Malware Types Cheat Sheet

Cheat Sheet · What Each Type Does, How It Spreads, How To Defend.

Not all malware is the same. Knowing what you're dealing with — virus, ransomware, spyware — tells you how it got in and what to do next.

The 8 Major Types

Type	What It Does	How It Spreads
Virus	Infects files and replicates when those files are run	Email attachments, infected downloads, USB drives
Worm	Self-replicates across networks without user action	Network vulnerabilities, automated exploitation
Trojan	Pretends to be legitimate software; opens a back door	Pirated software, fake utilities, 'free' VPNs and PC cleaners
Ransomware	Encrypts files and demands payment for the key	Phishing emails, RDP attacks, software vulnerabilities
Spyware	Secretly monitors and exfiltrates data (keystrokes, screenshots, camera)	Trojans, malicious browser extensions, drive-by downloads
Adware	Aggressive ads, browser hijacking, search redirects	Bundled with free software, fake browser extensions
Rootkit	Hides at the OS level; very hard to detect	Sophisticated targeted attacks, often delivered by other malware
Fileless malware	Runs entirely in memory; no file on disk	Phishing links, Office macros, PowerShell exploits

Universal Defences

1. **Patch promptly.** Most successful infections exploit vulnerabilities patched months before.
2. **Run modern AV.** Defender (Windows) or XProtect (Mac) is fine for most users; add a second-opinion scanner like Malwarebytes.
3. **Don't run as admin.** Use a standard user account for daily work; only escalate when needed.
4. **Email & attachment caution.** Especially .zip, .iso, .exe, .htm, Office docs asking you to enable macros.
5. **3-2-1 backups.** If ransomware hits, you wipe and restore — don't pay.
6. **Browser extension hygiene.** Review every 30 days. Remove anything you don't actively use.

Warning Signs Of Active Infection

- Sudden slowdown, fans running hot when idle, battery draining 2-3× faster.
- Pop-ups outside the browser; new toolbars or homepage you didn't install.
- Unknown processes hogging CPU. New programs you didn't install.
- Account lockouts; friends report weird messages from you.
- Camera / mic indicator turns on by itself.

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 →