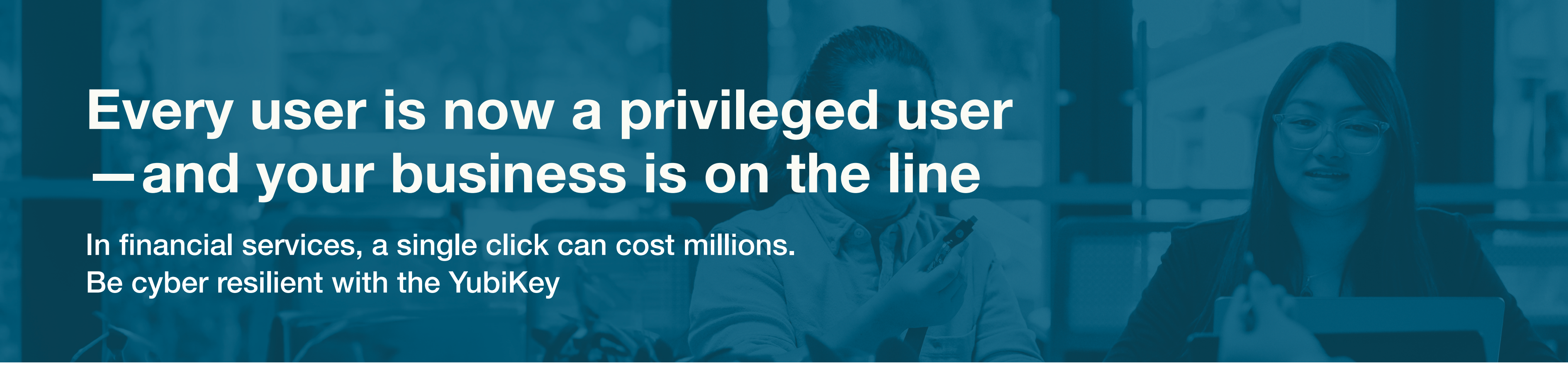

Every user is now a privileged user —and your business is on the line

In financial services, a single click can cost millions.
Be cyber resilient with the YubiKey

AI is changing the game—your definition of 'privileged users' needs to change with it.

With GenAI able to create targeted attacks at scale, financial services organizations need to expand their definition of 'privileged users' beyond the traditional IT function. Privileged users can include users across the C-suite, HR, finance, legal and customer teams that have access to company IP, and critical customer data. In reality, every user is a privileged user because once an attacker steals user credentials and infiltrates, they can easily adapt permissions and move laterally across the organization.

74% of all breaches involve the human element via error, privilege misuse, use of stolen credentials, or social engineering.[1]

80% of security breaches involve privileged credentials[2]

$5.56 million The average cost of a data breach in financial services[3]

Proactive security means phishing-resistant authentication for every user

Usernames and passwords are easily hacked, and legacy mobile-based authenticators such as SMS, OTP and push notification apps are highly susceptible to phishing attacks and account takeovers. According to the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63-4, only two forms of authentication currently meet the mark for phishing-resistant multi-factor authentication (MFA): Smart Card/PIV and FIDO2/WebAuthn.

Privileged users across the organization, whether in IT or outside of IT, need to be secured with phishing-resistant authentication. If only some user groups are secured with phishing-resistant authentication, it can create security gaps, leaving your organization vulnerable to modern cyber threats. Think of it as locking the front door of the house, but leaving the back door wide open. The safest defense? **Treat every user like a privileged user** and understand that not all MFA is created equal to protect them.

Privileged users
IT admins, C-Suite, Finance, HR

Remote & office workers

Office Workers

Shared workstations
bank tellers, call center employees

High-risk transition

Commercial and retail banking customers

An enterprise is only a truly phishing-resistant enterprise if ALL users, who are part of the attack surface, are considered "privileged users" and protected with phishing-resistant authentication. You need authentication that moves with the users no matter how they work, across devices, platforms and systems.

[1] https://www.verizon.com/business/resources/reports/dbir/
[2] Forrester Wave for Privileged Identity Management, Q4 2023
[3] https://www.ibm.com/reports/data-breach

yubico

Protect all users with the passkeys that reside in security keys

Stop phishing attacks and account takeovers

The YubiKey contains highest assurance passkeys that offer phishing-resistant multi-factor and passwordless authentication. These passkeys are immune to compromise, unlike other passkeys, and offer highly portable, user-friendly authentication, and are securely generated and stored in a hardware form factor. Attacks are getting more sophisticated with AI and while a human may be misled into inputting their credentials on a fake phishing website, the YubiKey never falls for it.

The YubiKey secures **8 out of the Top 10** largest banks around the world[7]

Why choose the YubiKey for phishing-resistant authentication?

- Reduce risk of credential theft by 99.9% and stops account takeovers while delivering 203% ROI
- Reduce help desk costs by up to 75%[5] with self-service password resets, and help lower cyber insurance premiums by 30%
- Provide secure user access at scale on any device with the best user experience
- Drive regulatory compliance to GDPR, SOX, SOC2, PCI DSS 4.0, GLBA, PSD2, NIS2, E8MM and more
- Bridge to modern passwordless with multi-protocol support for Smart Card/PIV, FIDO2/WebAuthn, FIDO U2F, OTP and OpenPGP
- Deploy the most secure passkey strategy: hardware-backed that is purpose-built for security, FIPS 140-2 validated and Authenticator Assurance Level 3 (AAL3) compliant
- Yubico and trusted partners provide services to support global distribution of YubiKeys to anyone, anywhere

[5] https://www.yubico.com/resource/tei-forrester-report/

[6] Forrester Wave for Privileged Identity Management, Q4 2023

[7] China-based banks not included

> “A security key is the ‘Gold Standard’ for authentication, something you physically have. For me, the YubiKey was the only choice. I didn’t look elsewhere.”

afni | **Brent Deterding**
CISO, Afni

Read our case study
yubi.co/Afni

Contact us
yubi.co/contact

Yubico (Nasdaq Stockholm: YUBICO) is a modern cybersecurity company on a mission to make the internet safer for everyone. As the inventor of the YubiKey, we set the gold standard for secure, simple login, stopping account takeovers with phishing-resistant, hardware-backed authentication.

Our technology secures people in over 160 countries, delivering fast, passwordless access. Dual-headquartered in Stockholm and Santa Clara, we believe strong security should be within everyone’s reach. Learn more at www.yubico.com.

yubico