

Practical home and family protection tools. These examples are not endorsements. Choose what fits your needs, budget, and comfort level.



Password Management

Reused or weak passwords remain the #1 cause of account compromise. **What to look for**

- Secure password generation
- Works across desktop and mobile
- Optional breach monitoring

Examples

- Proton Pass – best free option
- 1Password – long-established, feature rich
- BitWarden – free & paid options

Download and keep your password manager recovery keys safe. Don't use password managers built into browsers.

Endpoint Protection (Personal & Small Organization Use)

Antivirus alone is no longer enough.

Baseline protection

- Microsoft Defender (built into Windows)

Optional enhancements / alternatives

- Bitdefender Premium Security (replaces Defender)
- Sophos Home (replaces Defender)
- Malwarebytes Free (manually scan for malware, does not replace Defender)

Layered security improves detection and response.

Multi-Factor Authentication (MFA)

MFA blocks most account takeovers—even if your password is stolen. **Authentication apps**

- Microsoft Authenticator – best for business, especially Microsoft-centric orgs
- Google Authenticator – simple, secure, harder to recover if device is lost
- Authy – Encrypted cloud backups, easy recovery if device is lost

Use app-based MFA whenever possible; avoid SMS-only authentication if alternatives exist. Use separate MFA and Password Manager tools.

Browser Security & Privacy

Why it matters: Most phishing and fraud attempts start in the browser. **Helpful browser tools**

- uBlock Origin – blocks malicious ads, trackers, and scripts
- Malwarebytes Browser Guard – stop tech support scams, block malicious sites
- Have I Been Pwned – alerts if your email appears in a data breach

Install only necessary extensions—too many can increase risk.

Email & Scam Awareness (Technology + Behavior)

Many financial losses occur because requests are trusted without verification. **Best practices**

- Verify payment or account changes using a known phone number
- Be skeptical of urgency or pressure ("act now", "final notice")
- Watch for subtle sender-address changes
- Never rely on email alone for financial decisions

Safer DNS (An Easy Win)

Secure DNS can block malicious websites before they load. **More secure than most ISP defaults**

- NextDNS – simple to set up and use, granular controls
- Cloudflare for Families – established content filtering provider
- Quad9 – non-profit managed, focused on privacy

Many phishing and malware sites are automatically blocked without user interaction.