yubico

Protecting healthcare by cultivating phishing-resistant users

Organizations across the Healthcare and Public Health (HPH) sector are facing a growing rate of cyber attacks. With the average cost of a data breach being USD $4.88 million,[1] the highest across any industry since 2011, fundamental changes are required across the healthcare ecosystem to ensure both confidentiality and safety of patient data and compliance to cyber insurance mandates and government regulations.

Prioritizing the human layer

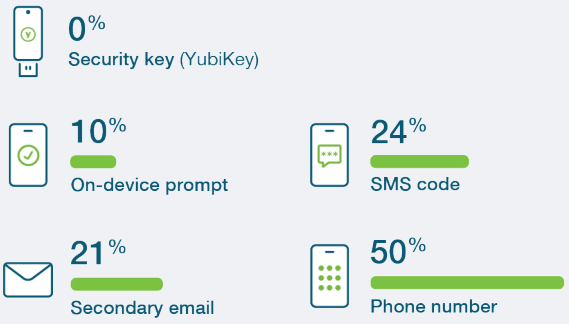
Legacy authentication including username and passwords, and mobile-based authenticators such as SMS, OTP, and push notification, are leaving healthcare organizations exposed to modern cyber threats. Usernames and passwords are easily hacked, and mobile-based authenticators are highly susceptible to phishing attacks, account takeovers, SIM swaps and man-in-the-middle (MitM) attacks. SMS, OTP, and push notification apps also don't provide the best user experience.

Prioritizing the human layer is about challenging the drawbacks of conventional MFA and removing security responsibilities from your users, by eliminating passwords completely and moving to passwordless authentication.

Accelerating passwordless and cultivating phishing-resistant users with the YubiKey

The YubiKey from Yubico provides strong phishing-resistant two-factor, multi-factor, and passwordless authentication at scale. The hardware authenticator protects the private secrets on a secure element that cannot be easily exfiltrated, preventing remote attacks. YubiKeys are the only solution proven to stop 100% of account takeovers in independent research,[2] and are deployed across various healthcare organizations including health plans and payers, health technology organizations, healthcare delivery organizations, and pharmacies to help them stay protected against modern cyber threats.

Risk of account takeovers



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

The YubiKey offers multi-protocol support enabling modern, strong authentication across legacy and modern applications and systems with support for FIDO2, FIDO U2F, OTP, Smart Card, and OpenPGP authentication protocols.

YubiKeys require no software installation, battery, or cellular connection, making them ideal for mobile-restricted environments and shared workstation environments that are common across healthcare ecosystems. A user can simply insert the YubiKey into a USB port and touch the key to authenticate.

YubiKeys also support tap-and-go authentication using NFC. When combined with a silicone wristband, the YubiKey can solve critical pain points around sanitation and efficiency.

For regulated healthcare environments, YubiKeys are also available in FIPS 140-2 validated form factors that meet the highest authenticator assurance level 3 (AAL3) requirements from NIST SP 800-63B.

With the YubiKey, healthcare organizations can implement FIDO2 passwordless, Smart Card passwordless, or a hybrid strategy depending on the infrastructure and use cases that need to be addressed.

The only effective approach to remove phishing from an organization's threat landscape is to ensure that every user within the organization becomes phishing-resistant—and that resistance must move with the users no matter how they work, across devices, platforms and systems. Deploying phishing-resistant authentication across the entire user lifecycle, including the registration, authentication and recovery processes, is what creates a phishing-resistant user.

Easily procure and distribute YubiKey authentication solutions at scale

Yubico helps organizations easily procure and distribute YubiKeys to employees wherever they work, anywhere in the world—at the office, in the hospital or lab, or even at home.

With YubiKey as a Service, organizations receive a service-based and affordable model for purchasing YubiKeys. This enables healthcare organizations to rapidly procure the latest YubiKeys in a way that meets their technology and budget requirements. This service also makes it easy to choose form factors, access customer support, and more.

With YubiEnterprise Delivery, or local channel partners, organizations receive turnkey service with shipping, tracking, and returns of Yubico products—all securely handled by logistics experts. It also helps with inventory management with delivery of keys as needed by the business.

Choose the trusted authentication leader

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

YubiKeys are produced in the USA and Sweden, which ensures a high level of security and quality control over the entire manufacturing process.

[1] IBM, Cost of a Data Breach Report 2024

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

> "We are taking care of people 24 hours a day, 365 days a year. It's critical that we have a reliable method to access healthcare systems anytime, anywhere. The YubiKey provides that for us"
>
> **Jonas Philipsen**
> IT Consultant, Herning Kommune

The YubiKey 5 Series

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

The YubiKey 5 FIPS Series

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

Contact us
yubi.co/contact

Learn more
yubi.co/healthcare

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 passwordless authentication using the highest assurance passkeys to customers in 160+ countries. For more information, visit: www.yubico.com.