

Zenonym

A 10-item baseline audit covering passwords, 2FA, updates, DNS, encryption, backups, and more.

No special hardware required.

Published: September 2026 | By Zenonym Research Team



Generate a unique, strong password for every account. Use Bitwarden, 1Password, or KeePass.
If you reuse passwords, a single breach exposes everything.



Prefer a hardware security key (YubiKey) over SMS.
If you must use an app, use Authy or Aegis.
Never rely on SMS-based 2FA alone - SIM swaps defeat it.



Enable auto-updates for your OS, browser, and apps.
Most exploited vulnerabilities are patched within days of discovery.
Outdated software is the most common attack vector.



uBlock Origin blocks malicious ads and invisible trackers.
Consider NextDNS or Pi-hole for network-wide blocking.
Ads are the #1 malware delivery vector for average users.



Configure DNS-over-HTTPS (DoH) or DNS-over-TLS (DoT).
Prevents your ISP from seeing every domain you visit.
Cloudflare (1.1.1.1) and Quad9 (9.9.9.9) both support it.



Automatic on iOS and Android. On Windows, turn on BitLocker.
On macOS, enable FileVault. On Linux, use LUKS at install time.

A stolen device without encryption is a compromised device.

☐

Change the default admin password.
Use WPA3 (or WPA2 if WPA3 unavailable). Disable WPS.
Hide your SSID if possible. Update the firmware regularly.

☐

Keep 3 copies of your data, on 2 different media types,
With 1 copy offsite. Encrypt your backups.
Test restoration at least once. Ransomware waits for no one.

☐

Remove old email addresses and phone numbers from recovery.
Do not use SMS as 2FA backup - use offline recovery codes.
Check haveibeenpwned.com for forgotten breached accounts.

☐

Disable location access for apps that do not need it.
Uninstall browser extensions you no longer use.
Each installed app is a potential attack surface.



DNS leak test

Visit dnsleaktest.com - your ISP name should not appear in results.



Breach check

Search haveibeenpwned.com - no password should be shared across breached accounts.



Port scan

Run: `nmap -sT -p 1-1024 localhost` - no unexpected services should be listening.

Published by Zenonym Research Team | September 2026 | This checklist is free to share and print for personal use.