Supercharging telcos against modern cyber threats in an interconnected world

Secure your critical systems and customers with phishing-resistant authentication

Cyber threats are evolving

In an always-connected society, telecommunications are vital for both global communities and critical infrastructure. Because of the crucial services they provide, telcos have become an enticing target for cyber criminals looking to cause mass disruption to public life and safety. Cyber attacks such as ransomware, AI-driven phishing, MiTM attacks, and SIM swapping continue to create widespread damage for telcos. Not only can these attacks expose sensitive data, disrupt critical services, and enable malicious actors to spy on network transmissions, they also damage brand reputation and customer loyalty.

30%+ of communications service providers reported that they had experienced eight or more breaches in the past year
Source

750 million users had their data leaked in a single attack on India's Department of Telecommunications at the start of 2024–accounts for 85% of the country's population
Source

74 million U.S. telecommunications customers had their data leaked on the dark web in Q1 of 2023 alone
Source

53% of global telcos believed the cost of cybersecurity breaches to their organization would exceed $3 million in 2023
Source

21% of telco-focused ransomware attacks in 2023 targeted Europe-based companies
Source

68% of breaches involved a human element in 2024
Source

Phishing-resistant authentication is a must-have for telecommunications providers

Cyber criminals aren't breaking in; they're logging in using stolen credentials obtained through phishing. Passwords are inherently weak and easily stolen, and while any form of multi-factor authentication (MFA) will offer better security, not all MFA is created equal. Basic or legacy forms of MFA can be easily bypassed by malicious actors and create costly downtime risk for organizations.

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 MFA: Smart Card/PIV and FIDO2/WebAuthn.

It is critical that phishing-resistant authentication be the first line of defense for every global telco organization, with a comprehensive strategy that includes:

- **Privileged users**
  Engineers, IT and security admins, C-Suite, HR, finance, and sales
- **Remote staff, office workers, & field technicians**
- **Shared workstations**
  Call center employees
- **Retail environments**
  Shared devices or point-of-sale (POS) systems
- **Manufacturing and supply chain**
  Internal users, third parties & contractors
- **Customer accounts and loyalty programs**

yubico

Stop account takeovers, maximize business continuity, go passwordless, and cultivate phishing-resistant users with the YubiKey

Modern security for the modern enterprise

The YubiKey is a modern hardware security key that offers phishing-resistant multi-factor and passwordless authentication that enables telecommunications organizations to secure the critical systems used to support voice and data services including wired and wireless phone, satellite, cable and Internet services. Where people can't, won't, or don't use mobile phones, YubiKeys provide always-on phishing-resistant authentication, even when servicing remote locations.

With the YubiKey for modern authentication, telcos can drive business continuity and cyber resilience, satisfy cyber insurance and regulatory requirements, all while ensuring the best security and user experience for employees and end-customers alike.

It is the most secure and user-friendly option for protecting all users across business units; providing phishing-resistant authentication that moves with users no matter how they work across devices, platforms and systems and across the entire user lifecycle.

> "Instead of YubiKey being a highly recommended solution for our clients, we're moving towards making it a required solution. We are building it into our hosting suite, and into our user fees."

Dustin Morse
Business Operations Manager | Retail Control Systems
Read the case study yubi.co/RCS

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
- Help lower cyber insurance premiums by 30% Source
- Provide secure user access at scale on any device with the best user experience
- Does not need battery or cellular connectivity to function
- Cultivate phishing-resistant users and a phishing-resistant enterprise
- 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
- Drive regulatory compliance to GDPR, CCPA, FedRAMP, TSA, BSI-KritisV, E8MM, SOCI Act, NIS2 Directive, SOX, SOC2, PCI DSS 4.0.1, PSD2, eIDAS

Contact us
yubi.co/contact

Learn more in our white paper:
yubi.co/wp-telco

Yubico (Nasdaq Stockholm: YUBICO) is the inventor of the YubiKey, the gold standard in phishing-resistant multi-factor authentication (MFA). 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

yubico