Beginner's Guide To Malware Protection

Guide · What Different Malware Does, How It Spreads, And The Layered Defence That Stops It.

Who this is for: anyone who wants to understand what malware actually is, how to prevent infection, and what to do if their device is acting strange. Not just rules — the why behind the rules.

What Malware Is

Malware is any software that does something the device's owner didn't intend — usually for the attacker's benefit. It comes in many forms, but they all share three lifecycle stages: **delivery** (how it gets on your device), **execution** (what it does), and **persistence** (how it stays). Defending against malware means breaking the chain at one or more of these stages.

The 8 Major Types

Type	What It Does
Virus	Infects files and replicates when those files are opened or executed
Worm	Self-replicates across networks without any user action
Trojan	Pretends to be legitimate software; opens a back door once installed
Ransomware	Encrypts files and demands payment for the decryption key
Spyware	Secretly monitors and exfiltrates data (keystrokes, screenshots, mic)
Adware	Aggressive advertising, browser hijacking, search redirects
Rootkit	Hides at the operating-system level; very hard to detect
Fileless malware	Runs entirely in memory; no file on disk to scan

How It Gets In

- **Phishing** — clicked link, downloaded attachment.
- **Drive-by download** — visiting a compromised website triggers automatic download.
- **Trojan disguise** — 'free PC optimiser,' fake VPN, pirated software.
- **USB drives** — from untrusted sources or 'found' in parking lots.
- **Software vulnerabilities** — unpatched software exploited remotely.
- **Malicious browser extensions** — installed accidentally or via fake update prompts.
- **Compromised legitimate software** — supply-chain attacks (rare but devastating).
- **RDP / network exploitation** — for businesses with remote access exposed to the internet.

The Layered Defence

Layer 1 — Don't Get It Onto The Device

- Don't open unexpected attachments. Verify with the sender via a different channel first.
- Don't download 'free' utility software unless from a vendor you trust by name (the App Store, the Microsoft Store, well-known direct-download sites).
- Pirated software is malware delivery. Almost always bundled.
- Hover over links before clicking. Check destination URLs.
- If a website tells you to install a special viewer / driver / update — close it. Real updates come from system settings, not random websites.

Layer 2 — Stop It From Executing

- Modern OS (Windows 11, recent macOS) blocks unsigned executables by default — don't override this.
- Don't run as administrator for daily work. Use a standard user account.
- Office macro warnings exist for a reason. Don't enable macros in documents from outside your organisation.
- Browser warnings ('this site may be deceptive') — believe them.

Layer 3 — Catch It If It Runs

- Microsoft Defender (built-in to Windows) is solid and free.
- macOS XProtect (built-in) is solid for App Store apps.
- Add a second-opinion scanner: Malwarebytes Free or ESET Online Scanner. Run monthly.
- Endpoint Detection & Response (EDR) tools are worth the upgrade for SMBs.

Layer 4 — Recover If It Wins

- **3-2-1 backups** are the ultimate ransomware defence. With clean backups, you wipe and restore — never pay.
- Recovery codes for MFA stored offline (so account compromise doesn't lose them).
- Document your recovery plan BEFORE you need it.

Warning Signs Of Active Infection

- Sudden slowdown; fans running hot when idle; battery draining 2-3× faster.
- Pop-ups outside the browser (system tray, fake 'Microsoft warnings').
- Browser hijack (new homepage, search engine, redirects).
- Unknown processes hogging CPU in Task Manager / Activity Monitor.
- New programs you didn't install.
- Account lockouts; friends report weird messages from you.
- Webcam / mic indicator turning on by itself.

4-Step Response If Infected

1. **Disconnect from the internet.** Wi-Fi off, ethernet unplugged. Stops data exfiltration and remote control.
2. **Reboot into Safe Mode.** Windows: Shift + Restart → Troubleshoot → Startup Settings → Safe Mode with Networking. Mac: hold Shift on startup.
3. **Run two scanners.** Built-in plus second-opinion. Quarantine everything flagged.
4. **Change passwords from a clean device.** Email first, then bank, then everything else. Enable MFA. Sign out of all sessions.

When To Call A Pro

- Ransomware screen demanding payment.
- Anything related to a work device — call IT first.
- Banking-trojan symptoms (browser modifies what you see on bank sites).
- Two scans in a row find new malware after cleaning.
- You're unsure. Bad cleanups create false confidence.

Where To Go Next

- **Use the Malware Spot-Check Card** — quick warning-signs reference.
- **Use the Malware Types Cheat Sheet** — type-by-type breakdown.
- **Run the Personal Device Security Audit** — score your devices' defences.

PRO TIP

Set Your Phone To Auto-Lock In 30 Seconds.

Single biggest defense against opportunistic device theft. iPhone: Settings → Display & Brightness → Auto-Lock. Android: Settings → Display → Screen Timeout.

Visit Making Sense Of Security →