, decision trees and recovery resources. No subscription. No security background required. Instant digital download.

Ultimate Windows Survival System

Ten PDF resources plus the Windows Repair Toolkit.

START HERE

- [START HERE - Read First](#)

CORE WINDOWS SURVIVAL SYSTEM

- [The Grumpy Sysadmin Windows Survival Guide](#)
- [The Windows Repair Playbook](#)
- [Windows Debloat Playbook](#)

BACKUP, REPAIR AND RESET PLANNING

- [Before You Click Reset This PC Checklist - Expanded Edition](#)
- [Windows Pre-Repair Backup Checklist - Expanded Edition](#)
- [Windows Repair Decision Tree](#)

RECOVERY, UPDATES AND MAINTENANCE

- [Windows Recovery USB Toolkit Guide](#)
- [Windows Update Survival Checklist](#)
- [Windows Monthly Maintenance Checklist](#)

INCLUDED TOOL

- [Grumpy Sysadmin Windows Repair Toolkit](#)

Secure Your Digital Life in 7 Days

Twenty-one PDF resources organized into seven focused missions.

START HERE

- Secure Your Digital Life in 7 Days - complete roadmap

DAYS 1-3

- Windows Security Hardening - Playbook + Quick-Start Checklist
- Browser & Online Privacy Lockdown - Guide + Quick-Start Checklist
- Account Lockdown - Playbook + Quick-Start Checklist
- Home Wi-Fi & Router Lockdown - Guide + Quick-Start Checklist

DAYS 4-5

- Smartphone Security - Playbook + Quick-Start Checklist
- Scam & Phishing Defense - Guide + Quick-Start Checklist
- Identity Theft & Fraud Defense - Guide + Quick-Start Checklist

DAYS 6-7

- Backup & Ransomware Recovery - Playbook + Quick-Start Checklist
- Security Emergency Response - Playbook + Quick-Start Checklist

PRINT AND KEEP

- Emergency Security Card
- Security Checkup - Maintenance Routine

Choose the Right Starting Point

Start with the situation you have today. Don't bounce between guides or run every tool simply because it exists.

YOUR SITUATION	START HERE
I think I was hacked, scammed, or compromised	Use Day 7 - Security Emergency Plan first. Work from a trusted device when possible, secure primary email and critical accounts, contact the real organization directly, preserve evidence, and recover deliberately.
I want to secure everything before trouble starts	Begin with Secure Your Digital Life in 7 Days. Follow Days 1 through 7 in order, then print the recurring maintenance resources.
Windows is broken, unstable, freezing, or throwing errors	Begin with the Windows Repair Playbook. Back up important files first. Use the Repair Toolkit only when the playbook points you toward an automated repair action.
Windows is slow, bloated, or irritating	Begin with the Windows Debloat Playbook, then use the Windows Survival Guide. Don't start deleting protected folders or running random Internet scripts.
I am considering Reset This PC	Use the Windows Repair Decision Tree, then the Windows Pre-Repair Backup Checklist, then the Before You Click Reset This PC Checklist. Don't skip the backup work.
Everything works and I want to keep it that way	Complete the seven-day security plan, create recovery media, then use both the Security Checkup - Maintenance Routine and Windows Monthly Maintenance Checklist.

If an account or device may be compromised, don't wipe, reset, reinstall, or erase it until you understand what access or evidence could be lost.

SAMPLE
thegrumpysysadmin.com - full version has 483 pages

The Seven Day Security Roadmap

Use the main Secure Your Digital Life in 7 Days guide as your daily checklist. Open the matching folder when you want the deeper playbook and quick-start reference.

1	Lock Down Windows Review Windows Security, firewall, encryption, administrator access, browsers, privacy, extensions, downloads, and remote-access tools.
2	Secure Your Accounts Protect primary email, password manager, Microsoft, Google, and Apple accounts, financial accounts, cloud storage, shopping accounts, and carrier access.
3	Lock Down Your Home Network Secure router administration, firmware, Wi-Fi encryption, WPS, remote management, guest access, and connected devices.
4	Secure Your Smartphone Review device lock, operating-system updates, app permissions, account protection, lost-device features, backups, and recovery options.
5	Scam and Identity Defense Build verification habits, enable important alerts, protect sensitive records, and know where to begin if fraud or identity theft appears.
6	Protect Your Files and Backups Identify irreplaceable files, improve backup separation, check cloud and external backups, and perform an actual restore test.
7	Build Your Security Emergency Plan Document what to do after a suspicious click, account takeover, lost phone, fraudulent transaction, malware, or ransomware warning.

Grumpy rule: A backup you've never tested is a comforting theory.

The Windows Readiness Roadmap

The Ultimate Windows Survival System is organized by task. Use the folder that matches the problem instead of treating the ZIP file like a digital junk drawer.

FOLDER	WHAT IS INSIDE	USE IT FOR
01 - Core Windows Survival System	Windows Survival Guide; Windows Repair Playbook; Windows Debloat Playbook	Daily control, structured troubleshooting, repair order, cleanup, and performance.
02 - Windows Repair Toolkit	PowerShell-based repair toolkit and instructions	Automated repair actions. Read the instructions and run only the action you understand.
03 - Backup Repair and Reset Planning	Pre-Repair Backup Checklist; Repair Decision Tree; Before You Click Reset This PC Checklist	The safety-first section before major repairs, resets, or uncertain decisions.
04 - Recovery USB and Emergency Tools	Windows Recovery USB Toolkit Guide	Create and maintain recovery media before Windows refuses to cooperate.
05 - Windows Update Protection	Windows Update Survival Checklist	Prepare before major updates and verify Windows afterward.
06 - Monthly Maintenance	Windows Monthly Maintenance Checklist	Keep startup apps, storage, security, updates, drivers, and general performance under control.

Safest full system order

1	Back up important files Use the Pre-Repair Backup Checklist before major changes, repairs, resets, debloating, or update troubleshooting.
2	Identify the real problem Use the Repair Decision Tree when you are unsure whether to repair, reset, update, debloat, or leave the system alone.
3	Repair in order Use the Repair Playbook first, followed by the Repair Toolkit only when appropriate.
4	Prepare and maintain Create recovery media, prepare for updates, and use the monthly maintenance checklist.

FLAGSHIP SYSTEM ONE

Ultimate Windows Survival System

A practical system for maintaining, troubleshooting, repairing and recovering a Windows PC.

ACTUAL PAGES FROM THE COMPLETE PRODUCT

SECTION 2: Windows Is Slowing You Down on Purpose

(And It Turns This Stuff Back On... Without Telling You)

Let's talk about the part nobody likes to hear.

That stuff you just fixed?

👉 **Windows will turn some of it back on.**

👉 And it enables even more junk by default.

Not because your system is broken...

Because that's how Windows is designed.

⚠️ Reality Check (This Is Important)

Windows today is not just an operating system.

It's:

- A data collection platform
- An advertising platform
- A "suggestion engine"

And all of that runs in the background...

👉 Using YOUR system resources.

💡 Grumpy Reality Check:

Microsoft isn't trying to make your PC faster.

They're trying to make Windows do more... whether you want it or not.

🎯 What We're Doing in This Section

We are going to:

- ✓ Turn OFF hidden features that slow your system down
 - ✓ Stop Windows from "helping" you in ways that hurt performance
 - ✓ Prevent this stuff from quietly coming back
-

Windows Is Broken... Now What

Let's get one thing out of the way:

👉 If your system is acting weird, freezing, crashing, or just not doing what it's supposed to...

Something is wrong.

Not "Windows being Windows."

Not "it'll fix itself."

👉 Something is broken.

The goal here is simple:

Figure out what kind of problem you actually have—before you make it worse trying to fix it.

How to Quickly Identify the Problem

Before you start running commands or clicking random fixes you found online...
you need to answer one question:

👉 **What is actually broken?**

Is it Windows, an app, or hardware?

Start here:

- Does the issue happen everywhere, or just in one program?
- Is the whole system slow, or just one task?
- Are you getting errors, or just weird behavior?

Quick breakdown:

If EVERYTHING is broken:

- System is slow
- Explorer is freezing
- Updates are failing

👉 This is likely a **Windows / OS issue**

Reset Windows Update Components (Step-by-Step)

This is the **real fix**.

Not guessing.

Not hoping.

👉 This clears everything Windows Update relies on and rebuilds it cleanly.

⚠ Before you start

- You need to be **Administrator**
 - Close all open apps
-

Step 1 — Open Command Prompt (Admin)

- Click Start
 - Type: **cmd**
 - Right-click → **Run as administrator**
-

Step 2 — Stop update services

Run these one at a time:

```
net stop wuauserv  
net stop cryptSvc  
net stop bits  
net stop msiserver
```

👉 This stops everything Windows Update is using

Step 3 — Rename update folders

Run:

```
ren C:\Windows\SoftwareDistribution SoftwareDistribution.old  
ren C:\Windows\System32\catroot2 catroot2.old
```

👉 This forces Windows to rebuild its update cache

Start Here: The Fast Triage Grid

Use this page when the PC is acting weird and you need to decide which section to jump to first.

Symptom / Question	If Yes	Next Step	Done
PC is slow	Slow at startup or slow all the time?	Go to PC Is Slow	☐
Windows will not boot	Does the PC power on but Windows will not load?	Go to Windows Will Not Boot	☐
Blue screen or crashes	Did it happen once or repeatedly?	Go to Blue Screens or Crashes	☐
Internet is broken	Only this PC or all devices?	Go to Internet or Network Is Broken	☐
Printer/scanner broken	Offline, duplicated, or not printing?	Go to Printer or Scanner Is Broken	☐
Audio, camera, or mic broken	Missing device or wrong device selected?	Go to Audio, Camera, or Microphone Is Broken	☐
Apps keep crashing	One app or many apps?	Go to Apps Will Not Open or Keep Crashing	☐
Update failed	Error code, repeated failure, or rollback needed?	Go to Windows Update Failed	☐
Files missing	Deleted, moved, hidden, or OneDrive redirected?	Go to Files Are Missing or OneDrive Is Confusing Everything	☐

Stop and Back Up First If...

Some problems are annoying. Others are warning signs that you should stop repairing and protect your data first.

Situation	Stop and Back Up
The drive is clicking, grinding, or making strange noises	☐
Files are disappearing or becoming corrupted	☐
Windows is unstable but still boots	☐
You are considering Reset This PC	☐
You are considering reinstalling Windows	☐
You see signs of ransomware or file encryption	☐
BitLocker recovery appears and you are unsure what changed	☐
The PC will not boot reliably but you can still access files sometimes	☐
You do not have another copy of important files	☐

Grumpy Rule

Do not keep poking a dying drive because you are curious.

Curiosity is great. Data recovery bills are not. If the data matters, back it up before the repair becomes the disaster.

FLAGSHIP SYSTEM TWO

Secure Your Digital Life in 7 Days

Seven focused missions for protecting Windows, accounts, Wi-Fi, phones, files and recovery plans.

ACTUAL PAGES FROM THE COMPLETE PRODUCT

DAY 5 — Build Your Scam & Identity Defenses

Many attacks don't break into your computer. They talk you into opening the door. Today has two parts because recognizing manipulation and preparing for identity/fraud problems are related — but they aren't the same job.

TODAY'S MATERIALS

1. PART A: Scam & Phishing Defense Quick-Start Checklist + Guide

Complete this first. Learn the warning signs, verification habits, and rules that prevent an attacker from talking you into helping them.

2. PART B: Identity Theft & Fraud Quick-Start Checklist + Identity Theft & Fraud Defense Guide

Then prepare the financial, credit, documentation, and response protections you want in place before something suspicious appears.

PART A — SCAM & PHISHING DEFENSE

- ☐ Stop using links in unexpected messages to reach important accounts. Open the official app or type the known website yourself.
- ☐ Never give a caller or message sender an MFA/verification code.
- ☐ Never approve an unexpected MFA prompt you didn't initiate.
- ☐ Don't install remote-access software because an unsolicited caller tells you to.
- ☐ Treat urgency, secrecy, threats, unusual payment methods, and "act now" language as reasons to slow down.
- ☐ Create a family rule: financial or emergency requests involving money get verified through a second known contact method.

PART B — IDENTITY & FRAUD DEFENSE

- ☐ Enable transaction and login alerts on important financial accounts where available.
- ☐ Review recent bank and credit-card activity.
- ☐ Know how to freeze your credit and where to contact the major credit bureaus if you need to respond to identity theft.
- ☐ Review what personal information you routinely expose through social media and public profiles.
- ☐ Protect tax, medical, insurance, Social Security, and other sensitive records.
- ☐ Document what you would do first if a fraudulent account or transaction appeared.

VERIFY IT

- ☐ You can explain to another family member why a verification code should never be handed to a caller.
- ☐ Your major financial accounts can alert you to suspicious activity.
- ☐ You know where to start if your identity is stolen.
- ☐ You have a second-channel verification rule for urgent money requests.

5. Separate Guests and Smart Devices

Guest Wi-Fi isn't just for visitors. It can also keep less-trusted devices away from your main computers and phones. Smart TVs, cameras, speakers, plugs, robot vacuums, and random IoT gadgets often have weaker update habits and fewer security controls.

What to do

- Enable guest Wi-Fi for visitors instead of giving out the main password.
- Use guest isolation if available so guest devices can't see your main devices.
- Consider a separate IoT network for cameras, smart TVs, printers, and other smart devices.
- Keep work computers, personal computers, and phones on the main trusted network.
- Put devices that only need internet access on the guest or IoT network when possible.

Don't do this

- Don't give every visitor permanent access to the main network.
- Don't assume a smart device is trustworthy because it has a nice app.
- Don't isolate a printer or smart hub without testing whether the devices that need it can still reach it.

Grumpy Rule

Your smart TV doesn't need to be best friends with your tax documents.

Device type	Suggested network	Notes
Main computer	Main trusted Wi-Fi	Needs access to normal home resources
Work laptop	Main or dedicated work Wi-Fi	Follow employer requirements
Phones/tablets	Main trusted Wi-Fi	Use guest only for visitors
Smart TVs	Guest or IoT Wi-Fi	Usually only need internet access
Cameras	IoT Wi-Fi	Review remote access settings carefully
Printers	Main or IoT Wi-Fi	Test printing before isolating
Game consoles	Main or guest Wi-Fi	May need UPnP or specific rules
Visitors	Guest Wi-Fi	Do not share main password by default

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.

DAY 6 — Protect Your Files and Backups

Security isn't only about keeping attackers out. It's also about surviving the day a drive dies, ransomware encrypts files, a laptop disappears, cloud sync helpfully synchronizes a bad deletion, or somebody discovers that "backup" meant "another folder on the same computer."

TODAY'S MATERIALS

1. START WITH: Backup & Ransomware Recovery Quick-Start Checklist

Use it to make sure the critical backup protections are actually in place.

2. GO DEEPER WITH: Backup & Ransomware Recovery Playbook

Use the playbook for backup design, cloud-vs-local tradeoffs, separated/disconnected protection, ransomware response, restore testing, and recovery priorities.

DO THIS TODAY

- ☐ Identify the files you can't replace: photos, documents, financial records, creative work, business files, password exports, and other critical data.
- ☐ Confirm those files exist in more than one physical or logical location.
- ☐ Use the 3-2-1 idea as a target: three copies of important data, on two different types/locations of storage, with at least one copy separated from the primary system.
- ☐ Don't treat synchronization alone as a complete backup strategy.
- ☐ Keep at least one backup protected from routine modification by the main PC when practical.
- ☐ Confirm cloud backup/sync services are actually running and not paused, full, signed out, or failing.
- ☐ Confirm external backup drives are healthy and recent.
- ☐ Back up password-manager recovery information and encryption recovery keys appropriately.
- ☐ Document how you would restore your most important files.

VERIFY IT — THE RESTORE TEST

Don't admire a "Backup completed successfully" message and declare victory. Restore something.

- ☐ Restore or open several files from the backup, including at least one older file.
- ☐ Confirm filenames, folders, and dates look reasonable.
- ☐ Confirm you can access the backup without depending on the computer being backed up.
- ☐ Confirm you know the credentials or encryption key required to restore protected backups.
- ☐ Write down the date of the successful test.

YOU'RE DONE FOR TODAY WHEN...

- ☐ Important files exist in more than one location.
- ☐ At least one copy is separated from routine changes on the primary computer when practical.
- ☐ Backup jobs are current and accessible.
- ☐ You successfully restored something instead of simply trusting a status message.

A backup you've never tested is a comforting theory.

YOU HAVE SEEN THE SAMPLE

THE COMPLETE SYSTEM GOES MUCH FURTHER.

The full download gives you all 32 PDFs, 483 pages of practical guidance, the Windows Repair Toolkit, both flagship systems and the START HERE guide that ties everything together.

BUILT FOR PEOPLE WHO WANT TO:

- Keep Windows running without random button-mashing
- Protect accounts, devices, files and the home network
- Prepare before failures, scams or security emergencies
- Know what to do next when something goes wrong

GET THE COMPLETE DIGITAL SURVIVAL SYSTEM

shop.thegrumpysysadmin.com

Instant download | One-time purchase | 30-day money-back guarantee

The Grumpy Sysadmin