Keeping financial services organizations ahead of modern cyber threats

Stop account takeovers and ensure business continuity with modern phishing-resistant authentication

Cyber pressure keeps growing

Cyber criminals are increasing their attacks—both in quantity and sophistication—on financial services organizations such as banking, insurance, fintech, payment services and others. Modern attacks such as QR-code phishing and AI-driven phishing are rising in prevalence. At the same time, tighter security regulations and tougher scrutiny from regulators and cyber insurance providers is driving financial services organizations to execute the modern phishing-resistant cybersecurity strategies.

$6.08 million

The global average cost of a data breach in the financial services industry in 2024

Source

40%

of financial services cyber attacks disrupt key business processes

Source

over 26%

Financial services professionals' global click rate in phishing emails, making them the second-most likely to open a phishing email

Source

44%

of breaches were driven by ransomware in 2024, up from 32% in 2023

Source

23%

of ransomware attacks on financial services organizations were due to compromised credentials

Source

Phishing-resistant authentication is critical for every user

Across financial services, account lockouts due to credential theft or even user error can have major downtime and revenue implications. To secure user accounts, while any MFA is better than a username and password alone, not all MFA is created equal. Legacy mobile-based authentication such as SMS, OTP and push notification apps are not phishing resistant and create costly downtime risk for organizations. According to the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63-B4, only two forms of authentication currently meet the mark for phishing-resistant MFA: Smart Card/PIV and FIDO2/WebAuthn. Additionally, any MFA solution where users are unable to perform self-service password resets themselves can create an IT bottleneck and lower productivity.

It is critical that phishing-resistant MFA be the first line of defense for every financial services organization, with a comprehensive strategy that includes:

Privileged users
IT admins, C-suite, finance, HR

Remote workers

Office workers

Shared workstations
Bank tellers, call center employees

High-risk transitions

Commercial and retail banking customers

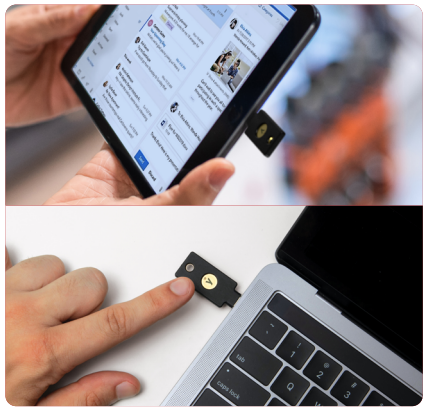
yubico

Stop account takeovers, maximize business continuity and go passwordless with the phishing-resistant YubiKey

Modern security for the modern enterprise

The YubiKey is a modern hardware security key that offers phishing-resistant multi-factor and passwordless authentication and is highly suitable for banking, fintech, insurance, payment services and other financial organizations to secure privileged users, office workers, remote employees, call center employees, shared workstations and devices, and even for securing customer-facing digital services.

With the YubiKey for modern authentication, financial services organizations can drive business continuity and satisfy cyber insurance and regulatory requirements, all while ensuring the best security and user experience for employees and end-customers alike.



Why choose the YubiKey for phishing-resistant authentication?

- Reduce risk of credential theft by 99.9% and stops account take-overs while delivering 203% ROI
  Source
- Reduce help desk costs by up to 75% with self-service password resets
  Source
- Help lower cyber insurance premiums by 30%
  Source
- Provide secure user access at scale on any device with the best user experience
- Bridge to modern passwordless with multi-protocol support for Smart Card/PIV, FIDO2/ WebAuthn, FIDO U2F, OTP and OpenPGP on a single key
- Deploy the most secure passkey strategy: device-bound that is purpose-built for security, FIPS 140-2 validated and Authenticator Assurance Level 3 (AAL3) compliant. YubiKeys also offer highest-assurance security compared to built-in platform authenticators that may have vulnerable TPM firmware
- Drive regulatory compliance to FFIEC, GDPR, SOX, SOC2, PCI DSS 4.0, GLBA, PSD2, eIDAS, CFPB Circular 2022-04
- Drive secure bootstrapping for new user devices—company owned or BYOD

Yubico (Nasdaq 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 passwordless authentication using thhighest assurance passkeys to customers in 160+ countries. For more information, visit: www.yubico.com

Learn more in our white paper
yubi.co/wp-finserv

Contact us
yubi.co/contact

yubico