5 SIMPLE WAYS TO SECURE YOUR SYSTEM

Comprehensive Security Checklist

Your Complete Security Hardening Guide

This checklist provides step-by-step instructions for implementing five critical security measures on your computer. Each section includes detailed instructions for Windows, with additional guidance for Linux and macOS systems.

Estimated Total Time: 45-60 minutes
Difficulty: Beginner to Intermediate

Created by: Advaith Banigandlapati
Based on: CyberPatriot Competition Experience
Generated: February 01, 2026

TABLE OF CONTENTS

TIP #1: ENABLE BITLOCKER DRIVE ENCRYPTION

Difficulty: Beginner | Time: 10 minutes

What It Does:

Full-disk encryption that protects your data if your computer is lost or stolen. Even if someone removes your hard drive, they cannot access your files without the encryption key.

Windows Instructions:

- Open Start menu and search for 'BitLocker'
- Click 'Manage BitLocker'
- Click 'Turn on BitLocker' next to your C: drive
- Wait for system compatibility check to complete
- Select 'Enter a password' as unlock method
- Create a strong password (12+ characters, mixed case, numbers, symbols)
- Save recovery key to USB drive OR print it (CRITICAL - store safely!)
- Choose encryption mode: 'Encrypt used disk space only' for existing PCs
- Run system check and restart computer
- Verify encryption started (check BitLocker status)

Linux Alternative (LUKS Encryption):

Most Linux distributions offer full-disk encryption during installation. For existing systems, use LUKS (Linux Unified Key Setup):

- Backup all data before proceeding
- Use cryptsetup: `sudo cryptsetup luksFormat /dev/sdX`
- Open encrypted partition: `sudo cryptsetup open /dev/sdX encrypted`
- Format and mount the encrypted partition

macOS (FileVault):

- Open System Preferences → Security & Privacy → FileVault
- Click 'Turn On FileVault'
- Save recovery key to iCloud OR write it down securely
- Restart and verify encryption is enabled

■ **Common Mistakes:**

- Not saving recovery key in separate location
- Using weak password
- Storing recovery key on encrypted drive
- Forgetting to encrypt external drives with sensitive data

TIP #2: ENABLE AND MONITOR AUDIT LOGS

Difficulty: Intermediate | Time: 15 minutes

What It Does:

Creates detailed records of system events: login attempts, file access, system changes, and security events. Essential for detecting suspicious activity and intrusions.

Windows Instructions:

- Press Win + R, type: secpol.msc, press Enter
- Navigate to Local Policies → Audit Policy
- Enable SUCCESS and FAILURE for: Audit Account Logon Events
- Enable SUCCESS and FAILURE for: Audit Account Management
- Enable SUCCESS and FAILURE for: Audit Logon Events
- Enable SUCCESS and FAILURE for: Audit Policy Change
- Enable SUCCESS and FAILURE for: Audit Privilege Use
- Enable SUCCESS and FAILURE for: Audit System Events
- Press Win + R, type: eventvwr.msc to view logs
- Navigate to Windows Logs → Security
- Right-click Security → Properties
- Set Maximum log size to at least 100 MB
- Select 'Archive the log when full'

Linux (rsyslog/journald):

- Check logs: `sudo journalctl -xe`
- View auth logs: `sudo tail -f /var/log/auth.log`
- Configure persistence: Edit `/etc/systemd/journald.conf`
- Set Storage=persistent in journald.conf
- Restart journald: `sudo systemctl restart systemd-journald`

macOS:

- Open Console app (Applications → Utilities → Console)
- View system logs in left sidebar
- Terminal: `log show --predicate 'eventMessage contains "login"'`

■ **Pro Tip:**

Key Event IDs to watch (Windows):

- 4624 = Successful login
- 4625 = Failed login attempt (multiple = possible attack)
- 4720 = User account created
- 4732 = User added to security group

Review your Security logs weekly!

TIP #3: CONFIGURE STRONG PASSWORD POLICIES

Difficulty: Beginner | Time: 10 minutes

What It Does:

Enforces security rules for all passwords: minimum length, complexity requirements, expiration periods, and password history. Prevents weak passwords system-wide.

Windows Instructions:

- ■ Press Win + R, type: secpol.msc, press Enter
- ■ Navigate to Account Policies → Password Policy
- ■ Set 'Minimum password length' to at least 12 characters
- ■ Enable 'Password must meet complexity requirements'
- ■ Set 'Enforce password history' to remember 5 passwords
- ■ Set 'Maximum password age' to 90 days
- ■ Set 'Minimum password age' to 1 day
- ■ Navigate to Account Policies → Account Lockout Policy
- ■ Set 'Account lockout threshold' to 5 invalid attempts
- ■ Set 'Account lockout duration' to 30 minutes
- ■ Set 'Reset account lockout counter after' to 30 minutes

Linux (PAM - Pluggable Authentication Modules):

- ■ Edit: `sudo nano /etc/pam.d/common-password`
- ■ Add line: `password requisite pam_pwquality.so minlen=12 ucredit=-1 lcredit=-1 dcredit=-1 ocredit=-1`
- ■ Edit: `sudo nano /etc/login.defs`
- ■ Set PASS_MAX_DAYS to 90
- ■ Set PASS_MIN_DAYS to 1
- ■ Install: `sudo apt install libpam-pwquality`

macOS:

- ■ System Preferences → Users & Groups → Login Options
- ■ Click lock icon and authenticate
- ■ Click 'Join...' → 'Open Directory Utility'
- ■ Edit → Change Password Policy
- ■ Use pwpolicy command: `sudo pwpolicy -setglobalpolicy 'minChars=12'`

TIP #4: SET STRONG PASSWORDS IN LOCAL USERS AND GROUPS

Difficulty: Beginner | Time: 5 minutes

What It Does:

Ensures all existing user accounts have strong passwords that meet security requirements. Password policies only apply to NEW passwords - this fixes existing weak passwords.

Windows Instructions:

- Press Win + R, type: lusrmgr.msc, press Enter
- Click on 'Users' folder
- Review all user accounts listed
- Identify Administrator accounts (high priority)
- Check for Guest account (should be disabled)
- Look for unrecognized accounts (security risk)
- Right-click each user → 'Set Password'
- Create password: 12-16+ characters, mixed case, numbers, symbols
- Use different password for each account
- Right-click Guest → Properties → check 'Account is disabled'
- For each account: verify 'User cannot change password' is UNCHECKED
- Verify 'Password never expires' is UNCHECKED
- Click 'Groups' folder → double-click 'Administrators'
- Remove unnecessary users from Administrators group

Linux:

- List users: `cat /etc/passwd`
- Change password: `sudo passwd username`
- Disable account: `sudo usermod -L username`
- Delete account: `sudo userdel username`
- Check sudo access: `sudo cat /etc/sudoers`

macOS:

- System Preferences → Users & Groups
- Click lock icon to make changes
- Select each user → Change Password
- Disable Guest User if present
- Review admin users (uncheck 'Allow user to administer this computer' for non-admins)

TIP #5: CREATE ANTIVIRUS QUICK SCAN AT STARTUP

Difficulty: Intermediate | Time: 5 minutes

What It Does:

Automatically runs antivirus scan every time your computer starts, catching malware before it can activate. Provides extra protection layer against boot sector viruses and rootkits.

Windows Instructions (Windows Defender):

- Press Win + R, type: taskschd.msc, press Enter
- Click 'Create Task...' in right panel
- Name: 'Windows Defender Startup Scan'
- Check 'Run with highest privileges'
- Select 'Run whether user is logged on or not'
- Configure for: Windows 10 (or your version)
- Go to 'Triggers' tab → Click 'New...'
- Begin the task: 'At startup'
- Delay task for: 1 minute
- Check 'Enabled' → Click OK
- Go to 'Actions' tab → Click 'New...'
- Action: 'Start a program'
- Program/script: C:\Program Files\Windows Defender\MpCmdRun.exe
- Add arguments: -Scan -ScanType 1
- Click OK
- Go to 'Conditions' tab
- Uncheck 'Start only if computer is on AC power'
- Go to 'Settings' tab
- Check 'Run task as soon as possible after scheduled start is missed'
- Click OK → Enter password if prompted
- Right-click your task → 'Run' to test
- Verify scan completed in Windows Security

Linux (ClamAV):

- Install ClamAV: `sudo apt install clamav clamav-daemon`
- Update signatures: `sudo freshclam`
- Create startup script in `/etc/init.d/` or systemd service
- Add to crontab: `@reboot /usr/bin/clamscan -r /home`
- Enable ClamAV daemon: `sudo systemctl enable clamav-daemon`

macOS:

- macOS has built-in XProtect (automatic)
- For third-party: Install ClamXAV or Sophos
- Configure scheduled scan in antivirus preferences
- Or use Automator to create startup application

TROUBLESHOOTING GUIDE

BitLocker Issues:

Problem: BitLocker option not available

- Solution: BitLocker requires Windows Pro/Enterprise/Education. Windows Home doesn't support it.
- Alternative: Use VeraCrypt (free, open-source encryption)

Problem: 'This device can't use a Trusted Platform Module (TPM)'

- Solution: Use USB key or password-only mode
- Run: gpedit.msc → Computer Config → Admin Templates → Windows Components → BitLocker
- Enable 'Require additional authentication at startup'

Problem: Encryption is very slow

- Normal: Encryption can take hours for large drives
- You can use your computer during encryption
- Don't turn off or hibernate during initial encryption

Audit Log Issues:

Problem: Can't open secpol.msc

- Solution: secpol.msc only available on Pro/Enterprise/Education editions
- Use Group Policy Editor: gpedit.msc → Computer Config → Windows Settings → Security Settings

Problem: Security log fills up quickly

- Increase log size: Right-click Security log → Properties → Increase max size
- Enable archiving: Select 'Archive the log when full, do not overwrite events'
- Create automated backup: Use Task Scheduler to backup logs weekly

Problem: Too many events, can't find what I need

- Use Event Viewer filters: Right-click log → Filter Current Log
- Filter by Event ID (4624, 4625, etc.)
- Filter by date range or keywords

Password Policy Issues:

Problem: Policy changes don't affect existing passwords

- Expected behavior: Policies only apply to NEW passwords
- Solution: Force password reset for all users using lusrmgr.msc
- Or set 'Maximum password age' to force periodic changes

Problem: Account locks out too frequently

- Adjust 'Account lockout threshold' to higher value (10-15 attempts)
- Increase 'Reset account lockout counter after' to 60 minutes
- Educate users about password requirements

User Account Issues:

Problem: Can't access lusrmgr.msc

- Only available on Pro/Enterprise/Education editions
- Alternative: Use Computer Management → Local Users and Groups
- Or use Command Prompt: net user [username] *

Problem: Forgot to save a recovery password before changing

- If user is still logged in: Control Panel → User Accounts → Manage Another Account
- Create password reset disk immediately
- If locked out: Use admin account or password reset disk

Task Scheduler Issues:

Problem: Scheduled scan doesn't run

- Check task is enabled: Task Scheduler → Find task → Ensure 'Ready' status
- Verify path to MpCmdRun.exe is correct
- Check History tab for error messages
- Ensure 'Run with highest privileges' is checked

Problem: Task runs but scan doesn't complete

- Increase startup delay to 2-3 minutes
- Check Windows Security for scan results
- Try running MpCmdRun.exe manually to test
- Check system resources - scan may be too heavy for startup

ADDITIONAL RESOURCES & VERIFICATION

How to Verify Your Security Hardening:

After completing all five tips, verify your system is properly secured:

Security Measure	Verification Method
BitLocker	Control Panel → BitLocker → Verify 'On' status
Audit Logs	eventvwr.msc → Security log should show recent events
Password Policy	secpol.msc → Verify settings match recommendations
User Passwords	lusrmgr.msc → Check account properties
Startup Scan	taskschd.msc → Find task and verify 'Ready' status

Best Practices Summary:

✓ Review audit logs weekly for suspicious activity
✓ Keep all software and Windows updated
✓ Use different, strong passwords for each account
✓ Consider using a password manager (LastPass, 1Password, Bitwarden)
✓ Enable Windows Defender Real-Time Protection
✓ Create regular backups of important data
✓ Don't disable security features for convenience
✓ Educate other users on the system about security
✓ Keep recovery keys and passwords in secure, separate locations
✓ Re-audit your system every 3-6 months

Additional Learning Resources:

- CyberPatriot: www.uscyberpatriot.org
- NIST Cybersecurity Framework: www.nist.gov/cyberframework
- Microsoft Security Documentation: docs.microsoft.com/security
- SANS Security Resources: www.sans.org/security-resources
- OWASP Top 10: owasp.org/www-project-top-ten

YOUR SECURITY SCORE

After completing all five security measures, calculate your security improvement score. Each completed tip significantly reduces your attack surface and improves your overall security posture.

Security Measure	Completed?	Security Value
BitLocker Encryption	■	25 points
Audit Logs Enabled	■	20 points
Password Policies	■	20 points
Strong User Passwords	■	20 points
Startup Antivirus Scan	■	15 points
	Total:	**/100 points**

90-100 points: Excellent! Your system has strong baseline security.

70-89 points: Good progress. Complete remaining measures for full protection.

50-69 points: Fair. You're on the right track - keep going!

Below 50: Your system needs immediate security improvements.

Congratulations on taking control of your cybersecurity!

Remember: Security is an ongoing process, not a one-time task. Stay vigilant, keep learning, and regularly review your security measures.

Created by Advaith Banigandlapati | CyberPatriot Competitor
Portfolio: [Your Website] | GitHub: @advaithbanigandlapati-coder
Questions? Contact: advaithaltacc@gmail.com