E-BOOK

Got Phished?
How to Get MFA Right the First Time

SECRET DOUBLE OCTOPUS

Contents

Introduction:

We're Heading for Phishing-resistant MFA — and How You Get There Matters

According to CISA, 90% of successful data breaches still start with a phishing attack[1] which research shows 94% of organizations sustained in the recent past[2]. The ongoing success of phishing means even organizations that followed industry best practices still aren't safe — and it's time to change directions.

Following best practices isn't enough

Most standards require the use of MFA to strengthen identity verification and stop phishing. Some treat phishing as a 'people problem' and mandate investments in training users not to spot fake emails, links, and increasingly texts. This shifts the onus of improving security to HR and the blame onto users who continue to take the bait. Phishing training experts at KnowBe4 reported that, after a whole year of training, 5.4% of users still click bad links—a fact that should signal the death-knell of awareness training as a solution to phishing.

What's the missing piece of the puzzle?

Ongoing attacks, government mandates, and rising cyber insurance premiums all point to one thing: it's time for enterprises to become phishing-resistant. In this book we'll see why getting rid of passwords is the best and fastest way to do that. We'll cover:

- The foundational flaw and why most MFA can't stop phishing
- A fast, simple way to become phishing-resistant right now — without starting over
- How MFA can achieve high-assurance authentication for every user logging into every business service or application from any device, at any location at any time

> **"Insanity is doing the same thing over and over again and expecting different results."**
>
> Albert Einstein

[1] https://www.cisa.gov/stopransomware/general-information
[2] https://www.egress.com/blog/phishing/phishing-statistics-round

Chapter 1:

MFA vs. Phishing-resistant MFA

Phishing has been around since the ‘90s so it’s tempting to conclude it’s a problem that can’t be fixed. Investments in email security, spam filtering, and user education all move the needle, but adversaries still only need one valid username/password combo to gain access and start working their way toward your crown-jewel assets and even your supply chain.

In an attempt to avert disaster...

Regulators turned up the heat

Businesses worldwide face federal and industry mandates that push toward Zero Trust security postures and phishing-resistant MFA:

- Edicts such as memorandum 22-09, from the Biden administration’s Office of Management & Budget (OMB), mandate phishing-resistant MFA for the government supply chain by 2024
- De facto cybersecurity frameworks like MITRE ATT&CK stress phishing resistance
- Cyber insurance discounts for demonstrating phishing-resistance won’t lag far behind

Mandating phishing-resistance puts the responsibility where it belongs — on innovative technology solutions – but does not immediately translate into actionable best practices.

Does ‘phishing-resistant’ always mean passwordless?

Most MFA continues to use credentials — the highly vulnerable “something users know”— as the first factor in verifying identity. Weak second factors also may be easily thwarted with social engineering attack strategies. These foundational flaws keep MFA intrinsically vulnerable to phishing, and in turn ransomware, malware, and third-party attacks that often involve innovative, targeted techniques and “man in the middle” attacks.

Since the term ‘phishing-resistant MFA’ first appeared in the Biden administration’s M22-09 presidential memo, the industry consensus seems to have coalesced around achieving resistance to three types of attack techniques:

- **Impersonation.** Pretending to be a legitimate user
- **Social engineering.** The use of deception to manipulate workers into divulging confidential information that is used for fraudulent purposes
- **Man-in-the-middle (MITM) attacks.** Attackers sit between a target and legitimate site and send messages designed to trick users into attempting to authenticate into fraudulent sites—usually replicas of known legitimate sites—where they then capture working credentials and session cookies.

In each case, though not specified, the use of a passwordless MFA based on cryptographic key-pair binding offers the most obvious, logical, and effective approach.

MFA also creates friction and a lot of work for everybody

Where two-factor authentication (2FA) mostly just asked users to do one other simple thing to prove their identity — usually typing in a 4- or 6-digit one-time passcode (OTPs) sent via text — today’s MFA layers more annoying steps into the log-in process. Physical USB-type security keys, smart cards with X.509 certificates, facial scanners, thumbprint readers, and voice recognition now all may be part of the process.

	Passwordless MFA	Traditional MFA
Impersonation resistant	Yes	No
Social engineering resistant	Yes	No
Man-in-the-middle resistant	Yes	No
Lost/Theft reuse resistant	Yes	No
Insider’s collusion resistant	Yes	No

The more complicated we make logging into things the more stakeholders dislike MFA for good reason:

- **The average worker spends up to 5% of their time,** about 22 minutes a day, just interacting with IT infrastructure4
- **Cost goes up as IT buys,** ships, and maintains smart cards, hardware tokens, and biometrics readers across the enterprise workforce
- **Up to 50% of Help Desk calls** involve credentials — to the tune of over $1 million per year in lost productivity

Where do we go from here?

Piling on more steps will never be enough to check the box on phishing-resistance or fix the other shortcomings of conventional MFA. One obvious way to right the ship is to eliminate the use of passwords from the user authentication equation. So let’s look at three ways to do that.

Chapter 2:

Taking Passwords Out of the Equation

The goal of authentication — verifying the identity of someone trying to access certain resources — does not intrinsically need to include passwords, but it pretty much always has. A passwordless approach to MFA delivers less risk, with fewer steps and problems—in less time.

For the record...

Passwordless MFA is MFA...

It's MFA that takes the perennially vulnerable "what users know" out of the equation—and the phish out of the sea once and for all. A passwordless approach to MFA replaces passwords, "something users know," with a mix of stronger pillars of identity verification. One is "something users have," typically their phone or PC, the other is something users "are," verifiable with biometrics to:

- Streamline the login process
- Relieve users of the password management burden
- Eliminate MFA fatigue among users and Help Desk professionals
- Up-level Identity and Access Management (IAM) toward Zero Trust Identity

Users can't share what they don't know exists. A passwordless MFA workflow satisfies the intent of mandates requiring Zero Trust and phishing-resistance as well as growing pressure from cyber insurance carriers to finally put a stop to phishing.

So, how do you do it?

The Cybersecurity & Infrastructure Security Agency (CISA) implementation guide lists two options for implementing phishing-resistant MFA:

- Public key infrastructure (PKI)-based government-issued PIV and CAC ID smartcards
- FIDO/WebAuthn authentication
- And Secret Double Octopus (SDO) adds a third option: Desktop-to-app pinning with mobile push

CISA recognizes that neither of the first two approaches addresses the full spectrum of enterprise workforce applications. Even in cloud-first organizations, some percentage of apps still use directories that will continue to require passwords for the foreseeable future. In the meantime, CISA, NIST, MITRE ATT&CK, and other mandates and security frameworks prescribe phishing-resistant MFA.

PKI charts a difficult path

PKI uses certificates for authentication. Most PKI implementations exist within government agencies or other heavily regulated industries where workers carry smart cards with embedded X.509 tokens. PKI also requires significant retooling of both applications and directory infrastructures to get full use case coverage. Until then, systems may be incompatible with common use cases like Radius VPN, Linux-based services, and mission-critical custom and legacy apps that are dependent on password directories and PKI unsupported protocols.

Newer software-based solutions like Microsoft's Windows Hello for Business (WHfB) use internally signed certificate-issuing infrastructure without physical smartcards but still don't offer full use case coverage. Unfortunately, WHfB, for example, only works with other Microsoft technology.

FIDO only works for web

CISA calls FIDO, "the only widely available phishing-resistant authentication" but it's only "widely available" for web or browser-based services. To date, the FIDO Alliance has yet to release a standard for how FIDO2 tokens communicate with corporate apps that work with directories. A bridging function, like the Octopus platform described below, translates the FIDO2 token registered in the FIDO2 server to password directories and ultimately to corporate apps.

Pre-pinning adds the missing "link"

PKI and FIDO2 use public/private key pairs to establish trust. Users pre-register their FIDO2 devices with specific web sites or SSO portals. This approach resists phishing, including advanced MITM attacks because, no matter what information users inadvertently let slip, including the public key used in authentication, the hacker's device won't have the private key needed to decode the signing public key and verify identity. The private key never leaves the FIDO2 vault within the FIDO key or token. **The same approach can be implemented without hardware-based FIDO tokens or physical keys.**

Octopus desktop-to-app pinning / mobile push

To expand the use of pinning — and passwordless MFA — beyond web applications, SDO created desktop-to-application pinning. A software-based Octopus passwordless agent installed on user devices lets devices be directly pinned to individual SSO portals and other workforce resources without additional hardware. The SDO agent prompts the trusted platform module (TPM) already inside the user's computer to generate a private key. The platform binds the private key with the public key to conduct secure identity verification via keypairs, all within software.

100% coverage with 0 change to your infrastructure

It pays to do passwordless right. If you've reached the end of the road with your existing solution, SDO can help bridge gaps and supplement existing strategies and solutions with the fastest path to full passwordless MFA use case coverage. Our customers achieve:

- Less risk
- Less friction
- Less change
- Less cost

But since our main focus is phishing, let's take a closer look at the benefits of passwordless phishing-resistant MFA.

Chapter 3:

Four Ways Passwordless MFA Stops Modern Phishing Attacks

1. Phishing for credentials

Passwordless MFA stops phishing campaigns aimed at tricking users into giving up their credentials because, so far as users are concerned, credentials don't exist.

2. Attacks on traditional MFA

Phishing-resistant MFA shields the workforce from techniques such as push bombing that target MFA itself. As we've seen with highly publicized recent attacks, users will give in when flooded with too many push notifications and/or fake messages from IT to approve the requests — even at 3 AM when they aren't logging into anything.

Cryptographic pinning of apps to devices makes it impossible for hackers to start unauthorized authentication. They can't, because they won't have the right private key tucked away in the TPM vault or the right fingerprint/retina needed to finish the challenge.

3. Attacks on desktop and corporate applications

Many companies still rely heavily on the likes of VPNs, thick client apps, and devices that use Mac or Linux OSs. Password directory-friendly passwordless MFA with direct pinning makes it possible to include any device or application.

4. MITM attacks

Automated MITM attacks succeed with devastating silence once the bait is clicked, without exploiting passwords or second one-time passcode (OTP) factors. Automatically generated messages trick users into attempting to authenticate into fraudulent locations to capture session tokens. With the token, the attacker gains full access to the victim's account to modify credentials for account takeover or pivot off the victim toward more valuable company assets.

MITM exploits and campaigns employ multiple techniques:

- **Physical proximity.** Attackers create fake unsecured Wi-Fi hotspots in places like coffee shops. When patrons unknowingly connect, the would-be hacker in the middle gains access to data, including credentials and cookies.
- **"Man-in-the-browser" (MITB).** Emails prompt users to click links and install malware that records data sent between the victim's device and specific sites like company SSO portals or financial institutions.
- **SIM swapping.** Cybercriminals learn enough to impersonate users, answer security questions, and ask mobile carriers to reassign cell phone numbers to a new SIM card that lets them access victims' data remotely.
- **MFA prompt / push bombing / MFA fatigue.** These social engineering attacks leverage the fact that MFA frustrates users by impersonating IT (and other legitimate entities)

Phishing-resistant MFA stops the start of push bombing and MITM attacks and bombarding users with verification prompts until they give in and approve the request.

The only ways to stop these attacks is for the user to spot the fake URL, which is especially unlikely with long URLs, or by applying phishing-resistant MFA pinning with a key pair challenge that prevents the user from connecting to fake SSO portals or directly to web apps. Users take FIDO tokens and register a set of PKI keys with the real site. The registration process links the username, the site's URL, and the keys together in such a way that anyone attempting to authenticate with a particular username would need to have the private key or token to decode the signed public key. This process also catches the slight, otherwise-easy-to-miss discrepancy between the real and fake URLs.

Along with the inherent benefits of passwordless, the Octopus Authenticator delivers a suite of phishing-resistant capabilities that work with password directories. In the next chapter, we'll run through a checklist for getting MFA right the first time or modernizing quickly so users stop getting phished.

Chapter 4:

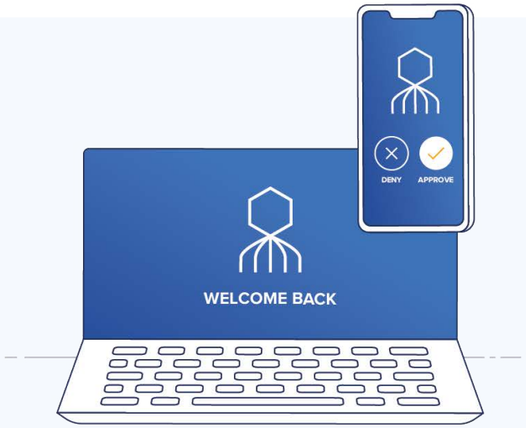
The Five Criteria for Phishing-resistant Passwordless MFA

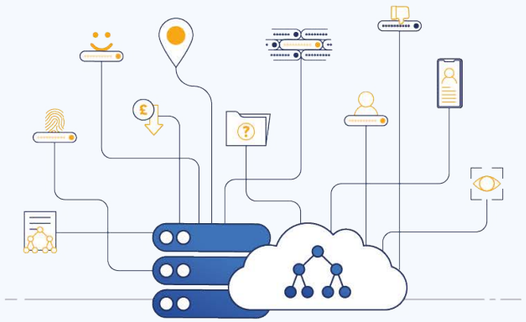
1. Users never need to set or change passwords

The key word here is “never.” Some solutions claiming to be passwordless actually mean “passwords-less-often.” Similarly, single sign-on (SSO) streamlines access significantly but isn’t passwordless, or phishing-resistant for that matter. Users still must know their password and enter credentials upon startup, or “just once a day,” and all other times access apps not supported by SSO. The password, and threat of phishing, continues to exist.

2. User login gets decoupled from directories

A picture is worth 1,000 words:





With directories remaining password-centric for the foreseeable future, coexisting with passwords on the back end is a must. Decoupling the back and front ends lets users be passwordless everywhere, right now while the majority of non-Web business applications continue to use passwords to authenticate into directories. Decoupling makes it easy to replace the backend passwords with ephemeral one-time tokens, and shift the management of token generation to the behind-the-scenes realm of IT.

With Octopus, **IT can start onboarding users in less than hour** with this “password directory-friendly” approach without applications and identity directories being retooled or upgraded until IT feels ready. The de-coupling of user-side MFA from directories enables our third criteria:

3. All applications become phishing-resistant

Otherwise, you can’t really check the box. Combining biometrics with pre-pinning makes it virtually impossible for anyone else to access devices and privileged applications and databases. Users get what they need to maximize productivity: A single workflow for desktop, corporate apps, privileged access, and web apps.

4. MFA works with mobile push

While many users are able to buy, expense, and provision FIDO keys on their own, most vastly prefer the simplicity of push notifications, and so does IT. There’s nothing to buy, nothing to carry, and best of all, nothing to lose. Users love mobile push because it’s fast and easy and doesn’t require external devices (though biometrics like fingerprint readers can still be used for a second or third factor of verification).

5. MFA stops modern attacks

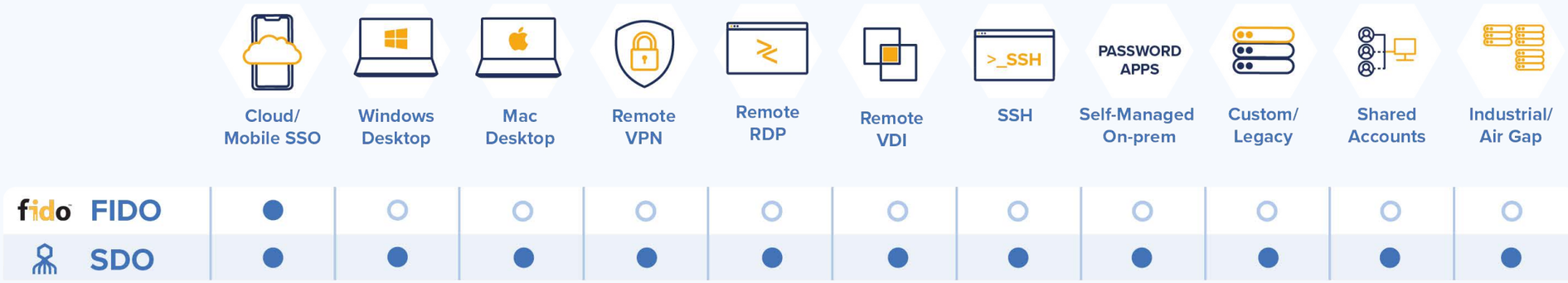
This is a pretty big topic, worthy of its own short chapter.

Chapter 5:

FIDO2 is the Future

FIDO2 passkey is clearly the future of passwordless authentication, mainly because it is phishing-resistant. But FIDO2 only works with web apps through its WebAuth supported protocol. But enterprises are so much more than Web Apps. Leaving essential on-prem and legacy apps behind doesn't do enough to solve the phishing threat.

Every business needs a continuity strategy for FIDO authentication fallback, and the directory password is the cheap and flexible mechanism of choice for the foreseeable future. As long as any IT-managed desktops, apps, and services require a password-based authentication, the user must know the password, which leaves the business exposed.



Converting everything in the enterprise to FIDO2 is a heavy lift that requires recoding of apps and re-architecting of directory infrastructures—and it's a long way off. Octopus extends FIDO2 authentication for enterprise-wide passwordless MFA, working with modern SSO and FIDO2 IDP integrations as well as password-based applications, only without the passwords.

Chapter 6:

Change is Hard. Octopus is Easy.

Keep IT in control

SDO's approach eliminates passwords from the user experience to protect your business and satisfy the intent of Zero Trust mandates to become phishing-resistant. We offer the only solution that can do this today for all enterprise use cases while keeping IT in control of the journey to a full passwordless, Zero Trust infrastructure.

SDO decouples user login and back-end directory infrastructures and uses FIDO, PKI, and desktop-to-app signed pinning to streamline authentication and stop phishing. Our approach achieves the full promise of passwordless MFA — reduced risk, cost, friction, Help Desk calls, and phishing – for every app, device, user, and location across your enterprise.

No passwords, no gaps, no change.

Curious?

Run your own information through the Passwordless MFA ROI Calculator to see what you stand to save.

SECRET DOUBLE OCTOPUS

About Secret Double Octopus

Secret Double Octopus is a leader in workforce passwordless and MFA solutions.

Its industry-leading Octopus platform offers mid-market to Fortune 100 enterprises the ability to move to a higher security, more frictionless authentication future progressively, from MFA to end-to-end, unified passwordless authentication. No other desktop MFA and enterprise passwordless platform matches the robustness and flexibility of the Octopus solution to leverage existing MFA authenticators and support legacy on-premise applications.

The company has been designated a Gartner “Cool Vendor” and more recently named “Best-in-Class” passwordless solution by AITE Group.

Secret Double Octopus delivers the industry’s broadest workforce use case coverage for passwordless MFA making SDO a clear leader in phishing-resistance, enabling compliance, and reducing cyber insurance premiums. Our industry-leading platform offers mid-market to Fortune 100 enterprises the ability to progressively move to a higher security, more frictionless authentication – from MFA to end-to-end, unified passwordless authentication.

From leveraging existing MFA authenticators to supporting legacy on-premises applications, no other desktop MFA and enterprise passwordless platform offers comparable robustness and flexibility. The company has been designated a Gartner “**Cool Vendor**”, named “Best-in-Class” passwordless provider by AITE Group and a **2023 SINET16 Innovator**.

Learn more at **doubleoctopus.com**