yubico

WHITE PAPER

The top 5 mobile authentication misconceptions

Demystifying the myth versus reality of legacy MFA

Contents

Introduction

$3.89 Million

average breach cost[3]

$1+ Million

breach cost when **remote work** is factor[4]

100+ Attacks

every day for 70% of organizations[5]

61%

of data breaches traced back to **credentials**[6]

Despite the growing tide and sophistication of cyber attacks, many organizations continue to use legacy authentication methods such as usernames and passwords or mobile-based authenticators, to secure access to critical and sensitive applications and data. But these methods don't offer the best security—they are highly susceptible to phishing attacks, man-in-the-middle (MiTM) attacks, malware, SIM swapping, and account takeovers. They also don't offer the best user experience. Across these organizations, the results are unexpected: attacks that penetrate their defenses, and employees who are frustrated. Why is this happening?

While any form of multi-factor authentication (MFA) offers better security than legacy username and password based authentication, not all forms of MFA are created equal. Research by Google, NYU, and UCSD, based on 350,000 real-world hijacking attempts, proved that SMS and mobile authenticators are not very effective in preventing account takeovers and targeted attacks. The research revealed that a SMS-based OTP only blocked 76% of targeted attacks and a push app only blocked 90%.[1] That's, at minimum, a 10% penetration rate. With this approach, it's not a matter of if you will be attacked—it's a matter of when.

Usernames and passwords and mobile-based authentication also contribute to authentication complexity, making employees overwhelmed with the authentication experience. The average employee has to use and remember 191 passwords, 61% of which are the same or similar.[2] And where mobile-based authentication such as SMS and OTP are used for two-factor (2FA) or MFA, employees are required to wait for and enter codes delivered by SMS or authenticator apps. All of this adds to the time and complexity of authentication, and reducing employee productivity, all while leaving the organization exposed.

As organizations move into the new way of working, where remote and hybrid work is the long-term norm, it's imperative to realize that relying on perimeter security is no longer effective, and that legacy, weak authentication methods such as usernames and passwords, and mobile-based authenticators, can put your organization at risk of being hacked. Organizations that are using usernames and password based authentication today, or those that are using mobile-based authenticators, or other forms of legacy MFA should reevaluate their long-term MFA strategy and consider moving to modern MFA solutions.

In this whitepaper, we'll reveal the true picture of mobile authentication, and show that focusing on employees is how organizations can find a more secure, user-friendly MFA approach.

Common forms of mobile authentication

There are many different forms of mobile authentication, each offering various degrees of security and user experience. While certain forms of mobile authentication offer greater security than others, it's important to note that no mobile-based authenticator can stop account takeovers 100%.

53%

of organizations continue to choose mobile-based authentication as their MFA form factor.[7]

OTP

A one-time passcode or password (OTP) is a code that is valid for only one login session or transaction, typically sent via SMS to a mobile phone.

TOTP

TOTP (time-based one-time password) is a code (token), generated using HMAC (sharedSecret, timestamp) that changes every few seconds or minutes, typically sent via SMS, or sometimes an authenticator app.

Push Apps

An authentication attempt sends an alert to an app on a user's mobile device. Users view the authentication details and approve or deny access.

Authenticator Apps

An authenticator app installed on a mobile device that is TOTP based and generates a random passcode every 30 seconds to be used for sign-in or two-factor authentication.

Built-in Authentication

A built-in authenticator (also referred to as a platform authenticator) is built into a particular client device platform, and leverages either an internal trusted platform module (TPM) or secure element, tying the credential to the device.

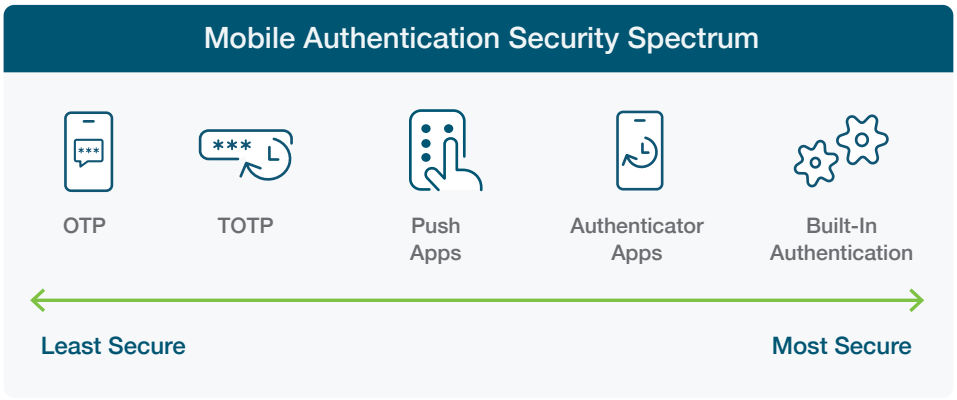
In the next section we'll cover the top five mobile authentication misconceptions that put organizations at risk of account takeovers and increased Opex and Capex costs, if not addressed.

Misconception #1: Mobile authentication is secure

Reality: Mobile authentication is putting organizations at risk

Mobile devices have a large attack surface that includes the apps, operating systems, secure element technology, and communication, each another vector of attack– not to mention the implication if a device is lost or stolen, it also eliminates all access to 2FA/MFA and subsequently the apps.

Security remains the top misconception about mobile authentication—not all types of mobile authentication methods are created equal. It's important to remember that mobile devices are built for communication, not security. The security spectrum of mobile authentication below depicts a decreasing risk profile from left to right—but is never eliminated completely. Many organizations think that "mobile authentication is good enough". But really, **every mobile authenticator can be phished.**



In mobile-based MFA, the second factor is tied to the mobile device. This is a red flag, because of three aspects: there is no real guarantee that the private key ends up on a secure element on the mobile device, the OTP code or private key could be intercepted in some way, and it is impossible to ensure proof of possession; or in National Institute of Standards and Technology (NIST) terms—impossible to prove it is impersonation resistant. Mobile devices have a large attack surface that includes the apps, operating systems, secure element technology, and communication, each another vector of attack—not to mention the implication if a device is lost or stolen, it also eliminates all access to 2FA/MFA and subsequently the apps.

Today's hackers increasingly hijack one-time use codes and push notifications through interception or phishing, with the attacker and account takeover all but invisible to the user. The risk of SMS interception is so high that NIST called for SMS to be deprecated as a method of authentication.[8]

In a recent VICE article, a white-hat hacker demonstrated how easy it was to redirect text messages to take over a volunteer's social media accounts.[9] All it took was just $16 and a few seconds to completely, and invisibly, take over accounts that had been protected by OTP-based MFA.

Today's cyber criminals have ample and inexpensive tools at their disposal to make phishing websites, inject malware onto the device, intercept text messages or utilize SIM swapping to intercept, bypass, or otherwise thwart legacy MFA in a way that is almost undetectable to the end user.

Every mobile authenticator can be hacked

Account takeovers occur when a hacker successfully gains access to a user's credentials. This can come from many forms:

- Phishing
- Credential stuffing
- Brute force attack
- Man-in-the-middle (MiTM) attack
- Malware
- OAuth phishing
- SIM swapping

After arresting 10 people for hijacking mobile phones, the EU police agency Europol said the criminal network is believed to have stolen personal information and more than $100 million (€82.4 million) in cryptocurrencies, stating that "sim swapping" can be done either by fooling the phone company with "social engineering techniques" or by using a "corrupt insider."[10]

As noted in the draft Federal Zero Trust Strategy, "many approaches to multi-factor authentication will not protect against sophisticated phishing attacks, which can convincingly spoof official applications and involve dynamic interaction with users. Users can be fooled into providing a one-time code or responding to a security prompt that grants the attacker account access."[11]

When mobile authentication relies on people, it creates a recipe for risk. People make mistakes. They don't update their software. They download an insecure app. They click a link or answer a call that was actually a phishing attack. In other words, no amount of security training can entirely eliminate the risks of modern phishing attacks.

If you have believed all along that mobile authentication is secure, you're not alone. Only 22% of respondents Yubico surveyed are aware that security could be a problem with SMS-based authentication.[12] Malicious actors therefore have a long runway to penetrate organizational defenses with insufficient account security in place today.

Phishing

Attackers trick users into giving up sensitive information such as credentials.

Credential stuffing

Stolen credentials used to gain unauthorized access to user accounts through large-scale automated login requests directed against a web application.

Brute force attack

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

Man-in-the-middle (MiTM) attack

Attacker secretly relays and possibly alters communications between two parties.

Malware

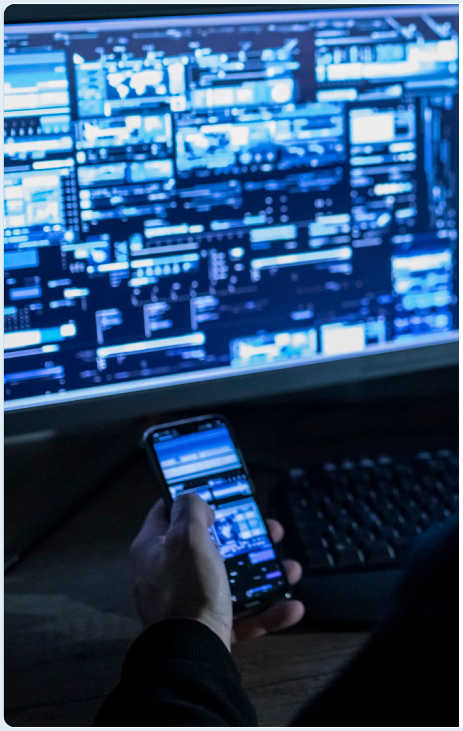
Software-based attack designed with malicious intent to gain access to a network or to cause damage to data and systems

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.

SIM swapping

A SIM swapping attack is also known as SIM splitting, SIMjacking, SIM hijacking and port-out scamming. It is a scam that targets a weakness in some forms of 2FA in which a call or text message sent to a mobile phone is used as the second factor, exploiting the ability of subscriber identity module (SIM) cards to be ported by mobile service providers from device to device bearing different telephone numbers.



Teen hackers exploited mobile authentication weaknesses at Twitter

In 2020, a small group of teenagers targeted Twitter employees with a spear phishing attack to obtain access to employee credentials and the internal network.[13] The attackers then seized high-profile accounts, including those of several cryptocurrency companies, and launched a scam that netted over $118,000 in bitcoin.[14] All without malware, exploits, or backdoors.

An investigation report released by the New York State Department of Financial Services noted that Twitter used application-based MFA to authenticate employees, the most common form of MFA.[15] During the attack, hackers tricked employees into entering stolen credentials on a phishing site, mirrored in real-time on the real Twitter site, triggering a request for authentication to the employee's smartphone.

A hacker stole cryptocurrency from 6,000 customers bypassing SMS MFA

A crypto exchange disclosed that a threat actor stole cryptocurrency from 6,000 customers after using a vulnerability to bypass the company's SMS multi-factor authentication security feature.

For customers who used SMS texts for 2FA, the third party took advantage of a flaw in the SMS Account Recovery process in order to receive an SMS two-factor authentication token and gain access to the customers account.[16]

These attacks only demonstrate how simple it is for social engineering to bypass mobile authentication-based MFA.

Misconception #2: Mobile authentication is cost effective

Reality: It's more expensive than you think

Organizations continue to face rising costs associated with cyber attacks and data breaches, including the loss of business, system downtime, ransomware payout and recovery costs, legal and audit costs, as well as regulatory fines and reputational damage.

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 associated with devices, productivity, and support—not to mention the cost of a potential data breach. All together, it is estimated that the total cost of enterprise mobility can be as high as $1,840 per owned device.[17]

Device costs

If regulatory compliance requires MFA and the organization requires employees to use mobile-based MFA, then the organization must take on the costs for the device, recurring service costs, enterprise device management software, mobile security software, as well as phone replacement costs to keep up with the demand for new devices. Some organizations may offer a monthly stipend to support work use of personal devices as an alternative.

Support & productivity costs

Forrester estimates 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.[18] In fact, many of the same password-based problems persist in mobile authentication, increasing costs without the net benefit to security.

Any form of mobile authentication applied and enforced at scale will require ongoing policy enforcement, user training and IT support. Even the easiest forms of 2FA and MFA mobile authentication—OTP, TOTP, 2FA apps—create a huge support burden if codes are delayed, users get locked out of their accounts, or users need to register new devices. 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).[23] Any time a user struggles with mobile authentication, they are not being productive. Authentication is a mission-critical service: If employees can't log into the apps or portals they use, they can't do their job.

Risk

Unfortunately, it's often a data breach that brings organizations face-to-face with the true cost of mobile authentication, and the increased percentage of remote and hybrid workers may increase the risk of a successful data breach. Approximately 73% of IT workers believe that remote workers pose a greater security threat, being more vulnerable to spear phishing attacks and more likely to use insecure devices.[24]

Mobile device management is complicated by BYOD and demands by users to own and control their own phone and to use the apps they want. Sixty percent of organizations consider mobile devices the biggest security risk,[25] including worries about "Shadow IT"—the unmonitored and unsecured use of unauthorized apps for work.

With credentials the prime vector for data breach, inadequate authentication could be a $4.37 million dollar mistake, the average cost of a data breach in the past year where credentials have been compromised.[26]

$1 Million

annual cost just for password-related support costs, for several large U.S based organizations in different verticals[19]

60%

of IT service desk interactions are related to password resets[20]

$70

the average helpdesk labor cost for a single password reset[21]

$5.2 Million

the amount an average company loses annually in productivity due to account lockout[22]

Misconception #3: Mobile authentication is user-friendly

What happens if a device is lost, damaged or offline? Is there a backup way to access the apps? If the answer isn't obvious, the answer with mobile authenticators is a 'no.'

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, if passwords are already a burden for users and IT, mobile authentication can make that frustration worse due to incorrect expectations and potential disruption.

User experience

43% of organizations cite user experience as the top obstacle to using MFA.[27] Mobile authenticators involving SMS or push codes introduce additional cumbersome steps, adding to user fatigue. Multiplied across apps and exacerbated by timed log-outs, this could force users to authenticate hundreds of times a day. All of this time exists before a user can become productive.

If an OTP message is delayed or fails, users can be left waiting. In March of 2021, several million SMS messages, including OTP codes, were not delivered when a commercial SMS blocking regulation was enforced.[28] Beyond SMS, mobile authenticators require a charged, unbroken device that is connected to the Internet. What happens if a device is lost, damaged or offline? Is there a backup way to access the apps? If the answer isn't obvious, the answer with mobile authenticators is a 'no.'

IT complexity

41% of organizations cite complexity as an obstacle to MFA adoption.[29] As noted in Misconception #2, supporting passwords (first factor) and mobile authentication (second factor) requires a significant investment of IT time. Yes, mobile authentication is easy to roll out. But it's not easy to manage.

IT teams face ongoing complexity with:

- Registering new devices
- Training
- Integrating MFA with new apps
- Device management
- Help desk requests including password resets

Misconception #4: Mobile authentication offers 360 degree coverage

Reality: Mobile authentication creates MFA gaps

Mobile authenticators can lead to MFA security gaps when users can't, don't, or won't use mobile-based authentication. Reasons include low cell coverage in certain geographic areas, employees who don't want to use personal devices for work, or don't want to allow admin access to their devices. There may also be union restrictions or compliance requirements, and some employees may not be able to even use a smartphone.

While organizations may prioritize or even mandate mobile-based MFA, there are almost always edge cases of employees that can't, don't, or won't use mobile authentication, creating MFA gaps if the fall back option is usernames and passwords. Let's take a look at some of the edge cases where organizations struggle to support mobile-based MFA:

Equality – users who don't have a smartphone or who live in low-connectivity areas may be challenged to support mobile authentication

Union – union regulations may restrict users from using their own mobile device for authentication

Restricted access – mobile authentication can't be used in mobile-restricted areas such as call centers, manufacturing floors, clean rooms. Use of mobile authenticators is also reliant on device battery and cellular signal, which may not always be available.

Legal – many organizations can't legally require employees to install or use corporate apps or 2FA / MFA on personal devices, so you may be required to provide corporate devices for this[30] (see device costs, Misconception #2)

Preference – employees may refuse to use their personal phones for work-related mobile authentication

Obstacles – unexpected loss of device, the need to register a new device, the need to register or set up multiple devices to support login on each

Privileged users – if we acknowledge that mobile-based MFA is not the strongest form of authentication (Misconception #1), it may not be suitable for privileged users and administrators whose credentials are a prime target. The caveat here is that today's sophisticated attacks make every user a privileged user, with a single credential being the starting point for lateral and escalated attacks.

> 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**

What is passwordless authentication?

Over the past few years, the term "passwordless" has gained momentum and now it is used by many security, authentication, and identity solution providers —each with their own unique nuance. There are a lot of different implementations of passwordless authentication and they all have tradeoffs. Some implementations of passwordless such as SMS, are specifically designed to address usability issues. Other implementations of passwordless such as smart cards, are specifically designed to address security issues. A future-looking passwordless strategy is FIDO2/ WebAuthn based.

FIDO2 is the newest FIDO Alliance specification for authentication standards (introduced in 2018), and WebAuthn is a web-based API that allows websites to update their login flow to add FIDO-based authentication on supported browsers and platforms. This is an evolving security ecosystem that will make adopting passwordless authentication easier.

Misconception #5: Mobile authentication is future-proofed

Reality: Mobile authentication isn't built for the long term

Security investments must provide adequate protection that is compliant with ever more stringent regulations over time. A truly future-proofed security investment should set an organization up well for secure and modern login flows, such as passwordless, as well as for long-term regulatory compliance. With updates to current regulations and net new regulations expected over the next few years, especially in the wake of COVID-19, mobile authentication, while considered good enough today, may not meet future compliance standards related to MFA.

Additionally the future of authentication is passwordless i.e. any form of authentication that doesn't require the user to provide a password at login. There are many different implementations of passwordless authentication today. Many refer to SMS verification as passwordless because you don't need to remember a password. Usually you're sent an OTP code that is valid for a short period of time that the user can use to authenticate themselves. (And the irony is that "OTP" stands for "one-time password" — that is the common usage of the term). As we've demonstrated, these forms of passwordless authentication are considered a weak form of authentication.

Smart card authentication is another form of passwordless. But traditional smart cards may be somewhat complex for administrators to implement and manage, and involve having a good strategy in place to implement at scale.

There are more secure forms of passwordless authentication that don't require SMS verification and that are kept separate from the device itself. By separating the device and the authenticator, you have a portable root of trust, allowing you to prove that you possess the unique hardware device containing the cryptographic material which was registered to the user account. This, combined with the username + password or PIN, satisfies true multi-factor authentication requirements by providing something you know, with something you are, or something you have.

The industry is moving toward passwordless login flows that are secure, fast and pain-free. FIDO2 is the newest FIDO Alliance specification for authentication standards to cover passwordless login flows. FIDO2 offers single-factor or multi-factor authentication, avoiding the most phishable components of a 2FA solution like SMS, and removing the need for username and password as a first factor.

Many applications that support OTP and other legacy methods don't yet support modern protocols like FIDO2 and WebAuthn. A rip and replace of legacy methods overnight is not pragmatic and can be costly. At the same time, having users carry multiple authentication devices is not desirable either. Going passwordless is not a "one and done" implementation, but rather a journey that often involves supporting both legacy, modern, and hybrid environments with strong authentication.

Modern, strong authentication with the YubiKey

> One multi-factor option—physical security keys—appears to be immune to these sophisticated scams.[31]
>
> **–Brian Krebs, Krebs on Security**

Yubico created the YubiKey, a modern hardware security key built for high security and usability.

The YubiKey uses modern protocols such as FIDO U2F and FIDO2 open authentication standards to help eliminate phishing-driven credential-based attacks and support the need for a user-friendly login flow. Yubico is also a core contributor to the FIDO Universal 2nd Factor (U2F) and FIDO2 open authentication standards, and has contributed to open identity standards organizations W3C, IETF, FIDO Alliance and OpenID.

The YubiKey provides strong phishing-resistant two-factor, multi-factor, and passwordless authentication at scale, with the hardware authenticator protecting the private secrets on a secure element that cannot be easily exfiltrated. The YubiKey is the only solution that is proven to stop 100% of account takeovers in independent research.[32]

It's the kind of protection that could have stopped the Twitter attack:

> 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 Department of Financial Services, Twitter Investigation Report[33]**

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 using a single key across a variety of legacy and modern infrastructures to support organizations no matter where they are on their passwordless journey.

Account takeover rates

Security key
0%

On-device prompt
10%

Secondary email
21%

SMS code
24%

Phone number
50%

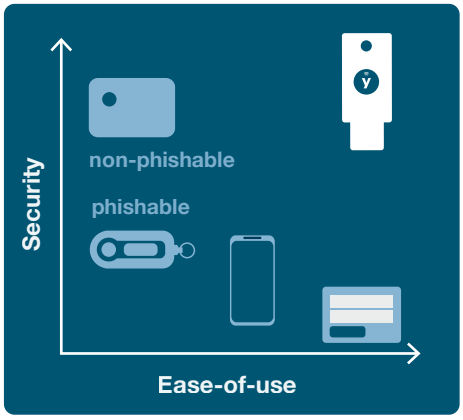
> Any form of MFA is better than just a username and password, but most MFA can still be phished. It didn't take long to realize we needed stronger authentication for all employees that couldn't be phished. YubiKeys made the most sense. And when I first used a YubiKey Nano, I loved the experience — I left it in my computer and simply touched it to authenticate.
>
> **– Daniel Jacobson**
> **Senior Director of IT, Datadog[34]**

The versatile YubiKey requires no software installation or battery so just plug it into a USB port and touch the button, or tap-n-go using NFC for secure authentication. YubiKeys don't require batteries, have no breakable screens, don't need a cellular connection, and are water- and crush-resistant.

The YubiKey provides the convenience needed to support today's modern in-person, hybrid, and remote employees.

	Mobile authentication	YubiKey
Always secure	X	✓
Cost effective	X	✓
User friendly	X	✓
360 degree coverage	X	✓
Future-proofed	X	✓

Summary



For many years, choosing an approach to MFA and passwordless required a tradeoff between security and user productivity / ease of use. Smart cards offer high security, storing the secret on the card, but deployment is costly and not practical across every device an employee might need to access. On the flip side, the ubiquity of mobile devices introduced the concept of convenience and ease of use to MFA, but did mobile authentication deliver everything we hoped (and believed) it would?

In this whitepaper, we learned that the security of mobile authentication is a spectrum, with some forms doing a lot better than others. We learned that there are a lot of hidden costs to mobile authentication - and some not so hidden costs no organization wants to face. We learned that easy-to-implement does not always mean easy-to-use or easy-to-manage. And that the industry is moving to passwordless authentication while mobile authentication is stuck in the past.

Thankfully there is a way forward. The YubiKey is a more secure, easy-to-use MFA solution designed to meet organizations where they are and be a true bridge to passwordless - seamlessly supporting legacy infrastructures as well as modern, cloud-based systems that leverage the latest standards like WebAuthn and FIDO2.

Sources

[1] Kurt Thomas, Angelika Moscicki, New research: How effective is basic account hygiene at preventing hijacking, (May 17, 2019), https://security.googleblog.com/2019/05/new-research-how-effective-is-basic.html

[2] Amber Steel, LastPass Reveals 8 Truths about Passwords in the New Password Exposé, (November 1, 2017), https://blog.lastpass.com/2017/11/lastpass-reveals-8-truths-about-passwords-in-the-new-password-expose/

[3] IBM, 2021 Cost of Data Breach Report, (Accessed September 14, 2021), https://www.ibm.com/security/data-breach

[4] IBM, 2021 Cost of Data Breach Report, (Accessed September 14, 2021), https://www.ibm.com/security/data-breach

[5] Red Canary, The State of Incident Response 20201, (Accessed September 16, 2021), https://redcanary.com/resources/guides/the-state-of-incident-response-2021/

[6] Verizon, 2021 Data Breach Investigations Report, (Accessed May 18, 2021), https://www.verizon.com/business/resources/reports/dbir/2021/masters-guide/

[7] 451 Research, 2021 Yubico and 451 Research Study, (April 2021), https://pages.yubico.com/work-from-home-policies-driving-mfa-adoption

[8] Rob Lemos, The state of two-factor authentication by text: What security pros need to know, (Accessed Sept 14, 2021), https://techbeacon.com/security/state-two-factor-authentication-text-what-security-pros-need-know

[9] Joseph Cox, A Hacker Got All My Texts for $16, VICE, (March 16, 2021), https://www.vice.com/en/article/y3g8wb/hacker-got-my-texts-16-dollars-sakari-netnumber

[10] Euronews, SIM swapping: 10 arrested in Europe over €82.4m scam to hijack celebrities' phones, (February 10, 2021), https://www.euronews.com/2021/02/10/sim-swapping-10-arrested-in-europe-over-82-4m-scam-to-hijack-celebrities-phones

[11] WhiteHouse.gov, Federal Zero Trust Strategy (EO 14028), Accessed Sept 16, 2021, https://zerotrust.cyber.gov/federal-zero-trust-strategy

[12] 451 Research, 2021 Yubico and 451 Research Study, (April 2021), https://pages.yubico.com/work-from-home-policies-driving-mfa-adoption

[13] Twitter, An update on our security incident, (July 18, 2020), https://blog.twitter.com/en_us/topics/company/2020/an-update-on-our-security-incident

[14] New York State Department of Financial Services, Twitter Investigation Report, (Accessed Sept 14, 2021)

[15] Department of Financial Services Twitter Investigation Report, Oct 14, 2020, https://www.dfs.ny.gov/Twitter_Report

[16] Hackers rob thousands of Coinbase customers using MFA flaw, https://www.bleepingcomputer.com/news/security/hackers-rob-thousands-of-coinbase-customers-using-mfa-flaw/

[17] Wandera, Uncovering the True Costs of Enterprise Mobility, (Accessed September 14, 2021), https://www.clevermobile.it/risorse/file/wandera/tcowhitepaper.pdf

[18] LastPass, New Forrester Report: The Real Cost of Password Risks, (May 18, 2018), https://blog.lastpass.com/2018/05/new-forrester-report-real-cost-password-risks/

[19] Forrester Report: Best Practices: Selecting, Deploying, And Managing Enterprise Password Managers, (January 8, 2018)

[20] Gartner, 3 Simple Ways IT Service Desks Should Handle Incidents and Requests, (Aug 2019)

[21] Forrester Research, Best Practices: Selecting, Deploying, and Managing Enterprise Password Managers, (January 8, 2018)

[22] Ponemon Institute, 2019 State of Password and Authentication Security Behaviors Report, (Accessed September 14, 2021), https://pages.yubico.com/2019-password-and-authentication-report

[23] LocknCharge, The True Cost of Lost or Missing Mobile Devices, (Accessed September 12, 2021), https://www.locknCharge.com/cost-of-lost-devices/

[24] OpenVPN, Remote Work is the New Future - But Is Your Organization Ready for It? (Accessed September 13, 2021), https://openvpn.net/blog/remote-workforce-cybersecurity-quick-poll/

[25] Verizon, Mobile Security Index 2021 Report, (Accessed September 14, 2021), https://www.verizon.com/business/resources/reports/mobile-security-index.html/

[26] IBM, 2021 Cost of Data Breach Report, (Accessed September 14, 2021), https://www.ibm.com/security/data-breach

[27] 451 Research, 2021 Yubico and 451 Research Study, (April 2021), https://pages.yubico.com/work-from-home-policies-driving-mfa-adoption

[28] FE Online, OTP messages not coming through? You are not alone, here's why this is happening, (March 9, 2021), https://www.financialexpress.com/industry/technology/otp-messages-not-coming-through-you-are-not-alone-heres-why-this-is-happening/2209041/

[29] 451 Research, 2021 Yubico and 451 Research Study, (April 2021), https://pages.yubico.com/work-from-home-policies-driving-mfa-adoption

[30] https://www.shouselaw.com/ca/blog/do-i-get-reimbursed-for-business-use-of-my-personal-cell-phone/

[31] Brian Krebs, Voice Phishers Targeting Corporate VPNs, Krebs on Security, (August 19, 2021) https://krebsonsecurity.com/2020/08/voice-phishers-targeting-corporate-vpns/

[32] Kurt Thomas and Angelika Moscicki, New research: how effective is basic account hygiene at preventing hijacking, (May 17, 2019), https://security.googleblog.com/2019/05/new-research-how-effective-is-basic.html

[33] New York State Department of Financial Services, Twitter Investigation Report, (Accessed September 14, 2021)

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

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.