yubico

Why your one time password (OTP) legacy MFA is setting you up for a security breach

We're at a crisis point for cybersecurity. During the COVID health crisis, cyberattacks shot up 300%.[1] The average cost of a data breach reached an all-time high in 2022, ringing up at a whopping $4.35M.[2] Ransomware, which often starts with malicious actors stealing user credentials and logging into corporate systems, is on the rise and damages are expected to exceed $30 billion worldwide in 2023.[3]

Legacy MFA exposes organizations to security risks

Despite the growing tide and sophistication of cyber attacks based on credential compromise, and the legacy MFA fatigue users have faced, many organizations have continued to use these outdated and ineffective methods involving one-time passwords (OTPs), SMS and mobile authentication apps, all of which are easily circumvented by modern cyber threats. In fact in the latter half of 2022, several global organizations were successfully breached, costing them their reputation and customers. 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.

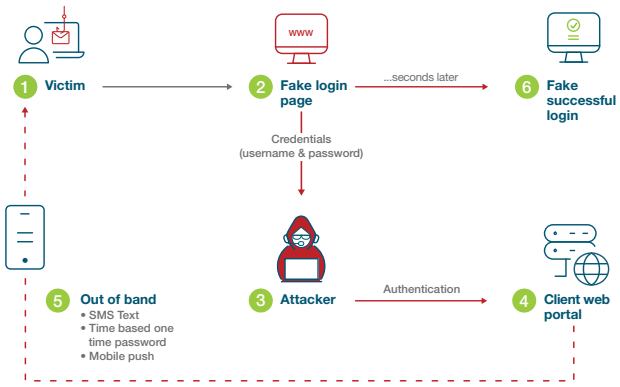

Figure 1: Legacy MFA is defeated by phishing scams as the attacker can easily intercept the SMS text

How modern, phishing-resistant MFA protects effectively against modern cyber threats

Phishing-resistant MFA is an authentication process that is immune to attackers intercepting or even tricking users into revealing access information. Credentials are specific to a particular website and removes reliance on users to visually assess if the site is legitimate. In other words, passwords, one-time passcodes, security questions and push notifications are not considered phishing-resistant. The only authentication solutions that are truly phishing-resistant—as defined by recent compliance mandates[4]—are based on FIDO2/ WebAuthn and Smart card/PIV authentication protocols.

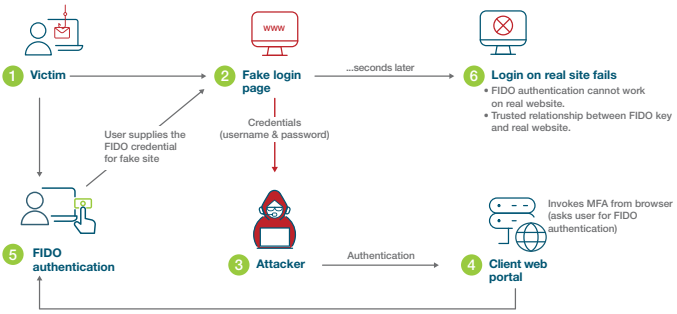

Figure 2: Modern MFA stops phishing by establishing a trusted relationship between the security key and the real website

Real world results prove FIDO security keys stop 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.[5] 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.

YubiKeys deployed in:

- **9 of the top 10** global technology companies
- **4 of the top 10** U.S. banks
- **5 of the top 10** global retailers

Research by Google, NYU, and UCSD based on 350,000 real-world hijacking attempts. Results displayed are for targeted attacks.

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, based on modern authentication protocols such as FIDO/WebAuthn, to secure user access with the strongest levels of phishing defense along with providing the best user experience. When the user registers their security key with a legitimate website/URL, the key is bound to that web portal origin, so even if the user is fooled by a phishing email pointing to a fake website, the security key is never fooled.

YubiKeys offer 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.[6] A recent Forrester Consulting Total Economic Impact™ study of five enterprises indicated that the composite organization experienced 203% ROI over three years, reduced credential theft risk by 99.9% and reduced password-related helpdesk tickets by 75%.

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

Yubikeys offer a modern strong MFA solution designed to meet organizations' security 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.

Users can register one single YubiKey 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.

Summary

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. For strong phishing-resistant two-factor, multi-factor, and passwordless authentication at scale, the most security conscious and high risk organizations in the world trust the YubiKey.

Forrester Consulting Total Economic Impact™

A recent study of five enterprises indicated that the composite organization experienced:

203% ROI over three years

99.9% reduction in credential theft risk

75% reduction in password-related helpdesk tickets

[1] FBI Sees Cybercrime Reports Increase Fourfold During COVID-19 Outbreak, April 2020
[2] IBM Security, Cost of a Data Breach Report, July 2022
[3] Infosecurity magazine, August 2022
[4] U.S. White House Office of Management and Budget (OMB) Memo 22-09
[5,6] New research: How effective is basic account hygiene at preventing hijacking, May 2019

Yubico AB
Kungsgatan 44
2nd floor
SE-111 35 Stockholm
Sweden

Yubico Inc.
5201 Great America Pkwy, #122
Santa Clara, CA 95054, USA
844-205-6787 (toll free)
650-285-0088