

7.2 Glossery

Term

3-2-1 Rule

Account recovery

Admin account

Adware

Antivirus

Attack Surface

Authenticator app

Backup

Biometric

BitLocker / FileVault / LUKS

Botnet

Browser extension

Caller ID spoofing

Captive portal

Cloud

Definition

A backup strategy: keep 3 copies of your data, on 2 different types of storage, with 1 copy stored offsite (like in the cloud).

The backup ways to prove an account is yours (like a recovery email, phone number, or recovery codes) if you forget your password or lose your phone.

A computer account that can install software and change system settings. Use it rarely.

Unwanted software that shows ads or tracks you for ads.

Software that looks for and blocks malicious software (malware). Built-in options are usually enough when combined with updates.

The sum of the attack vectors where an attacker can attempt an attack.

An app that generates time-based codes for multi-factor authentication (MFA). Works even without cell service.

A second copy of your files you can restore if your device is lost, stolen, damaged, or encrypted by ransomware.

Using your body (fingerprint, face) to unlock a device or app.

Full-disk encryption tools built into operating systems. BitLocker (Windows), FileVault (macOS), and LUKS (Linux) scramble your entire hard drive so data can't be accessed without your password.

A network of infected devices controlled by attackers to launch coordinated cyberattacks, send spam, or mine cryptocurrency without the owners' knowledge.

A small add-on to your web browser. Only install ones you truly need and trust.

When scammers fake the phone number that appears on your caller ID to make it look like a call is from your bank, the IRS, or another trusted source.

The web page that appears when you connect to some WiFi networks (like at hotels or airports) requiring you to agree to terms or enter a password before accessing the internet.

Someone else's computers you access over the internet (like iCloud, Google Drive, OneDrive).

Data breach	When sensitive information is stolen from a company or organization's systems, often exposing passwords, emails, credit card numbers, or personal data of users.
DDoS attack	Distributed Denial of Service attack. When many compromised devices flood a website or service with traffic to overwhelm it and make it unavailable.
Default gateway	The IP address of your router. Your computer uses this to access the internet and other networks.
Encryption	A way to scramble data so only someone with the right key can read it. Examples: FileVault (macOS), BitLocker (Windows), built-in encryption on iPhone and Android.
End-to-end encryption (E2EE)	Only the sender and receiver can read messages; even the service provider cannot.
Firewall	A security feature that controls which network traffic is allowed. Your router and computer have one built in.
Firmware	The permanent software programmed into a hardware device (like a router or smart device) that controls how it operates. Like an operating system, but specifically for that device.
Guest network	A separate wireless network for visitors and untrusted devices that keeps them isolated from your main network, computers, and files.
IoT (Internet of Things)	Any device that connects to the internet but isn't a traditional computer or phone, like smart speakers, thermostats, security cameras, or smart light bulbs.
IP address	Internet Protocol address. A unique number assigned to each device on a network that identifies it, like a street address for your computer or phone.
ISP	Internet Service Provider. The company that provides your internet connection (like Comcast, AT&T, Verizon).
Keylogger	Malicious software that records everything you type on your keyboard to steal passwords and sensitive information.
Kill switch (VPN)	A VPN feature that automatically blocks all internet traffic if the VPN connection drops, preventing your data from being exposed.
Malware	Malicious software designed to harm, spy, or steal (viruses, ransomware, spyware, trojans).
Multi-factor authentication (MFA)	Adding a second step to log in (like a code or prompt) so a stolen password alone is not enough.
Operating system (OS)	The main software that runs your device (Windows, macOS, Linux, iOS for iPhone, Android).
Passkey	A newer, phishing-resistant sign-in method that uses cryptography instead of passwords. Passkeys are stored on your device and use biometrics or a PIN to unlock, but the biometric data never leaves your device.

Passphrase	A longer, easy-to-remember password made of several words.
Password manager	A secure app that creates and stores unique passwords for every account.
Phishing	A fake message (email/text/DM) that tries to trick you into clicking a link, opening an attachment, or sharing a code or password.
PIN	Personal Identification Number. A numeric password, typically 4-6 digits, used to unlock devices or authenticate transactions.
Quishing	QR code phishing. A scam using QR codes in emails or texts to trick you into visiting fake websites that steal your information.
Ransomware	Malware that locks your files and demands payment to unlock them.
Recovery codes	Backup codes provided when you enable multi-factor authentication that let you access your account if you lose your phone or authenticator app.
Remote wipe	Erasing a lost or stolen device over the internet.
SIM-swap	A criminal moves your phone number to their SIM card to receive your text messages and calls.
Social engineering	The art of manipulating people into giving up confidential information or taking actions that compromise security. Attackers exploit human psychology (trust, fear, urgency) rather than technical vulnerabilities.
Software update	A fix or improvement for your device or app. Turning on automatic updates closes security holes.
SSID	Service Set Identifier. The name of your wireless network that appears when you search for available WiFi networks.
UPnP	Universal Plug and Play. A feature that lets devices automatically open ports in your router. Convenient but can be exploited by malware to bypass your firewall.
URL	Uniform Resource Locator. The web address you type into your browser (like https://www.example.com).
USB	Universal Serial Bus. The common rectangular port and cable used to connect devices like keyboards, mice, external drives, and phones to your computer.
Virtual private network (VPN)	A service that encrypts your internet traffic and routes it through the VPN provider. Useful on public Wi-Fi; not a magic invisibility cloak.
VLAN	Virtual Local Area Network. A way to separate devices on a network into isolated groups so they can't communicate with each other, improving security and organization.

WEP / WPA / WPA2 / WPA3

WiFi security protocols. WPA3 is the newest and most secure, WPA2 is older but still secure, WPA (original) is outdated, and WEP is completely broken and should never be used.

WPS

WiFi Protected Setup. A feature designed to make connecting devices easier using a PIN, but it has security flaws that make it easy for attackers to crack your WiFi password.

Zero-knowledge encryption

Encryption where even the service provider cannot access your data because they never have your encryption keys. Only you can decrypt your files.

Revision #1

Created 2026-07-12 22:31:37 UTC by Chris Landis

Updated 2026-07-12 22:32:10 UTC by Chris Landis