



**Cyber Wise Corp**

# Cybersecurity Assessment Report

Expert-reviewed by CISSP-certified security professionals

**Prepared for: Sarah and Michael Chen**

[Address withheld for privacy], Phoenix, AZ, 85016

## OVERALL SECURITY POSTURE

# B

**Strong**

Score: 16/20 (80.0%)

Report ID: DEMO-HOM

Generated May 03, 2026

## Executive Summary

# B

### Strong - Score: 16/20 (80.0%)

Your security is solid and above the typical household or small business. A few targeted improvements will move you into the top tier. None of the gaps put you at immediate risk.

### Your Top Priorities

#### > Device Security (3/5)

1) Enable BitLocker on the Windows desktop today (Settings > Privacy & Security > Device Encryption).

#### > Network Security (4/5)

1) Disable WPS in the router admin panel (Wireless > Advanced) - this is the highest-impact change you can make in 60 seconds.

#### > Data Security (4/5)

1) Add a third backup tier: an encrypted external drive stored at a relative's house or in a safe deposit box, refreshed every 6 months.

### What You Are Doing Well

#### + User Awareness (5/5)

All adults in the household use 1Password with strong unique passwords for every account (audited 247 entries during the assessment).

#### + Data Security (4/5)

Backup strategy: iCloud is active for both iPhones and the MacBook (encrypted, current as of yesterday).

#### + Network Security (4/5)

Single-router setup using a Netgear R7000P (firmware updated within the last 90 days).

### ! CRITICAL FINDINGS - Address Within 7 Days

- ! HP printer on the LAN has an open Telnet port (TCP 23) and the admin interface is using the default 'admin/admin' credentials. Combined, this is remotely exploitable from anywhere on the home network and could be used to pivot to other devices. Address within 7 days.
- ! TP-Link smart plug retains factory default credentials. Devices like this have been the entry point for the Mirai botnet and similar IoT-based attacks. Change the password through the Kasa app today.

## Report Information

---

<b>Report ID</b>	DEMO-HOM
<b>Client</b>	Sarah and Michael Chen
<b>Service Address</b>	[Address withheld for privacy], Phoenix, AZ, 85016
<b>Service Type</b>	Home Assessment
<b>Assessor</b>	Jordan Reyes - Grand Canyon University
<b>Expert Reviewer</b>	Robert Hibler, CISSP, CCSP, CISM
<b>Generated</b>	2026-05-03 09:10 UTC

## Assessor's Full Summary

---

This household demonstrates strong overall cybersecurity hygiene that puts them in the top 20% of homes we assess. Password practices, MFA adoption, and patching discipline are all excellent. The grade was held back primarily by Device Security: two IoT devices with default credentials (a smart plug and a printer) and missing disk encryption on the Windows desktop. None of these are immediate emergencies, but the printer with open Telnet plus default admin is a meaningful exposure that should be closed this week. With the items in the THIS WEEK and THIS MONTH sections of the roadmap addressed, this household would move solidly into the A range. Special call-out: the family's password and MFA discipline is a model example - many households we assess have one strong user and several weak ones, which creates a single point of failure. This family has consistent practices across all members.

## Detailed Category Breakdown

---

Each category is scored on a 5-point scale. The 'industry baseline' shows the average score for households or small businesses we have assessed - use it to gauge where you stand relative to your peers.

### Network Security

**4/5 - B (Strong)**

*16% above industry baseline (64%)*

#### What this measures

Your home or office WiFi, router, and how cleanly your network is segmented.

#### Why it matters

Your network is the front door. A poorly configured router or weak WiFi password lets attackers onto your network without ever touching your devices, where they can intercept traffic, attack other devices, or use your bandwidth for illegal activity.

#### Threats this protects against

- \* Wardriving and unauthorized WiFi access
- \* Router admin compromise
- \* Lateral movement between devices

#### Assessor's findings at your location

Single-router setup using a Netgear R7000P (firmware updated within the last 90 days). WiFi encryption: WPA3 on the primary 5 GHz network, WPA2 on the 2.4 GHz network for legacy IoT devices. Primary WiFi password is 18 characters with high entropy. Router admin password was changed from the default 'password' to a unique strong password. A guest network is configured for visitors but is not isolated from the LAN - guest devices can still reach the network printer and smart hub. WPS (WiFi Protected Setup) is currently enabled, which is brute-forceable in roughly 4-10 hours.

#### Recommendations

1) Disable WPS in the router admin panel (Wireless > Advanced) - this is the highest-impact change you can make in 60 seconds. 2) Enable router auto-update so security patches install without you needing to remember. Netgear calls this 'Automatic Firmware Update' under Administration. 3) Enable AP isolation on the guest network so guest devices can reach the internet but not your internal devices. 4) Consider migrating IoT devices to the guest VLAN once isolation is on; this limits blast radius if a smart bulb or doorbell is ever compromised.

## Device Security

**3/5 - D (Needs Attention)**

*2% above industry baseline (58%)*

### What this measures

Operating system patching, endpoint protection (antivirus/EDR), disk encryption, and IoT device hygiene.

### Why it matters

Devices are where attackers actually do damage - installing ransomware, stealing data, or pivoting to other systems. An unpatched OS or default-password IoT device is the most common entry point in residential breaches.

### Threats this protects against

- \* Ransomware
- \* Credential theft via malware
- \* IoT botnet recruitment (Mirai-style)

### Assessor's findings at your location

Three primary computers assessed: a Windows 11 desktop (build 23H2, fully patched, Microsoft Defender active), a 2021 MacBook Air running macOS Sonoma 14.4 (also fully patched, XProtect active), and a Chromebook used by a teenager (auto-updates working). Disk encryption status: BitLocker NOT enabled on the Windows desktop, FileVault enabled on the MacBook, Chromebook encrypted by default. IoT inventory: Ring doorbell (firmware current), Nest thermostat (firmware current, password changed from default), four Philips Hue bulbs (firmware current), one TP-Link smart plug still using its default password 'admin/admin', one older HP printer with default admin password and an open Telnet port on the LAN. Two iPhones and one iPad - all on iOS 17.4 with automatic updates enabled.

### Recommendations

1) Enable BitLocker on the Windows desktop today (Settings > Privacy & Security > Device Encryption). Without it, a stolen laptop = stolen data. 2) Change the TP-Link smart plug password (the smartphone app settings, not the WiFi password). Default credentials on internet-connected devices are the #1 vector for residential botnet recruitment. 3) Disable Telnet on the HP printer via its web admin interface and change its admin password. If you only use the printer locally, also block its WAN access in your router's parental controls. 4) For the Chromebook user (teenager), consider enabling Family Link to monitor downloaded extensions, which is the most common malware vector for this age group.

## Data Security

4/5 - B (Strong)

28% above industry baseline (52%)

### What this measures

Backup strategy, where files are stored, and how data is shared with others.

### Why it matters

If something goes wrong - hardware failure, ransomware, theft - your backup is the only thing standing between an inconvenience and a catastrophe. The 3-2-1 rule (3 copies, 2 different media, 1 offsite) remains the gold standard.

### Threats this protects against

- \* Ransomware encryption (no recovery without backup)
- \* Hardware failure / theft
- \* Accidental data exposure via misconfigured cloud sharing

### Assessor's findings at your location

Backup strategy: iCloud is active for both iPhones and the MacBook (encrypted, current as of yesterday). The Windows desktop is using OneDrive Personal Vault for sensitive documents (encrypted, MFA-protected). A 4 TB external drive is connected to the MacBook and runs Time Machine weekly. No third offsite backup, which is the missing leg of the 3-2-1 rule. Cloud sharing posture: checked Google Drive and OneDrive sharing settings - 2 documents currently shared 'with anyone who has the link' (an old shopping list and a meal plan, both non-sensitive). Photo backup: iCloud Photos enabled, no other copies. Family financial documents (tax returns, bank statements) are in OneDrive Personal Vault - good.

### Recommendations

1) Add a third backup tier: an encrypted external drive stored at a relative's house or in a safe deposit box, refreshed every 6 months. This is your insurance against ransomware - if your local AND cloud backups encrypt at the same time (which has happened), the offline copy is the only thing that gets you back. 2) Audit and revoke the two 'anyone with link' shares - even non-sensitive documents indexed by search engines reveal information about you. 3) Consider a paid Backblaze or iDrive subscription as a fully separate cloud backup (different vendor than iCloud/OneDrive).

## User Awareness

5/5 - A (Excellent)

39% above industry baseline (61%)

### What this measures

Password practices, multi-factor authentication adoption, and ability to recognize phishing.

### Why it matters

Over 80% of breaches start with a human element - reused passwords, falling for a phishing email, or skipping MFA prompts. The strongest technical controls fail if a single account gets compromised through social engineering.

### Threats this protects against

- \* Phishing and credential theft
- \* Account takeover via password reuse
- \* SIM-swap attacks bypassing SMS-only MFA

### Assessor's findings at your location

All adults in the household use 1Password with strong unique passwords for every account (audited 247 entries during the assessment). MFA enabled on: primary email (Gmail with hardware key), banking (3 accounts, all using authenticator app rather than SMS), Apple ID, Microsoft account, 1Password itself, and major shopping sites. The teenager's accounts use the family 1Password but MFA is uneven on social media. Phishing test: showed the household 5 simulated phishing emails - 5 of 5 correctly identified as suspicious by the adults, 3 of 5 by the teenager. Family discussed and understands the 'verify through a separate channel' rule for any payment, login, or urgent request. No password reuse detected.

### Recommendations

1) Enable MFA on the teenager's social media accounts (Instagram, TikTok, Snapchat) using the authenticator app. Account takeover for teens is most often used to scam their friends and family contacts. 2) Have the teenager complete a free 30-minute phishing awareness module (several available from CISA at [cisa.gov/secure-our-world](https://cisa.gov/secure-our-world)). 3) Rotate the 1Password master password annually as a healthy hygiene habit.

## 30 / 60 / 90 Day Remediation Roadmap

---

A practical sequence for addressing the items in this report. Most items can be done in well under the suggested timeframe - the windows are deliberately generous so progress feels achievable. If you only do the THIS WEEK items, you will close the highest-impact gaps.

### THIS WEEK - Critical Findings (P0)

- ! HP printer on the LAN has an open Telnet port (TCP 23) and the admin interface is using the default 'admin/admin' credentials. Combined, this is remotely exploitable from anywhere on the home network and could be used to pivot to other devices. Address within 7 days.
- ! TP-Link smart plug retains factory default credentials. Devices like this have been the entry point for the Mirai botnet and similar IoT-based attacks. Change the password through the Kasa app today.

### THIS MONTH - High-Risk Categories (P1)

*(Nothing in this tier - well done.)*

### THIS QUARTER - Medium-Risk Improvements (P2)

#### > Device Security

- 1) Enable BitLocker on the Windows desktop today (Settings > Privacy & Security > Device Encryption). Without it, a stolen laptop = stolen data.

### NEXT 6 MONTHS - Optimization (P3)

#### > Network Security

- 1) Disable WPS in the router admin panel (Wireless > Advanced) - this is the highest-impact change you can make in 60 seconds.

#### > Data Security

- 1) Add a third backup tier: an encrypted external drive stored at a relative's house or in a safe deposit box, refreshed every 6 months.

#### > User Awareness

- 1) Enable MFA on the teenager's social media accounts (Instagram, TikTok, Snapchat) using the authenticator app.

## Appendix: Glossary

---

### MFA / 2FA

Multi-Factor Authentication. Requires a second proof of identity (app code, hardware key, biometric) beyond just a password. Use an authenticator app (Authy, Google Authenticator, 1Password) over SMS when possible - SMS can be intercepted via SIM swapping.

### WPA3 / WPA2

WiFi encryption standards. WPA3 is current and strongest (mandatory on devices sold after 2020). WPA2 is acceptable if WPA3 is not supported. WEP and "Open" are obsolete and easily cracked.

### Endpoint Protection

Software that detects and blocks malicious activity on a device (antivirus, anti-ransomware). Modern operating systems have decent built-in options (Microsoft Defender, XProtect on macOS) - third-party tools add features but built-in is far better than nothing.

### IoT

Internet of Things - smart devices like thermostats, doorbells, smart bulbs, voice assistants. They run software, connect to the internet, and often have weak default security. Treat each one as a tiny computer that could be hijacked.

### Phishing

Fraudulent emails, texts, or calls designed to trick you into revealing credentials or clicking malicious links. Modern phishing is highly convincing - always verify unexpected payment, login, or "urgent" messages through a separate channel.

### Password Manager

Software that generates and stores unique strong passwords for every account, protected by one master password. Examples: 1Password, Bitwarden, Apple Keychain. Eliminates the #1 weakness: password reuse.

### Backup Rule (3-2-1)

3 copies of important data, on 2 different types of media (local drive + external), with 1 copy offsite (cloud or physically remote). Protects against device failure, theft, fire, and ransomware.

### NIST CSF

National Institute of Standards and Technology Cybersecurity Framework. The U.S. government standard for security practices, organized around five functions: Identify, Protect, Detect, Respond, Recover. CWC assessments align with this framework.

## Free + Low-Cost Tools We Recommend

---

CWC has no financial relationship with any of these vendors.

### Have I Been Pwned ([haveibeenpwned.com](https://haveibeenpwned.com))

Check if your email or password has appeared in a data breach. Sign up for notifications to get alerted to future breaches.

### Bitwarden ([bitwarden.com](https://bitwarden.com))

Free, open-source password manager with cross-device sync.

### Authy ([authy.com](https://authy.com))

Free authenticator app for MFA codes - works across devices with encrypted cloud backup.

### Microsoft Defender (Built into Windows 10/11)

Solid baseline antivirus and ransomware protection - already on your Windows PC. Just keep it enabled.

#### **Tailscale ([tailscale.com](https://tailscale.com))**

Free for personal use - secure WireGuard-based VPN for remote access to your home network.

#### **CIS Benchmarks ([cisecurity.org/cis-benchmarks](https://cisecurity.org/cis-benchmarks))**

Free hardening guides for Windows, macOS, routers, and more. Not light reading but authoritative.

## **When to Reassess**

---

Schedule a fresh assessment whenever any of the following happens:

- > It has been 12 months since your last assessment.
- > You moved to a new home or office (new network, new threat surface).
- > You added significant new technology - smart home system, business server, IoT cluster.
- > You experienced a security incident, even a small one (suspicious email, unauthorized login alert, lost device).
- > A family member or employee left the household / business with shared access to accounts or devices.

## **About This Report**

---

This assessment was performed in person by a Cyber Wise Corp assessor and reviewed for accuracy and completeness by a CISSP-certified security professional before delivery. Our methodology aligns with the NIST Cybersecurity Framework (Identify, Protect, Detect, Respond, Recover) and the CIS Critical Security Controls.

No assessment can identify every possible vulnerability, and no recommendation guarantees protection against all threats. This report reduces your risk - it does not eliminate it. For questions about any finding or recommendation, contact us through [cyberwisecorp.com/contact](https://cyberwisecorp.com/contact).