Every user is a privileged user

To protect your business against modern cyber threats you need to cultivate phishing-resistant users

Expand your definition of ‘privileged users’

In today’s digital world, the idea of “privileged users” has expanded beyond the IT function to include any business users who possess access to exploitable systems or IP such as customer, HR, finance, legal, or sales data. This level of access makes any user a desirable target for credential theft, but directly attacking such users isn’t the only way cyber criminals can gain access to your critical systems. These threats can be costly and harmful to the business.

Once cyber criminals gain access to critical systems through a phishing attack or account takeover, they can move laterally within an organization. Further making the case that every user across the business is a privileged user and should be protected as such.

68%

of all breaches involve the human element via error, privilege misuse, use of stolen credentials, or social engineering.

Source

60%+

of credential issues account for compromise factors, which could be addressed by stronger identity management within the organization

Source

#1

User carelessness was the most common cause of sensitive information loss in worldwide organizations in 2023

Source

68%

of respondents in a global survey reported feeling more vulnerable to identity theft than they did a few years ago

Source

$4.9 million

is the average cost of data breaches initiated by malicious insiders, which is 9.5% higher than the USD 4.45 million cost of the average data breach

Source

Phishing-resistant users creates phishing-resistant enterprises

Deploying phishing-resistant authentication across the entire user lifecycle, including registration and recovery processes, is what creates a phishing-resistant user. 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 multi-factor authentication (MFA): Smart Card/PIV and FIDO2/WebAuthn.

If traditional IT privileged users are secured with phishing-resistant MFA but the rest of the business still relies on passwords and legacy mobile-based authentication (SMS, OTP and push notification apps), which are not phishing resistant, this leaves vulnerable gaps in the cybersecurity infrastructure. 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.

An enterprise is truly a phishing-resistant enterprise if **all** users are considered “privileged users” and protected with phishing-resistant authentication.

- **High access users** — IT and security admins, C-Suite, HR, finance, and sales
- **Remote & office workers** — across business units
- **Third party access** — contractors and freelancers
- **Shared workstations** — call center employees, consultants, retail staff, etc
- **Manufacturing and supply chain**
- **End customers**

yubico

Protect all users with phishing-resistant authentication

Stop phishing attacks and account takeovers

“Attacks are becoming privileged-based, identity-based and pretty much every report reinforces that identity is the real number one problem. As a security company, we have to practice what we preach, use all of our own products, and have very strict controls on any type of privileged access within our environment. Once the YubiKey started to be adopted, it became a very strong case for the right way to do things to protect the organization.”

BeyondTrust

Morey J. Haber, Chief Security Officer
Read our case study
yubi.co/BeyondTrust

“Return on investment in cybersecurity is a very complicated matter, but I would say the return is very good. We have a token that ensures maximum security for access to certain systems. That was the goal: we achieved it, easily and painlessly. And the product works very well.”

FLUIDRA

Ángel Uruñuela, CISO
Read our case study
yubi.co/Fluidra

The YubiKey is a purpose-built, hardware security key that fast-tracks modern enterprises to passwordless with phishing-resistant multi-factor authentication. It is the most secure and user-friendly option for protecting all users across business units; providing authentication that moves with users no matter how they work across devices, platforms and systems. 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 is never fooled.

Why choose the YubiKey for phishing-resistant authentication?

- Reduce risk of credential theft by 99.9% and stops account takeovers while delivering 203% ROI Source
- Reduce help desk costs by up to 75% with self-service password resets Source
- 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
- Support the ‘Trust nothing, verify everything’ Zero Trust approach with strong user identity and device authentication
- Help lower cyber insurance premiums by 30% Source
- 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
- Yubico and trusted partners provide services to support global distribution of YubiKeys to anyone, anywhere
- Introduce or expand use of the YubiKey in your organization to provide the strongest form of authentication

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

Contact us
yubi.co/contact

Learn more
yubi.co/privilegedusers

yubico