CS-025 · Passwords & Authentication

Multi-Factor Authentication (MFA)

Requiring more than one kind of proof so a stolen password alone is not enough.

Executive Summary

Multi-factor authentication requires a user to present two or more different types of evidence to prove identity, drawn from something you know, something you have, and something you are. Because an attacker rarely holds more than one factor, MFA blocks the large majority of account takeover attempts that rely on a stolen or guessed password. Not all methods are equal, and phishing resistant options are the strongest.

What It Is

Multi-factor authentication, often shortened to MFA and sometimes called two-factor when exactly two are used, strengthens login by combining evidence from different categories called factors. The knowledge factor is something you know, such as a password. The possession factor is something you have, such as a phone running an authenticator app or a hardware security key. The inherence factor is something you are, such as a fingerprint or face scan. True multi-factor authentication mixes categories, so two passwords are not multi-factor. The goal is that compromising one factor does not grant access, because the attacker still lacks the others.

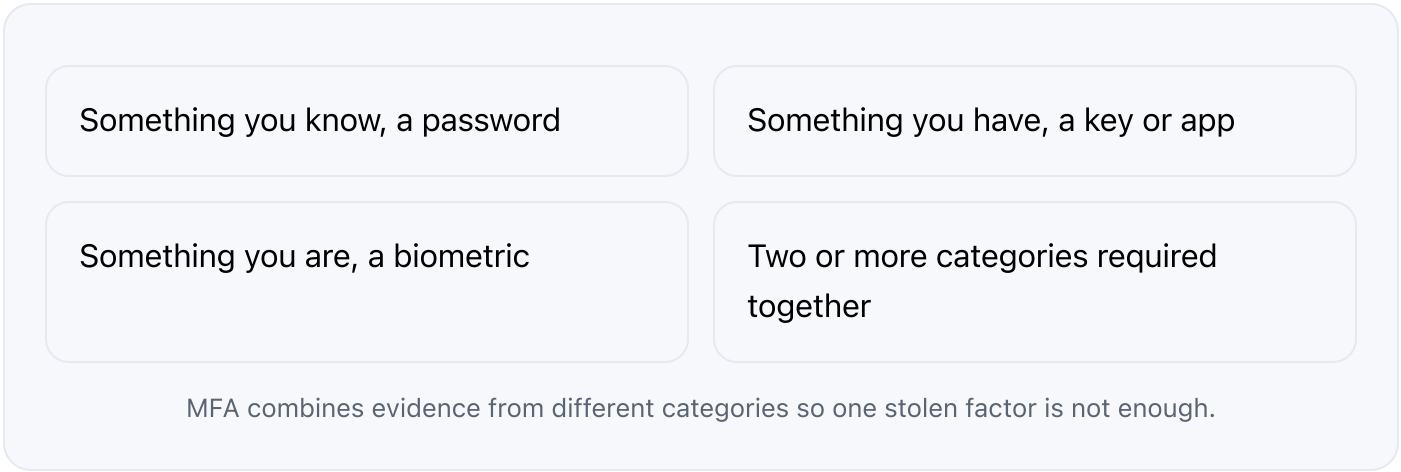
Why It Matters

Passwords are stolen, phished, guessed, and reused constantly, so a login protected by only a password is fragile. Adding a second factor is one of the single most effective defenses against account takeover, because a remote attacker with a stolen password still cannot present the user's device or biometric. Regulators, cyber insurers, and frameworks increasingly treat MFA as a baseline expectation, especially for administrators, remote access, and email. For a professional, knowing the factors, the relative strength of different methods, and how attackers try to bypass MFA is essential to designing, auditing, and defending modern authentication.

How It Works

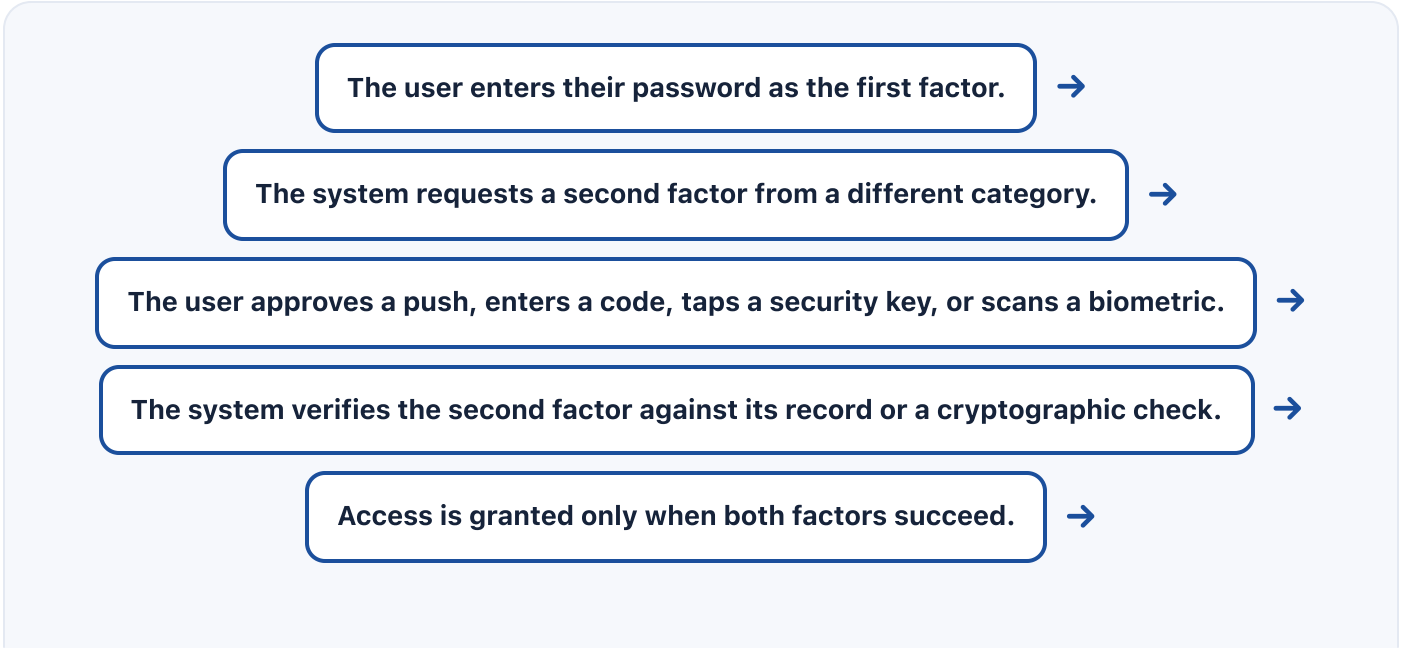
After a user enters a password, the system challenges for an additional factor. Common possession methods include a time based one time code generated by an authenticator app, a push notification approved on a trusted device, or a hardware security key that signs a cryptographic challenge. Inherence methods verify a fingerprint or face against a stored template, often on the device itself. The strongest methods are phishing resistant, meaning they bind the login to the real site so a fake page cannot relay the response. One time codes and push prompts can be phished or fatigued into approval, while standards based security keys and passkeys resist that by design.

Architecture Diagram



MFA combines evidence from different categories so one stolen factor is not enough.

Visual Workflow



High value actions may re prompt for a factor to confirm sensitive changes.

Common Attacks

- Phishing pages that relay one time codes to the real site in real time
- MFA fatigue, spamming push prompts until a tired user approves one
- SIM swapping to intercept codes sent by text message
- Stealing session tokens after login to skip the MFA challenge entirely
- Social engineering help desks into resetting or disabling a user's MFA

Common Mistakes

- Treating text message codes as strong when they are the weakest common option
- Enabling MFA for regular users but leaving admin accounts on password only
- Allowing unlimited push prompts with no number matching or rate limit
- Having no secure, verified process for MFA reset and recovery
- Assuming MFA alone protects against stolen session tokens after login

Best Practices

- Enable MFA everywhere, and require it first for admins, email, and remote access
- Prefer phishing resistant methods such as security keys and passkeys
- Use authenticator apps or push with number matching over text message codes
- Rate limit and alert on repeated failed or ignored MFA prompts
- Secure the enrollment, reset, and recovery process against social engineering
- Protect and shorten session lifetimes so stolen tokens expire quickly

Quick Checklist

- [x] MFA enabled on all accounts, admins and email first
- [x] Phishing resistant methods offered and preferred for high value access

- [x] Text message codes minimized in favor of apps or keys
- [x] Number matching or prompt rate limiting configured for push
- [x] MFA reset and recovery process verified and hard to social engineer
- [x] Session lifetimes limited and re prompts on sensitive actions

Recommended Tools

Authenticator app
Generates time based codes or approves push prompts as a possession factor

Hardware security key
Signs a cryptographic challenge for phishing resistant authentication

Passkey
Device bound credential offering strong phishing resistant login

Identity provider with MFA policy
Enforces and manages MFA across many connected applications

Industry Standards

NIST SP 800-63B
Defines authenticator types and assurance levels, favoring phishing resistant options

FIDO2 and WebAuthn
Open standards behind security keys and passkeys for phishing resistant authentication

CISA Guidance on MFA
Practical direction to adopt MFA and move toward phishing resistant methods

Career Relevance

MFA is central to identity and access management engineering, where professionals design enrollment, policy, and recovery. SOC analysts investigate MFA bypass and fatigue attacks; security engineers deploy phishing resistant methods and harden sessions; and GRC analysts map MFA to regulatory and insurance requirements during audits. Understanding both the

strength of different methods and how attackers defeat them is a core competency for the roles AI-Governance-Jobs.com serves.

Interview Questions

- What are the three authentication factor categories, with an example of each?
- Why is text message based MFA weaker than an authenticator app or security key?
- What does phishing resistant MFA mean, and which methods provide it?
- How does an MFA fatigue attack work, and how do you defend against it?
- Why can stolen session tokens let an attacker bypass MFA after login?

Related Certifications

CompTIA Security+ | **ISC2 Certified in Cybersecurity (CC)** | **ISC2 SSCP**

Further Reading

- NIST SP 800-63B Digital Identity Guidelines
- CISA: More Than a Password
- FIDO Alliance

Key Takeaways

- MFA combines two or more different categories of evidence to prove identity.
- A stolen password alone cannot pass a well designed MFA challenge.
- Phishing resistant methods like security keys and passkeys are the strongest.
- Text message codes are the weakest common factor and can be intercepted.
- Attackers target MFA through phishing, fatigue, and stolen session tokens.

FAQ

▶ **Is two-factor authentication the same as MFA?**

▶ **Which MFA method is the most secure?**

▶ **Can attackers get past MFA?**

Related Careers

RELATED ROLES

Iam Engineer | Soc Analyst | Security Engineer

RELATED CERTIFICATIONS

CompTIA Security+ | ISC2 Certified in Cybersecurity (CC) | ISC2 SSCP

CURRENT OPENINGS

Live roles are on the job board.

Browse all jobs

GUIDES & SALARY

Career guides | Role roadmaps | Salary data | Career tools

SUGGESTED LEARNING PATH

1. Ground the basics with CS-001 Cybersecurity
2. Study this sheet: **Multi-Factor Authentication (MFA)**
3. Go deeper: Passwords
4. Go deeper: Password Managers
5. Validate it: work toward **CompTIA Security+**
6. Find the role: browse current openings

RELATED SHEETS

CS-022 Passwords | CS-024 Password Managers | CS-026 Passkeys | CS-032 Phishing | CS-062 Authentication