The Grumpy Sysadmin

Account Lockdown Quick-Start Checklist

Secure your email, passwords, MFA, and recovery access before one bad password turns into a really expensive lesson.

Before you trust your accounts, slow down. Your password isn't the whole plan. If your email, password manager, MFA app, or recovery options are wrong, one leaked password or lost phone can turn into account theft, banking problems, cloud lockouts, and a week of digital misery.

> ***Grumpy Rule: Your email account isn't just another login. It's often the reset button for everything else. Protect that first, or enjoy playing account-recovery roulette with support forms.***

1. Lock Down Your Main Email Account First

Start with the account that receives password reset links. If this account falls, everything connected to it gets easier to attack.

Email Account Check	Done
Main email password is unique and not reused anywhere else	☐
MFA is turned on for the email account	☐
Recovery email and phone number are current	☐
Suspicious forwarding rules or filters have been checked	☐
Recent login activity has been reviewed	☐
Old devices and sessions you do not recognize are removed	☐
Recovery codes or backup access are saved somewhere safe	☐

> ***Grumpy Rule: If criminals control your email, they don't need to guess every password. They just click "forgot password" and let your inbox do the damage.***

2. Stop Reusing Passwords

Unique passwords matter more than clever passwords. One reused password can turn one breach into ten compromised accounts.

Password Check	Done
Password manager access is confirmed before changing anything	☐
A strong master password is used for the password manager	☐
Email, banking, and shopping passwords are unique	☐
Old reused passwords are changed on important accounts first	☐
Password manager duplicate/reused password report has been reviewed	☐
Browser-saved passwords on old or shared devices are reviewed	☐
No important passwords are stored in plain text on the desktop	☐

> ***Grumpy Rule: Your brain isn't a password manager. It's barely reliable for remembering why you walked into the kitchen.***

3. Turn On MFA Without Locking Yourself Out

Multi-factor authentication helps, but only if you set it up with a backup plan. Security that locks out the owner isn't a strategy.

MFA Check	Done
MFA is enabled for email, banking, password manager, and cloud accounts	☐
Authenticator app or passkey is used where available	☐
SMS is not the only MFA method on critical accounts if better options exist	☐
At least one backup MFA method is configured	☐
You know how to sign in if your phone dies or is replaced	☐
Recovery codes were saved immediately after enabling MFA	☐
MFA prompts are never approved unless you personally started the login	☐

Grumpy Rule: MFA is supposed to keep criminals out. Bad MFA planning can also keep you out. Congratulations, now the door hates everyone equally.

4. Save Recovery Codes and Backup Access

Recovery codes are boring right up until they become the only way back into your account.

Recovery Check	Done
Recovery codes are downloaded or printed for critical accounts	☐
Codes are stored offline in a safe location	☐
Codes are labeled by account without exposing the password	☐
The only copy is not inside the account it is meant to recover	☐
Old recovery emails and phone numbers are removed or updated	☐
Backup access is documented for your password manager	☐
Recovery codes are replaced after one is used	☐

Grumpy Rule: A recovery code saved only in the account it unlocks isn't a recovery plan. It's a locked safe with the key inside, because apparently we needed a sequel.

5. Check the Accounts That Can Hurt You Most

Don't try to fix every login on the Internet today. Lock down the accounts with the biggest blast radius first.

Account to Review	Checked
Main email account	☐
Password manager account	☐
Banking and credit card accounts	☐
Microsoft, Google, and Apple accounts	☐
Cell phone carrier account	☐
Amazon and major shopping accounts	☐
Cloud storage accounts	☐
Tax, insurance, medical, and government accounts	☐

Grumpy Rule: You don't have to secure the entire Internet before lunch. Start with the accounts that can empty your wallet, reset your life, or lock you out of your own stuff.

6. Make a Simple Emergency Access Plan

The goal isn't just keeping criminals out. It's making sure you, or someone you trust, can still get back in during a real emergency.

Emergency Access Check	Done
A trusted spouse or family member knows where emergency instructions are	☐
Password manager emergency access or recovery process has been reviewed	☐
A sealed/offline emergency sheet exists for critical recovery details	☐
You know what to do if your phone is lost or replaced	☐
You know which email account controls password resets	☐
Important accounts have been reviewed after any phone or email change	☐

Grumpy Rule: The worst time to figure out account recovery is when you're already locked out, angry, and searching help articles written by someone who thinks "simply sign in" is useful advice.

Final "Do Not Ignore This" Check

Final Check	Done
Main email account has a unique password and MFA enabled	☐
Password manager access is confirmed	☐
Critical accounts use unique passwords	☐
MFA is enabled on email, banking, cloud, and password manager accounts	☐
Recovery codes are saved somewhere offline and safe	☐
Recovery email and phone numbers are current	☐
Old devices, sessions, and suspicious account activity were reviewed	☐
Emergency access plan exists before something goes wrong	☐

If any critical box is unchecked, stop pretending the account is "secure enough." Fix the basics before the next bad login attempt tests your optimism.

Grumpy Rule: Account security isn't one magic password. It's passwords, MFA, recovery, devices, sessions, and not clicking "approve" like a tired Windows user on autopilot.

After You Tighten Account Security: Verify Before You Celebrate

Security changes should protect you without stranding you. After making changes, make sure the important stuff still works.

After-Lockdown Check	Done
You can sign in to email from at least one trusted device	☐
Password manager opens and syncs normally	☐
MFA prompts work as expected	☐
Recovery codes are stored where you can actually find them	☐
Banking, cloud, and shopping accounts still sign in normally	☐
Emergency access instructions are understandable and current	☐

Grumpy Rule: The job isn't done when you flip on MFA. It's done when the accounts are safer and you can still get back in. Annoyingly important detail.

Want the Full Account Lockdown Playbook?

This free quick-start checklist points you at the accounts and settings that matter most. The full playbook goes deeper and walks through the setup, decisions, recovery details, and maintenance routine that are easiest to miss.

Full Playbook Includes	Covered
Step-by-step account lockdown priority plan	☐
Password manager setup and cleanup guidance	☐
Master password and emergency access planning	☐
MFA method comparison and setup workflow	☐
Recovery code storage and review system	☐
Email account security audit walkthrough	☐
Banking, cloud, shopping, and phone carrier checklist	☐
Lost phone, stolen password, and suspicious login response plan	☐
Monthly account security maintenance checklist	☐

Grumpy Rule: The free checklist is enough to point at the obvious account problems. The full playbook is the better plan when you want to know exactly what to change, where to check, and what to do when something already smells wrong.

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

Final Word

You don't need to turn every account into a government bunker. You do need unique passwords, MFA, current recovery information, saved recovery codes, and a simple plan before something breaks.

Account security doesn't stay fixed on its own. Review it now. Check it again when you change phones, emails, or password managers. Stay grumpy.