GLOSSARY

Security terms, in human.

No acronym left unexplained. Search a term, or filter by category.

All downloads →

CICADA | RESOURCES

2

2FA

IDENTITY

Two-factor authentication. A second proof of identity beyond a password, such as a code or a security key.

Also called: two-factor authentication

3

3-2-1 backup

DATA

Three copies of your data, on two different types of storage, with one copy kept offline or off-site.

Also called: 3-2-1 rule

A

Admin account

IDENTITY

An account with permission to change settings, install software or manage other users. Should be separate from everyday accounts.

AI voice cloning

THREATS

Using AI to copy a person's voice from recordings, often to impersonate a boss or relative on a call.

Attack surface

CONCEPTS

Everything an attacker can see or reach: logins, websites, remote access, email, suppliers and people.

B

Backup

DATA

A separate copy of data that you can restore after deletion, ransomware or device failure. Cloud sync alone is not a backup.

Also called: backups

BEC

THREATS

Business email compromise. An attacker takes over or impersonates a work mailbox to approve payments or steal data.

Also called: business email compromise

BitLocker

DEVICES

Microsoft's built-in disk encryption for Windows. Makes data unreadable if a laptop is stolen.

Blue team

CONCEPTS

The defenders in a security exercise: the people who monitor, detect and respond.

Breach

CONCEPTS

An incident where data or systems are accessed without permission. Not every breach involves malware.

Also called: breaches

Brute force

THREATS

Trying many passwords until one works. Long, unique passwords and rate limits defeat it.

Business continuity

RESPONSE

The plan for keeping essential work going during and after a disruption, including a cyber incident.

BYOD

DEVICES

Bring your own device. Personal phones or laptops used for work, which need clear security rules and remote wipe.

Also called: bring your own device

C

CISO

CONCEPTS

Chief information security officer. The person accountable for security strategy, usually only in larger organisations.

Also called: chief information security officer

Clickjacking

THREATS

Tricking someone into clicking a disguised button or link, often inside an invisible frame.

Cloud sync

DATA

Keeping files mirrored between devices. Convenient, but deletions and ransomware can spread to every copy. It is not a backup.

Containment

RESPONSE

The first phase of incident response: stopping an attack from spreading before you investigate or recover.

Credential

IDENTITY

A username, password, token or key used to prove identity and gain access.

Also called: credentials

Credential stuffing

THREATS

Using usernames and passwords leaked from one site to break into another, because people reused them.

Credential theft

THREATS

Stealing logins through phishing, malware, reuse or a breached service.

CSRF

THREATS

Cross-site request forgery. A malicious site makes a logged-in browser perform an unwanted action.

Also called: cross-site request forgery

Cyber hygiene

CONCEPTS

The routine basics: updates, backups, strong authentication and sensible access. Boring, and highly effective.

Cyber insurance

RESPONSE

A policy covering some costs of a cyber incident. Check what it requires you to do, and who to call first.

D

Dark web

THREATS

Parts of the internet reachable only with special software, often used to sell stolen data and access.

Data breach

DATA

Unauthorised access to personal or business data. May trigger legal notification duties.

Data minimisation

DATA

Keeping only the data you actually need, for only as long as you need it.

Denial of service

THREATS

Overwhelming a service so legitimate users cannot use it. Often automated and short-lived.

Also called: DoS

DKIM

EMAIL

A DNS record that cryptographically signs your outgoing email, helping receivers confirm it wasn't altered.

DMARC

EMAIL

A DNS record that tells receivers what to do when email using your domain fails authentication, and sends you reports.

DNS

CONCEPTS

The system that turns domain names into internet addresses. Email authentication records live here.

Also called: domain name system

Domain hijacking

THREATS

Taking control of a domain through a compromised registrar account or DNS provider.

E

EDR

DEVICES

Endpoint detection and response. Software that watches devices for suspicious behaviour and can isolate them.

Also called: endpoint detection and response

Email header

EMAIL

The hidden routing and authentication information at the top of an email. Useful when deciding whether a message is genuine.

Also called: email headers

Encryption

DEVICES

Scrambling data so it can't be read without a key. Essential on laptops and phones.

Endpoint

DEVICES

A laptop, phone, server or other device that connects to the network. Each one needs updates and protection.

Also called: endpoints

Exploit

THREATS

A technique or tool that takes advantage of a vulnerability.

Also called: exploits

F

FileVault

DEVICES

Apple's built-in disk encryption for macOS.

Firewall

NETWORK

A filter that controls which network traffic is allowed in or out. Often built into a router.

H

HTTPS

CONCEPTS

The encrypted version of the web protocol. It protects traffic in transit, but does not prove a site is honest.

I

Identity provider

IDENTITY

The service that signs people in and applies MFA, such as Microsoft Entra ID, Google Workspace or Okta.

Also called: IdP

Immutability

DATA

A setting that prevents data being changed or deleted for a fixed period, a strong defence against ransomware.

Incident response

RESPONSE

The plan and actions taken after a security event: contain, investigate, recover, learn.

Invoice fraud

THREATS

A scam that changes bank details or payment instructions, often using a compromised supplier mailbox.

Also called: payment diversion

K

Keylogger

THREATS

Software or hardware that records keystrokes to capture passwords and messages.

L

Lateral movement

THREATS

An attacker moving from one compromised account or device to others inside the network.

Least privilege

IDENTITY

Giving people only the access they need for their job, and no more.

M

Malvertising

THREATS

Malicious adverts, sometimes on legitimate sites, that lead to malware or fake support pages.

Malware

THREATS

Any software designed to cause harm: viruses, spyware, ransomware, remote-access tools.

Managed service provider

CONCEPTS

An outsourced IT provider. Their access to your systems makes their security part of yours.

Also called: MSP

MFA

IDENTITY

Multi-factor authentication. A second check after your password: an app code, a passkey, a security key or a prompt.

Also called: multi-factor authentication, two-step verification

---

MFA fatigue

THREATS

Bombarding someone with login prompts until they approve one by mistake. Number matching and passkeys help stop it.

Also called: MFA bombing

Microsegmentation

NETWORK

Splitting a network into small zones so a compromised device cannot reach everything else.

Misconfiguration

CONCEPTS

A setting left open or wrong, such as a public storage bucket or an admin panel with no MFA.

N

Network segmentation

NETWORK

Separating networks so guests, devices and business systems cannot reach each other by default.

P

Passkey

IDENTITY

A phishing-resistant login method that uses your device's biometrics or PIN instead of a password.

Also called: passkeys

Password manager

IDENTITY

A tool that generates and stores unique passwords in an encrypted vault. The practical fix for password reuse.

Password spraying

THREATS

Trying a few common passwords across many accounts to avoid lockouts. MFA and unique passwords defeat it.

Patch

DEVICES

A software update that fixes a security flaw. Most attacks exploit flaws that already have a patch available.

Also called: patches, patching

Patch management

DEVICES

The routine of applying software fixes consistently, including the devices people forget.

Payload

THREATS

The harmful part of an attack, such as the code that encrypts files or steals data.

Penetration test

CONCEPTS

An authorised, simulated attack used to find weaknesses. Useful, but not a substitute for the basics.

Also called: pen test

Pharming

THREATS

Redirecting a domain to a malicious site through DNS or local network tampering.

Phishing

THREATS

A fraudulent message designed to make you click, pay, log in or hand over information.

Also called: phishing email

Privilege escalation

THREATS

Gaining more access than intended, such as turning a normal user into an administrator.

Q

Quarantine

EMAIL

Isolating a suspicious email or file so it cannot run or be opened normally.

Quishing

THREATS

Phishing that uses a QR code to move the victim onto a phone and away from email filters.

Also called: QR phishing

R

Ransomware

THREATS

Malware that encrypts your files and demands payment. Good offline backups are the reliable way out.

Also called: ransomware attack

RDP

NETWORK

Remote Desktop Protocol. Lets someone control a Windows machine remotely; dangerous if exposed directly to the internet.

Also called: remote desktop protocol

Recovery code

IDENTITY

A one-time code that gets you back into an account if your MFA device is lost. Store it offline.

Also called: recovery codes

Red team

CONCEPTS

An authorised group that attacks systems to test defences, often in a controlled exercise.

Remediation

RESPONSE

Fixing a weakness or reducing its risk, with an owner and a deadline.

Risk register

RESPONSE

A simple list of risks, their likelihood and impact, the owner and the agreed action.

Root cause

RESPONSE

The underlying reason an incident happened, not just the symptom that was noticed first.

RPO

RESPONSE

Recovery point objective. How much data you can afford to lose, measured in time, for example, one hour of work.

RTO

RESPONSE

Recovery time objective. How long the business can tolerate being offline before the cost becomes unacceptable.

S

Sandbox

CONCEPTS

An isolated environment used to open or run something suspicious without risking the real system.

Security key

IDENTITY

A hardware device used as a phishing-resistant second factor, such as a YubiKey.

Also called: security keys

Session hijacking

THREATS

Stealing an active login session or cookie so the attacker does not need the password.

SIM swap

THREATS

Convincing a mobile provider to move a phone number to a new SIM, often to intercept SMS codes.

Also called: SIM swapping

Smishing

THREATS

Phishing by text message, often using a delivery, bank or tax story.

Also called: SMS phishing

Sniffing

THREATS

Capturing network traffic to read unencrypted information.

SOC

CONCEPTS

Security operations centre. The team and tools that monitor for and respond to incidents.

Also called: security operations centre, security operations center

---

Social engineering

THREATS

Manipulating people rather than systems: urgency, authority, trust and secrecy are the usual tools.

Spam

EMAIL

Unsolicited bulk email. Annoying, and sometimes the first stage of a scam.

Spear phishing

THREATS

Phishing written for one specific person, using details from their work or public profiles.

SPF

EMAIL

A DNS record listing which servers are allowed to send email for your domain.

Spoofing

EMAIL

Faking a sender address, domain, caller ID or website to look trustworthy.

SQL injection

THREATS

Inserting database commands into an input field to read or change data. Proper coding and patching prevent it.

Also called: SQLi

SSO

IDENTITY

Single sign-on. One login gives access to many apps, which is convenient but makes that login a high-value target.

Also called: single sign-on

Supply chain attack

THREATS

Compromising a supplier or software provider to reach their customers. Your security depends partly on theirs.

T

Threat actor

CONCEPTS

The person or group behind an attack. Could be an opportunist, a criminal group or a state-backed team.

Threat intelligence

CONCEPTS

Information about current attackers, campaigns and indicators, used to prioritise defences.

Token

IDENTITY

A digital key issued after sign-in that lets an app act on your behalf. Tokens can be stolen.

Also called: tokens

Trojan

THREATS

Malware disguised as legitimate software or a document.

Typosquatting

THREATS

Registering a lookalike domain with a small typo to catch mistyped traffic.

V

Vishing

THREATS

Voice phishing, a phone call designed to extract information or persuade you to act.

VPN

NETWORK

A private, encrypted connection between a device and your network. Should be paired with MFA.

Also called: virtual private network, VPNs

Vulnerability

CONCEPTS

A weakness that could be exploited. It may be in software, a configuration or a process.

Also called: vulnerabilities

W

Whaling

THREATS

Phishing aimed at senior people, often using authority and a payment or data request.

X

XSS

THREATS

Cross-site scripting. Injecting code into a web page so it runs in someone else's browser.

Also called: cross-site scripting

Z

Zero trust

NETWORK

An approach that checks identity and device on every request instead of trusting anything inside the network.

Also called: zero-trust

Zero-day

THREATS

A flaw with no fix available yet. Rare compared with unpatched, known vulnerabilities.

Generated free at resources.cicadacs.com · General guidance, not an audit or legal advice.