THREATS LIBRARY

JULITH GmbH
Awareness-as-a-Service

Passwords & MFA — from risk to defence

More than three quarters of all data breaches involve compromised or weak credentials. We explain the 2026 state of the art — passkeys, FIDO2, MFA fatigue — and what employees need to do about it in practice.

min read: 8 min **Updated:** 14 March 2026 **Risk:** High risk
Source: awareness-as-a-service.com/en/resources/threats/passwords-mfa

Why are passwords and MFA so critical?

The password has been the weakest link in the security chain for decades — and simultaneously the one most frequently exploited. **Compromised or weak credentials** are implicated in more than three quarters of data breaches, according to the Verizon DBIR. Possession of credentials means no malware is needed.

Multi-factor authentication (MFA) was introduced as the counterweight: anyone who must supply a second factor (code, push confirmation, hardware token) in addition to a password is protected against pure password compromise. Attackers have adapted, however: **MFA fatigue** (also called push bombing) has established itself as its own attack technique — attackers send mass push confirmations until an irritated user approves one.

In 2026, the passwordless future is drawing closer. **Passkeys** (FIDO2/WebAuthn) replace passwords with cryptographic key pairs that are phishing-resistant, device-bound, and cannot be reverse-decrypted. Major platforms (Microsoft, Google, Apple) already support them in production environments.

At a glance

01

Password reuse is the biggest risk

Anyone using the same password on multiple sites risks one breach opening all their other accounts. Credential stuffing exploits exactly this.

02

MFA is not a cure-all

SMS OTP is weaker than app-based TOTP, which is weaker than FIDO2/passkeys. MFA fatigue and adversary-in-the-middle attacks bypass SMS and push.

03

Passkeys are production-ready in 2026

For many enterprise applications, FIDO2/passkeys are already available. They are phishing-resistant because they are domain-bound — a fake website cannot use the key.

How to recognise password and MFA risks

Password reuse
Employees using their company password for personal services too. A breach at any personal service opens the corporate account.

Passwords on post-its or in plain-text files
Handwritten or digitally unprotected passwords are accessible to anyone with physical or digital access to the workstation.

MFA fatigue (push bombing)
Anyone who receives an unexpected MFA push request they did not trigger should reject it — not approve it out of convenience.

Account sharing
Shared accounts (e.g. company social media) cannot be individually revoked and cannot be cleanly separated after a departure.

Weak password policies
"Password1!" meets many formal requirements (upper, lower, digit, special character) but is trivial to guess. Policies that mandate complexity but not length create false security.

How to protect yourself

For employees

- **Use a password manager:** One unique, long random string per account — the manager remembers everything. Recommended options include Bitwarden, 1Password, and KeePassXC.
- **Enable MFA everywhere** it is available — at minimum app-based TOTP (Google Authenticator, Aegis). Activate passkeys when offered.
- **Reject and report unexpected MFA push requests.** You did not initiate a login — so the request is coming from someone else.
- **Never share passwords** — not even with IT helpdesk or a manager. No legitimate system asks for this.
- **Change passwords when compromise is suspected** — not on a fixed routine (routine rotation leads to predictable and weaker passwords).

For administrators

- **Plan FIDO2/passkey rollout for all critical systems** — Microsoft Entra, Okta, Ping Identity, and other IAM platforms already support this in production.
- **Enable MFA fatigue protection:** Number Matching (user must confirm a displayed number) and Additional Context (location, app name) in the push configuration.
- **Password spraying and credential stuffing protection:** Account lockout policies, anomaly detection for unusual login geographies, HIBP integration on password changes.
- **Harden privileged accounts:** Admin accounts get FIDO2, not SMS MFA, no shared accounts.
- **Provide an enterprise password manager** — lower the barrier to good behaviour and it is more likely to happen.

Real cases

CASE 01 · INSURANCE COMPANY · DE · Q2/2025

A credential stuffing attack against the customer portal: attackers used a list from a fitness-app data breach and tried those email/password combinations. Several hundred customer accounts were taken over within a single night.

Damage: customer data compromised, mandatory GDPR notification · **Detection:** anomaly detection triggered after 3 hours · **Lesson:** Rate limiting and HIBP integration on login would have blocked the attack significantly earlier.

CASE 02 · NGO · CH · Q1/2026

An employee habitually approved an MFA push request at 2:07 am without thinking. The attacker had the password from an old breach and sent push requests until one was confirmed. Through the compromised account, donor data and financial reports were downloaded.

Damage: data breach, major donor trust affected · **Detection:** user reported access problems the next morning · **Lesson:** Number Matching would have prevented the accidental confirmation.

What to do if it happens?

THE FIRST 15 MINUTES

1. **Change the password immediately** — from a device that is not compromised.
2. **Invalidate all active sessions** (on most services: "sign out all devices").
3. **Inform IT Security** — especially if a corporate account is affected.
4. **Check MFA devices:** Were new devices or apps registered as a second factor without your knowledge?
5. **Check other accounts using the same password** and change those immediately too.
6. **HIBP check (haveibeenpwned.com):** See whether your email address appears in known data breaches.

Frequently asked questions

How long should a secure password be?

At least 16 characters if it is still a classic password. Length matters more than complexity: "Coffee-Monday-Blue-42" is more secure than "P@ssw0rd!". Better still: let a password manager generate a random 24-character string.

What is the difference between TOTP and FIDO2?

TOTP (Time-based One-Time Password, e.g. Google Authenticator) generates a new code every 30 seconds — but it can be intercepted and relayed by an attacker in real time (adversary-in-the-middle). FIDO2/passkeys are domain-bound: a fake website cannot use the key because the domain check is built into the protocol.

Should IT know an employee's password?

No. Passwords should be known only to the user and stored at the provider only as a hash. When IT needs to reset a password, this is done through a reset process — not through knowledge of the current password.

Are password managers themselves secure?

Commercial password managers (Bitwarden, 1Password) are recommended by security experts and audited regularly. The risk from a single compromised master password is real — which is why the master password must be strong and used only for the manager. MFA on the manager account is mandatory.

Related topics

Weak credentials are the entry point for phishing, CEO fraud, and deepfake-assisted attacks. AI-powered attacks make password compromise faster and more convincing than ever.