The path to Zero Trust

Why phishing-resistant MFA is a must

While cyber crime has become more sophisticated over the past 10 years, the most frequent cause of security breaches remains the most obvious: credential theft.

> Stolen credentials are the No. 1 most common entry point in cybersecurity breaches
>
> Source: Verizon 2023 Data Breach Investigations Report

Multi-factor authentication (MFA) is the most effective form of protection against credential theft, but its efficacy is often undermined by two common implementation issues.

Failure Point #1
MFA hasn't been implemented organization-wide. This includes employees, contractors, *and* partners.

Failure Point #2
MFA does not include phishing-resistant factors that add adequate protection against phishing-related credential theft.

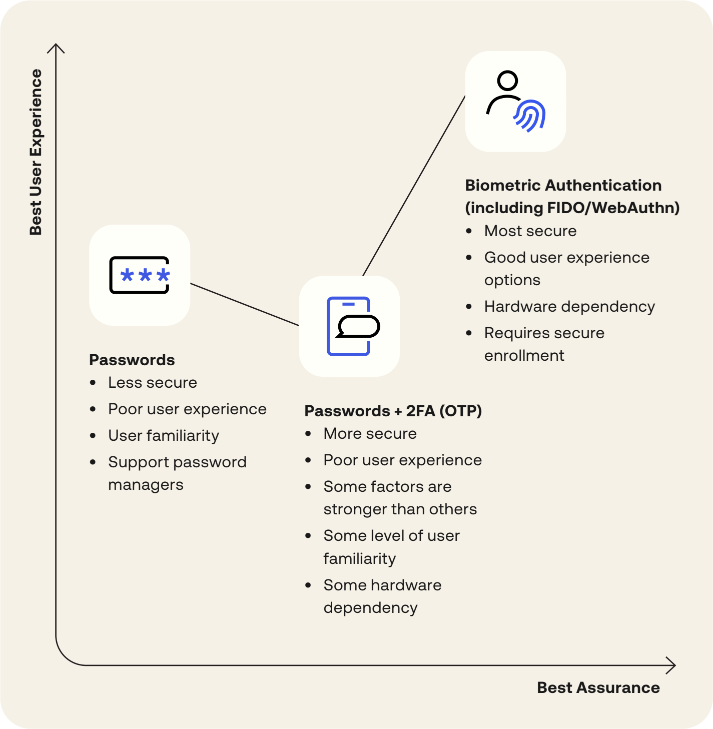
To truly achieve Zero Trust, organizations must embrace phishing-resistant MFA. Without it, they leave themselves open to potentially catastrophic breaches.

> 89% of organizations experienced a phishing attack in 2022
>
> Source: HubSpot, 2022 State of Passwordless Security Report

Not all types of MFA are created equal

Security professionals agree: MFA is superior to the traditional combination of username and password. However, the practical efficacy of MFA depends on the factors being used, and the security of these factors depends on a number of variables.

- The assurance level of the factor
- The deployability of the factor
- The availability to pair the factor with context (e.g., user, device, network context)



Biometric Authentication (including FIDO/WebAuthn)

- Most secure
- Good user experience options
- Hardware dependency
- Requires secure enrollment

Passwords

- Less secure
- Poor user experience
- User familiarity
- Support password managers

Passwords + 2FA (OTP)

- More secure
- Poor user experience
- Some factors are stronger than others
- Some level of user familiarity
- Some hardware dependency

It's time to make phishing-resistant factors a priority

The continued success of social engineering cyberattacks (i.e., attacks that hinge on manipulating users into giving their personal information away) has underscored the importance of ensuring that the factors involved in MFA are phishing resistant.

So, how do you know if a given factor is phishing resistant? It will have all three of the following characteristics.

1. **No shared secrets**
   The factor employs cryptography to keep authentication data private end to end.
2. **Origin bound**
   Authentication credentials are tied to a specific domain, adding a layer of context-specific security.
3. **Trusted**
   Authenticator attestation helps verify credentials are from a trusted authenticator.

Source: U.S. National Institute of Standards and Technology (NIST)

In plain language: Phishing-resistant MFA is a better way to ensure only users with valid credentials can access sensitive resources. This level of protection is essential when it comes to securing your workforce against the continuing onslaught of cybercrime.

Balance strong security with superior UX

As companies continue to strengthen their security posture, they must give special focus to the role of MFA in their Identity and Access Management (IAM) solution. Phishing-resistant factors are a must: They give your organization the best available protection against Identity threats and, when deployed correctly, offer the ideal balance of security assurance and positive user experience.

> "Okta is behind our device registration, phishing resistance, and device posture assessment, effectively helping us deliver on a Zero Trust strategy. It's all of those — and one day it will also help us go passwordless."
>
> – Eric Richard, SVP of Engineering and Chief Information Security Officer, HubSpot

Ready to learn more about your MFA options?

Contact our team and learn more about Identity's role in protecting against threats here:
okta.com/resources/whitepaper-anatomy-of-identity-based-attacks