yubico

Passwordless 101:

How to make your organization phishing-resistant today

Going passwordless might be the best thing you'll ever do for your organization. It's a three-in-one shot to dramatically improve security, simplify the user experience and reduce overhead. Password-focused environments will always be more phishable and less safe, and every step away from them will toughen your security posture.

However, the journey to passwordless can be a long and winding road if you don't set yourself up for a successful implementation. In this paper, we'll explain what passwordless authentication is and explore your best approach for going passwordless so you can defend your organization against phishing and credential theft today—and tomorrow.

What is passwordless authentication?

At its most basic definition, passwordless authentication is any form of authentication that doesn't require the user to provide a password at login.

Going passwordless is a journey rather than an overnight destination. To get there, most enterprises will begin by moving their legacy multi-factor authentication (MFA) to a modern MFA solution that offers strong phishing defense. A move away from legacy MFA to modern MFA then sets an organization up for a move into passwordless authentication.

While there are many examples of MFA in use today, not all MFA is equal in its strength of security and defense against phishing. First, let's take a look at the options available today.

Legacy MFA

SMS

SMS verification usually involves sending the user a One-Time-Password (OTP), often in the form of a 6-digit code.

Email magic link

This method creates a unique link with an embedded token and delivers it to an email address. Clicking the link verifies the user for that particular service.

What SMS verification and email magic links gain in usability they lose in security: both methods are highly susceptible to phishing. Users can be easily tricked into typing in a fake OTP or clicking on a "phishing bait" magic link.

Modern MFA

Smart cards

In this solution, a user inserts their smart card into a reader, and validates it with a unique PIN. This method is one of the most effective ways to protect against remote phishing attacks, but traditional smart cards may be complex for administrators to implement and manage at scale.

Biometric readers

Biometric readers use something uniquely biological (a face, a fingerprint, an iris, or other feature) as a credential. As more modern devices are available with built in platform authenticators such as TouchID, FaceID, and others, the use of biometrics is growing quickly.

PINs

PINs are often paired with local devices like biometric readers or smart cards. Since a PIN is always tied to a physical device, it is considered more secure than legacy MFA because it does not reside on a server that can be breached, nor does it have to be sent over a network.

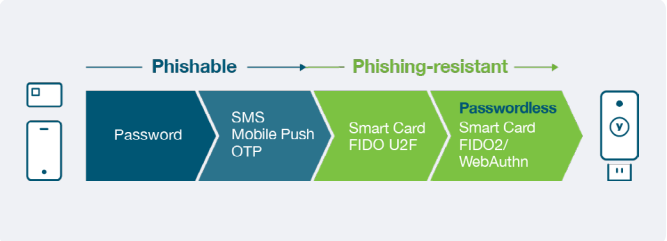

Figure 1: Passwordless is a journey, and it's already begun

How do you create a passwordless strategy?

The first step to creating a passwordless strategy is to assess your existing environment, investments, and resources.

There are two questions worth asking here:

- Do you operate in the cloud, on-premises, or in a hybrid environment?
- How do you prioritize security levels, user experience, and cost?

These elements are sometimes in conflict, so it's worth knowing how you will negotiate the trade-offs if you have to make tough choices.

This will help determine which road to passwordless will work best and most efficiently for your organization and users.

Paths to Passwordless

Smart card passwordless approach

Organizations with an on-premise infrastructure should consider implementing a smart card-based passwordless approach. This offers both the benefits of strong security and a passwordless user experience.

Smart cards are eminently less phishable than a password-based system, and are used effectively in some of the most security-conscious organizations in the world today. As mentioned, traditional smart card deployments are complex and time-consuming. Organizations should consider simplifying smart card deployment with a strong authentication solution that is both easy for IT to adopt and doesn't saddle users with extra hardware like smart card readers.

FIDO2/WebAuthn passwordless approach

FIDO2 is the newest FIDO Alliance specification for authentication standards, and WebAuthn is a web-based API that allows websites to update their login pages to add FIDO-based authentication on supported browsers and platforms. This is an evolving security ecosystem that can help cloud-first organizations advance towards passwordless. For cloud-first environments, FIDO2/WebAuthn passworldless may be an effective passwordless strategy.

If you have cloud-based applications like Office 365 or other SaaS applications, such as Salesforce federated with Azure AD (AAD), and operate under AAD or a hybrid AD-AAD backend environment, then FIDO2 passwordless is probably your best first step. If you are working with other IAM providers such as Okta, Duo, or Ping, you can also consider a FIDO2/WebAuthn-based passwordless approach.

Hybrid passwordless approach

Increasingly, enterprises are choosing to combine different types of passwordless approaches to create a solution that solves their needs. An organization might use FIDO2/WebAuthn passwordless for computer login and federated web apps and a smartcard passwordless approach for secure remote access (RDP, VPN, VDI).

Future-proofing your passwordless approach

There are many ways to achieve phishing-resistant passwordless authentication. All strategies lead to stronger security, a better user experience, and peace of mind for your whole organization.

No matter which direction you take, you can future-proof your investment with hardware-based security keys such as the YubiKey 5 Series. The YubiKey 5 Series works seamlessly with a smart card, FIDO2/WebAuthn, and hybrid passwordless approach. It's also compatible across a range of technical environments, from legacy applications to a modern cloud environment.

You don't have to make any new software or peripheral investments before integrating the YubiKey 5 Series as part of your system. YubiKeys kickstart your journey to passwordless—strongly enhancing your overall security posture, simplifying deployment, and future-proofing your security investment as your needs continue to evolve, and as compliance regulations become more stringent.

And, as you determine the best passwordless strategy for your organization, you can put an end to phishing immediately using YubiKeys as a second factor on top of a password.

Yubico: Making passwordless possible

Since our inception, Yubico has advocated for open security standards to achieve security and usability at scale. Yubico paved the way by pioneering the WebAuthn and FIDO open standards, and worked with tech giants like Google, Microsoft, and Apple to integrate these standards into the operating systems and browsers we use every day. These standards, paired with a YubiKey, allow for strong passwordless authentication across devices, apps, and services without any additional proprietary software.

The YubiKey Family

The YubiKey is available in multiple form factors for desktop, laptops and mobile devices.

About Yubico As the inventor of the YubiKey, Yubico makes secure login easy. As a leader in setting global standards for secure access to computers, mobile devices, and more, Yubico is also a creator and core contributor to the FIDO2, WebAuthn, and FIDO Universal 2nd Factor (U2F), and open authentication standards. For more information, please visit: www.yubico.com.

Yubico AB
Kungsgatan 44
2nd floor
SE-111 35 Stockholm
Sweden

Yubico Inc.
530 Lytton Avenue, Suite 301
Palo Alto, CA 94301 USA
844-205-6787 (toll free)
650-285-0088