yubico

Not all MFA is created equal

Mobile MFA lures cybercriminals

The average cost of a data breach broke an 18-year high in 2022, ringing up at a whopping $4.35M, a 2.6% increase from 2021.[1] Despite the growing tide and sophistication of cyber attacks, many organizations continue to use legacy multi-factor authentication (MFA) methods like usernames and passwords, and mobile-based authenticators, to secure access to critical and sensitive applications and data. Across these organizations, the results are unexpected: attacks that penetrate their defenses, and employees who are frustrated.

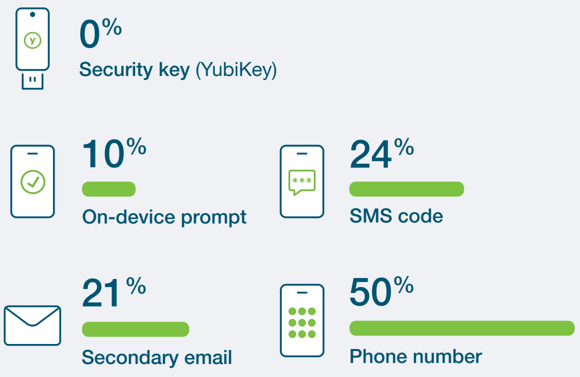
Why mobile authentication puts your organization at risk

While any form of MFA offers better security than legacy username and password based authentication, not all forms of MFA are created equal. In fact, mobile-based MFA such as SMS, OTP, and push notifications are highly susceptible to phishing attacks, man-in-the-middle (MiTM) attacks, malware, SIM swapping, and account takeovers.

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.[2] The research found that a SMS-based one-time password (OTP) only blocked 76% of targeted attacks and a push app only blocked 90%. That's a 10% penetration rate at minimum. With this approach, it's not a matter of if you will be attacked—it's a matter of when.

On top of weaker security, mobile authenticators also don't offer an easy user experience. When 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. And, all of this depends on the availability of cellular connectivity, the phone being sufficiently charged, and other nuances that can affect the user experience. This adds to the time and complexity of authentication and reduces employee productivity, all while leaving the organization exposed.

Risk of account takeovers



What is phishing-resistant MFA?

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

[1] IBM, Cost of a data breach report 2022

[2] Kurt Thomas and Angelika Moscicki, New research: how effective is basic account hygiene at preventing hijacking, (May 17, 2019)

Mobile authentication also creates gaps in your MFA framework

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. Not only can there be low cell coverage in certain geographic areas, employees also may not 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. If the fall back option is usernames and passwords, this makes the organization even more vulnerable to phishing and account takeovers.

As organizations move into the new way of working, where remote and hybrid work is the norm, relying on perimeter security is no longer effective. Organizations using mobile-based authenticators today need to reevaluate their long-term MFA strategy and consider moving to modern phishing-resistant MFA solutions. In these scenarios, a hardware security key provides organizations with broad coverage of business scenarios and user groups while ensuring the best security and user experience.

Building a secure, long-term MFA strategy

In order to make your organization highly phishing resistant, user accounts should be secured with strong 2FA or MFA that uses purpose-built hardware security keys to secure user access with the strongest levels of phishing defense, along with providing the best user experience. With hardware security keys supporting modern authentication protocols, users can register one single security key to hundreds of services with a unique public/private key pair generated for each service. The secrets are never shared between services, and the private key is stored in the secure element on the hardware key and cannot be exfiltrated. Additionally, hardware security keys require the user to tap or touch a button for authentication to prove user presence. In this manner hardware security keys stop remote, MiTM, and phishing attacks, so unlike SMS or any mobile app authentication, only the registered service is allowed to initiate the authentication request.

Organizations also have to account for new and updated regulations expected over the next few years, especially in the wake of COVID-19. While mobile authentication might be considered 'good enough' today, it may not meet future MFA compliance standards. 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.

YubiKeys offer modern phishing-resistant authentication at scale, and a bridge to passwordless

The YubiKey from Yubico is a hardware security key that is purpose-built for high security and designed to stop phishing and other forms of account takeover in their tracks, delivering strong authentication at great scale. It's the only solution proven by independent researchers to stop 100% of account takeovers, including bulk and targeted phishing attacks.[3]

Yubikeys offer a modern strong MFA solution designed to meet organizations' needs for office workers, privileged users, remote or hybrid workforces, mobile restricted environments, shared workstations, third party entities/supply chain, and even end customers. A single YubiKey works seamlessly across legacy and modern systems and applications with multi-protocol support for SmartCard(PIV), OTP, OpenPGP, FIDO U2F, and FIDO2/WebAuthn. And, for organizations looking to begin their journey to passwordless, the YubiKey offers a bridge from where organizations are today to a modern passwordless future without a rip and replace.

Set your organization up with a future-proofed security investment that not only offers strong security but can help you navigate the evolving compliance landscape. The most security conscious and high risk organizations in the world trust the YubiKey for strong phishing-resistant two-factor, multi-factor, and passwordless authentication.

	Mobile Authentication	YubiKey
Phishing resistant	–	✓
Always secure	–	✓
Cost effective	–	✓
User friendly	–	✓
360° coverage	–	✓
Future proof	–	✓

The YubiKey 5 Series

Contact us
yubi.co/contact

Learn more
yubi.co/mfa

[3] Kurt Thomas and Angelika Moscicki, New research: how effective is basic account hygiene at preventing hijacking, (May 17, 2019)

About Yubico As the inventor of the YubiKey, Yubico makes secure login easy. As a leader in setting global standards for secure access to computers, mobile devices, and more, Yubico is also a creator and core contributor to the FIDO2, WebAuthn, and FIDO Universal 2nd Factor (U2F), and open authentication standards. For more information, please visit: www.yubico.com.