



BEST PRACTICES GUIDE

How to get started with phishing-resistant MFA to secure retail and hospitality

Six deployment best practices to accelerate adoption at scale



68%



of breaches involve the use of stolen credentials.²

90%



of hospitality IT professionals cite phishing as a top concern.³

Choosing the right MFA approach for retail and hospitality

With increasing cyber threats and tightening regulatory and cyber insurance requirements, the retail and hospitality sector faces mounting pressure to strengthen authentication. The presence of payment card data makes these industries a lucrative target, with 25% of retail and 19% of accommodation and food service breaches involving payment data, including a heavy proportion of attacks focusing on eCommerce and POS terminals.¹ Across all industries, the use of stolen credentials is now the most popular entry point for breaches which amplifies how attractive and useful credentials are to malicious threat actors.² In retail and hospitality, these risks are exacerbated by shared devices or kiosks and a high prevalence of password sharing.

Beyond the need to strengthen authentication, retail and hospitality organizations are also driven by the need to reduce the friction in the authentication experience. Passwords and mobile-based authentication and the overuse of shared logins can negatively impact customer service delivery. With highly distributed locations and a workforce subject to high turnover or seasonal fluctuations, organizations are also looking for a secure multi-factor authentication (MFA) solution that is frictionless to deploy and manage. Further, customer-facing technology must be supported by efficient, unobtrusive authentication to allow front-desk staff and sales associates to provide a high level of attention.

Today, the regulatory bodies and cyber insurers are beginning to acknowledge the importance of MFA, but also that **not all forms of MFA are created equal**. Most basic authentication methods, including SMS, mobile authentication and one-time passcodes, are susceptible to phishing, social engineering and attacker-in-the-middle attacks, leading to account takeovers.

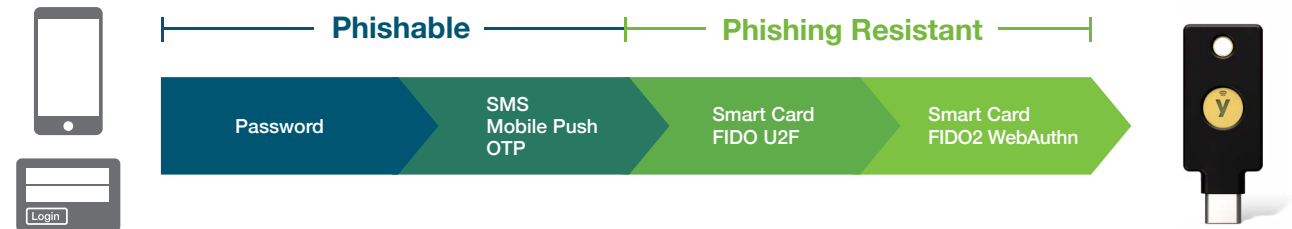
Acknowledging this, standards are being revised to require individual log-ins protected by phishing-resistant MFA, including evolving FTC standards,⁴ the Payment Card Industry Data Security Standard (PCI DSS v4.0)⁵ and the requirement for strong authentication under the EU Payment Services Directive 2 (PSD2).⁶ In particular, Requirements 8 and 12 of PCI DSS v4.0 specifically call out the need for an information security policy and programs, including user training and technical control oversight.



Based on the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63-B4, two forms of authentication currently meet the mark for phishing-resistant MFA: PIV/smart card and the modern FIDO2/WebAuthn authentication standard.

What is phishing-resistant MFA?

Phishing-resistant multi-factor authentication (MFA) refers to an authentication process that is immune to attackers intercepting or even tricking users into revealing access information. It requires each party to provide evidence of their identity, but also to communicate their intention to initiate through deliberate action.



YubiKey offers phishing-resistant MFA

Yubico created the **YubiKey**, a hardware security key that supports **phishing-resistant two-factor, MFA and passwordless authentication at scale with an optimized user experience.**

The YubiKey is a multi-protocol security key, supporting both PIV/smart card and FIDO2/WebAuthn standards along with OTP, which integrates seamlessly into both legacy and modern environments, helping organizations bridge to a passwordless future. YubiKeys work with hundreds of products, services and applications including leading identity and access management (IAM) platforms, privileged access management (PAM) solutions and cloud services. With flexible 'YubiKey as a Service' offerings, the YubiKey is a cost-effective solution to support shared workstation and kiosk environments subject to high turnover and seasonal staff, along with being highly durable to support the fast-paced and agile workforce.

Modern hardware security keys such as the YubiKey are an ideal option for strong phishing-resistant MFA because they don't require external power or batteries, or a network connection—a user can use a single key for secure access to hundreds of applications and services with the secrets never shared between services. The YubiKey cultivates phishing-resistant users which then creates phishing-resistant enterprises. Many authentication solutions are exposed to vulnerabilities via remote attacks due to the compromises necessary to integrate them on a mobile device, such as a smartphone or tablet. The purpose-built hardware, including the touch sensor, on the YubiKey verifies that the person logging in is a real physical human, and not a trojan or remote hacker.

What are passkeys?

Passkeys are a new term in the industry, but the concept is not new. Passkeys are a new name for FIDO2 passwordless-enabled credentials, a standard that is replacing passwords and phishable MFA logins with more secure passwordless experiences. There are different passkey implementations:

Synced passkeys live in the cloud, which means credentials on a smartphone, tablet or laptop can be shared between devices. While synced passkeys enable easier credential recovery in the case of a lost or stolen phone or laptop, the FIDO credential is harder to track, so it is suitable for lower security assurance scenarios.

Device-bound passkeys offer enterprises greater control of their FIDO credentials compared to synced passkeys. However, there are different types of device-bound passkeys—those that reside in general purpose devices such as smartphones, laptops and tablets, and those that reside in hardware security keys purpose built for strong security. Device-bound passkeys in modern FIDO security keys offer the highest security assurance and provide enterprises with trusted credential lifecycle management and attestation abilities. With this passkey approach enterprises can deliver the simplest user onboarding and credential recovery experience across devices and platforms, all while staying in compliance with the most stringent requirements across industries.



More Value

Reduce support tickets by 75%



High return

Experience ROI of 203%



Strongest Security

Reduce risk by 99.9%



Faster

Decrease time to authenticate by >4x



Durable

IP68 certified, dust-proof, crush-resistant and water-resistant

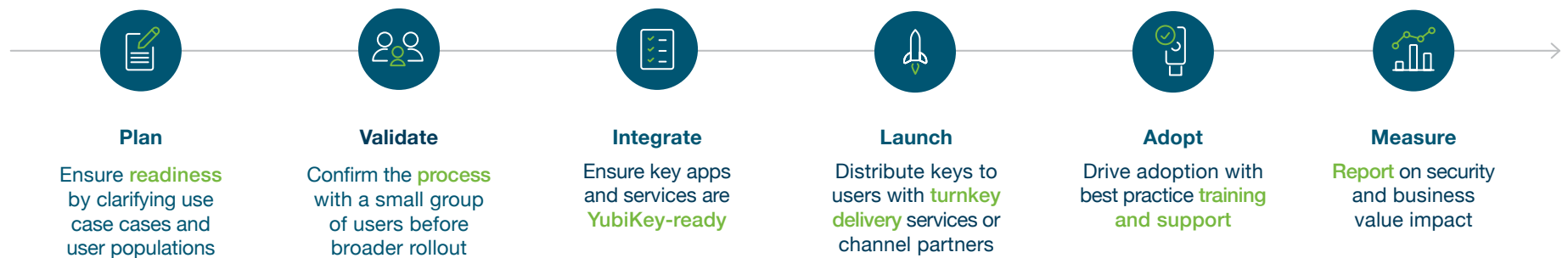
Given the threat landscape, the need for modern phishing-resistant MFA gets clearer on a daily basis. **But how do you start the journey?** The remainder of this guide will detail six key best practices for a successful MFA and YubiKey deployment.



Six key best practices to accelerate the adoption of phishing-resistant MFA

Getting started is easy. Based on Yubico's experience assisting hundreds of customers to deploy phishing-resistant MFA, we have created a six step deployment

process to plan for and accelerate the frictionless adoption of phishing-resistant MFA at scale as well as corporate secrets and OT environments.



01. Plan

Clarify use cases and ensure readiness

A **phased approach** is the best way to ensure a frictionless deployment. Put your **high value users and data first**, then expand. Rank use cases and user populations based on risk, workforce location, business impact and ease of technical integration.

Determine use cases

Top scenarios for modern, phishing-resistant MFA



Privileged access

Protect sensitive data and targeted employees who have elevated access to systems or data.



Shared devices

Enable secure and efficient access to shared devices (e.g. shared workstations or kiosks, POS terminals, RFID scanners).



Remote work

Add an extra layer of protection, providing secure access to VPN, IAP, IAM, & IdP platforms.



Software supply chain

Protect code access and implement trusted code-signing.



Customer-facing locations

Mix of users, and shared devices that tie into the brand's corporate environment.



Cruise ships

Specialized requirements to support a fully independent IT infrastructure.

User groups



Office and hybrid workers

Sophisticated attacks and lateral escalations make every user a privileged user. Improve security and productivity for office workers.



Call center

Verify call center agent identity to provide access to key systems and shared workstations, in mobile-restricted environments.



Customer-facing workers

Use shared devices that tie into the brand's corporate environment (e.g. retail stores, hospitality locations, cruise ships).



Third Party

Protect third-party or franchisee access to systems and data.



End customers

Protect customer accounts from fraud and build loyalty and trust with deployments to key customer segments.

“ We are taking great strides in protecting the safety of our guests and colleagues by requiring phishing-resistant MFA methods for all applications that can expose both PII and Card Holder data. We also believe that having Guest Services colleagues looking down at their phone to complete an MFA response or approval does not portray the message we want, to someone walking past the front desk. It lends itself to the perception the colleague is engaged in their cell phone for social media or other personal activity. Using a YubiKey not only provides a more seamless experience for the colleague while keeping our data safe, but also allows those colleagues to keep their cell phones stored away while performing guest-facing roles.”

Art Chernobrov | Director | Identity, Access, and Endpoints | Hyatt Hotels Corporation

Assemble key stakeholders

While the number of resources on the project can vary based on the size and breadth of the YubiKey deployment, key stakeholders within the following departments can





positively influence the implementation of phishing-resistant MFA across the organization. It's important to have buy-in across all teams to ensure a smooth rollout:



Engage Yubico experts as needed

With a tried and true process that hundreds of organizations have followed already, and with a ‘YubiKey as a Service’ model, Yubico offers flexible and cost-effective solutions to heighten solutions and

streamline authentication. No matter where you are on your MFA journey, we’ll meet you there, offering best-in-class technical and operational guidance in support of your YubiKey implementation and rollout.

YubiEnterprise Services*		Yubico Professional Services	
 YubiKey as a Service	 YubiEnterprise Delivery	 Deployment 360	 Deployment planning
Simplifies how businesses procure, upgrade and support YubiKeys	Global turnkey YubiKey distribution through YubiEnterprise Delivery or local channel partners	Turnkey planning, technical integration and deployment support	Jump start with workshops and projects to review use cases or develop a customized strategy

* YubiEnterprise Services are available for organizations of 500 or more users.



Works with YubiKey

YubiKeys, the industry's #1 security keys, work with hundreds of products, services, and applications. To browse YubiKey compatibility go to yubi.co/wwwyk.



02. Validate

Confirm the process with a small group of users

Validate with a small group of users across a priority use case for confirmation and feedback, leveraging Yubico best practice resource guides, videos and engagements. **Practice, learn and then move forward with expansion.**



03. Integrate

Ensure your environment is YubiKey-ready

YubiKeys can work with over 1,000 applications and services and secure your users' work and personal digital lives with no shared secrets between the services, enabling high security and privacy at scale. To ensure that YubiKeys are integrated seamlessly with

key applications and services you wish to secure, below are some critical questions to think about. It's considered a best practice to first answer these questions for your pilot program, then circle around for each expanded deployment.



Who

Who needs access?

Employees, contractors, third parties, supply chain



What

What authentication approach will you take?

MFA (password and strong second factor), passwordless



Where

Where in your environment do you require strong authentication?

Corporate systems and E-comm hardware/servers, shared workstations and POS terminals, network, apps, and dev tools

How do you manage access?

IAM, IdP, PAM, SSO, VPN



How

How does location impact deployment?

Remote, hybrid, on-premise, multi-location

What types of devices need to be supported?

Owned, BYOD, desktop, laptop, smartphone, tablet, POS terminals, inventory scanners

Prepare to deploy

After ensuring that your environment is YubiKey ready, it's time to create a plan to deploy YubiKeys across your organization. Optimizing deployment involves

organizational change management through effective communication, training and support. Yubico offers a variety of Professional Services to help you deploy quickly:

Yubico Professional Services



Deployment planning

Rollout plan development and ongoing assistance



Integration services

Architecture and infrastructure review, vendor integration analysis



Implementation projects

Technical engagements to implement YubiKeys in your environment



Service bundles

Flexible consulting hours for when & how you need them



What?

Increase awareness

Build up **user training and support** materials



Why?

Boost engagement

Demonstrate value to the **organization** and the **user**



04. Launch

Get keys in hands and plan Go Live events

We want your deployment to be as frictionless as possible for all teams and all users. This includes simplifying deployment plans, helping you answer

critical questions about how you will distribute keys to users and how you will manage the YubiKey lifecycle.



Distribution

Self-service | Channel Partner | YubiEnterprise Delivery



Key management

Onboarding | Support | Offboarding

YubiKey rollout best practice recommendations

Once your users have their YubiKeys, the next step involves registering the keys with the applications and devices they will use. We recommend that each user has a second YubiKey as a backup, and if users cannot locate a YubiKey, revoking and replacing keys

is the recommended next step. If a user leaves the organization, some organizations retrieve YubiKeys prior to their departure while others prefer to allow departing users to keep their YubiKeys and continue using it for their own personal accounts.



Offer **flexibility and choice** since YubiKeys are available in a variety of form factors



Two YubiKeys per person for backup



Future-proof with **extra keys** to cover for churn or lost/stolen keys



Encourage **security** with personal use policies



Plan an event to make the future of your organization's security exciting

Why users love the YubiKey



Faster



Easier



More Secure

Go Live events

Support the launch with a series of kick-off communications that introduce the YubiKey to users—communicate early, often. The ideal Go Live communications make users **excited** about the modern features of the YubiKey.





How to?

Educate users

Have clear calls to action on how to **get started** & how to **get help**



Instead of YubiKey being a highly recommended solution for our clients, we're moving towards making them a required solution. We are building it into our hosting suite, and into our user fees."

Dustin Morse | Business Operations Manager | Retail Control Systems



05. Adopt

Support adoption and boost engagement

At Yubico, we believe success should not be measured by how many YubiKeys you have, but by **how many keys are being used**.

While the Go Live communications educate users on the 'what YubiKeys are' and the 'why they are important', support teams need to be prepared to explain the **how**, with FAQs available to help with any questions that may

arise for onboarding and troubleshooting (e.g. what to do in case of a lost key).

Effective education and awareness is important during this phase in order to showcase to your user community why the company invested in the YubiKey, and the direct benefits to users. The YubiKey's simple user experience requires minimal training and on-going support for users.



06. Measure

Report on security and business impact

We know **the truth is in the numbers**. Validate the pilot against these metrics, then expand to other users to increase the overall business impact.

Deployment metrics:

Number of keys distributed, users activated, applications enabled

Performance metrics:

Support time reductions related to password resets, productivity increases related to login times

Security metrics:


Security threats mitigated, simplified compliance or audit reporting

User metrics:

Ease of onboarding, ease of use, satisfaction

Ready for scale

Yubico offers expert consulting services, including operational and technical workshops, implementation projects, on-demand resources and custom engagements, designed to jump-start and accelerate your YubiKey deployment at scale.



Professional Services

Expert consulting services, including operational and technical workshops, implementation projects on-demand resources and custom engagements, designed to jump-start and accelerate your YubiKey deployment.

Yubico is leading the charge toward a more secure and frictionless authentication future. Our team of experts provides technical and operational guidance to help streamline your YubiKey implementation and rollout.


Services Offered

Deployment 360 Program
A turnkey program packaging all of the essential elements and expertise to ensure your successful YubiKey deployment

Workshops
Interactive sessions designed to help jump-start YubiKey integrations and deployments

Technical Implementation Projects
Tailored projects designed to facilitate your YubiKey

To download the Professional Services Solution Brief go to yubi.co/ps



YubiEnterprise Services*		Yubico Professional Services		
YubiKey as a Service	YubiEnterprise Delivery	Launch planning	Training and support	Analytics and reporting
Cost effective and flexible YubiKey procurement	Global turnkey YubiKey distribution through YubiEnterprise Delivery or local channel partners	Create a marketing and communication plan tailored to your users	Best practice training and support materials and processes	Customized metrics and dashboard design

* YubiEnterprise Services are available for organizations of 500 or more users.



YubiKey as a Service

Gain leading, phishing-resistant authentication security for less than the price of a cup of coffee per user, per month. YubiKeys as a service, via subscription, delivers peace of mind in an uncertain world.

Learn more yubi.co/YKSvc



YubiEnterprise Delivery

Yubico and trusted partners provide IT teams with powerful capabilities to manage delivery of hardware security keys to users globally and accelerate the adoption of strong authentication.

Learn more yubi.co/delivery



Ready to get started?

There is no question that phishing-resistant MFA is the solution to secure retail and hospitality organizations against modern cyber threats and to streamline critical authentication experiences. Though the path to phishing-resistant MFA and passwordless can seem daunting, it doesn't have to be.

YubiEnterprise Services*



YubiKey as a Service



YubiEnterprise Delivery

Yubico Professional Services



Deployment 360

Service hour bundles



Workshops

Implementation projects

* YubiEnterprise Services are available for organizations of 500 or more users.



Don't know where to start? The good news is that you don't need to know all the answers upfront about how many keys to buy, what kind, how to integrate them into your environments, preconfiguration options or how to get keys in the hands of end users. No matter where you are on your MFA journey, we'll meet you there.

Modern enterprises recognize that security as a service can take all the guesswork out of achieving success. When you choose YubiKeys as a service, you make decisions as you go with our insight and help, simplifying the process of scaling YubiKeys to wider circles of users as your business needs grow. We include success guides and priority support to help you be successful as quickly as possible.

If you want a closer partnership on any of the six steps of this plan, [Yubico's Professional Services](#) team is here to help.



Contact us
yubi.co/contact



Learn more
yubi.co/ps

Sources

¹ Verizon, [2024 Data Breach Investigations Report](#), (Accessed May 28, 2024)

² Verizon, [2024 Data Breach Investigations Report](#), (Accessed May 28, 2024)

³ HospitalityTech, [Ninety Percent of Hospitality IT Professionals Cite Email Phishing Attacks as a Top Concern](#), (November 2021)

⁴ James Dempsey, [The FTC's rapidly evolving standards for MFA](#), (November 8, 2022)

⁵ PCI SSC, [PCI DSS v4.0](#), (March 2022)

⁶ European Central Bank, [The revised Payment Services Directive \(PSD2\)](#), (March 2018)

⁷ Forrester, [The Total Economic Impact of Yubico YubiKeys](#), (September 2022)



About Yubico

Yubico (Nasdaq First North Growth Market Stockholm: YUBICO) is the inventor of the YubiKey, a hardware security key that is the gold standard in phishing-resistant multi-factor authentication (MFA). Yubico's solutions offer organizations and users deployment expertise and operational flexibility as YubiKeys work across hundreds of consumer and enterprise applications and services.

Yubico is a creator and core contributor to the FIDO2/passkey, WebAuthn, and FIDO Universal 2nd Factor (U2F) open authentication standards, and is a pioneer in delivering modern, hardware-based passkey authentication security at scale to customers in over 160 countries.

For more information, please visit: www.yubico.com.