yubico

Securing financial services with modern, phishing-resistant MFA

The financial services industry is constantly under cyber attack

The financial services industry is highly targeted by cyber attackers, with the cost of a data breach across financial services averaging $5.90 million.[1] Financial services organizations face cybersecurity challenges on two fronts—on the workforce side they face identity phishing threats against employees, while commercial and retail banking customers face account takeover threats related to online and mobile banking.

Not all MFA is created equal

The financial services industry was an early adopter of mobile- based authentication such as SMS, OTP, and push notifications, but while any form of multi-factor authentication (MFA) is better than a password alone, not all MFA is created equal. Passwords are easily breached and MFA in the form of security questions, SMS codes, OTP, and push notifications are susceptible to phishing attacks, SIM swaps, and attacker-in-the-middle attacks. Mobile-based authenticators also don't offer the best user experience.

Phishing-resistant MFA can be a powerful first line of defense for financial services organizations—whether protecting organizational or customer assets.

What is phishing-resistant MFA?

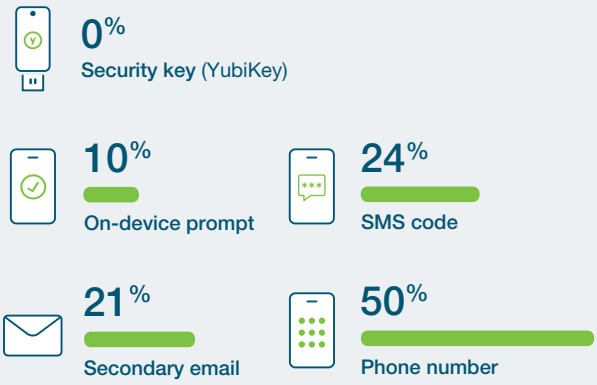
Phishing-resistant MFA processes rely on cryptographic verification between devices or between the device and a domain, making them immune to attempts to compromise or subvert the authentication process. According to the National Instituteof Standards and Technology (NIST) Special Publication (SP) 800-63, only two forms of authentication currently meet the mark for phishing-resistant MFA: PIV/Smart Card and the modern FIDO2/WebAuthn authentication standard.

Modern, phishing-resistant multi-factor and passwordless authentication with the YubiKey

To reduce enterprise-wide identity phishing and customer-facing account takeovers, Yubico offers the YubiKey, for strong and simple multi-factor and passwordless authentication.

YubiKeys are proven to offer the highest levels of security against account takeovers in independent research, preventing targeted attacks along with a 203% return on investment (ROI).[2]

Risk of account takeovers



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

YubiKeys are highly suitable for remote and hybrid workers, office workers, mobile-restricted areas, shared workstations and devices, customer-facing digital services, and for users that can't, won't, or don't use mobile authentication. They are simple to deploy and use—a single YubiKey can be used across legacy and modern applications, services, and devices, with multi-protocol support for Smart Card, OTP, OpenPGP, FIDO U2F and FIDO2/WebAuthn on a single key, offering a bridge to modern passwordless authentication.

YubiKeys are also FIPS 140-2 validated to NIST SP 800-63B Authenticator Assurance Level 3 (AAL3), and ensure compliance to SOX, PCI DSS 4.0, PSD2, GDPR and CFP Circular 2022-04.

Common use cases the YubiKey solves for the financial sector

1. Secure remote and hybrid workers

Phishing-resistant MFA should be one of the top requirements for remote and hybrid work policies. YubiKeys provide highest-assurance MFA, and are easily integrated into existing systems and infrastructure including identity and access management systems such as Microsoft, Okta, Duo, Ping and Hypr. With the YubiKey, financial services organizations can ensure remote and hybrid workers have secure access to computers, VPN, and password managers—no matter where they work. YubiKeys can even be used to securely generate one-time time-based passcodes.

2. Secure high-risk, high-value transactions

Employees that perform high-risk, high-value transactions on a daily basis are often the target of cybercriminals. Access to high-risk systems can be strengthened by requiring strong and modern MFA using YubiKeys, ensuring only authorized account access and authorized high-value transactions.

3. Secure privileged users

Privileged users are prime targets for cybercriminals as they have greater access to sensitive company and customer information. Financial services organizations can strengthen privileged access management and stop targeted attacks by ensuring that authentication security best practices are followed by requiring privileged users to authenticate with phishing-resistant hardware security keys such as the YubiKey.

4. Secure call center workers

With high employee churn, seasonal peaks, and other challenging business dynamics, call center environments need a secure, yet simple approach to verify agent identities before providing access to critical systems and data. YubiKeys offer strong security that can securely verify the identity of call center agents before they are given access to PII and other sensitive data, or make any changes to a customer account, such as raising a credit limit. And unlike mobile phones that can capture images of customer and financial data, YubiKeys offer a secure and compliant authentication solution.

5. Secure shared workstations/terminals

Employees who work on shared workstations and devices are common in banks and call centers. Tellers move from one station to another and supervisors move to authorize transactions. Users in these environments are often part-time employees with higher turnover and may have minimal commitment to the organization, creating insider threat risks. The YubiKey ensures strong authentication across shared access terminals and shared workstations and devices to help prevent unauthorized access to high-value systems and resources.

6. Secure high net-worth customers

Compared to username and passwords, SMS, and OTP codes, YubiKeys offer the strongest security to protect commercial banking clients and online and mobile banking accounts of high net-worth clients against account takeovers. Providing customers with easy to use strong authentication can help financial services organizations drive new customer acquisition and help with customer retention. Integrating support for YubiKeys into online and mobile banking is simple. Financial services organizations such as Vanguard, Morgan Stanley and KeyBank offer client-facing strong authentication solutions with support for FIDO hardware security keys.

Easily procure and distribute YubiKey authentication solutions at scale

Yubico offers flexible and cost-effective enterprise plans that help organizations with 500 users or more move away from legacy and broken MFA and accelerate towards phishing-resistant authentication at scale.

With YubiEnterprise Subscription, organizations can benefit from a predictable OPEX model, the flexibility to meet user preferences with choice of any YubiKey, upgrades to the latest YubiKeys, and faster rollouts with easy access to Deployment Services, Priority Support and a dedicated Customer Success Manager.

Subscription customers are also eligible to purchase additional services and product offerings, such as YubiEnterprise Delivery, a global turnkey hardware key distribution service through Yubico and trusted partners to residential and office locations across 49 countries.

Trusted authentication leader

Yubico is the principal inventor of the WebAuthn/FIDO2 and U2F authentication standards adopted by the FIDO alliance and is the first company to produce the U2F security key and a multi-protocol FIDO2 authenticator.

YubiKeys are produced in the USA and Sweden, maintaining security and quality control over the entire manufacturing process.

The YubiKey 5 Series

From left to right: YubiKey 5C NFC, YubiKey 5 NFC, YubiKey 5Ci, YubiKey 5C, YubiKey 5 Nano and YubiKey 5C Nano

Contact us
yubi.co/contact

Learn more
yubi.co/finance

[1] IBM Cost of a Data Breach Report 2023

[2] Forrester, The Total Economic Impact of Yubico YubiKeys

Yubico (Nasdaq First North Growth Market Stockholm: YUBICO) is the inventor of the YubiKey, the gold standard in phishing-resistant multi-factor authentication (MFA), and a creator and contributor to FIDO open authentication standards. The company is a pioneer in delivering hardware-based passkey authentication to customers in 160+ countries. For more information, visit: www.yubico.com.