# SECURITY AUDIT CHECKLIST

Zikhona secures systems and designs futures.

Contents

PROJECT OVERVIEW ........................3
Password Security Audit ...................4
Firewall Configuration Review...........5
Software & System Updates.............6
Antivirus & Malware Protection .........7
■ 5. Encryption & Data Protection .9
■ 6. User Access Control Review.....10
■ SUMMARY OF SECURITY IMPROVEMENTS ...........................11
REFLECTION & LEARNING.............11
CONCLUSION...............................12

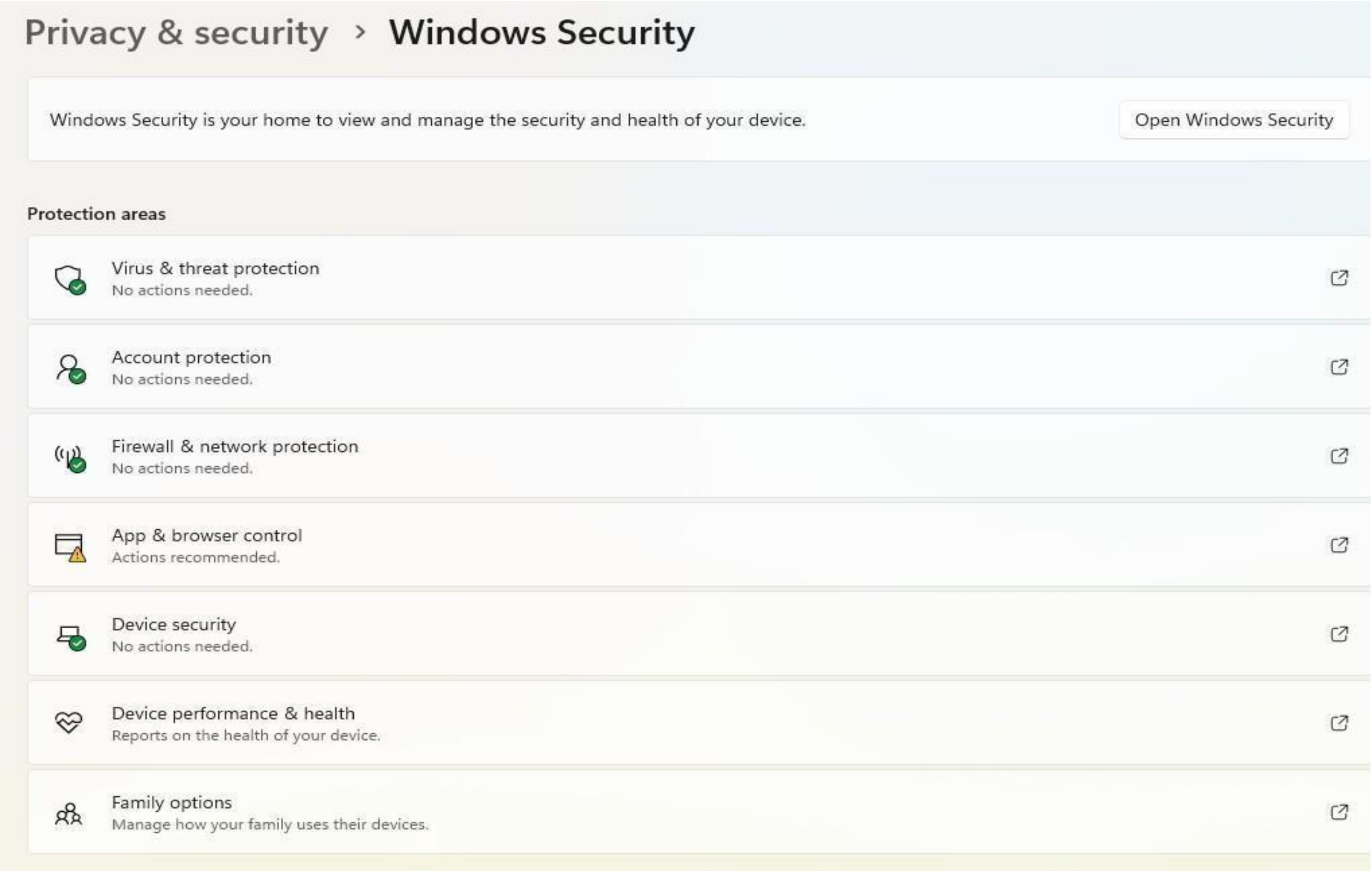
# IT Security: Defense Against the Digital Dark Arts

Focus Areas: Encryption & Authentication | Firewalls | Security Best Practices

## PROJECT OVERVIEW

This project focuses on performing a basic system security audit to identify, strengthen, and maintain essential protection mechanisms within a personal or organizational IT environment. The audit covers password security, firewall protection, software updates, encryption, and access control.

Picture 1: System’s main security dashboard .



Privacy & security > Windows Security

Windows Security is your home to view and manage the security and health of your device.

Protection areas

Virus & threat protection
No actions needed.

Account protection
No actions needed.

Firewall & network protection
No actions needed.

App & browser control
Actions recommended.

Device security
No actions needed.

Device performance & health
Reports on the health of your device.

Family options
Manage how your family uses their devices.

## Password Security Audit

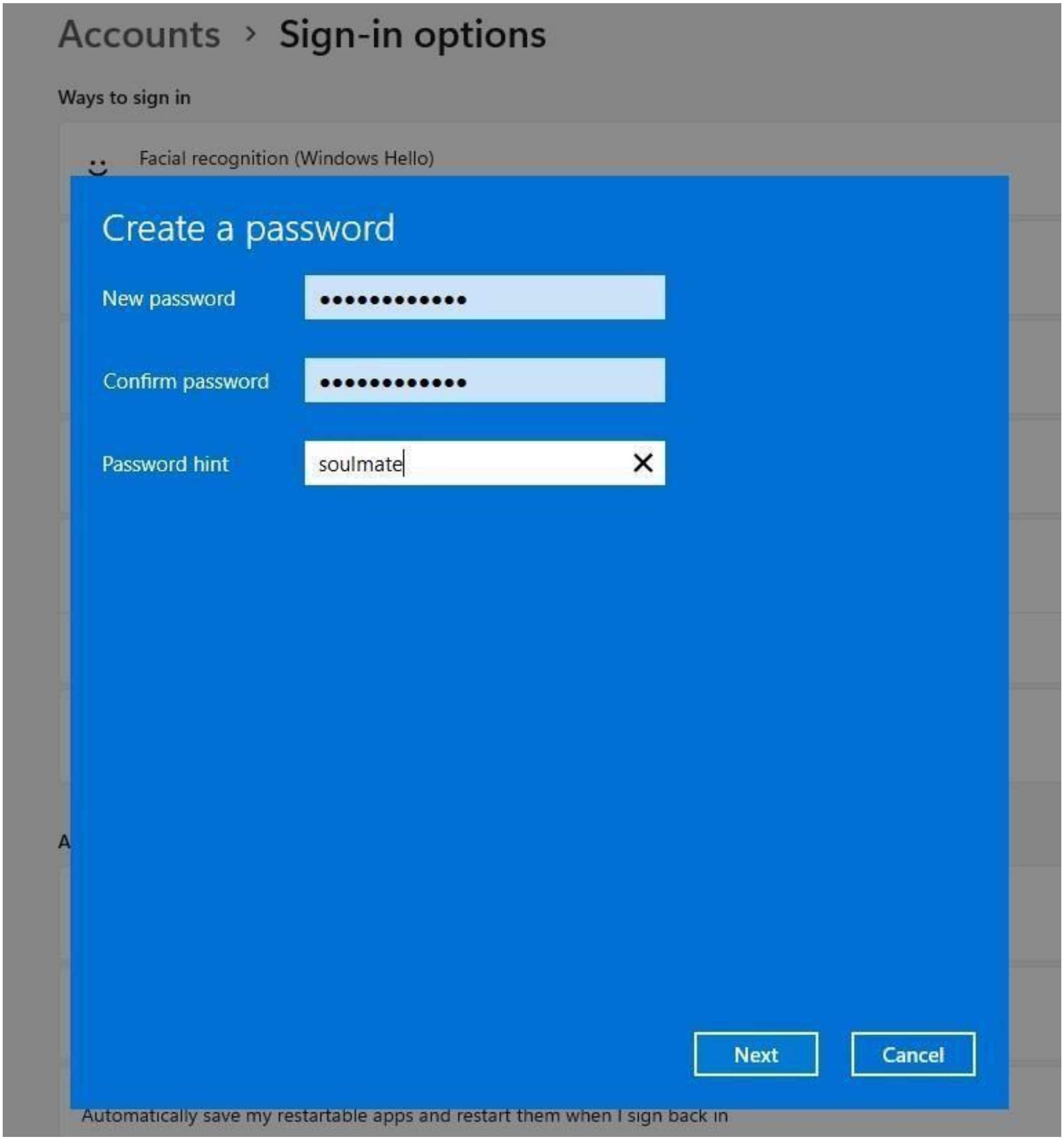
Objective: Assess password strength and update weak or reused credentials.

Actions Taken:

- Replaced short passwords with passphrases of 12+ characters combining uppercase, lowercase, symbols, and numbers.
- Enabled Two-Factor Authentication (2FA) on critical accounts (email, cloud storage, admin login).
- Stored credentials securely using a password manager.

Outcome: Improved credential integrity and reduced risk of brute-force attacks.

Picture 2: Password manager or password policy settings



Accounts > Sign-in options

Ways to sign in

Facial recognition (Windows Hello)

Create a password

New password: ●●●●●●●●●●●●●

Confirm password: ●●●●●●●●●●●●●

Password hint: soulmate

Automatically save my restartable apps and restart them when I sign back in

## Firewall Configuration Review

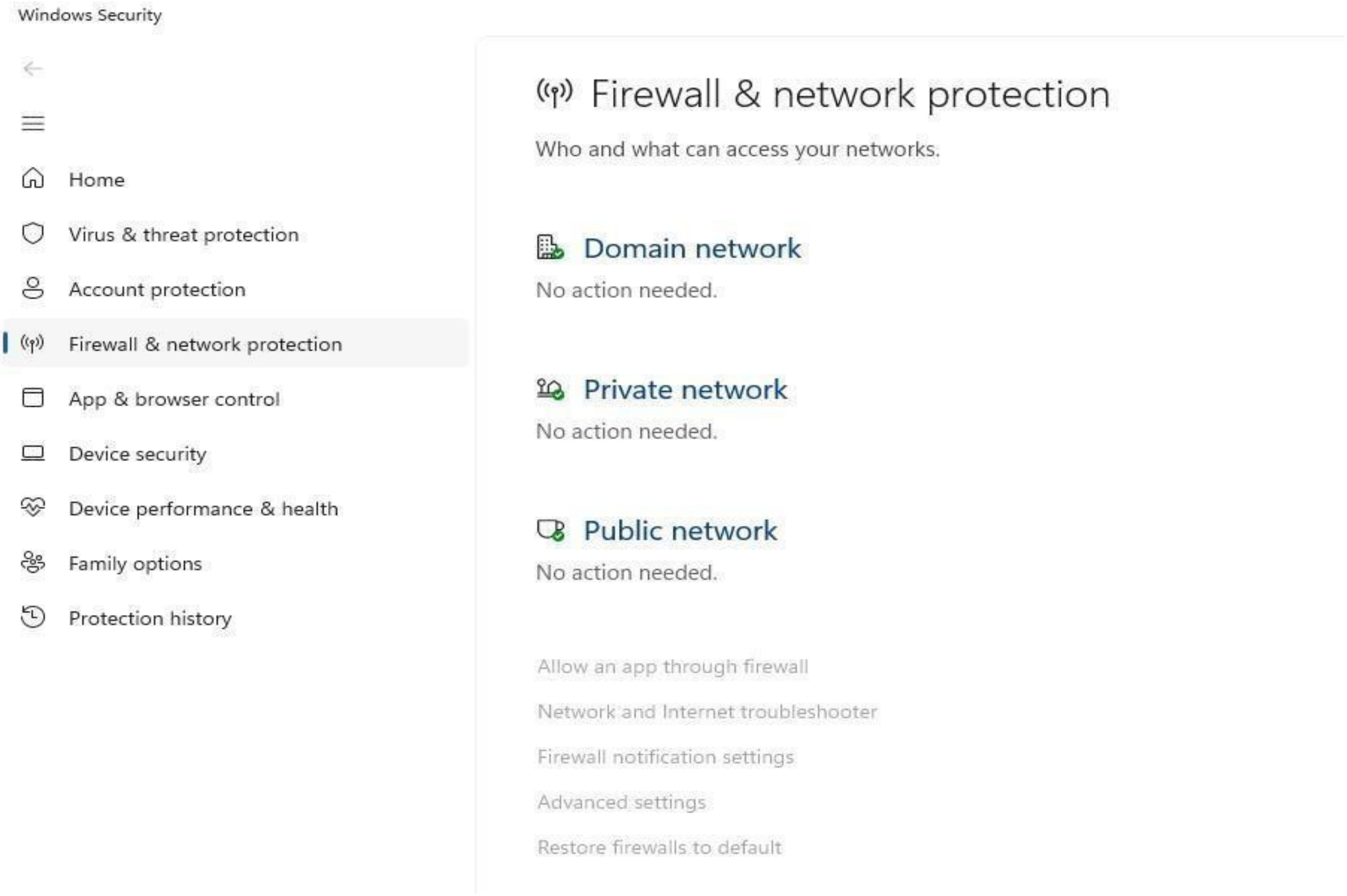
Objective: Verify firewall activity and confirm it’s filtering inbound and outbound traffic.

Actions Taken:

- Ensured Windows Defender Firewall is active.
- Created custom rules to block unused ports.
- Assessed connection restrictions for external traffic.

Outcome: Enhanced perimeter defense and minimized exposure to external threats.

Picture 3: Firewall settings showing 'Firewall is ON' for all network profiles.



Windows Security

Firewall & network protection

Who and what can access your networks.

Domain network

No action needed.

Private network

No action needed.

Public network

No action needed.

Home
Virus & threat protection
Account protection
Firewall & network protection
App & browser control
Device security
Device performance & health
Family options
Protection history
Allow an app through firewall
Network and Internet troubleshooter
Firewall notification settings
Advanced settings
Restore firewalls to default

## Software & System Updates

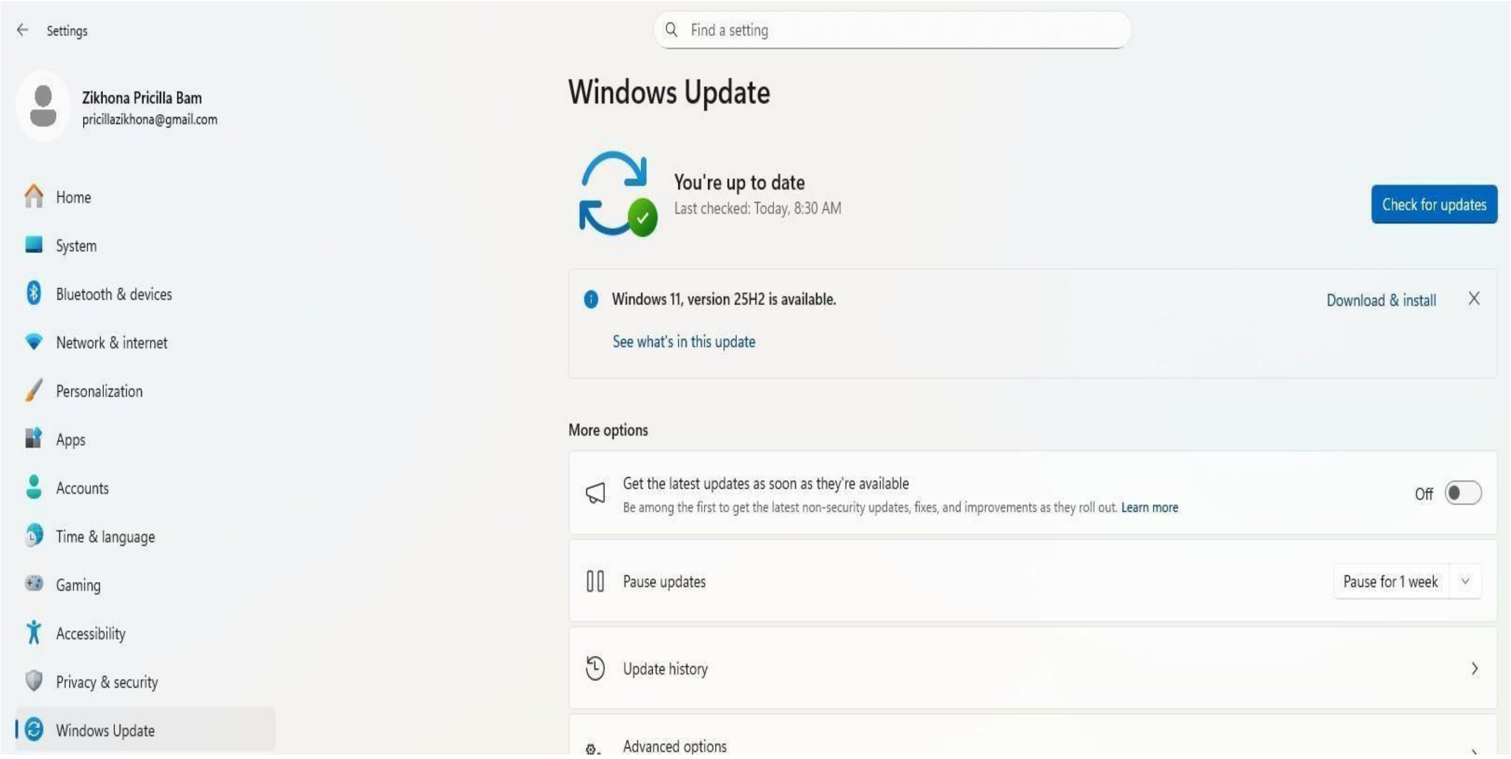
Objective: Ensure systems and applications are fully updated.

Actions Taken:

- Performed full Windows Update and browser patches.
- Enabled automatic updates for continued protection.

Outcome: Reduced vulnerability exposure and improved system patch management.

Picture 4: Screenshot of system update status.



Zikhona Pricilla Bam
pricillazikhona@gmail.com

Windows Update

You're up to date
Last checked: Today, 8:30 AM

Windows 11, version 25H2 is available.
See what's in this update

More options

Get the latest updates as soon as they're available — Off
Be among the first to get the latest non-security updates, fixes, and improvements as they roll out. Learn more

Pause updates — Pause for 1 week

Update history

Advanced options

## Antivirus & Malware Protection

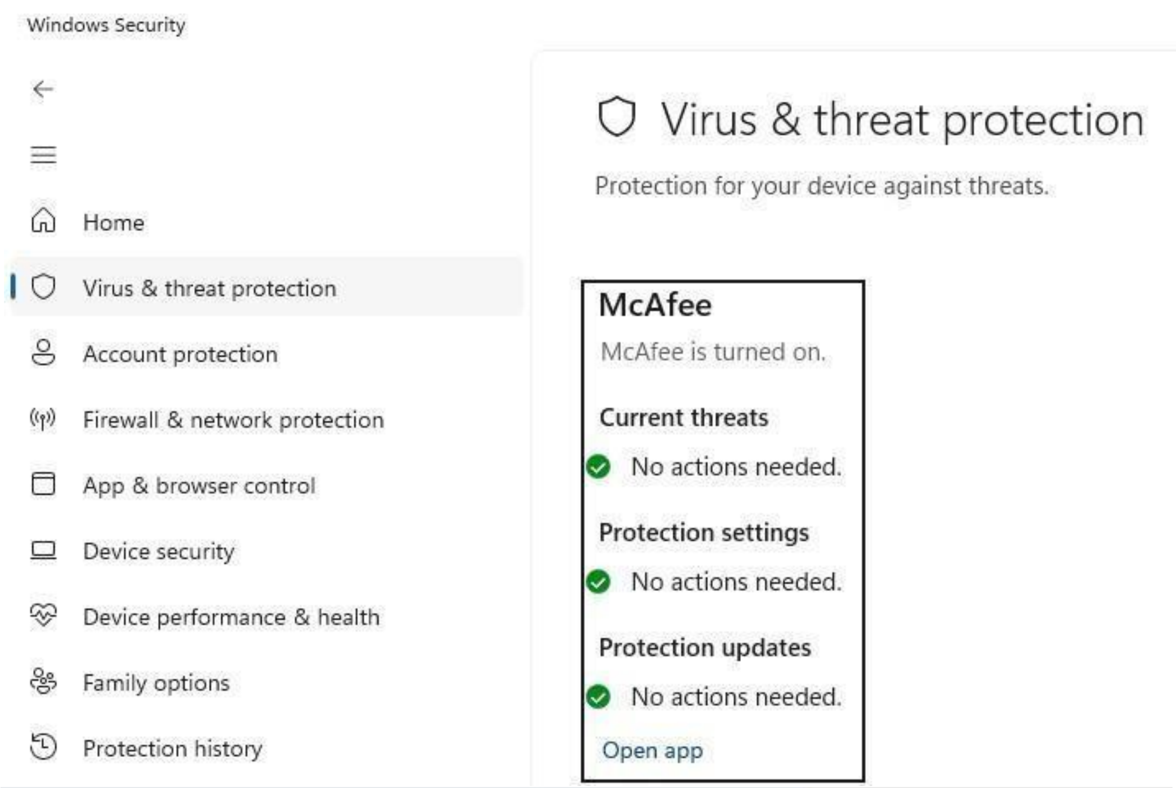
Objective: Verify antivirus software is updated and scanning regularly.

Actions Taken:

- Confirmed real-time protection is enabled.
- Completed a full system scan (no threats detected).
- Scheduled weekly automatic scans.

Outcome: Maintains defense against malware and ransomware.

Picture 5: Antivirus dashboard showing scan results.



Virus & threat protection

Protection for your device against threats.

McAfee

McAfee is turned on.

Current threats

✓ No actions needed.

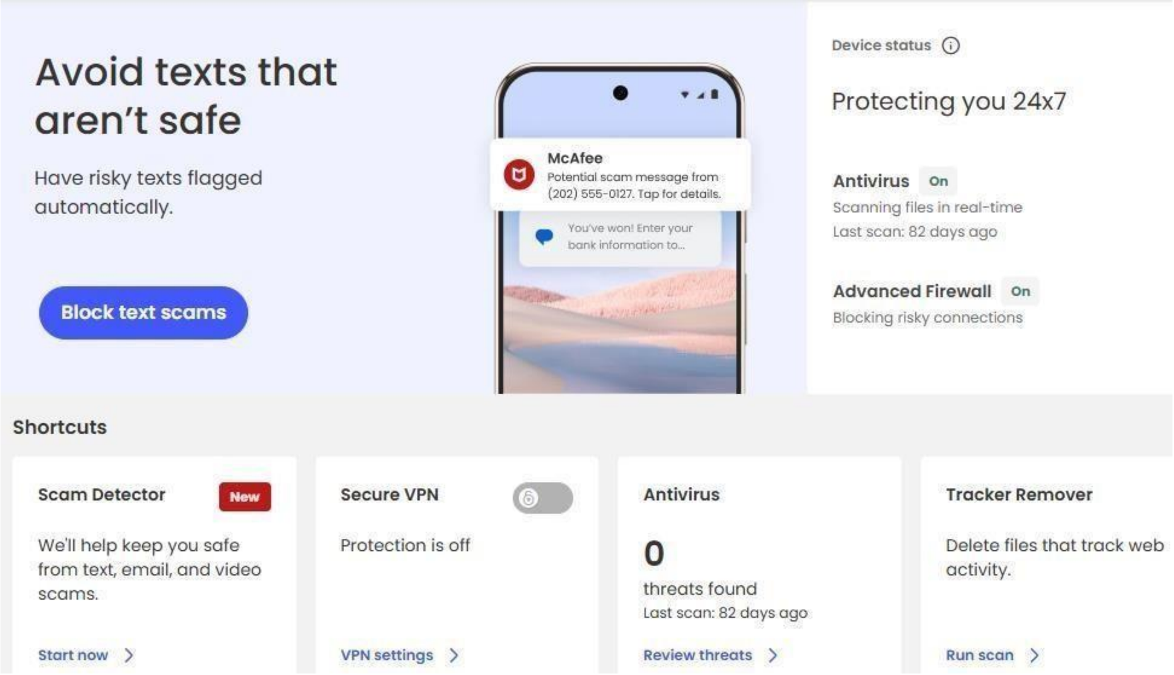
Protection settings

✓ No actions needed.

Protection updates

✓ No actions needed.

Open app



Avoid texts that aren't safe

Have risky texts flagged automatically.

McAfee
Potential scam message from (202) 555-0127. Tap for details.

You've won! Enter your bank information to...

Device status

Protecting you 24x7

Antivirus On
Scanning files in real-time
Last scan: 82 days ago

Advanced Firewall On
Blocking risky connections

Shortcuts

Scam Detector New
We'll help keep you safe from text, email, and video scams.
Start now >

Secure VPN
Protection is off
VPN settings >

Antivirus
0
threats found
Last scan: 82 days ago
Review threats >

Tracker Remover
Delete files that track web activity.
Run scan >

## 5. Encryption & Data Protection

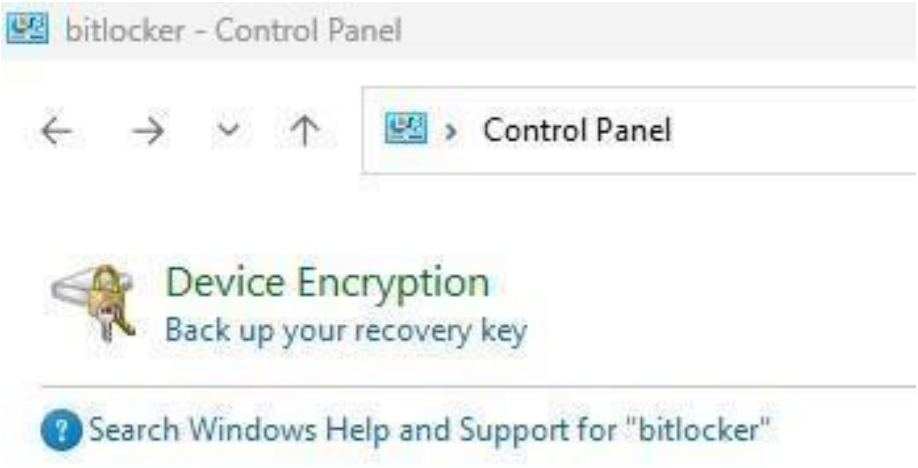
Objective: Confirm encryption is active for sensitive data.

Actions Taken:

- Verified disk encryption (BitLocker/File Vault) is active.
- Ensured HTTPS/TLS for secure communication.
- Recommended encryption for backup drives.

Outcome: Improved data confidentiality and protection from thieves.

Picture 6: Screenshot of encryption settings.



bitlocker - Control Panel

Control Panel

Device Encryption

Back up your recovery key

Search Windows Help and Support for "bitlocker"

## 6. User Access Control Review

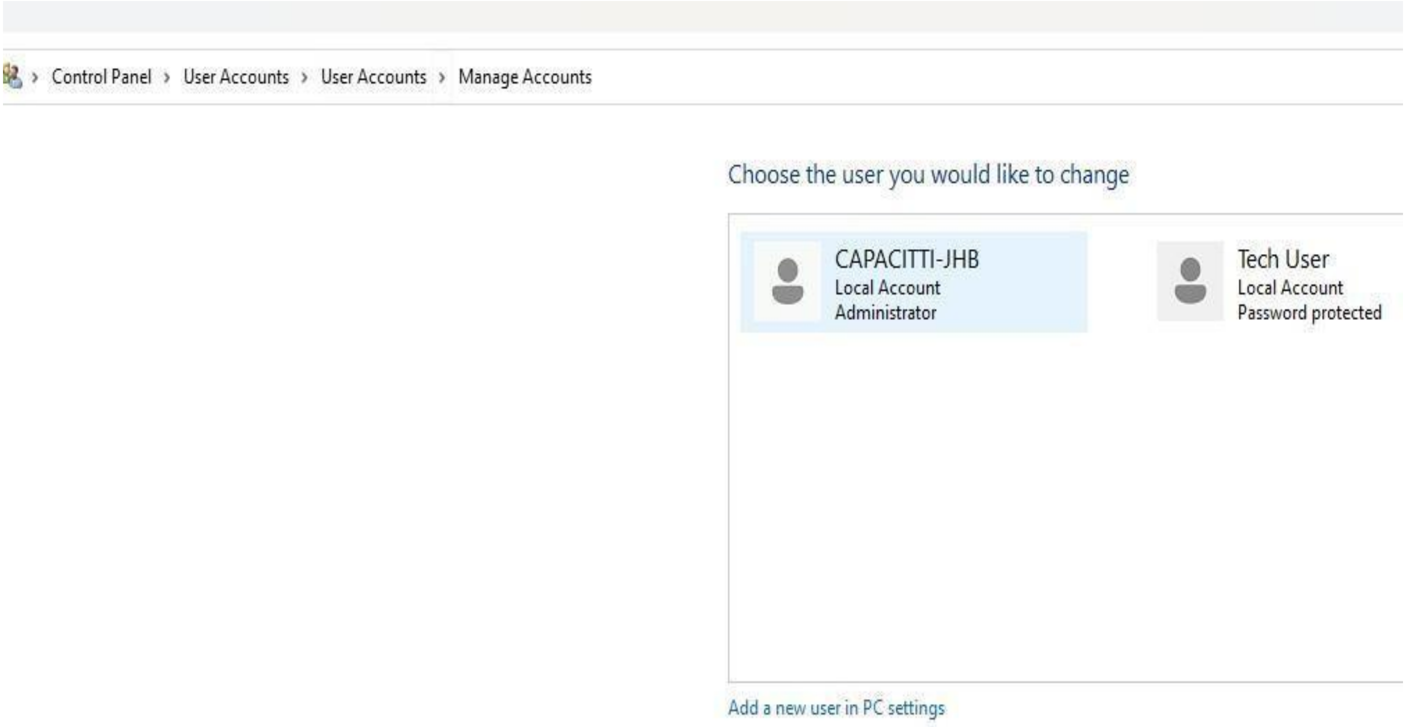
Objective: Review user permissions and minimize admin accounts.

Actions Taken:

- Disabled unused accounts.
- Converted admin accounts to standard users.
- Applied least privilege principle for daily operations.

Outcome: Reduced insider threat potential and unauthorized configuration risks.

Picture 7: User accounts list showing limited admin access.



› Control Panel › User Accounts › User Accounts › Manage Accounts

Choose the user you would like to change

CAPACITTI-JHB
Local Account
Administrator

Tech User
Local Account
Password protected

Add a new user in PC settings

## ■ SUMMARY OF SECURITY IMPROVEMENTS

| ■ Area | ■ Status | ■ Key Improvement |
|---|---|---|
| Passwords | ■ Strengthened | Introduction: MFA & password manager |
| Firewall | ■ Active | Custom rules for better control |
| Updates | ■ Automated | Scheduled patches weekly |
| Antivirus | ■ Up to Date | Real-time scanning enabled |
| Encryption | ■ Enabled | Disk & communication encryption verified |
| Access Control | ■ Tightened | Reduced admin privileges |

## REFLECTION & LEARNING

This audit demonstrated that cybersecurity relies on multiple layers of defense — from strong authentication to initiative-taking maintenance. Continuous vigilance, timely updates, and awareness are key to maintaining resilience against modern threats. Combining technical controls with human behavior forms the foundation of robust digital protection.

## CONCLUSION

Security is a moving target — staying safe means staying initiative-taking. Regular audits, updates, and security awareness are essential steps toward building a sustainable cybersecurity culture.