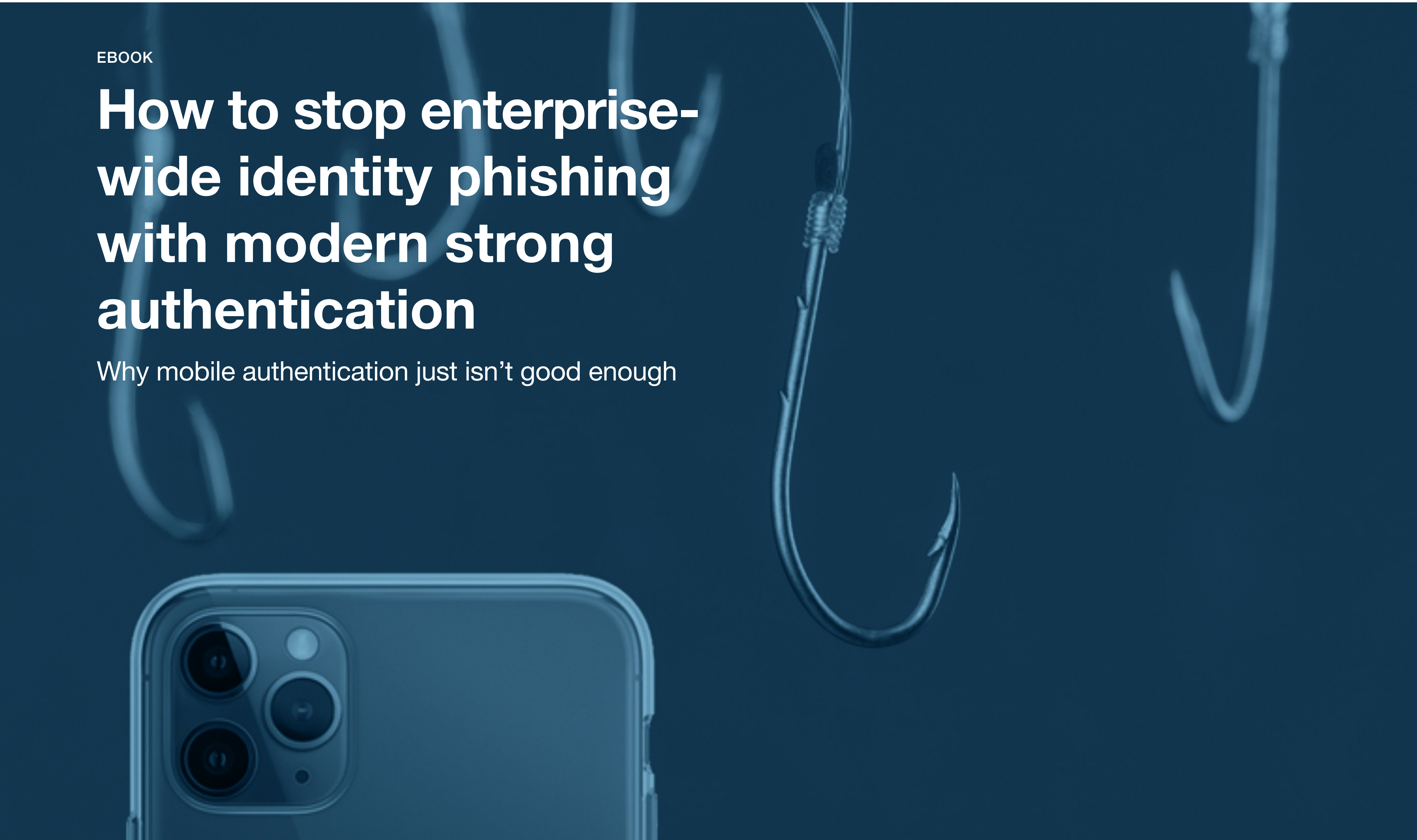
yubico

EBOOK

How to stop enterprise-wide identity phishing with modern strong authentication

Why mobile authentication just isn’t good enough



Contents

The evolving nature of phishing attacks

$14.8 million

is the average annual cost of phishing in 2021, up from $3.8 million in 2015[2]

75%

of organizations around the world experienced a phishing attack in 2020[3]

74%

of phishing attacks targeting US businesses were successful[4]

96%

of phishing attacks arrive by email[5]

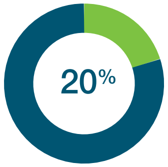
In recent years, phishing attacks have increased dramatically. According to a study published by the Anti-Phishing Working Group (APWG), the number of phishing attacks nearly doubled in 2020 and remained at near-record levels in the first quarter of 2021.[1] The same study recorded an all-time high of 245,771 attacks in January 2021. Of course, the true number of phishing attacks is likely much higher, and may never be known for certain as many attacks go undetected or unreported.

What is identity phishing?

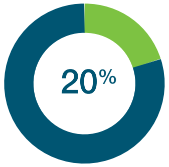
Phishing is the fraudulent practice of inducing people to reveal sensitive personal information such as credit card numbers and passwords. Phishing attackers send what appears to be legitimate communications by text, email, or other electronic communication from reputable companies and other trustworthy entities to lure users to phishing websites. These professional-looking sites are designed to elicit sensitive data and personally identifiable information. Typically, a phishing attack aims to get the victim to either reveal sensitive information or download malware.

Reveal sensitive information. The goal of these phishing messages is to trick the victim into revealing a username and password or other sensitive data — anything needed to breach an account or system. The attacker sends an email designed to look just like a message from a trusted sender. Because many employees reuse passwords across both business and personal accounts, this increases the chances of a successful phishing attack and breach.

Download malware. Many phishing emails work just like ordinary spam, but with a distinct intent to infect the victims' computers with malware, or ransomware in many cases. Attackers frequently go after "soft targets" such as HR professionals who receive emails with resume attachments every day. In place of a legitimate resume, they might receive attachments with malicious embedded code. This kind of attack is more time-consuming, but the potential rewards can be well worth the hacker's time and effort.



Nearly **one in five** companies that suffered a malicious data breach in 2020 was infiltrated due to lost or stolen credentials[6]



Almost **20%** of all employees are likely to click on phishing email links and, of those, a staggering **67.5%** go on to enter their credentials on a phishing website[7]

Common Types of Phishing Attacks

There are a number of different types of phishing attacks today:

Spear Phishing

Personal phishing attempts directed at particular companies or individuals are known as spear phishing.[8] Unlike typical phishing attempts that cast a broad net, spear phishing attackers increase their probability of success by collecting and leveraging the target's personal details to appear legitimate. For instance, attackers may use spear phishing to disguise themselves as trusted co-workers or other users, and trick employees into providing access to financial data or other sensitive information.

Spear Phishing versus Phishing

Spear phishing is the targeted version of standard phishing. A regular phishing campaign will send a mass communication to as many potential victims as possible. In contrast, spear phishing is very specific and takes aim at a particular organization or certain individual(s) they want to compromise. Attackers conduct careful research into their targets to increase their chances of success with a more personalized phishing attack.

Because phishing emails are sent in bulk and impersonal, they often contain typos, spelling errors, and other mistakes that allow users to detect their malicious intent. Trusted links and logos help disguise these subtle hints, but even so, the errors are there. On the other hand, spear phishing emails appear to come from trusted sources and contain convincing details, making them more challenging to detect.

Whale Phishing

Whaling phishing, trap fishing, or simply whaling, is a type of spear phishing attack that takes aim at high-profile targets such as senior executives. The difference between whaling and spear phishing is the role of the victim within the company. Spear phishing usually goes after specific yet lower-level employees, while whaling exclusively targets high-ranking individuals within an organization.

Catphishing and Catfishing

Catphishing attackers pose online in order to gain access to a person's resources or information, or to otherwise force them to do something. Catfishing is a related but specifically romantic or sexual concept, in which the phishing attacker creates a social network presence to lure the victim into a social relationship for access to resources or to gain control.

The high cost of phishing on Business Email Compromise

While the dramatic rise in phishing attacks is alarming, so is the level of sophistication and success at breaching enterprise organizations. For instance, Business Email Compromise (BEC) scams have become harder to detect and more costly as the average wire transfer request in BEC attacks grew from $48,000 in Q3 2020 to $85,000 in Q1 2021.[9]

Some BEC attacks specialize in impersonating senior executives to gain access to valuable corporate data. For instance, in one type of scam, the attacker poses as an executive to request access to internal financial documents, such as a recent aging report from the accounting department. An aging report lists all unpaid customer accounts, as well as customer contact names and email addresses. Using this information, the scammer contacts all of the victim's customers and directs them to pay their overdue invoices to a new bank account controlled by the attacker.[10]

Clone Phishing

Clone phishing attacks copy the contents of legitimate emails that may have contained links or attachments. Clone phishing steals the original email and replaces it with a malicious version that seems to come from the original sender.

Voice Phishing/Vishing

Some phishing scams send voice messages claiming to be from trusted senders such as government entities or banks. These messages direct the victim to call a number, which works using a voice over IP (VoIP) service, to resolve a problem or provide sensitive information. Similarly, vishing or voice phishing skips the written message and reaches out with this kind of VoIP system and fake caller-ID data to spoof a trusted organization and elicit sensitive data.

SMS Phishing/Smishing

SMS phishing or smishing delivers malicious links, cell phone numbers, or other bait via SMS. Smishing is harder to detect because URLs may not be fully displayed due to the nature of mobile browsers. In addition, smishing messages often arrive in unexpected or strange formats, like other automated messages.

Regardless of the attack method—spear phishing, whale phishing, smishing, or vishing—the overall goal is to trick victims into giving up valuable information, such as corporate credentials, access to financial and other accounts, personal information, and more.[11] The problem is, the more information hackers are able to harvest, the easier it is for them to impersonate a trusted entity, such as a co-worker, financial services representative, company executive, or even a family member.

COVID-19 fueled an already growing phishing epidemic

Shortly after the COVID-19 pandemic began, employees moved en masse from working in offices to working from home. In many cases, these users were accessing business apps and data from from unsecured networks and personal devices, such as family laptops and tablets. The fear and uncertainty resulting from the pandemic created ideal conditions for phishing scams to flourish. COVID-19 phishing threats became so prevalent that many security organizations, such as the Federal Trade Commission, routinely published specific warnings to increase awareness of Internet-based fraud.[13]

In the second half of 2021 and beyond, the percentage of people working from home at least part-time is expected to double to 34.4% compared with 16.4% before the coronavirus outbreak.[14] And yet, despite these dramatic workforce changes that require greater vigilance both on the part of the organization and its users, many security problems still remain, especially password-based authentication. Keeping corporate applications and data safe requires not just employee security awareness and training but also strong, phishing-resistant authentication to protect against enterprise-wide identity phishing attacks.

According to the Cost of a Data Breach Report 2021, data breach costs rose 10% from $3.86 million to $4.24 million in 2020 - 2021. There was also a $1.07m cost difference where remote work was a factor in causing the breach, escalated by COVID-19, compared to those where remote work was not a factor. Additionally, organizations that had more than 50% of their workforce working remotely took 58 days longer to identify and contain breaches than those with 50% or less working remotely.

The report also states that phishing as the initial attack vector had the second highest average total cost of $4.65 million, followed by malicious insiders ($4.61 million), social engineering ($4.47 million), and compromised credentials ($4.37 million).[15]

> “Despite all the user training and password restrictions in place, usernames and passwords are not enough to secure access to critical systems these days. Bad actors can use password spraying or social engineering to gain access.
>
> **Jackie Alexander, Director of IT, City of Mission Viejo**[12]

Modern phishing versus mobile-based authentication

Why mobile authentication just isn't good enough

Not all types of multi-factor authentication (MFA) are up to the task of preventing modern phishing attacks. Similar to usernames and passwords, mobile-based authentication such as SMS, one-time passcode (OTP), and push notifications also rely on "shared secrets" that can be breached by malware, SIM swapping, and man-in-the-middle (MiTM) attacks. In 2018, an attacker compromised Reddit employee accounts on their cloud and source code hosting providers set up with SMS-based two-factor authentication.[17]

Below are commonly used mobile-based authentication forms, each with its strengths and weaknesses as it relates to phishing.

> Any form of MFA is better than just a username and password, but most MFA can still be phished. It didn't take long to realize we needed stronger authentication for all employees that couldn't be phished.
>
> **Daniel Jacobson, Senior Director of IT, Datadog[16]**

OTP or SMS via text or call

More than five billion people around the world today own a mobile phone, which is why OTP via SMS has become a popular method for MFA.[18] However, SMS networks and phones can and have been exploited by private companies, governments, criminal gangs, and even sophisticated hackers as well. They are also vulnerable to number porting fraud and pretexting/vishing.

Push Notification-based Apps

Push notification-based apps offer context for the user so they can decide whether to login by touching an approve or deny button rather than revealing information by entering a code. However, phishing attackers can use bots with ISPs that are similar to the user's device. If the user does not carefully read the approval message, this may be enough to cause a security breach.

Push notification-based OTP codes

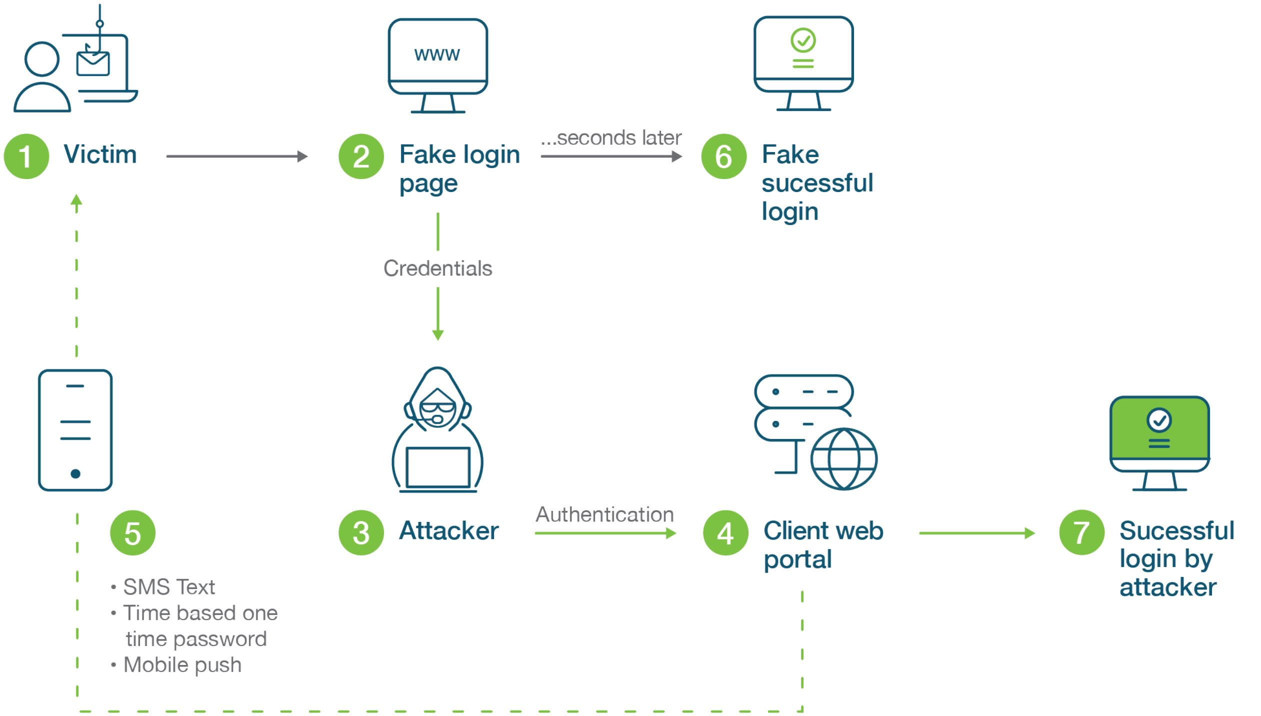
OTP via push notification is difficult for hackers to intercept when implemented correctly, but as with all OTP implementations, phishing may prompt the user to reveal the code.

OTP Apps

The OTP app embeds secret "seeds," typically in a hardware token or QR code. These seeds combine with the current time or a counter to produce a code that can only be predicted with the seed.

To validate the OTP codes, the secret seeds must be present on a highly secure server. A catastrophic breach of any seed manufacturer can obviously hurt customers. Also, OTP codes can be stolen by tricking users into visiting phony websites. Hackers can then forward the code to the real site and gain access.

How modern phishing beats mobile-based authentication



The diagram above shows an example of a successful phishing attack that is able to circumvent mobile-based two-factor authentication (2FA). In step 1, the attacker sends the victim a phishing email with a link that directs the victim to a fake login page that looks very similar to the real website. The victim enters their username and password which the attacker harvests and enters into the real website login screen in step 3. Because an OTP code is required for the second factor, the real website then sends out the OTP code to the victim in step 4, which the victim enters into the fake login page. In step 5 the attacker harvests the OTP code and enters it into the real website, gaining access to the account. The attacker usually also updates the account security settings to lock out the victim.

Best practices to protect against enterprise-wide identity phishing

Employee security training simply isn't enough to prevent phishing attacks. Once an attack has compromised an employee, partner, or vendor, it can quickly work its way through an organization — without anyone realizing it until significant damage has been done. By gathering just enough information, hackers can easily make themselves look like a trusted source, such as a colleague asking for a file, a vendor requesting an invoice payment, or a CEO requesting highly sensitive business financials. The enormous success of these attacks has cost companies across multiple industries more than $26 billion since 2018.[19]

Protecting enterprise resources requires a best-practice identity and access management strategy that prioritizes strong authentication. Although many enterprise organizations have moved toward authentication methods such as SMS and OTP, these approaches are vulnerable to threats such SIM swapping, malware, and MitM attacks. Relatively new threats, such as stealth SMS forwarding, may render OTPs more of a security risk in the near future.[20]

Aside from security and financial risks, mobile-based authenticators simply aren't feasible in many work environments that prohibit mobile devices, such as call centers, clean rooms, manufacturing floors, and research labs. So while any MFA is better than none, organizations need a more secure, scalable, and phishing-resistant way to reinforce identity access controls across the enterprise. It is important to remember that not all forms of MFA are created equal.

Outlined below are four ways enterprise organizations can protect against enterprise-wide identity phishing.

1 Deploy strong authentication as your first line of defense

By definition, strong authentication provides more than phishing-resistant security. It offers better usability, easy deployment, and rapid scalability, all of which are critical to easing the transition away from ubiquitous password-based authentication. Strong authentication must be highly intuitive to use and cost-effective to deploy in order to ensure consistent adoption across the entire workforce, and even across the supply chain.

Fortunately, many enterprise organizations have already started to replace risky password-based authentication with 2FA and MFA, which are relatively simple approaches that have become a common authentication method for consumer applications as well. There is also a movement towards eliminating passwords altogether as part of the authentication process due to the management overhead and risks they introduce.

However, the first step towards achieving passwordless security is to ensure that modern MFA practices are in place which inevitably involve a move away from legacy and vulnerable MFA approaches toward strong authentication that is phishing-resistant. As we've established mobile-based MFA can be hacked. Moreover it is not even an option in certain business scenarios such as where mobile devices are restricted altogether.

For this and other reasons, strong MFA should support multiple protocols that can not only meet today's immediate security requirements, but also enable the enterprise to be well-positioned to handle new threat vectors resulting from the growing sophistication of attacks. The modern MFA solution should also be easy to deploy to a diverse workforce across multiple regions, as well as to the company's larger ecosystem of partners, vendors, suppliers, and even end customers.

2 Implement a risk-based and step-up authentication approach

The fact is, every security strategy must be taken in phases, and there's no one-size-fits-all approach for every company or use case. To implement these phases, it's important to focus initial efforts on securing key phishing targets such as:

- **High-value applications:** These can include productivity applications like email, customer order and payment applications, and privileged applications like system administration. To secure these and other applications, it's important to identify and verify the users who access them, as well as where they may be coming from. For instance, user profiling and machine learning can help deliver more robust identity and access management (IAM) by applying behavioral and contextual algorithms to applications security. So, for instance, if an employee is trying to access a privileged accounting applications from an unusual device, network, or location, that anomaly can be flagged or escalated to verify the identity of the user.
- **High-value users:** Certain types of users, such as executives, domain admins, or other privileged employees may be subject to higher attack volumes due to their access to sensitive data. This type of user is also known as a Very Attacked Person (VAP) because they are highly valuable yet relatively easy targets to compromise.[21]
- **High-value resources:** Securing specific enterprise resources should also be part of a risk-based security approach. For instance, consider what types of authentication can work in mobile-restricted areas where SMS OTPs are prohibited. This is especially true in research labs or development areas where users must log into shared workstations and applications several times per day. By verifying the user's trusted identity, strong authentication can protect these resources from malicious actors and threats such as phishing and malware.

It's also important to manage the risk of insider threats, which can come from workers who simply practice poor security hygiene as well as those who willingly compromise company resources for revenge or financial gain, such as selling IP on the dark web. Preventing malicious threats from spreading across the company requires the ability to quickly identify and contain threats that result from anomalous behavior or unauthorized access attempts. Although machine learning and artificial intelligence offer some of the most robust analytical capabilities, simple MFA reporting can also provide helpful insight into potential authentication vulnerabilities.

3 Create a long-term MFA deployment strategy

The most important thing to remember about the journey to passwordless is to just get started. It's impossible to get there overnight, and the reality is that MFA initiatives are never truly complete. The threat landscape is continuously evolving, and so is the technology designed to combat it.

However, organizations can start with what they can reasonably do today. For instance, companies with a base of vendors and contractors can mandate strong authentication when accessing critical business apps. This can even include MFA using mobile OTP, which still provides a superior authentication method compared to just username and passwords. Other organizations may want to jump ahead and deploy hardware security keys across the workforce and supply chain. A partner can help plan this deployment by first starting with a test case of users, which can help ensure that the hardware security keys work across multiple devices, apps, and both modern and legacy systems. Eventually, these security keys can be deployed to VAPs, and then to the broader workforce.

For companies with hybrid or remote workers, or a geographically dispersed supply chain, it may be worth partnering with a hardware security key provider who can take care of the physical deployment. In other words, the provider can get the security keys into the hands of users wherever they are located — at home, in offices, and on job sites anywhere in the world. For many larger companies, this service can be a highly cost-effective way to accelerate the journey to passwordless by eliminating complicated delivery logistics.

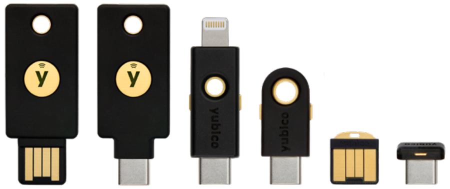
4 Get ready for FIDO2 and passwordless authentication

Implementing MFA is a great place to start. However, a standards-based solution, like authentication with FIDO2, provides even stronger protection against phishing.

For greater security and ease of use, FIDO2 specifications include WebAuthn, a web-based API that allows websites to update their login pages to add FIDO-based authentication on supported browsers and platforms. This enables users to leverage common devices to easily authenticate to online services in both mobile and desktop environments. WebAuthn functionality is essential to giving users an easier login experience using biometrics, mobile devices, and/or FIDO security keys. It provides a highly robust form of strong MFA that is far more secure than passwords.[22] With FIDO-based strong authentication, enterprises have a choice of deploying strong multi-factor authentication today and moving to a passwordless future tomorrow.

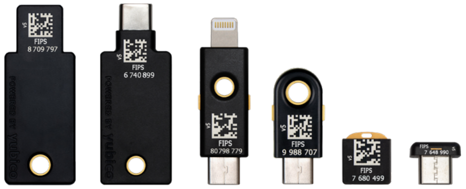
FIDO2 was introduced in 2018, and is the FIDO Alliance's newest set of specifications. It enables users to leverage common devices to easily authenticate to online services in both mobile and desktop environments. FIDO authentication mechanisms are not only phishing-resistant, they also provide robust protection against replay attacks, which occur when a cybercriminal eavesdrops and intercepts a secure network communication, such as an encrypted email message. The hacker is then able to delay or resend the message, which can mislead the receiver into performing what the hacker wants, such as depositing money into a fraudulent bank account.

Modern strong authentication with the YubiKey



The YubiKey 5 Series
From left to right: YubiKey 5 NFC, YubiKey 5C NFC, YubiKey 5Ci, YubiKey 5C, YubiKey 5 Nano and YubiKey 5C Nano.

YubiKey Bio Series - FIDO Edition
From left to right: YubiKey Bio FIDO Edition, YubiKey C Bio FIDO Edition



The YubiKey 5 FIPS Series
From left to right: YubiKey 5 NFC FIPS, YubiKey 5C NFC FIPS, YubiKey 5Ci FIPS, YubiKey 5C FIPS, YubiKey 5 Nano FIPS and YubiKey 5C Nano FIPS.

Yubico's phishing-resistant hardware security solution–the YubiKey–supports a "Trust nothing, verify everything" Zero-Trust security approach with strong user identity and device authentication. YubiKeys are purpose-built for security and designed to stop phishing and other forms of account takeover in their tracks, delivering strong authentication at great scale. Unlike mobile authenticators, they require no network connection, store no data, and don't require any client software to be installed.

The YubiKey:

- Offers strong hardware-backed authentication with one simple tap or touch, that is resistant to phishing attacks and account takeovers
- Works with hundreds of applications and services including leading identity access management solutions such as Microsoft, Okta, Ping, and Duo
- Supports multiple protocols on a single key enabling strong authentication for both legacy and modern applications, and delivering high ROI
- Is FIPS 140-2 validated (Overall Level 1 Certificate #3907 and Level 2 Certificate #3914, Physical Security Level 3) to meet the highest authentication assurance level 3 requirements (AAL3) of NIST SP800-63B guidelines
- Is available in multiple form factors for use across desktops, laptops, mobile devices and tablets

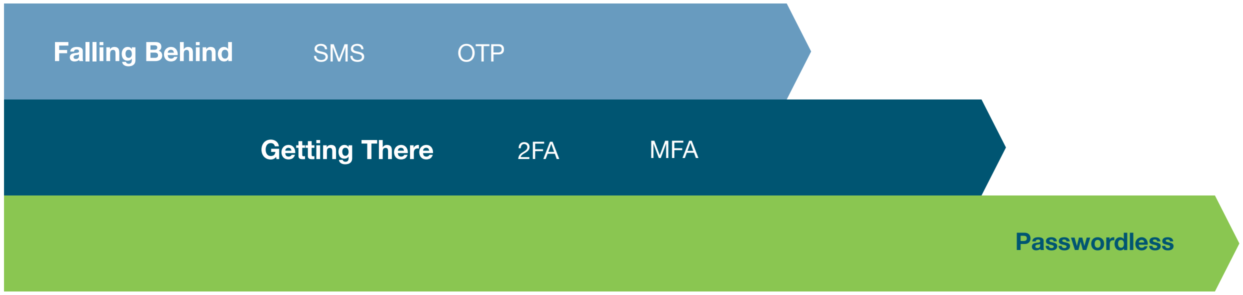
By supporting multiple authentication protocols on a single YubiKey, such as OTP, OpenPGP, and strong authentication protocols such as Smart Card, FIDO U2F, and FIDO2/WebAuthn, the YubiKey offers organizations the flexibility to deploy strong authentication across a variety of legacy and modern infrastructures. With YubiEnterprise Delivery, YubiKeys can be shipped directly to users, making it easy to secure hybrid and remote workers.

YubiKey offers a bridge to passwordless

Passwordless is a journey, not an overnight transition. With the YubiKey, organizations can implement FIDO2 passwordless, smart card password-less, or a hybrid strategy, depending on the existing infrastructure and use cases that need to be addressed. Because the YubiKey supports the broadest set of security protocols, a single security key can work across a wide range of modern and legacy applications and services, so organizations can gradually move to passwordless without disrupting business operations or user productivity.

Stop phishing attacks and start the journey to passwordless

> “An additional comfort comes from knowing that YubiKeys make email phishing expeditions much more difficult by successfully thwarting phishing and man-in-the-middle attacks.
>
> **Kane Narraway, Corporate Security Manager, Atlassian**[23]



It seems like passwords have been part of daily life forever, but because user experience and security needs have changed, passwords need to be eliminated completely to stop successful phishing attacks. For organizations just starting on the journey to passwordless, it’s important to begin by securing highly targeted, high-value users such as privileged admin accounts and remote workers. Protecting these users can have the biggest impact in the short term, and will provide some time to continue planning the long-term security roadmap.

The most important thing is to simply start now, because remote workforces that popped up overnight will be around for years to come. To protect all enterprise employees (and company resources) from successful phishing attacks, organizations must move past vulnerable authentication methods and become a fully passwordless enterprise.

The YubiKey was designed to support the evolutionary path toward passwordless with modern strong authentication. To learn more, please visit www.yubico.com.

Sources

[1] https://apwg.org/trendsreports/

[2] The 2021 Cost of Phishing Study, Ponemon Institute

[3] https://www.proofpoint.com/us/resources/threat-reports/state-of-phish

[4] https://www.proofpoint.com/us/resources/threat-reports/state-of-phish

[5] https://www.verizon.com/business/en-gb/resources/reports/dbir/

[6] https://www.ibm.com/security/data-breach

[7] https://terranovasecurity.com/2020-gpt-report/?utm_campaign=En_GPTReport2020&utm_medium=Google&utm_source=Ads&utm_content=NewAd3&gclid=CjwKCAjw6fCCBhBNEiwAem5SO8olgjFVtVzMA5pg-uSkRAho6S356pspA4bY3FBFk9FXCKW0Ksq-ExoCsHEQAvD_BwE

[8] https://www.yubico.com/resources/glossary/spear-phishing/

[9] https://www.helpnetsecurity.com/2021/06/14/phishing-levels-2021/

[10] https://www.agari.com/email-security-blog/ancient-tortoise-bec-attack-chain/

[11] https://expertinsights.com/insights/phishing-vishing-smishing-whaling-and-pharming-how-to-stop-social-engineering-attacks/

[12] https://www.yubico.com/resources/reference-customers/city-of-mission-viejo/

[13] https://www.ftc.gov/coronavirus/scams-consumer-advice

[14] https://www.reuters.com/article/us-health-coronavirus-technology/permanently-remote-workers-seen-doubling-in-2021-due-to-pandemic-productivity-survey-idUSKBN2772P0

[15] https://www.verizon.com/business/en-gb/resources/reports/dbir/

[16] https://www.yubico.com/resources/reference-customers/datadog-leads-in-authentication-best-practices-deploys-yubikeys-to-all-employees-enterprise-wide/

[17] https://www.reddit.com/r/announcements/comments/93qnm5/we_had_a_security_incident_heres_what_you_need_to/

[18] https://datareportal.com/global-digital-overview

[19] https://www.sans.org/webcasts/dont-bait-steps-avoid-phishing-attacks-120005/

[20] https://www.vice.com/en/article/y3g8wb/hacker-got-my-texts-16-dollars-sakari-netnumber

[21] https://www.brighttalk.com/webcast/15793/479907

[22] https://fidoalliance.org/fido2/fido2-web-authentication-webauthn/

[23] https://www.yubico.com/resources/reference-customers/atlassian/

yubico

About Yubico

Yubico sets new global standards for simple and secure access to computers, mobile devices, servers, and internet accounts.

The company's core invention, the YubiKey, delivers strong hardware protection, with a simple touch, across any number of IT systems and online services. The YubiHSM, Yubico's ultra-portable hardware security module, protects sensitive data stored in servers.

Yubico is a leading contributor to the FIDO2, WebAuthn, and FIDO Universal 2nd Factor open authentication standards, and the company's technology is deployed and loved by 9 of the top 10 internet brands and by millions of users in 160 countries.

Founded in 2007, Yubico is privately held, with offices in Sweden, UK, Germany, USA, Australia, and Singapore. For more information: www.yubico.com.