Common Cybersecurity Terms Cheat Sheet

Cheat Sheet · The 50 Words That Show Up Most In Security Articles.

When a cybersecurity article uses jargon, scan this list. Plain-English definitions, no fluff, organised by category.

Threats & Attacks

Term	Plain-English Definition
Phishing	A scam email/text designed to trick you into revealing credentials or clicking malware.
Smishing	Phishing over SMS — text messages instead of email.
Vishing	Phishing by voice call — fake bank, IRS, or 'tech support' calls.
Ransomware	Malware that encrypts your files and demands payment to unlock them.
Malware	Umbrella term for any malicious software (viruses, worms, trojans, spyware, etc.).
Trojan	Malware disguised as a legitimate program — opens a back door once installed.
Spyware	Software that secretly monitors what you do and sends data to an attacker.
Keylogger	Spyware that records every keystroke, capturing passwords as you type.
Zero-day	A previously unknown software vulnerability with no patch available yet.
Social engineering	Manipulating people (not computers) — the trick behind most successful attacks.
Credential stuffing	Trying leaked username/password pairs across many sites until one works.
SIM swap	Attacker tricks your carrier into porting your phone number to their SIM.

Defences & Tools

Term	Plain-English Definition
MFA / 2FA	Multi-Factor Authentication — a second login factor beyond just a password.
Authenticator app	App that generates rotating 6-digit codes for MFA. Better than SMS.
Password manager	App that generates, stores, and auto-fills strong unique passwords.
Hardware security key	Physical USB/NFC key (e.g., YubiKey) — the strongest 2FA available.
VPN	Encrypts internet traffic between your device and a server, hiding it from your network.
Antivirus / EDR	Software that scans for and blocks malware on your device.
Firewall	Filters which network traffic can enter or leave your device or network.
Encryption	Scrambling data so only someone with the key can read it.

Term	Plain-English Definition
End-to-end encryption	Only sender and recipient can read it — not even the service provider.
Sandboxing	Running untrusted code in an isolated environment so it can't harm the rest of the system.
DNS filtering	Blocking known-bad domains at the DNS level (e.g., NextDNS, Pi-hole).
WPA3 / WPA2	Wi-Fi security standards. WPA3 is current; older WEP is broken — never use it.

Authentication & Identity

Term	Plain-English Definition
Password hash	A scrambled version of a password. Sites should never store the original.
Salt	Random data added to a password before hashing — defeats rainbow-table attacks.
Passkey	Phishing-resistant login using a stored device key. Replacing passwords for many sites.
SSO	Single Sign-On — logging into many services through one master account (Google, Apple, etc.).
OAuth	The protocol behind 'Sign in with Google/Facebook' buttons.
Recovery code	One-time code that lets you regain access if you lose your MFA device. Save these.
Identity theft	Someone using your personal information to open accounts, file taxes, or commit fraud.
Dark web	Encrypted marketplaces where stolen credentials and identity data are bought and sold.
Credit freeze	Blocks new credit accounts from being opened in your name. Free at all 3 bureaus.

Privacy & Data

Term	Plain-English Definition
PII	Personally Identifiable Information — name, SSN, address, anything that identifies you.
Cookie	A small file websites store in your browser to remember you. First-party = OK, third-party = trackers.
Fingerprinting	Identifying a device by its unique config (fonts, screen, plugins). Cookieless tracking.
Data broker	Companies that aggregate and sell your personal information (Spokeo, BeenVerified, etc.).
GDPR / CCPA	Privacy laws in the EU and California that grant you rights to your data.
Tracking pixel	Tiny invisible image embedded in emails/sites to detect when you opened them.
Email alias	A throwaway email that forwards to your real one. Stops cross-site tracking.
Breach	An incident where private data is exposed or stolen from a service.

Tech Concepts You'll See Often

Term	Plain-English Definition
HTTPS	Encrypted version of HTTP (the lock icon in your browser). Always use it.
IP address	Numerical address that identifies your device on a network.
DNS	The internet's phonebook — translates domain names (google.com) to IP addresses.
Patch / update	Software fix that closes security holes. Install promptly.
Backup	A second copy of your data stored separately, in case the first is lost or encrypted.
3-2-1 backup	3 copies of data, on 2 media types, with 1 offsite. The gold standard.