Safe Browsing Cheat Sheet

Cheat Sheet · In-Browser Habits That Prevent Most Infections And Scams.

Most browser-borne attacks are stopped by 30 seconds of awareness. These are the habits that keep your accounts and devices safe without slowing you down.

Inspect Before You Click

- **Hover the link.** Bottom-left corner of your browser shows the real destination URL.
- **Read the domain backwards.** The real domain is the last two parts before the slash. *amazon.security-team.com* = security-team.com (not Amazon).
- **Look for typosquats.** arnazon.com, paypa1.com, microsoft-secure.com — slight misspellings that look right at a glance.
- **Skip URL shorteners** (bit.ly, tinyurl) from anyone you don't fully trust. You can't see where they go.
- **Use a link expander** (unshorten.it, checkshorturl.com) if you have to follow a shortened link.

HTTPS & Certificates

- **Lock icon = HTTPS** — your traffic is encrypted between you and the site. Required for any site that takes a password or payment.
- **Lock icon does NOT mean the site is safe.** Phishing sites use HTTPS too. The lock just means encryption — not legitimacy.
- **Click the lock** for certificate details. The 'Issued to' line should match the company you expect.
- **Browser warns you** ('Your connection is not private' / 'Deceptive site ahead') — believe it. Back out, don't click 'Advanced.'

Downloads

- **Only download from the source.** If you want VLC, get it from videolan.org — not vlc-download-free.com.
- **Watch for double extensions.** 'invoice.pdf.exe' is an executable, not a PDF.
- **Mac:** if it's not in the App Store and you don't know the developer, think twice.
- **Windows:** SmartScreen warnings are usually right. Don't click through.
- **Free 'PC optimisers,' 'driver updaters,' and 'free VPNs'** are 95% malware. Always.

Public Wi-Fi Rules

- Treat any unfamiliar network as hostile. Anything you do is potentially watched.
- Use a VPN, or skip anything sensitive (banking, work logins) until you're on trusted Wi-Fi.
- Verify the network name with staff before joining 'Free_Hotel_WiFi' (could be impostor).
- Disable auto-join for unknown networks. iOS: Settings → Wi-Fi → toggle 'Auto-Join Hotspot.'

DID YOU KNOW?

1 In 4 Americans Reuses A Password Across 5+ Sites.

If yours is one of them, a single breach exposes your whole life. The fix is the password manager you've been putting off — Day 9 of our 30-Day Sprint walks you through it.

Visit Making Sense Of Security →