yubico

Transforming insurance organizations into phishing-resistant enterprises

Legacy authentication is putting insurers at risk

The average cost of a data breach across the financial services industry is USD $5.90 million[1], but for commercial and retail insurance providers that hold millions of sensitive PII and PHI customer records, the cost can be much higher. Many insurance firms become targets of class-action lawsuits for failure to protect and safeguard customer data[2] because they rely on weak forms of authentication to secure access to critical applications and data.

Usernames and passwords are easily hacked and while multi-factor authentication (MFA) can be a strong first-line of defense, **not all forms of MFA are created equal**. Legacy mobile-based authentication such as SMS, OTP codes, and push notification apps are highly susceptible to phishing attacks, malware, SIM swaps, and attacker-in-the-middle attacks. They also create MFA gaps across mobile-restricted areas such as call centers, require mobile reimbursement costs, and decrease productivity related to broken screens, low battery and low cell connectivity. Mobile authentications also don't offer the best user experience and can increase help desk costs related to account lockouts.

To stay protected against modern cyber threats including the latest AI-driven phishing attacks, insurance organizations require modern authentication security that ensures every user is phishing resistant while delivering the best user experience.

Insurance organizations must also recognize that solutions such as phishing prevention and awareness training, while valuable, are not sufficient to fully address the threat of phishing. It is essential that users remain phishing-resistant throughout the entire lifecycle of their accounts. This entails implementing phishing-resistant measures not only in authentication but also in registration and recovery processes.

"Starting on November 1, 2025, a Covered Entity will be required to use MFA for any individual accessing any Information Systems of the Covered Entity, regardless of location, type of user, and type of information contained on the information system being accessed."

New York Department of Financial Services
23 NYCRR 500, Nov. 2023

The YubiKey offers modern security for the modern business

Yubico offers the YubiKey—a FIPS 140-2 validated hardware security key for phishing-resistant MFA and passwordless authentication at scale. It is the only solution proven to completely eliminate account takeovers in independent research including bulk and targeted attacks.[3]

Risk of account takeovers

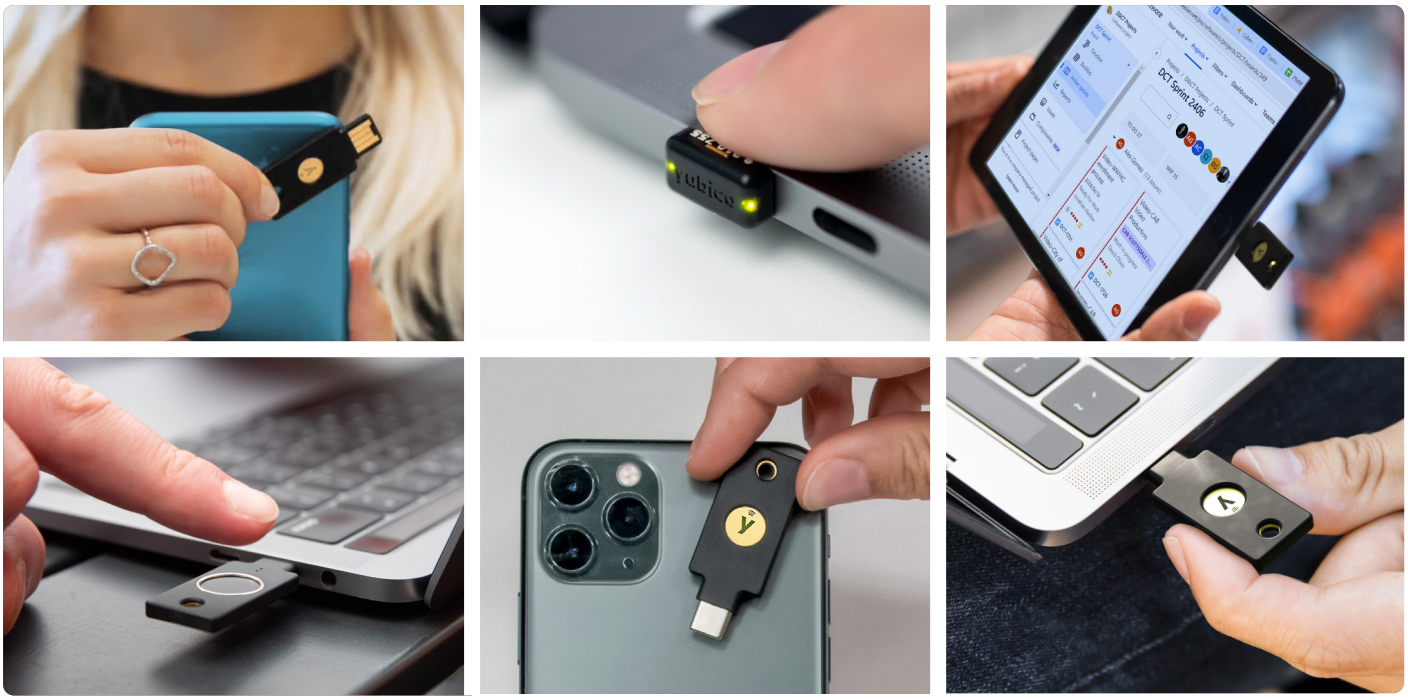
- 0% Security key (YubiKey)
- 10% On-device prompt
- 24% SMS code
- 21% Secondary email
- 50% Phone number

The combination of frictionless user experience, data breach prevention, mobile device and service cost savings, and the YubiKeys' versatility providing multi-protocol support results in high ROI for any environment. YubiKeys also enable self-service password resets, eliminating IT support costs related to help desk password-reset requests.

YubiKeys integrate seamlessly with existing identity and access management (IAM) and identity provider (IDP) solutions such as Microsoft, Okta, Hypr, GreenRocket, Duo, ForgeRock, and over 1,000 applications and services out-of-the-box with multi-protocol support for SmartCard (PIV), OTP, FIDO U2F, FIDO2/WebAuthn and OpenPGP, helping bridge to a modern passwordless future without a rip and replace.

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



YubiKeys are highly suitable for office workers as well as remote and hybrid employees and agent networks. A single YubiKey works across desktops, laptops, mobile, tablets, and notebooks, enabling users to utilize the same key as they navigate between devices. YubiKeys are also easily re-programmed, making them suitable for rotating-shift and temporary workers.

The total economic impact of YubiKeys[3]

Strongest Security
Reduce risk by
99.9%

High Return
Experience ROI of
203%

More Value
Reduce support tickets by
75%

Faster
Decrease time to authenticate by
>4x

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.

Once ready to purchase, Yubico is focused on helping insurance organizations easily access security products and services in a flexible and cost-effective way to heighten security across the employee base and agent network:

- With YubiEnterprise Subscription, organizations receive a service-based and affordable model for purchasing YubiKeys in a way that meets technology and budget requirements, providing priority customer support, easy form factor selection, backup key discounts, and replacement stock benefits
- With YubiEnterprise Delivery, organizations receive turnkey service with shipping—serving both domestic and international locations including residential addresses, tracking, inventory management, and returns of Yubico products—all securely handled by logistics experts.

Contact us
yubi.co/contact

Learn more
yubi.co/insurance

[1] IBM, Cost of a Data Breach Report 2023

[2] Class Actions Filed Over Builders Mutual, Progressive's Own Data Breaches, Jan 2024

[3] Kurt Thomas and Angelika Moscicki, New research: How effective is basic account hygiene at preventing hijacking

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.