SkillNewton

Cybersecurity Glossary Cheat Sheet

Around 80 cybersecurity terms in plain English: attacks, malware, defences, cryptography, identity, network security, CERT-In and the DPDP Act.

This glossary explains the cybersecurity terms you will meet in courses, job descriptions and incident reports, in plain English and grouped by theme. It covers common attacks and malware, the controls that stop them, cryptography, identity and access, network security and the Indian rules every organisation should know, including CERT-In reporting and the Digital Personal Data Protection Act 2023. Use it as a quick reference or to revise before an interview or exam.

How to use it

1. **Read one theme at a time.** Work through a section, such as threats and attacks, before moving on, so related terms stay connected.
2. **Pair attacks with defences.** For each attack, find the control in the defences or identity sections that reduces it, such as MFA against credential stuffing.
3. **Explain terms aloud.** Test yourself by explaining a term in one sentence without looking. Interviewers often ask for exactly that.
4. **Check the official source for compliance.** Laws and directions change. Confirm current CERT-In and DPDP requirements on the CERT-In and MeitY websites before relying on them.

Threats and attacks

Phishing	Fake emails, messages or websites that trick people into revealing passwords, paying money or opening malware.
Spear phishing	Phishing aimed at a specific person or organisation, using personal details to look convincing.
Smishing and vishing	Phishing by SMS (smishing) or by phone call (vishing), such as fake KYC update or courier messages.
Social engineering	Manipulating people rather than systems, for example pretending to be IT support to get a password.
Business email compromise (BEC)	A fraud where attackers use a hacked or look-alike email account to ask staff to pay fake invoices or change bank details.
Brute-force attack	Trying many passwords or keys until one works.
Credential stuffing	Trying usernames and passwords leaked from one site on other sites, relying on password reuse.
Password spraying	Trying a few common passwords against many accounts to avoid lockouts.
On-path (man-in-the-middle) attack	An attacker secretly sits between two parties to read or change their traffic.

Denial of service (DoS / DDoS)	Flooding a service so real users cannot reach it. Distributed (DDoS) attacks use many machines at once.
SQL injection	Inserting SQL into an input so the database runs the attacker's query. Prevented with prepared statements.
Cross-site scripting (XSS)	Injecting script into a web page that then runs in other users' browsers. Prevented by escaping output.

Malware

Malware	Any software designed to harm, spy on or take control of a device or network.
Virus	Malware that attaches to files or programs and spreads when they are run or shared.
Worm	Malware that spreads across networks by itself, without a user opening anything.
Trojan	Malware disguised as useful software, such as a cracked app or fake update.
Ransomware	Malware that encrypts or steals data and demands payment to restore or not leak it.
Spyware	Malware that secretly collects information about a user's activity.
Infostealer	Malware that grabs saved passwords, browser cookies and session tokens and sends them to attackers.
Keylogger	Software or hardware that records keystrokes to capture passwords and messages.
Rootkit	Malware that hides deep in the operating system to keep control and avoid detection.
Backdoor	A hidden way into a system that bypasses normal authentication.
Botnet	A network of infected devices controlled remotely, often used for DDoS attacks or spam.
Fileless malware	Malicious code that runs in memory or through built-in tools such as PowerShell, leaving few files to scan.

Defences and controls

Firewall	A device or software that allows or blocks traffic based on rules such as address, port and protocol.
IDS (intrusion detection system)	Monitors traffic or hosts and raises alerts on suspicious activity.
IPS (intrusion prevention system)	Like an IDS, but sits in the traffic path and can block suspicious activity automatically.
EDR (endpoint detection and response)	Software on laptops and servers that detects attacks, records activity and lets responders isolate devices.

SIEM	Security information and event management: collects logs from many systems and correlates them to spot incidents.
Patch management	Finding, testing and installing security updates on a regular schedule.
Vulnerability scanning	Automated checks for known weaknesses such as missing patches or weak settings.
Penetration testing	An authorised, simulated attack to find weaknesses before real attackers do.
Defence in depth	Using several layers of controls so one failure does not expose everything.
Principle of least privilege	Giving each user and program only the access it needs, and nothing more.
3-2-1 backup rule	Keep three copies of data, on two types of storage, with one copy offsite or offline.
Security awareness training	Teaching staff to recognise phishing and report incidents quickly.

Cryptography

Encryption	Turning readable data into ciphertext that only someone with the right key can read.
Symmetric encryption	The same key encrypts and decrypts. Fast; used for bulk data (for example AES).
Asymmetric encryption	A public key encrypts or verifies and a matching private key decrypts or signs (for example RSA, elliptic curve).
Hashing	A one-way function that turns data into a fixed-length value. Any change to the data changes the hash.
Salt	Random data added to each password before hashing so identical passwords get different hashes.
Password hashing	Using slow, salted algorithms such as bcrypt or Argon2 to store passwords, never plain text or fast hashes like MD5.
Digital signature	Proof, made with a private key, that data came from a particular sender and was not changed.
Digital certificate	A file that binds a public key to an identity such as a domain name, signed by a certificate authority.
Certificate authority (CA)	A trusted organisation that issues and signs digital certificates.
TLS	Transport Layer Security: the protocol that encrypts HTTPS and many other connections. Replaced SSL.
End-to-end encryption	Only the sender and recipient can read messages; the service provider in between cannot.
Key management	Creating, storing, rotating and destroying encryption keys securely.

Identity and access

Authentication	Proving who you are, for example with a password, passkey or fingerprint.
Authorisation	Deciding what an authenticated user is allowed to do.
Multi-factor authentication (MFA)	Requiring two or more kinds of proof: something you know, have or are.
Passkey	A phishing-resistant sign-in based on a key pair stored on your device, unlocked with a PIN or biometric.
Single sign-on (SSO)	One login gives access to many applications through a trusted identity provider.
Identity provider (IdP)	The service that authenticates users for other applications in SSO.
Role-based access control (RBAC)	Granting permissions to roles such as editor or admin, then assigning people to roles.
Privileged access management (PAM)	Tightly controlling, recording and limiting administrator accounts.
Zero trust	A model where no user or device is trusted by default; every request is verified, wherever it comes from.
Password manager	An app that creates and stores a unique, strong password for every account.
Session hijacking	Stealing a session cookie or token to use someone's logged-in session without their password.

Network security

VPN	Virtual private network: an encrypted tunnel between a device or site and another network.
Network segmentation	Splitting a network into zones so an attacker in one part cannot easily reach the rest.
VLAN	A virtual LAN that separates traffic on the same switches into isolated groups.
DMZ	A separate network zone for public-facing servers, kept apart from the internal network.
NAC (network access control)	Checks devices before they join the network, for example for an up-to-date OS.
WPA3	The current Wi-Fi security standard, with stronger protection against password guessing than WPA2.
Web application firewall (WAF)	Filters HTTP traffic to block attacks such as SQL injection and XSS before they reach the application.
DNS filtering	Blocking connections to known malicious or unwanted domains at the DNS lookup stage.

Port scanning	Probing a host to find open ports and services. Used by attackers and defenders (for example with Nmap).
Packet sniffing	Capturing network traffic to inspect it, for troubleshooting or, by attackers, to steal unencrypted data.
Honeypot	A decoy system set up to attract attackers and study their methods.
Attack surface	All the points where an attacker could try to get in: open ports, apps, accounts and devices.

Governance, risk and compliance (with India)

CIA triad	The three core goals of security: confidentiality, integrity and availability.
Risk assessment	Identifying assets, threats and vulnerabilities, then rating likelihood and impact to decide what to fix first.
Incident response plan	A written plan for detecting, containing, fixing and learning from security incidents.
ISO/IEC 27001	International standard for an information security management system (ISMS) that organisations can be certified against.
CERT-In	Indian Computer Emergency Response Team, the national agency for cyber incident response under MeitY.
CERT-In directions (April 2022)	Require reporting of listed cyber incidents to CERT-In within six hours of noticing them and keeping ICT logs for 180 days within India.
IT Act 2000	India's main law on electronic records, cybercrime and intermediaries; it set up CERT-In's statutory role.
DPDP Act 2023	Digital Personal Data Protection Act 2023: India's law on processing digital personal data, based on consent and other lawful uses.
Data Fiduciary	Under the DPDP Act, the organisation that decides why and how personal data is processed.
Data Principal	Under the DPDP Act, the person the personal data is about.
Personal data breach (DPDP)	Unauthorised processing, loss or disclosure of personal data. The Data Fiduciary must inform the Data Protection Board and affected people.
Data Protection Board of India	The body set up under the DPDP Act to handle breaches and complaints and impose penalties, up to Rs 250 crore for failing to take reasonable security safeguards.

Online version, with the matching free guide: skillnewton.com/resources/cheat-sheets/cybersecurity-glossary/
Learn this hands-on: Networking & Cybersecurity: Foundation & Practical Implementation – skillnewton.com/courses/networking-foundation-course/