

Cybersecurity Terminology:

A Visual Glossary



One shared defensive-security vocabulary for meetings, emails, and incident notices



For non-security staff, students, educators, and managers



Terms grouped by real-world scenario, each with a plain definition and visual anchor



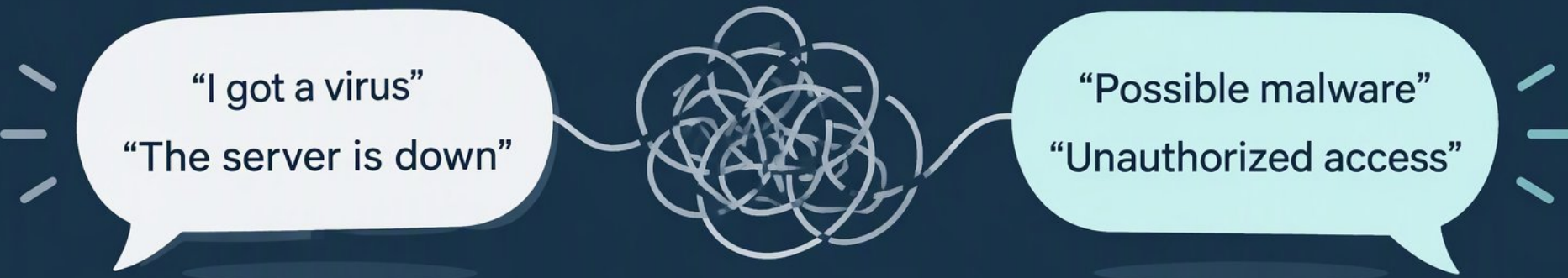
You will recognize key terms, ask better questions, and fix common mix-ups



Scope: defensive awareness vocabulary only — not penetration testing or legal advice



Why Shared Words **Matter**



“I got a virus”
“The server is down”

“Possible malware”
“Unauthorized access”



- Loose terms like 'virus' or 'hacked' trigger the wrong response



- 98% of non-IT staff report at least one security miscommunication



- 62% say miscommunication contributed to a real incident



- 61% of expert security terms are hard for general readers



- Workers want real-life examples, less jargon, and clear reporting steps

How to Read a Glossary Entry (and the Four Words Behind Everything)

CLEARER
TERMS
SAFER
TOMORROWS

- **Every entry:** plain meaning, visual anchor, mix-up note, action cue
- **Threat:** any circumstance or event that could harm operations, assets, or people
- **Vulnerability:** a weakness in a system, procedure, or control that could be exploited
- **Risk:** impact if something happens × likelihood it happens
- **Exploit:** the tool or action that turns a vulnerability into impact
- **Visual anchor:** threat actor → vulnerability → exploit → impact



Sample Glossary Entry



Threat

Plain meaning

any circumstance or event that could harm operations, assets, or people

Visual anchor

threat actor → vulnerability → exploit → impact

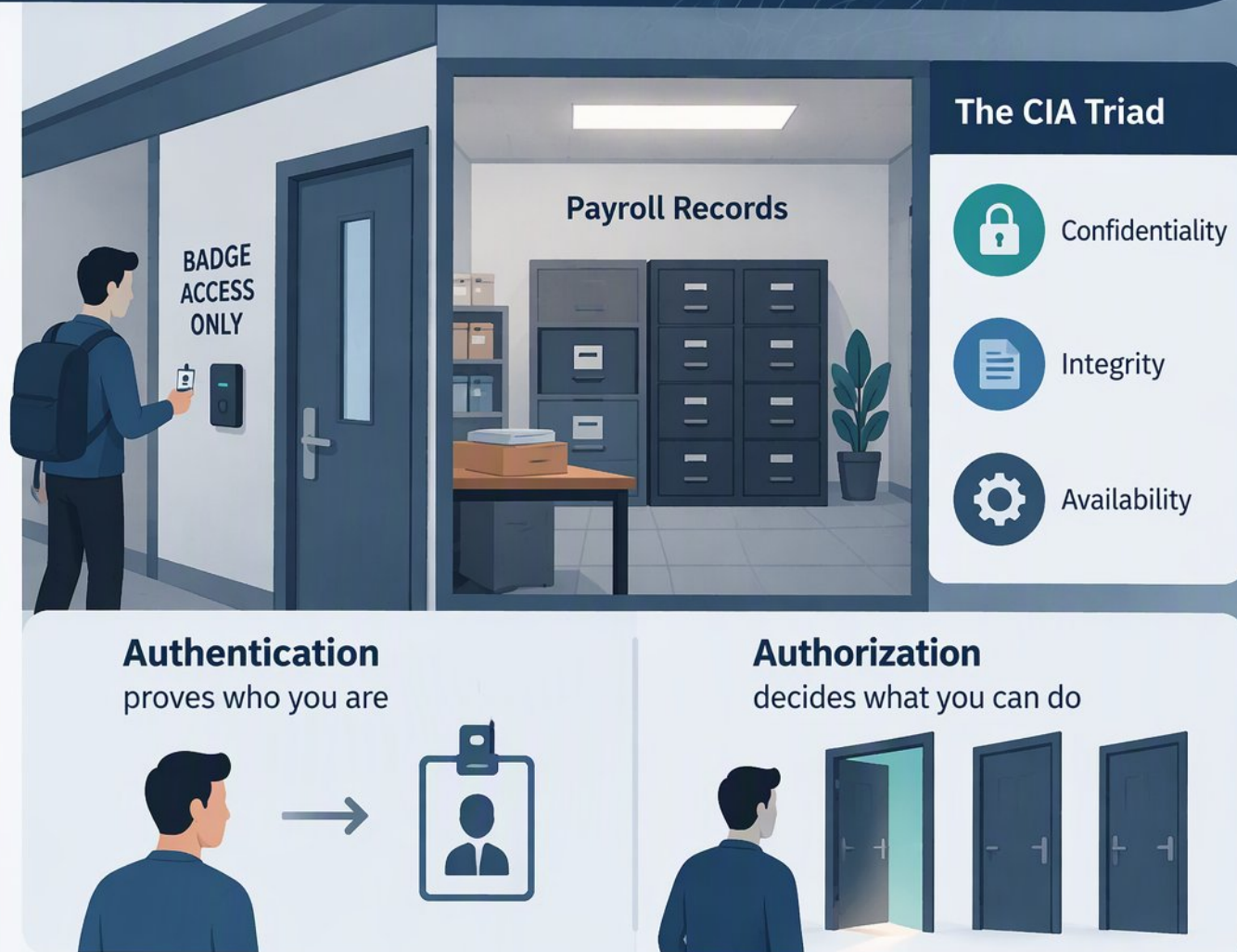
Mix-up note

Action cue

Assets, CIA, and the Everyday Words of Security

PEOPLE
KNOWLEDGE
SAFER TOMORROW

- **Asset and attack surface:** what you protect and where it's exposed
- **Confidentiality, integrity, availability:** the three ways security fails
- **Authentication** proves who you are; **authorization** decides what you can do
- **Identity, credentials, MFA:** the vocabulary of every login screen
- **Visual anchor:** one risk-chain diagram with a real asset filled in



Who Attacks, and What Malware Actually Means

PEOPLE | MOTIVES | MALWARE

Threat actors

cybercriminals, insiders,
hacktivists, nation-states,
opportunists



Motives

money, access, ideology,
disruption



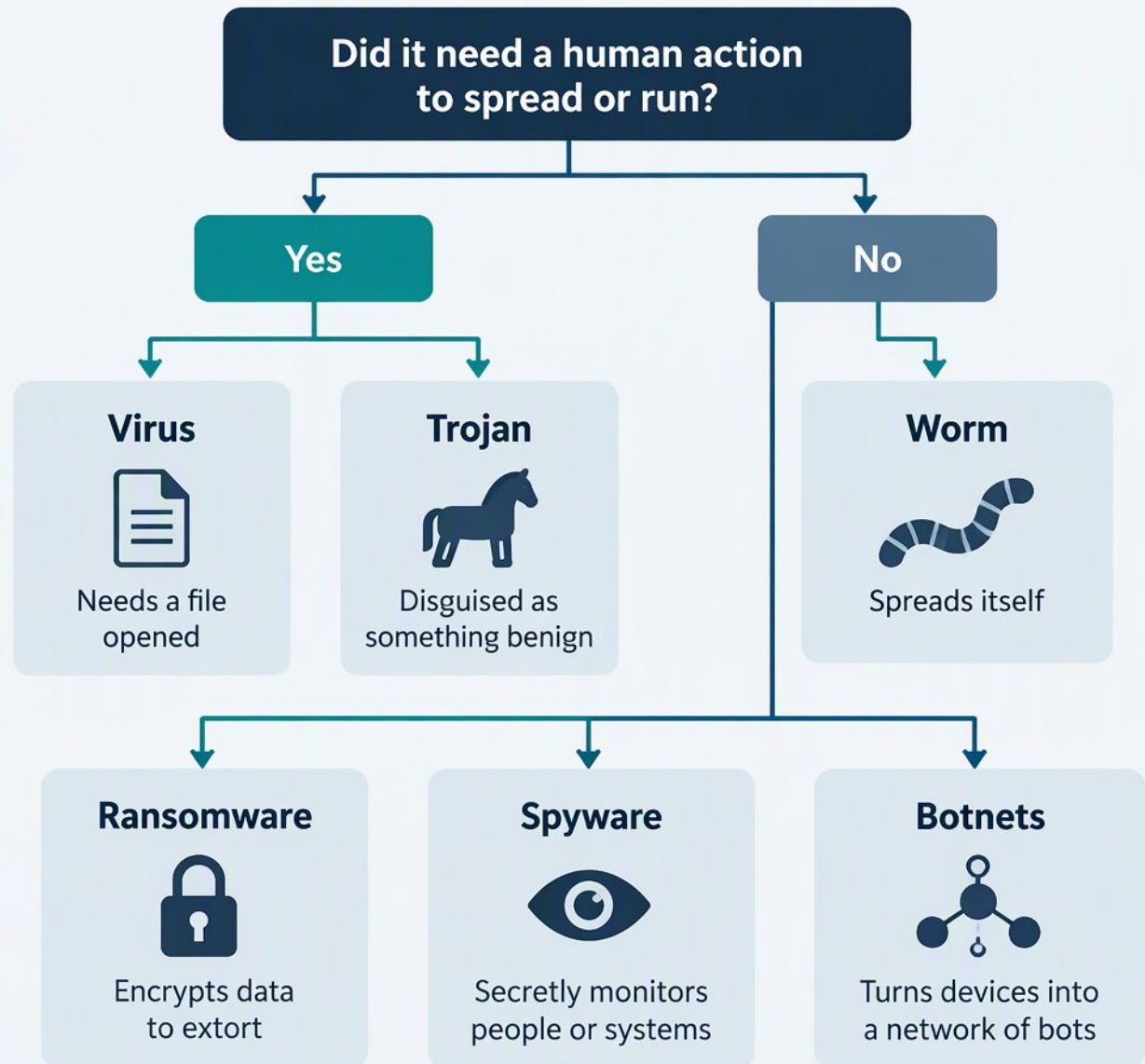
Malware

software built to harm
confidentiality, integrity,
or availability

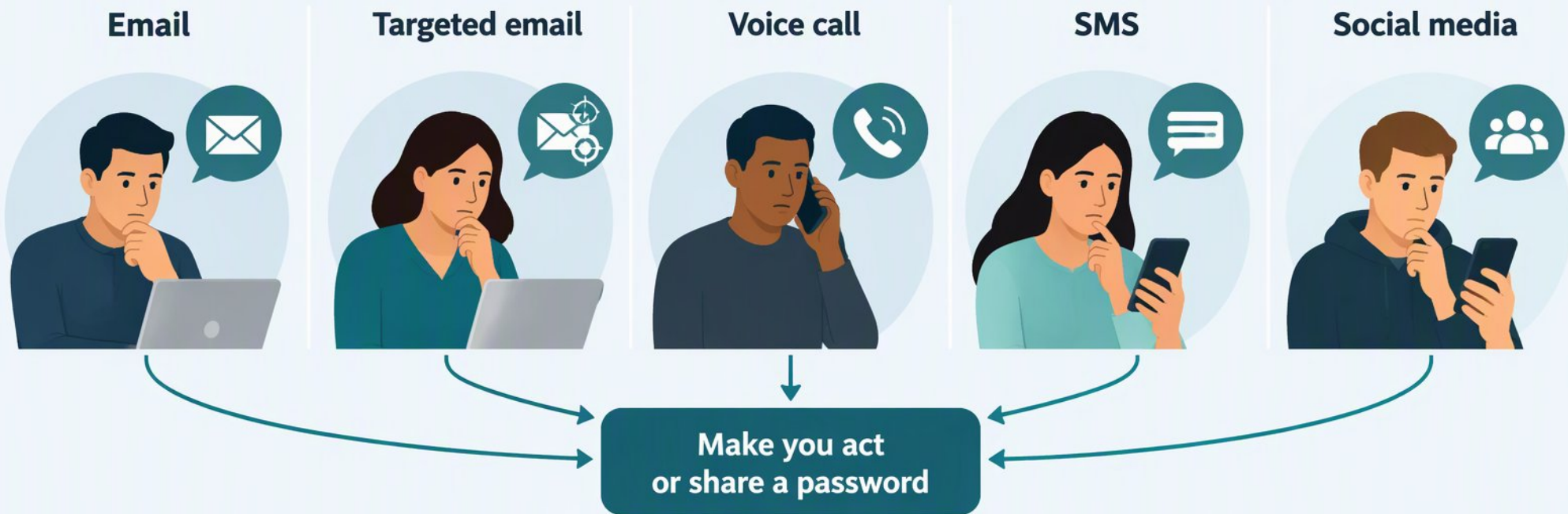
Family

virus, worm, trojan,
ransomware, spyware, botnets

Virus needs a file opened;
a worm spreads itself



Attacks on People: Phishing, Vishing, Smishing, and BEC



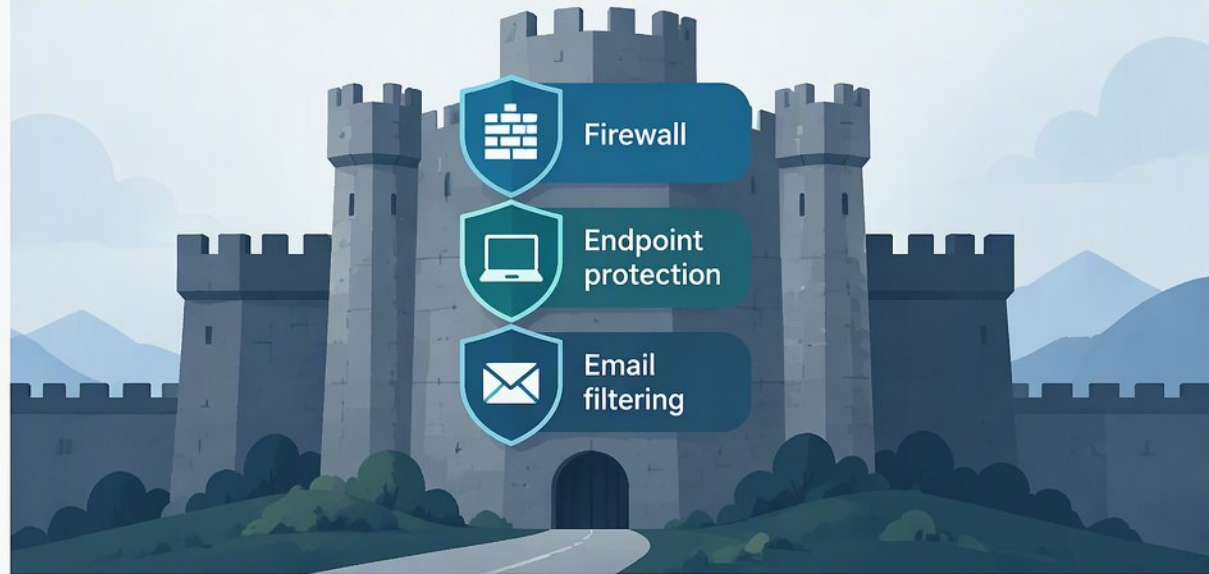
- Social engineering: manipulating someone into sharing information or access
- Spam is bulk messaging; phishing is a scam to make you act
- Same goal, different channels: email, voice, SMS, social media
- Stolen passwords can hurt more than a stolen laptop
- Disruption and trust attacks: DoS and supply-chain compromise



Defenses in Plain Language

PEOPLE
PRACTICES
SAFER TOMORROW

- Firewall, endpoint protection, email filtering: who gets in, what runs
- Encryption protects data at rest; HTTPS and VPN protect data in motion
- Three habits stop most incidents: backups, patching, and updates
- Cloud sync is not a backup — it copies deletions and ransomware too
- Least privilege and role-based access: admin rights for everyone is a risk



HTTPS and VPN
protect data in motion



Encryption protects
data at rest

Three habits
stop most
incidents:



backups



patching



updates

Passwords, MFA, and Passkeys Without the Jargon

SAFER PEOPLE
STRONGER TOMORROW

- **MFA:** two or more different factor types — something you know, have, or are



something
you know



something
you have



something
you are

- Not all MFA is equal: SMS, app codes, and push approvals can be phished or relayed
- **Passkeys:** a FIDO2 key bound to one website, unlocked by face, fingerprint, or PIN



One website

- Use passkeys wherever offered; elsewhere, use strong unique passwords plus two-step verification

“this login looks odd”



Deny



Report



Change
credentials

SIMPLE HABITS
STRONGER SECURITY

From Event to Incident: Detection and Response Words



- **Event:** any observable occurrence on computing assets



- **Adverse event:** an event with a negative consequence



- **Incident:** actually or imminently jeopardizes confidentiality, integrity, or availability



- **Detection words:** alert, monitoring, SIEM, and SOC



- **Response words:** plan, playbook, triage, severity, containment, eradication, recovery, review



- Incident is the event; a data breach is the subset where protected data is exposed



- **Timeline anchor:** prepare, detect, respond, recover, improve

prepare

detect

respond

recover

improve

Identity, Access, and Data-Handling Terms You Will Hear

- SSO, privileged account, service account, session hijacking, and MFA fatigue
- Phishing-resistant MFA: FIDO2 and passkeys only; SMS, app codes, and push approvals are phishable
- Data vocabulary: personal data, sensitive data, PII, classification, DLP, and retention
- Security policy protects systems and data; privacy policy covers how personal data is collected and used
- Visual anchor: a data-classification color scale that reads the same everywhere

Account Types



SSO



privileged
account



service
account

Phishing-Resistant MFA



FIDO2 and
passkeys only

Phishable MFA



SMS, app codes,
and push approvals
are phishable

Data Classification

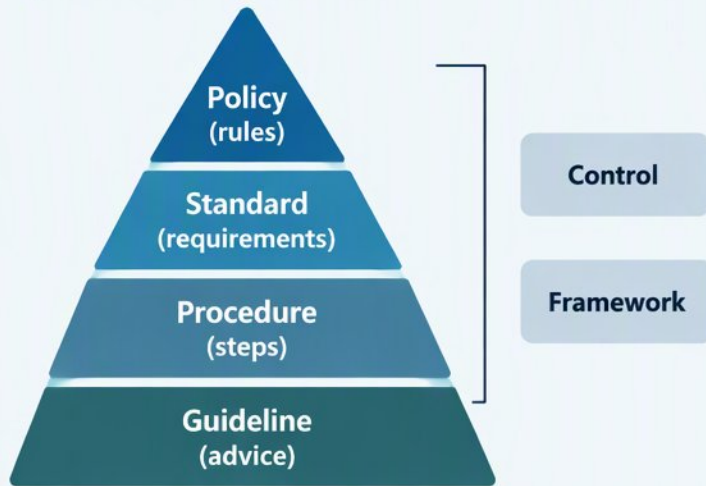


Compliance and Governance Terms Managers Should Know

COMMON TERMS. CLEARER CONTEXT. STRONGER DECISIONS.

Policy hierarchy

Policy hierarchy: policy (rules), standard (requirements), procedure (steps), guideline (advice) — plus control and framework.



NIST CSF 2.0

NIST CSF 2.0: six functions — Govern, Identify, Protect, Detect, Respond, Recover.



Standards and control frameworks

ISO/IEC 27001:2022: certifiable management system; CIS Controls v8.1: 18 prioritized hygiene controls.



ISO/IEC 27001:2022

Certifiable management system



CIS Controls v8.1

18 prioritized hygiene controls.

Regulations by who they protect

Regulations by who they protect: GDPR (EU residents), HIPAA (patients), PCI DSS (cardholders), SOC 2 (customers).



GDPR

(EU residents)



HIPAA

(patients)



PCI DSS

(cardholders)



SOC 2

(customers)

Compliance is not security

Compliance is not security: a certificate proves process, not that no one can get in.



A certificate proves process.



Not that no one can get in.

Practice: Match the Term to the Plain Meaning

REVIEW • THINK • APPLY



- Matching drill: pair formal definitions with everyday explanations for core risk words and the attack family



virus vs. malware



backup vs. sync



authentication
vs. authorization



incident vs. breach

- Mix-up correction round: virus vs. malware, backup vs. sync, authentication vs. authorization, incident vs. breach



- Scenario prompts: choose the right term and next action for a suspicious email, lost laptop, or odd login



- Role-based variants: manager, educator, and student versions of 'what do you say and do next?'



- Answer keys point back to the visual anchors used earlier in the deck

Say It, Report It, Teach It

SAME WORDS. SAFER SPACES. STRONGER LEARNERS.

PEOPLE
PRACTICE
PROGRESS

1. First Alert



2. Report It



3. Take Action



4. Lessons Learned



- Walk through one incident: first alert to lessons learned, plain words
- Report script: what you saw, when, device or account, what you did
- Team habit: same word, same meaning; correct mix-ups kindly; escalate early
- Educators: teach three or four terms in context; learners explain to a classmate
- Commit to ten terms you will use correctly; add more as they arise

RISK CHAIN



Threat actor



Vulnerability



Exploit



Impact

CLEAR TERMS. BRIGHTER FUTURES.

Your One-Page Glossary and Next Steps

- Handout: ten committed terms plus five common mix-ups
- Self-check: three questions per section, keyed to visual anchors
- Reinforce: one term per week, using a real example
- Authoritative sources: NIST CSRC, CISA, and NCSC passkey guidance
- Shared words make every non-specialist part of the defense

SAME
WORDS
STRONGER
TOGETHER

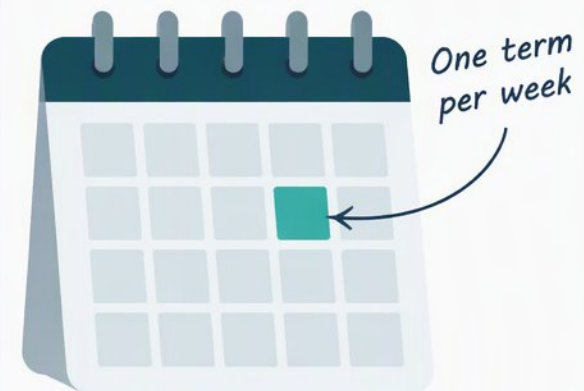
Your Glossary

	_____		_____
	_____		_____
	_____		_____
	_____		_____
	_____		_____

Common Mix-Ups

?	_____
?	_____
?	_____
?	_____
?	_____

Weekly Reinforcement



Authoritative Sources



PersonWise.

PersonWise • AI digital-human course platform



Scan the code or click anywhere to watch this course live, with voice Q&A

personwise.ai/t/02b2fde1/public