



WHITE PAPER

# The dark side of your mobile authentication strategy

Why you need to break up with legacy MFA and adopt modern, phishing-resistant MFA at scale



# Contents

<b>Not all MFA is created equal</b>	<b>3</b>
<b>Common forms of mobile authentication</b>	<b>4</b>
<b>Five common misconceptions related to mobile authentication</b>	<b>5</b>
Mobile authentication is phishing-resistant	6
Mobile authentication is cost-effective	10
Mobile authentication is user-friendly	11
Mobile authentication offers 360° coverage	12
Mobile authentication is future-proofed	13
<b>Yubikey offers simple, phishing-resistant MFA</b>	<b>14</b>
<b>Getting started is easy</b>	<b>16</b>

10-24%



attack penetration rate for mobile authentication<sup>10</sup>

82%



breaches tied to the **human element** social attacks, errors, misuse or credential theft<sup>11</sup>

\$1 million



per year cost for **password resets** alone<sup>12</sup>

92%



organizations were victims of **phishing**<sup>13</sup>

## Not all MFA is created equal

Despite the growing tide and sophistication of cyber attacks, organizations continue to rely on **legacy authentication** methods such as usernames and passwords and mobile-based authenticators to secure access to critical and sensitive applications and data. A recent Google Cloud report indicates that 50% of compromises of enterprise cloud environments in Q4 2022 could be attributed to weak passwords.<sup>1</sup>

Organizations face mounting pressure from regulators and cyber insurers to strengthen cybersecurity defenses with multi-factor authentication (MFA), adding one or more additional pieces of evidence to the authentication process. However, while any form of MFA will offer better security than password-based authentication alone, the truth is that **not all MFA is created equal**.

Legacy mobile-based MFA such as SMS, one-time passcodes (OTP) and push notification apps are highly susceptible to account takeovers from phishing, social engineering and man-in-the-middle (MiTM) attacks. And yet, up to 53% of organizations choose mobile-based authentication as their MFA form factor.<sup>2</sup> Why is that? Because most organizations remain **unaware of the security risks with mobile authentication**.

Today a data breach costs an average of \$9.44M in the US and \$4.35M globally<sup>3</sup>, but cyber attacks can also erode trust, disable critical infrastructure, disrupt core operations, increase cyber insurance premiums and result in the loss of intellectual property. Successful cyber attacks are the reason why regulators now specifically mandate **phishing-resistant MFA**, including the White House Executive Order 14028<sup>4</sup>, Office of Management and Budget (OMB) Memo 22-09<sup>5</sup> and the National Security Memorandum/NSM-8<sup>6</sup> in the US, NIS2<sup>7</sup> for the EU and the global PCI DSS v4.0 standard<sup>8</sup>. And yet across the industry, confusion still exists about what forms of MFA are truly secure or phishing-resistant.

The dark truth is that **no form of mobile authentication is phishing-resistant**. Further, your MFA strategy ROI can vary widely in terms of **cost, user experience, coverage** and even the ability to bridge to a **passwordless** future, depending on what MFA approach you choose.

In this whitepaper, we'll reveal the **top five mobile authentication misconceptions** to help you re-evaluate your long-term MFA strategy and to consider the shift to modern MFA. In fact, we'll demonstrate that **legacy mobile-based MFA is broken**, and how you can achieve modern, phishing-resistant MFA with an estimated **ROI as high as 203%**.<sup>9</sup>



“ Legacy mobile authentication solutions create **security** gaps and usability concerns when deployed at **scale**.

# Common forms of mobile authentication

The most common forms of mobile authentication rely on the **human element**—the manual entry of an output (code) or the approval of a sign-in request. The human element of authentication can have a direct impact on security risk, user productivity and support costs if the solution doesn't offer an optimal user experience. In fact, **82% of data breaches can be tied to the human element**—social attacks, credential theft, misuse or errors.<sup>14</sup>

## One-time passwords or passcodes (OTP)



Code valid for one transaction



Sent via text, email, voice or app



Code input by user

## Time-based one-time password (TOTP)



Code generated using HMAC, changing every few seconds or minutes shared secret, timestamp



Sent via text, email, voice or app



Code input by user

## Push authentication



An authentication attempt sends an alert to the user's mobile device



Sent via text or in-app



User approves or denies the access

## Authenticator app



Authenticator app installed on a mobile device



App generates TOTP-based code



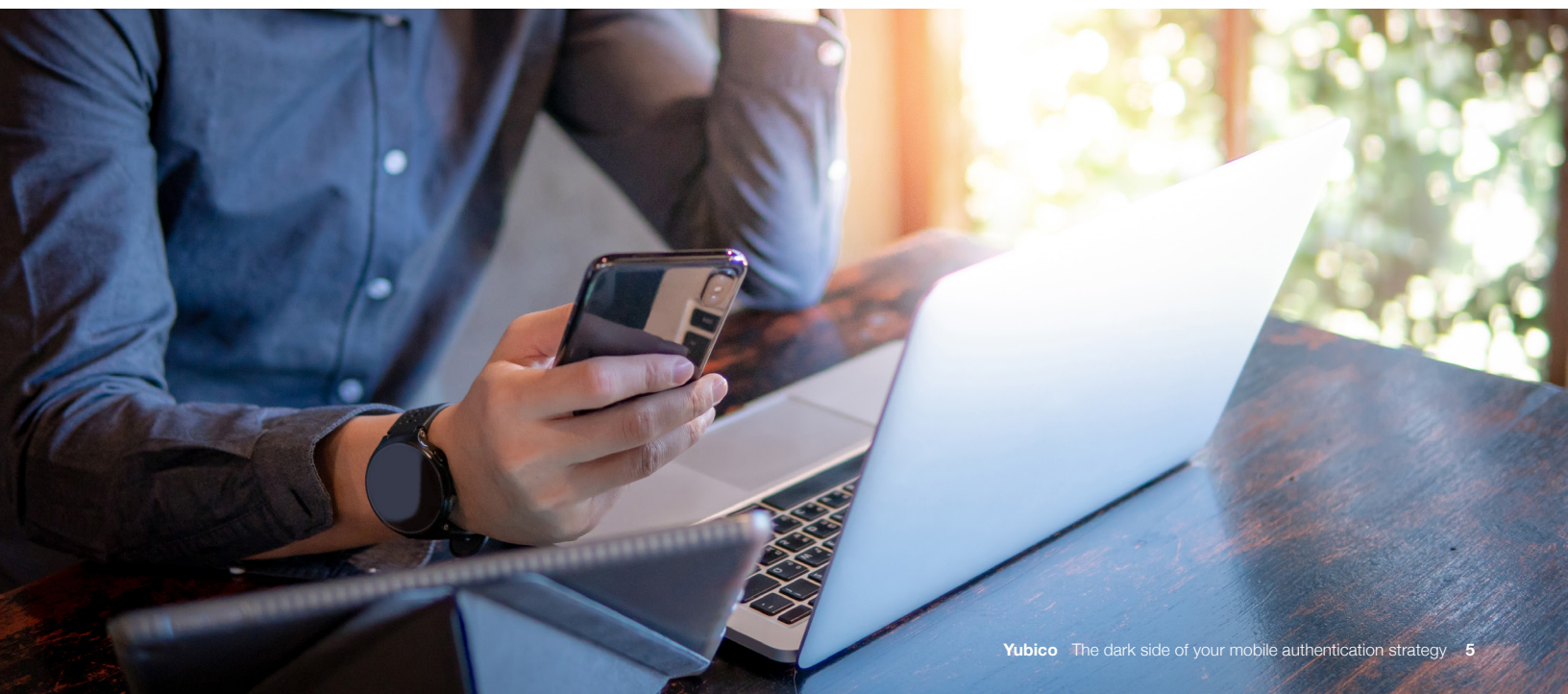
Code input by user



# Five common misconceptions related to mobile authentication

Below are the top five mobile authentication misconceptions that put organizations at risk of account takeovers and increased OpEx and CapEx costs, if not addressed:

MYTH		FACT
Mobile authentication is phishing-resistant	→	Every form of mobile authentication can be hacked
Mobile authentication is cost-effective	→	It's more expensive than you think
Mobile authentication is user-friendly	→	Mobile authentication is complex to use and manage
Mobile authentication offers 360° coverage	→	Mobile authentication creates MFA security gaps
Mobile authentication is future-proof	→	Mobile authentication does not support emerging regulations or passwordless



“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. YubiKeys made the most sense.”

Daniel Jacobson  
Senior Director of IT,  
Datadog

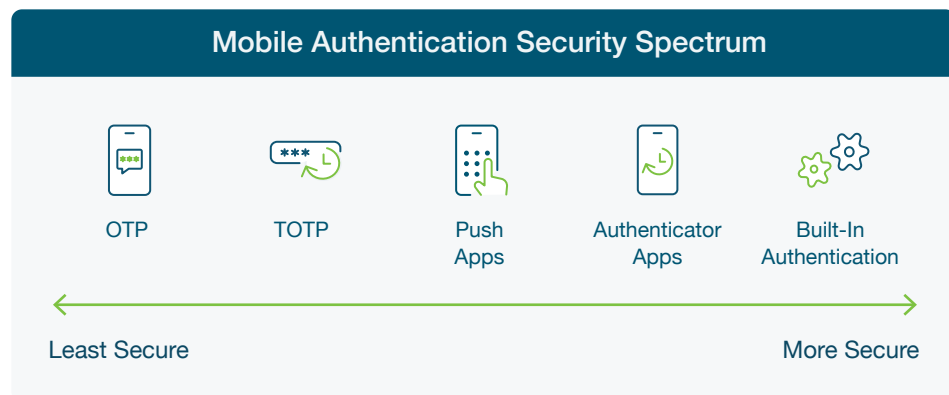
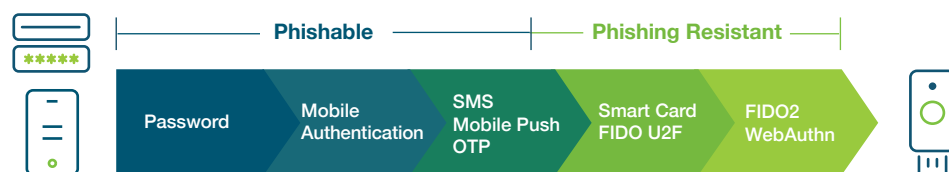
## Misconception #1: Mobile authentication is phishing-resistant

### Reality: Every form of mobile authentication can be hacked

Security is the top driver for MFA deployments, but while some forms of mobile authentication are more secure than others, **no form of mobile authentication is phishing-resistant.**

Phishing-resistant MFA processes rely on cryptographic verification between devices or between the device and a domain, making them immune to attempts to compromise or subvert the authentication process (e.g. phishing, brute force attacks).

According to the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63, **currently only two forms of authentication meet the mark for phishing-resistant MFA:** PIV/smart card and FIDO2/WebAuthn.



Today’s cyber threats are increasingly targeting legacy MFA including passwords and mobile authenticators that are vulnerable to modern cyber threats. In 2022, a social engineering attack on messaging service Twilio led to the compromise of the Twilio platform and its customers, undermining the security of the OTP services provided during that time<sup>15</sup>. In 2022 and 2023, phishing attacks and stolen credentials were used to access sensitive systems (e.g. Uber<sup>16</sup>) or data (e.g. American Airlines<sup>17</sup>) or via third party credentials (e.g. AT&T<sup>18</sup>, Chick-fil-A<sup>19</sup>).

MFA is critical, but not all MFA methods are created equal. Twitter used application-based MFA, which sent a request for authentication to an employee's smart phone. This is a common form of MFA, but it can be circumvented. During the Twitter Hack, the Hackers got past MFA by convincing the Twitter employees to authenticate the application-based MFA during the login. The most secure form of MFA is a physical security key, or hardware MFA, involving a USB key that is plugged into a computer to authenticate users. This type of hardware MFA would have stopped the Hackers, and Twitter is now implementing it in place of application-based MFA.

New York Depart of Financial  
Services  
Twitter Investigation Report  
October 2020

**When authentication is based upon knowledge or people, this is a recipe for risk.** People make mistakes—they can be fooled to approve authorization requests, supply OTP codes or install software. No amount of security training can eliminate the risks of modern phishing attacks against mobile authentication—the mobile device itself raises several red flags:



#### 1. Tampering

No guarantee that the private key ends up on a secure element on the mobile device



#### 2. Interception

The OTP code or private key could be intercepted



#### 3. Impersonation

No way to ensure proof of possession

In 2020, a small group of teenagers targeted Twitter employees with a spear phishing attack to obtain access to employee credentials and authenticator app codes, then accessed the internal network to seize high-profile cryptocurrency accounts and scam the public of over \$118,000 in bitcoin<sup>20</sup>. In another instance, a white-hat hacker demonstrated that just \$16 and a few seconds was all it took to completely and invisibly take over social media accounts that had been protected by OTP-based MFA<sup>21</sup>.

A Google, NYU, and UCSD analysis of 350,000 real-world hijacking attempts revealed that a SMS-based OTP only blocked 76% of targeted attacks and a mobile push app only blocked 90% of targeted attacks<sup>22</sup>. In other words, **mobile authentication experiences a 10-24% attack penetration rate**. In fact, the risk of SMS interception is so high that NIST called for SMS to be deprecated as a method of authentication<sup>23</sup>.

**If this is news to you, you're not alone.** Only 22% of respondents Yubico surveyed are aware that security could be a problem with SMS-based authentication<sup>24</sup>. While OTP authenticators are the least secure form of mobile authentication, they remain the top deployed authenticator across 58% of organizations<sup>25</sup>.



# Every mobile authenticator can be hacked

Account takeovers occur when a hacker successfully gains access to a user's credentials via:

## Phishing



A form of social engineering where attackers trick users into giving up sensitive information or installing malware.

## Man-in-the-middle (MiTM) attack



Attackers intercept credentials via a proxy server, secretly relaying and possibly altering communications between two parties.

## Malware



Software-based attack designed with malicious intent to gain access to a network or to cause damage to data and systems.

## OAuth phishing



Hackers use malicious third-party applications as a means for access. When users grant third-party access to an account, the hacker is able to gain access using an OAuth token instead of a password.

## MFA or push fatigue



Social engineering attack that repeatedly pushes 2FA requests to coerce users to confirm impersonator identity and grant access to accounts. Users accept out of habit, by accident, or to stop notifications.

## SIM swapping



Targets a weakness in some forms of 2FA in which a call or text message is sent to a mobile phone, exploiting the ability of subscriber identity module (SIM) cards to be ported by mobile service providers from device to device bearing different telephone numbers.

## Credential stuffing



Stolen credentials used to gain unauthorized access via large-scale automated login requests.

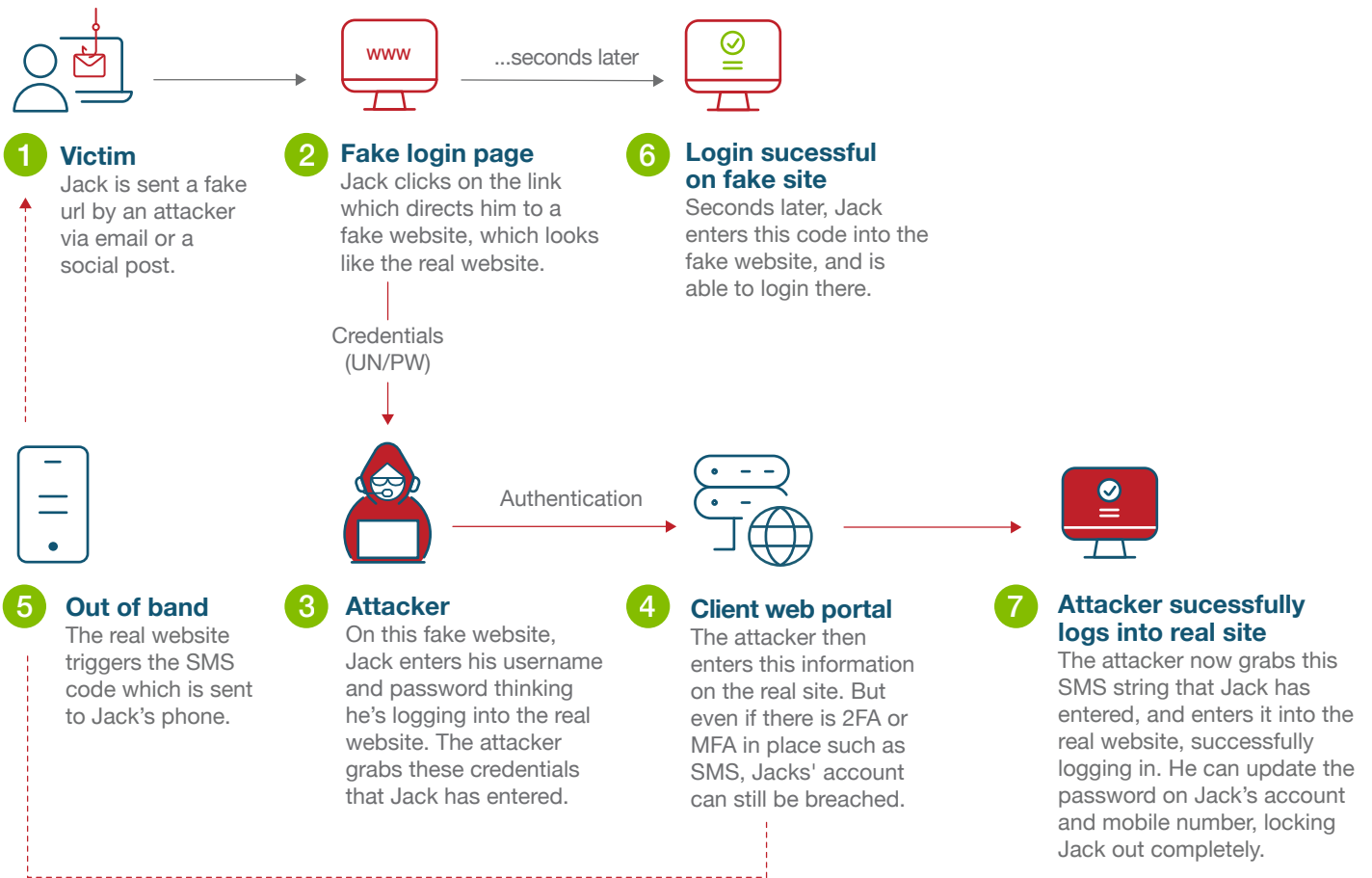
## Brute force attack



Systematic attack with all possible passwords and passphrases until the correct one is found.



# How fake login page defeats legacy MFA



## Device Costs



you must factor in the total cost of device ownership

## \$1 Million



large organizations spend up to \$1 million each year in staffing and infrastructure to handle password resets from employees

## \$5.2 Million



the average company loses \$5.2 million annually in productivity due to account lockouts

## 300%



cyber insurance premiums have gone up as much as 300% across high-risk industries

“When I’m going down by a third and others are going up by 20% or higher, that’s a really big win. In fact, I estimate our premiums are nearly half of what others are having to pay.”

Brent Deterding,  
CISO, Afni

## Misconception #2: Mobile authentication is cost-effective

### Reality: It’s more expensive than you think

Mobile authentication is perceived to be relatively inexpensive to roll out, leaving many organizations satisfied they have found a cost-effective solution for authentication. However, mobile authentication carries with it many hidden costs.

If you require employees to use mobile authentication, state law or union regulation may state that you cannot require employees to bear the mobility cost<sup>26</sup>. As a result, you must **factor in the total cost of device ownership**: hardware, recurring service costs, device management solutions, security solutions and even replacement costs to keep up with the demand for new devices. Some organizations also offer a monthly stipend to support enterprise use of personal devices.

Even in BYOD situations, **governance and support costs** remain high for legacy authentication. Forrester found that large organizations spend up to \$1 million each year in staffing and infrastructure to handle password resets from employees—and passwords only represent the first factor in 2FA or MFA authentication<sup>27</sup>. An estimated 10% of devices are lost, stolen or broken each year in organizations, another factor increasing the cost for mobile authentication (not to mention risk)<sup>28</sup>.

While security teams expend costly effort setting and managing password policies at scale, any time a user struggles with legacy authentication, they are not being **productive**. This includes forgotten passwords, account lockouts, password reset policies, time consuming workflows to generate and enter OTP/TOTP/push app codes, or the need to register new devices. Authentication is a mission-critical service: if employees can’t log into the apps or portals they use, they can’t do their job. In fact, the average company loses \$5.2 million annually in productivity due to account lockouts<sup>29</sup>.

As noted in the security section, the highest cost associated with legacy authentication comes from risk—the risk of **non-compliance or data breaches, disrupted operations, threats against critical infrastructure and the loss of intellectual property**. These risks only increase when we introduce complexities such as shared workstations and remote work. According to a recent survey, 40% of business leaders report cyber threats as the No. 1 business risk—one with the potential to decimate an organization and, in the worst cases, make recovery impossible<sup>30</sup>.

As a result of the potential for loss associated with cyber threats, **cyber insurance premiums** have gone up as much as 300% across high-risk industries, with new sub-limits and exclusions and a base requirement for MFA<sup>31</sup>. The onus is on you as an organization to demonstrate cybersecurity effectiveness, including MFA strategy, to make your organizational security profile more attractive to cyber insurers. Contact center specialist Afni was able to reduce its cyber insurance premiums by 30% by demonstrating how YubiKeys reduced its risk profile.

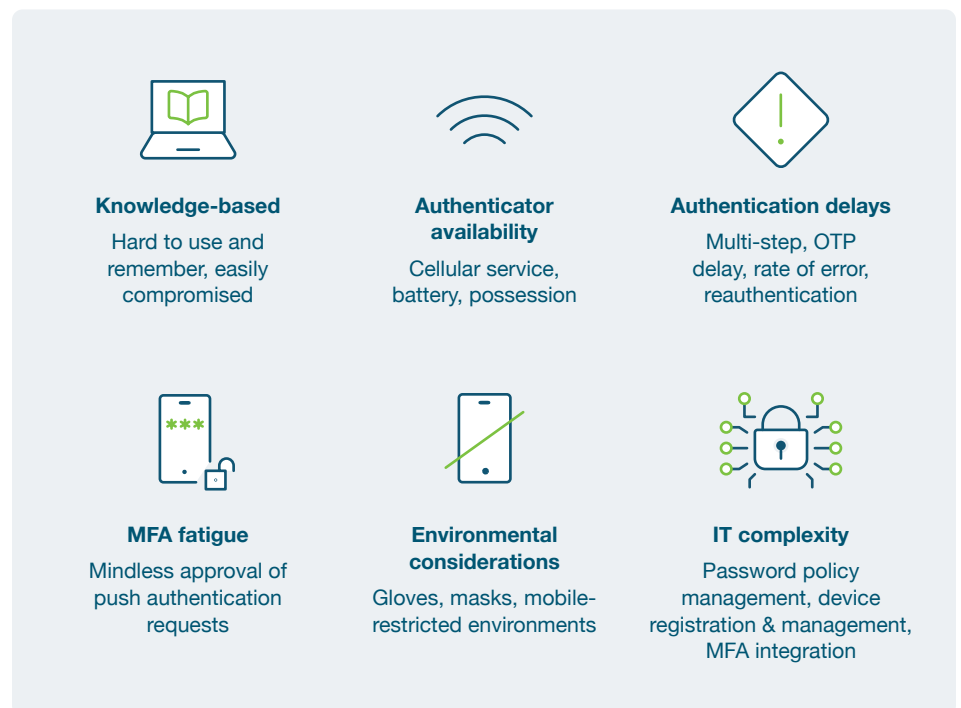


## Misconception #3: Mobile authentication is user-friendly

### Reality: Mobile authentication is complex to use and manage

With almost no barriers to implementation and high user awareness of mobile authentication methods, it's common to assume that mobile authentication will be user-friendly or simple.

The truth is, passwords alone are already a burden for users and for IT. When combined with mobile authentication, these usability challenges are not eliminated—instead, they increase.



According to a cross-vertical survey, 43% of organizations cite **user experience** as the top obstacle to using MFA<sup>32</sup>. With the average employee managing 50-120 passwords<sup>33</sup>, and policies to force resets and time-outs, users could be authenticating hundreds of times per day—and all of this is when MFA is working as expected, not to mention forgotten passwords, OTP delay or mobile devices that are lost, without charge or offline.

Although end-user experience is critical to employee experience and productivity metrics, usability considerations must also extend to **IT and help desk employees**. From an IT perspective, 41% of organizations cite complexity as an obstacle to MFA adoption<sup>34</sup>. Mobile MFA requires the support of both passwords and mobile authentication across the organization, increasing complexity associated with registering new devices, training, integrating MFA with new apps, device management and help desk requests for password resets or lost devices.

## Platform authenticators lack portability

In the shift away from legacy authentication, some organizations are choosing platform authenticators—authenticators built into smartphones and laptops in trusted platform modules (TPM) or secure elements. Platform authenticators rely on a user-supplied biometric (face or fingerprint) as an authentication factor, which can be used in combination with a possession-based authenticator for high assurance and FIDO2 phishing-resistant authentication.

While platform authenticators can be a good option for users with only one device, the average employee today uses at least two devices for work, not to mention any shared device or workstation needs. Since the cryptographic material for platform authenticators is embedded in the device itself, this form of authentication introduces **portability challenges** that make it difficult to switch between devices, access shared workstations or work in mobile-restricted environments.

## Misconception #4: Mobile authentication offers 360° coverage

### Reality: Mobile authentication creates MFA gaps

While organizations may prioritize or even mandate MFA, there are almost always gaps that mobile authentication cannot fill. Where gaps exist without a comprehensive MFA strategy, most organizations simply default to username and password.

#### Mobile authentication creates MFA gaps



##### Equality

users who don't have a smartphone or who live in low-connectivity areas.



##### Union restrictions

union regulations may restrict users from using their personal mobile device for enterprise use, including authentication.



##### Preference

employees may refuse to use their own phones for mobile authentication



##### Legal

many organizations can't legally require employees to install or use corporate apps or MFA on personal devices, requiring the expense of corporate-owned devices



##### Restricted access

mobile authentication can't be used in mobile-restricted areas such as call centers, manufacturing floors or clean rooms.



##### Availability

mobile authentication reliant on device battery, cellular signal and device presence is at risk if devices are forgotten, lost or stolen.



##### IT obstacles

mobile authentication may be disrupted by the unexpected loss of device, the need to register a new device, or the need to register or set up multiple devices to support login on each



##### Risk

most organizations recognize that certain user groups and authentication scenarios are higher risk, including privileged access and remote work, and that such risk requires a stronger level of authentication than is available with mobile authentication.



“ Passwordless login represents a massive shift in how billions of users, both business and consumer, will securely log in to their Windows 10 devices and authenticate to Azure Active Directory-based applications and services.”

Alex Simons,  
Corporate Vice President PM,  
Microsoft Identity Division

## Misconception #5: Mobile authentication is future-proofed

### Reality: Mobile authentication does not support emerging regulations or modern, phishing-resistant passwordless

MFA investments must provide organizations with protection that evolves as risk and compliance requirements do. To be future-proof, the MFA investment should reflect the growing regulatory requirement for **phishing-resistant MFA**, the need to implement **Zero Trust**, and modern login flows such as **passwordless**.

**Passwordless authentication** implementations are designed to **eliminate the security and usability weaknesses associated with passwords—but not all implementations can do both**. Sending an OTP code via SMS is an easy passwordless implementation—but not a secure or phishing-resistant one. A smart card is a secure, phishing-resistant passwordless implementation—but not an easy or inexpensive one.

**The future of passwordless is FIDO2/WebAuthn**, the combination of a phishing-resistant FIDO credential, also called a **passkey**, and the WebAuthn API that enables a simpler and more secure sign-in to websites and apps from common devices. However, a **passkey** is just the credential itself (a digital file), the **authenticator** is where the passkey lives—on a phone, laptop, hardware key or other device. And this is where we have a key difference.

A **synced passkey** lives on a smartphone, tablet or laptop where it can be copied and synced across many devices—like we saw with mobile authentication, this “mobility” makes it easy to use, but not always secure or easy to manage. A synced passkey is vulnerable because it is so easily shared (to new devices on a cloud account or via AirDrop), making it difficult to control identity and risk.

A **hardware-bound passkey** lives on a USB key that remains separate from everyday devices, but still allows easy authentication to devices and platforms—a future-proof passwordless solution that’s both **easy and secure**. [Learn more about passkeys here](#).

Like with mobile authentication, the evolution toward passwordless reinforces the need to separate devices being used from the authenticator. A hardware-bound passkey is a portable root of trust that allows you to prove that you possess the unique hardware device containing the cryptographic material which was registered to the user account. This, combined with a PIN, satisfies true multi-factor authentication requirements by providing **something you know**, with **something you are** and **something you have**.



In the past two years alone, the pressure to adopt phishing-resistant MFA has been added to several regulations and standards:



White House Executive Order 14028<sup>35</sup> / Office of Management and Budget (OMB) Memo 22-09<sup>36</sup>



National Security Memorandum/NSM-8<sup>37</sup>



NIS2<sup>38</sup>



PCI DSS v4.0<sup>39</sup>



FTC standards<sup>40</sup>



## Yubikey offers simple, 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 key, supporting both PIV/smart card and FIDO2/WebAuthn standards along with OTP and OpenPGP, integrating seamlessly into both legacy and modern environments, helping organizations **bridge to a passwordless future** supported by hardware-bound passkeys.

Modern hardware security keys such as the YubiKey provide an authentication process that is free of human error, offering organizations a path to zero trust that is proven to **reduce risk by 99.9%**. The YubiKey works across the organization and in places legacy MFA can't, free from reliance on external power, batteries or network connection.

The YubiKey is designed to deliver a great **user experience**, letting users securely log in to over one thousand **products, services and applications**, including leading identity and access management (IAM) platforms, privileged access management (PAM) solutions and cloud services, with the secrets never shared between services.

### The total economic impact of YubiKeys<sup>41</sup>:



#### Strongest Security

Reduce risk  
by  
**99.9%**



#### High Return

Experience ROI  
of  
**203%**



#### More Value

Reduce support  
tickets by  
**75%**



#### Faster

Decrease time to  
authenticate by  
**>4x**

“I wanted something that was unphishable. If we were going to go through all the trouble of redoing a lot of our identity and access management infrastructure, I wanted it to be future proof and resilient.”<sup>42</sup>

Derek Pitts,  
Director of enterprise security at  
Cloudflare

## Cloudflare stops phishing in its tracks with the YubiKey

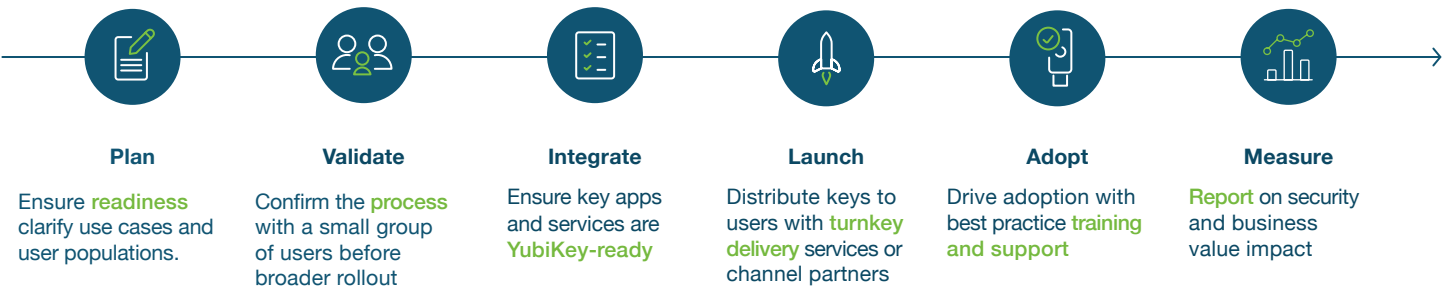
Cloudflare, one of the world's leading internet content delivery and security platforms, began making the move away from OTP technology to WebAuth/FIDO2 with the YubiKey in 2020, selectively enforcing the use of YubiKeys across its most sensitive infrastructure to support user adoption and engagement.

In 2022, when a phishing attack similar to the one that compromised Twilio began targeting Cloudflare employees, it did not matter that employees fell prey to the scam—the attack was stopped in its tracks by Cloudflare's own zero trust platform, supported by the YubiKey. “While the attacker attempted to log in to our systems with the compromised username and password credentials,” notes the Cloudflare team on their blog, “They could not get past the hard key requirement.”






# Getting started is easy

In this whitepaper, we uncovered the dark side of mobile authentication—that easy-to-use or deploy comes with hidden risk, cost, usability challenges, and gaps. Further, we explored how mobile authentication is holding organizations back on their journey to Zero Trust and passwordless.

Did mobile authentication deliver the secure, easy solution we had hoped (or believed) it would? No. Thankfully, there is a path forward. We have made it easy to deploy phishing-resistant MFA and passwordless with the YubiKey. We offer a simple [6 Step Best Practice Deployment Guide](#) to help accelerate modern MFA adoption at scale:



To remove all the guesswork out of planning, purchasing and delivery, Yubico offers professional services and as a service options and works with many channel partners to make getting started easy.

YubiEnterprise Services*		Yubico Professional Services		
 YubiEnterprise Subscription	 YubiEnterprise Delivery	 Deployment 360	 Workshops	 Implementation projects
Simplifies how businesses procure, upgrade and support YubiKeys	Global distribution to remote and in-office locations	Service hour bundles	Custom engagements	Technical engagements to implement YubiKeys in your environment

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

# Sources

- <sup>1</sup> Google Cloud, [April 2023 Threat Horizons Report](#), (April 2023)
- <sup>2</sup> 451 Research, [2021 Yubico and 451 Research Study](#), (April 2021)
- <sup>3</sup> IBM, [2022 Cost of Data Breach Report](#), (July 27, 2022)
- <sup>4</sup> The White House, [Executive Order on Improving the Nation's Cybersecurity](#), (May 12, 2021)
- <sup>5</sup> OMB, [M-22-09](#), (January 26, 2022)
- <sup>6</sup> The White House, [Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems](#), (January 19, 20220)
- <sup>7</sup> European Parliament, [The NIS2 Directive](#), (February 2023)
- <sup>8</sup> PCI, [PCI DSS: v4.0](#), (March 2022)
- <sup>9</sup> Forrester, [The Total Economic Impact of Yubico YubiKeys](#), (September 2022)
- <sup>10</sup> Kurt Thomas and Angelika Moscicki, [New research: how effective is basic account hygiene at preventing hijacking](#), (May 17, 2019)
- <sup>11</sup> Verizon, [2022 Data Breach Investigations Report](#), (May 24, 2022)
- <sup>12</sup> Forrester Research, Inc, [Optimize User Experience With Passwordless Authentication](#), (March 2, 2020)
- <sup>13</sup> Egress, [Email Security Risk Report 2023](#), (March 8, 2023)
- <sup>14</sup> Verizon, [2022 Data Breach Investigations Report](#), (May 24, 2022)
- <sup>15</sup> Pieter Arntz, [Twilio data breach turns out to be more elaborate than suspected](#), (August 29, 2022)
- <sup>16</sup> Lawrence Adams, [Uber hacked, internal systems breached and vulnerability reports stolen](#), (September 16, 2022)
- <sup>17</sup> Alicia Hope, [American Airlines data breach linked to a phishing campaign exposed sensitive customer and employee personal information](#), (September 28, 2022)
- <sup>18</sup> David Lumb, [AT&T Vendor Data Breach Exposed 9 Million Customer Accounts](#), (March 9, 2023)
- <sup>19</sup> WSQCTV, [Chick-fil-A announces app data breach, tells customers how to protect personal information](#), (March 4, 2023)
- <sup>20</sup> Twitter, [An update on our security incident](#), (July 18, 2020) ; New York State Department of Financial Services, [Twitter Investigation Report](#), (Accessed Sept 14, 2021)
- <sup>21</sup> Joseph Cox, [A Hacker Got All My Texts for \\$16](#), VICE, (March 16, 2021)
- <sup>22</sup> Kurt Thomas, Angelika Moscicki, [New research: How effective is basic account hygiene at preventing hijacking](#), (May 17, 2019)
- <sup>23</sup> Rob Lemos, [The state of two-factor authentication by text: What security pros need to know](#), (Accessed Sept 14, 2021)
- <sup>24</sup> 451 Research, [2021 Yubico and 451 Research Study](#), (April 2021)
- <sup>25</sup> LastPass and IDC, [Enabling the Future of Work with EPM, Identity and Access Controls](#), (February 23, 2022)
- <sup>26</sup> Shouse Labor Law Group, [Cell phone reimbursement—when are workers entitled to it?](#) (January 7, 2022)
- <sup>27</sup> Forrester Research, Inc, [Optimize User Experience With Passwordless Authentication](#), (March 2, 2020)
- <sup>28</sup> LocknCharge, [The True Cost of Lost or Missing Mobile Devices](#), (Accessed September 12, 2021)
- <sup>29</sup> Ponemon Institute, [2019 State of Password and Authentication Security Behaviors Report](#), (Accessed September 14, 2021)
- <sup>30</sup> PwC, [PwC Pulse Survey: Managing business risks](#), (August 18, 2022)
- <sup>31</sup> Ryan Smith, [Cyber insurers raising premiums, lowering coverage limits—report](#), (October 11, 2021)
- <sup>32</sup> 451 Research, [2021 Yubico and 451 Research Study](#), (April 2021)
- <sup>33</sup> LastPass and IDC, [Enabling the Future of Work with EPM, Identity and Access Controls](#), (February 23, 2022)
- <sup>34</sup> 451 Research, [2021 Yubico and 451 Research Study](#), (April 2021)
- <sup>35</sup> The White House, [Executive Order on Improving the Nation's Cybersecurity](#), (May 12, 2021)
- <sup>36</sup> OMB, [M-22-09](#), (January 26, 2022)
- <sup>37</sup> The White House, [Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems](#), (January 19, 20220)
- <sup>38</sup> European Parliament, [The NIS2 Directive](#), (February 2023)
- <sup>39</sup> PCI SSC, [PCI DSS v4.0](#), (March 2022)
- <sup>40</sup> James Dempsey, [The FTC's rapidly evolving standards for MFA](#), (November 8, 2022)
- <sup>41</sup> Forrester, [The Total Economic Impact of Yubico YubiKeys](#), (September 2022)
- <sup>42</sup> FIDO Alliance, [Cloudflare embraces FIDO to help improve its own security](#), (2023)
- <sup>43</sup> Cloudflare, [The mechanics of a sophisticated phishing scam and how we stopped it](#), (August 9, 2022)





## About Yubico

As the inventor of the YubiKey, Yubico makes secure login easy and available for everyone. The company has been a leader in setting global standards for secure access to computers, mobile devices, and more. Yubico is a creator and core contributor to the FIDO2, WebAuthn, and FIDO Universal 2nd Factor (U2F), and open authentication standards.

YubiKeys are the gold standard for phishing-resistant multi-factor authentication (MFA), enabling a single device to work across hundreds of consumer and enterprise applications and services.

Yubico has a presence around the globe. For more information, please visit: [www.yubico.com](http://www.yubico.com).