yubico

WHITE PAPER

Protecting insurance organizations against modern cyber threats

Stop account takeovers and go passwordless by cultivating phishing-resistant users

Contents

10-24%

attack penetration rate for mobile authentication[15]

94%

organizations were victims of phishing[16]

$1 million

per year cost for password resets alone[17]

Insurance's critical need for modern, strong authentication

No industry understands risk better than insurance, but insurance companies are in a precarious position—they have a duty to act in the best interests of their policyholders, yet policyholders' trust in them is damaged every time the industry endures a cyber attack.

Insurance organizations have long relied on security tools like firewalls, antivirus software, intrusion detection systems (IDS) and intrusion prevention systems (IPS), but those are no longer effective against today's sophisticated cyber criminals. With such a rich collection of personal, medical, and corporate data gathered throughout the underwriting and claims processes, the insurance industry is a prime target for cyber attacks. In fact, CNA Financial paid $40 million, the largest disclosed ransom payment in history, after a 2021 ransomware attack.[1]

In the years since, **cyber attacks against the insurance industry have grown exponentially.**[2] Look no further than the chaos created in early 2024 when cyber criminals attacked UnitedHealthcare's Change Healthcare, which processes roughly 50% of the medical insurance claims in the U.S.[3] Not only did it cost the insurance giant over $2 billion—including a $22 million ransom payment—the weeks-long attack cost physicians an estimated $100 million per day due to downed provider payment systems, while patients suffered through delayed prescription orders and were forced to pay out of pocket for life-and-death medications.[4]

While this attack generated news headlines and official responses from the U.S. Department of Health and Human Services, the U.S. House of Representatives, and the American Medical Association, it is certainly not the only recent major attack. In 2023, a cyber attack impacted nine million clients of Managed Care of North America (MCNA) Dental.[5] New York Life Insurance Company, Prudential Insurance, Sun Life, and Genworth Financial were all victims of the MOVEit file transfer cyber attack in 2023.[6] Then in 2024, Prudential Insurance was attacked again, this time by ransomware gang AlphV.

It shows that insurance companies can benefit from an insurance policy of their own: cyber insurance.

Along with attacks, the cyber insurance market is also growing exponentially—from a global market size of $5.9 billion in 2019 to an estimated $29 billion by 2027.[7] While it can reduce costs and mitigate damages across the enterprise, cyber insurance isn't a golden ticket to peace of mind, nor should it be your only proactive line of defense. According to the U.S. Government Accountability Office, cyber insurance is limited in its ability to cover potentially catastrophic losses from systemic cyberattacks.[8]

Your organization needs a strategy to prevent cyber attacks before they happen, which is why cyber insurance providers are increasingly requiring that multi-factor authentication (MFA) be in place before they write new policies.

The insurance industry lags behind

Even though cyber insurers see the value of MFA, the insurance industry as a whole has been slow to adopt it. At the beginning of 2023, only 40% of carriers were using it.[9] In May 2024, the Oversight and Investigations Subcommittee, part of the U.S. House Committee on Energy and Commerce, released a statement condemning the lack of MFA in the Change Healthcare attack: **"The attack occurred because UnitedHealth wasn't using multifactor authentication [MFA], which is an industry standard practice, to secure one of their most critical systems."**[10]

For many insurance organizations, a stronger cybersecurity strategy isn't a choice, but rather a regulatory requirement. Health insurance companies are required to comply with HIPAA regulations because they collect protected health information (PHI) and/or electronic health information (EHI). While HIPAA is intentionally technology-neutral, and thus, doesn't explicitly mandate MFA, it does require that organizations "implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed."[11] In its Special Publication, "Implementing the HIPAA Security Rule: A Cybersecurity Resource Guide," the National Institute of Standards and Technology (NIST) recommended that HIPAA-covered entities and business associates consider MFA to ensure authentication mechanisms are protected from inappropriate manipulation.[12]

Further, any insurance organization that allows policyholders to pay their premiums via credit card must adhere to PCI regulations. PCI DSS 4.0 made MFA mandatory for all access to the cardholder data environment—whether on premises or remote—and all system components.[13]

In this whitepaper, we'll demonstrate how insurance organizations can leverage the most phishing-resistant MFA-powered cybersecurity strategies to protect against modern cyber attacks that undermine their stability and erode public confidence.

> It is important to note that not all MFA solutions provide equal protection against authentication attacks, and there are critical implementation details that can impact the security and usability of an MFA deployment."
>
> Recommended Best Practices for Administrators: Identity and Access Management, Enduring Security Framework[14]

Not all MFA is created equal

The insurance industry has a vast threat surface that includes office workers, remote workers, privileged users, call centers, brokers, and agent networks. Combine that with the ever-growing number of attacks against the industry, and insurance organizations have a clear imperative: determine which forms of MFA provide the greatest protection.

Legacy forms of MFA such as SMS, mobile authentication and one-time passcodes (OTP) are susceptible to account takeovers from phishing, attacker-in-the-middle attacks, account takeovers, and SIM swaps at a penetration rate of 10-24%.[18] In fact, the risk of SMS interception is so high that NIST called for SMS to be deprecated as a method of authentication.[19]

Other key considerations include cost, user experience, and coverage. Legacy authentication carries many hidden governance and support costs around setting and managing password policies at scale, productivity costs associated with forgotten passwords, account lockouts and time consuming workflows to generate and enter OTP/TOTP/push app codes, and of course the costs associated with risk. Moreover, there are always gaps where mobile authentication does not work or is not an option—where users lack devices, where availability or mobile-restrictions may apply, as well as spark environments, among other scenarios.

MFA investments must provide insurance organizations with protection that evolves alongside risk. To be future-proofed, the MFA investment should reflect the growing need for phishing-resistant MFA and more modern login flows such as passwordless to make it easy and seamless for the end user.

What is phishing-resistant MFA?

NIST defines phishing-resistance in Special Publication (SP) 800-63 and Draft 800-63-4[20] as "the ability of the authentication protocol to detect and prevent disclosure of authentication secrets and valid authenticator outputs to an impostor relying party without reliance on the vigilance of the subscriber."

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. Currently, two forms of authentication meet the mark for phishing-resistant MFA: **PIV/Smart Card** and the modern **FIDO2/WebAuthn** authentication standard.

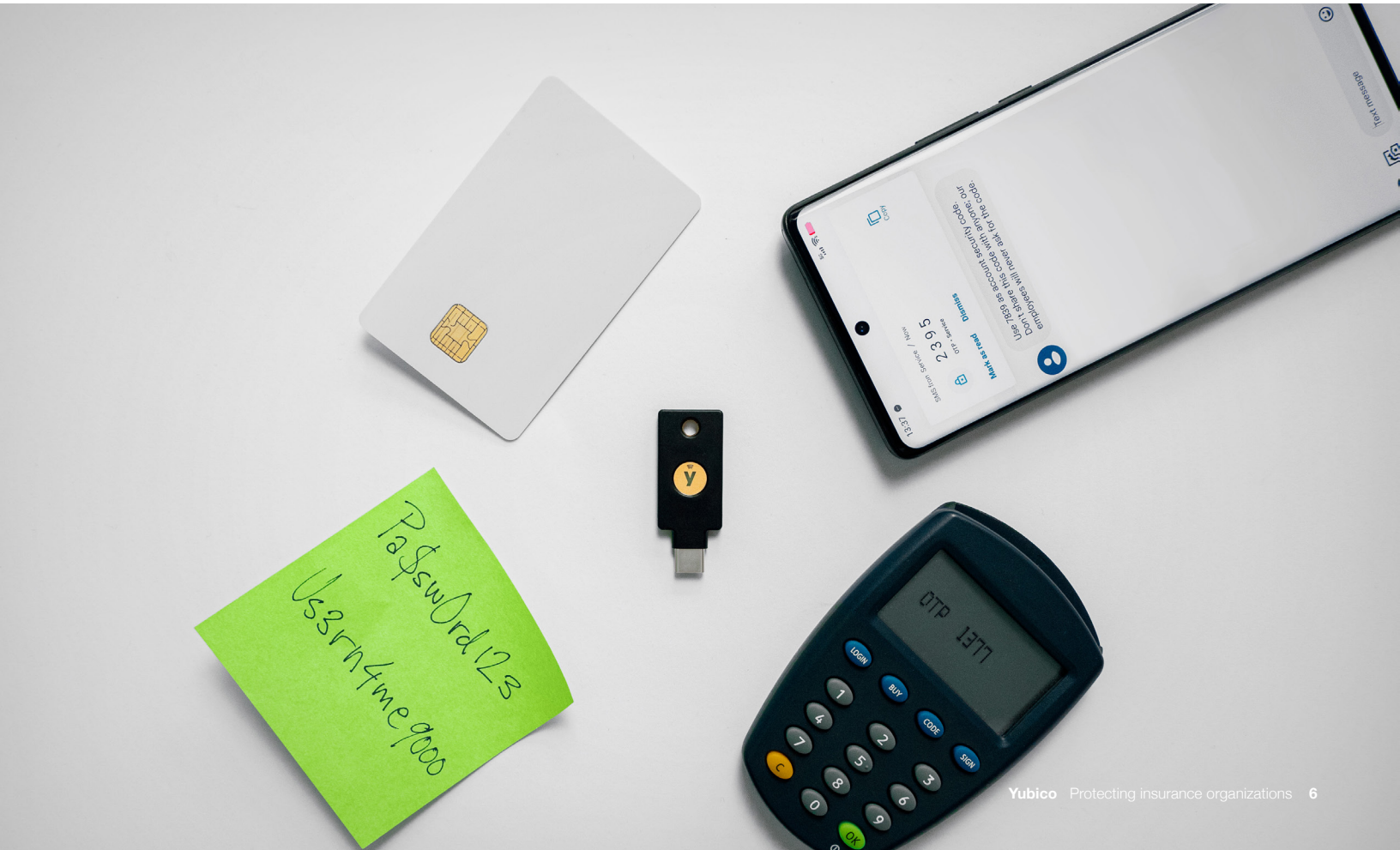
Plan for a passwordless future

Passwordless authentication is any form of authentication that doesn't require the user to provide a password, and includes Smart Card and FIDO2/WebAuthn. Going passwordless is a journey for most organizations, not necessarily an overnight change—first moving away from passwords and legacy forms of MFA, which are all highly vulnerable to phishing, and then moving to a modern MFA approach which offers strong phishing-defense. Once there, an organization is well poised to transition completely to passwordless.

Traditional Smart Cards/PIV do offer high security, but generally require high capital expenditure for smart card readers and physical cards, in addition to backend management platforms. Further, many organizations that deploy PIV face challenges around authentication where PIV is not available or practical—access to cloud services, mobile devices, air-gapped/isolated networks, contractors, partners and third-parties, just to name a few.

Due to this, many industries are moving toward a passwordless login flow leveraging modern authentication standards such as FIDO2/WebAuthn that work well with the cloud but don't necessitate a backend management system, which ultimately results in lower ongoing costs even as enterprises scale

FIDO2/WebAuthn is the most recent iteration of the FIDO standard, and uses public key cryptography for high security, where the private keys never leave the authenticator, enabling modern two-factor, multi-factor and even passwordless authentication.



The journey to phishing-resistant users

Modern organizations are moving towards the most effective phishing-resistant MFA strategy: phishing-resistant users. After all, attacks target users, and authentication starts and ends with the user.

1. **74%** of data breaches can be traced back to the human element including the use of stolen credentials, privilege misuse and phishing[21]

2. **"User carelessness"** was the most common cause of sensitive information loss in worldwide organizations in 2023[22]

Despite investments in MFA and the implementation of phishing-resistant authentication, organizations remain susceptible to phishing attacks.

3. **83%** of organizations who experienced a phishing attack in 2023 had a form of MFA in place that cyber criminals bypassed[23]

4. **Over 60%** of compromise factors come from gaps in users' credential lifecycle that attackers can exploit with relative ease[24]

For example, malicious actors can easily target enterprise users through the IT helpdesk, request a password reset and divert legitimate MFA codes to fraudulent devices such as smartphones and then access a user's email and other accounts. From there, they can infiltrate the corporate network and even install malware, setting the organization up for a ransomware attack. In this manner, even phishing-resistant MFA can be circumvented, and the organization falls out of phishing-resistance.

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.

Passkeys

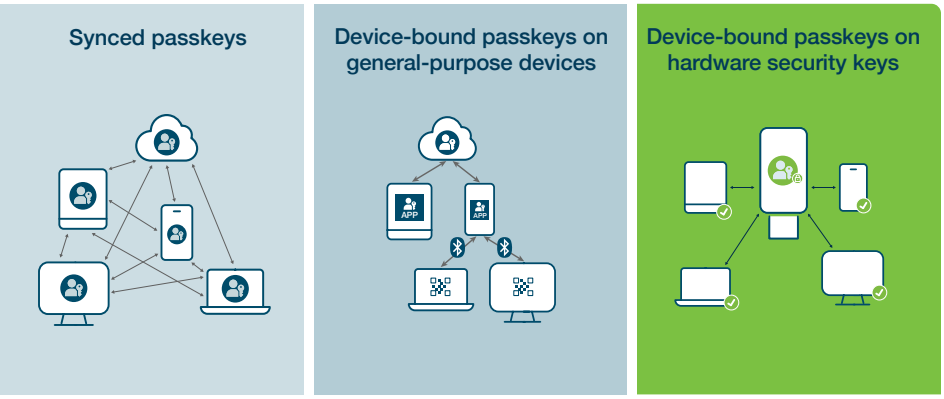
are a new name for **FIDO2 passwordless-enabled credentials**

Passkeys' role in creating phishing-resistant users

Passkeys are a new term in the industry, but the concept is not new. Passkeys are a name for FIDO2 passwordless-enabled credentials, a standard that is replacing passwords and phishable MFA logins with more secure passwordless experiences.

Synced or device-bound: What's the difference?

There are three different types of passkey implementations that you can roll out across your organization.



- **Synced passkeys** live in the cloud, which means credentials on a smartphone, tablet or laptop can be shared between devices. While synced passkeys enable easier credential recovery in the case of a lost or stolen phone or laptop, the FIDO credential is harder to track.
- **Device-bound passkeys on general purpose devices** such as smartphones, laptops and tablets offer enterprises greater control of their FIDO credentials compared to synced passkeys but are still backed by a password and offer weak security.
- **Device-bound passkeys on modern FIDO hardware security keys** highest-assurance security and provide enterprises with trusted credential lifecycle management and attestation abilities. With this passkey approach, organizations can deliver the simplest user onboarding and credential recovery experience across devices and platforms, all while staying in compliance with the most stringent requirements across regulated industries.

Modern, simple authentication for insurance organizations

Providing ultimate security to the insurance industry's myriad of threat scenarios is a critical priority, but considering the user experience is also important as this is an area in which the industry struggles as a whole. According to a recent study, customers' overall satisfaction with insurance digital experiences was lower in 2023 than in 2022.[25] Seamless experiences aren't just crucial for customers, though. They are also vital for employees to serve them properly. Adopting device-bound passkeys on modern FIDO hardware security keys **protects users across locations, devices and business units without sacrificing on security or experience.** And when users are well-protected and productive, so is the business.

The total economic impact of YubiKeys:

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

YubiKeys ensure phishing-resistant users

Yubico offers the YubiKey, a hardware security key that offers the highest-assurance, phishing-resistant MFA by supporting both FIDO2/WebAuthn and Smart Card/PIV authentication to ensure the highest protection against phishing-driven credential-based attacks.

By simply plugging a YubiKey into a laptop or tapping it against a smartphone to authenticate, YubiKeys help organizations create phishing-resistant users by using the highest-assurance passkeys in the market. The passkeys that reside in YubiKeys can be used to register the user and secure the other passkeys they use across devices and services. In other words, YubiKeys can be used to secure other forms of phishing-resistant MFA used within organizations to create phishing-resistant users, who then ultimately create phishing-resistance that can't be circumvented.

Hardware security keys such as the YubiKey are an ideal option for insurance employees both in the office and in the field because they don't require additional hardware, software, external power, batteries, or a network connection—a single key secures hundreds of products, services and applications, including leading identity and access management (IAM) platforms, privileged access management (PAM) solutions and cloud services, with the secrets never shared between services.

As a portable hardware root of trust, the YubiKey is proven to reduce risk against phishing attacks and account takeovers by 99.9% and serves as a user-friendly, cost-effective enabler of a Zero Trust security architecture. When you're ready, the YubiKey can also help bridge to modern login flows such as passwordless.

Yubico accelerates organizations' ability to create phishing-resistant users with out-of-the-box FIDO authentication. **The Yubico FIDO Pre-Reg service eliminates manual user registration,** enabling users to receive YubiKeys that are pre-registered with the organization's Identity Provider (IdP)—so organizations can seamlessly get started on the most secure form of passkey authentication for new and existing users, while reducing the burden on IT departments.

Yubico solutions meet you where you are on your cybersecurity journey, while paving the way to a modern authentication infrastructure. They're a worthwhile investment to feel confident in knowing that your data and intellectual property are secure and that you can maintain product integrity.

Deploy highest-assurance security at scale

To protect against the growing number of cyber threats, insurance organizations need a modern solution to create phishing-resistant users at scale and across a wide variety of complex authentication scenarios.

We have made it easy to safeguard your organization with the YubiKey. We offer a simple guide that details the six deployment best practices to accelerate adoption at scale, How to get started with modern phishing-resistant MFA.

Plan

Ensure readiness by clarifying use cases and user populations

Validate

Confirm the process with a small group of users before broader rollout

Integrate

Ensure key apps and services are YubiKey-ready

Launch

Distribute keys to users with turnkey delivery services or channel partners

Adopt

Drive adoption with best practice training and support

Measure

Report on security and business value impact

To remove all the guesswork out of planning, purchasing and delivery, Yubico offers YubiKey as a Service, a service-based and affordable model to simplify how organizations procure, upgrade and support YubiKeys, as well as streamlined global distribution to remote and in-office locations through YubiEnterprise Delivery and trusted channel partners.

If you want a closer partnership on any of the six steps in this plan, Yubico's Professional Services team is here to help.

Contact us
yubi.co/contact

Learn more
yubi.co/insuranceorg

Sources

1. Bloomberg, CNA Financial Paid $40 Million in Ransom After March Cyberattack (May 20, 2021)
2. Deloitte, Global Cyber Executive Briefing: Insurance
3. Gov Info Security, Change Healthcare's Breach Costs Could Reach $2.5 Billion (July 17, 2024)
4. NBC News, Patients struggle to get lifesaving medication after cyberattack on a major health care company (March 6, 2024)
5. Dark Reading, 9M Dental Patients Affected by LockBit Attack on MCNA (May 30, 2023)
6. Dark Reading, Insurance Companies Have a Lot to Lose in Cyberattacks (Oct 4, 2023)
7. Munich RE, Cyber Risks and Trends 2024 (April 4, 2024)
8. U.S. Government Accountability Office, Cyber Insurance: Action Needed to Assess Potential Federal Response to Catastrophic Attacks (June 21, 2022)
9. Property Casualty 360, The Insurance Industry Needs Multifactor Authentication Unity (July 12, 2022)
10. U.S. House of Representatives Energy & Commerce Committee, What We Learned: Change Healthcare Cyber Attack (May 3, 2024)
11. The HIPAA Journal, The HIPAA Password Requirements and the Best Way to Comply With Them (Feb 17, 2024)
12. NIST, Final SP 800-66r2, Implementing the HIPAA Security Rule: A Cybersecurity Resource Guide (Feb 14, 2024)
13. PCI Security Standards Council, PCI DSS v4.0 Resource Hub (March 31, 2022)
14. CISA and the NSA, Recommended Best Practices for Administrators: Identity and Access Management, (March 2023)
15. Kurt Thomas and Angelika Moscicki, New research: how effective is basic account hygiene at preventing hijacking (May 17, 2019)
16. Egress, Email Security Risk Report 2024, (March 2024)
17. Forrester Research, Inc, Optimize User Experience With Passwordless Authentication, (March 1, 2020)
18. Kurt Thomas and Angelika Moscicki, New research: how effective is basic account hygiene at preventing hijacking (May 17, 2019)
19. Rob Lemos, The state of two-factor authentication by text: What security pros need to know, Sept 14, 2021)
20. NIST, NIST SP 800-63-4 Digital Identity Guidelines (December 2022)
21. Verizon, 2023 Data Breach Investigations Report (June 6, 2023)
22. Statista, Most common causes of sensitive information loss in worldwide organizations in 2023
23. Egress, Must-know phishing statistics for 2024 (Jan 19, 2024)
24. Google Cloud, Threat Horizons August 2023 Threat Horizons Report
25. JD Power, Many Insurers Struggle to Deliver Seamless Digital Experience as Repair Cycle Times Rise (Dec 5, 2023)
26. Forrester, The Total Economic Impact of Yubico YubiKeys (Sep 2022)

yubico

About Yubico

Yubico (Nasdaq Stockholm: YUBICO) is the inventor of the YubiKey, a hardware security key that is the gold standard in phishing-resistant multi-factor authentication (MFA). Yubico's solutions offer organizations and users deployment expertise and operational flexibility as YubiKeys work across hundreds of consumer and enterprise applications and services.

Yubico is a creator and core contributor to the FIDO2/passkey, WebAuthn, and FIDO Universal 2nd Factor (U2F) open authentication standards, and is a pioneer in delivering hardware-based passwordless authentication using the highest assurance passkeys to customers in 160+ countries.

For more information, please visit: www.yubico.com.