yubico

Phishing-resistant MFA for Telecoms

Modern security with the YubiKey to bolster existing security approaches

The critical need for modern security

In an always-connected society, telecommunication organizations are a critical infrastructure that consumers and businesses heavily rely upon. Due to the crucial services they provide, telcos have become an enticing target for ransomware, phishing, man-in-the-middle (MitM) attacks, SIM swapping and the rise of AI enables malicious actors to craft convincing attacks at scale. The telco industry continues to face a rapidly evolving threat landscape, with cyberattacks often targeting the confidentiality of customer data and the availability and integrity of telecommunications services[1].

To protect against the ever-evolving sophistication of cyber attacks, strong multi-factor authentication (MFA) needs to be a foundational part of your holistic cybersecurity strategy. However, not all MFA is created equal. Legacy authentication such as usernames and passwords can be easily hacked. In addition to quality of security, it's also important to consider usability, portability, and scalability of authentication solutions. Without that, it can result in MFA gaps, low user adoption, and an increased risk of being breached.

Modern security with the YubiKey

Yubico offers the YubiKey—a hardware security key that contains the highest-assurance passkey, for phishing-resistant two-factor (2FA), multi-factor authentication (MFA), and passwordless authentication at scale.

This modern security solution can bolster existing security approaches—if you are using mobile-based MFA, it can be complemented with the YubiKey.

Safeguard people, technology, and data using the YubiKey

YubiKeys are the only solution proven to stop 100% of account takeovers in independent research[2], and are deployed across various telecom organizations to help them stay protected against modern cyber threats by securing their employees and customers, while driving regulatory compliance.

The YubiKey covers a broad range of business scenarios while ensuring the best security and user experience. It also enables self-service password resets which significantly reduces IT support costs. The YubiKey is simple to deploy and use—a single YubiKey can be used across both legacy and modern applications, services and devices, with multi-protocol support for Smart Card/PIV, OTP, OpenPGP, FIDO U2F and FIDO2/WebAuthn on a single key.

Here are five ways the YubiKey strengthens cybersecurity and business continuity for telecoms:

1. Secure access to critical systems and data for your broad user base

Strengthening security for your in-office or remote knowledge workers and executives, or in-store employees and their accounts, is the first critical step towards a modern, strong authentication journey. Securing employee access to critical systems, applications, and both employee and customer Personal Identifiable Information (PII) without interrupting productivity is crucial to staying protected from modern cyber threats. YubiKeys ensure that only authorized people have access to PII data and critical systems. They integrate seamlessly with existing IAM solutions such as Microsoft, Okta, Duo, and Ping, and provide secure authentication for thousands of applications and services, eliminating any rip or replace of existing solutions. Users get protected in minutes right out-of-the-box.

> "Once we had our YubiKeys in hand we were able to get them up and running across the company in less than three months, and we've seen the positive results after just one year of having them. That progress is even more important in today's environment where bad actors continue to wage sophisticated campaigns to attempt to infiltrate telecommunication networks. YubiKeys continue to be an important element of how we approach cyber protection.
>
> **Jeff Simon** | Chief Security Officer | T-Mobile

T-Mobile

Learn more:
yubi.co/t-mobile-release

2. Enhance the quality of customer service

Employees whether in third-party, franchisee or retail stores, directly reflect your brand as they engage with customers. With the YubiKey your employees provide more efficient customer service by not having to look down at their phone to authenticate. Instead, to authenticate users simply tap or insert then touch the YubiKey and, because the YubiKey arrives in a variety of form factors—including support for USB-A, USB-C, NFC, and Lightning port—authenticating to the full gamut of modern devices is simple, regardless of manufacturer or operating system. Additionally, YubiKeys with NFC capability have been demonstrably effective when combined with wearables such as wristbands and lanyards, for fast and easy authentication.

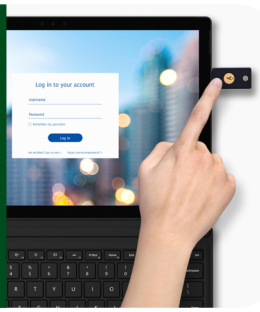
3. Secure shared workstations

Employees in physical stores often share computers, kiosks, and point-of-sale (POS) systems, which requires a streamlined authentication method that factors in: speed, ease of use, reliability and clearly distinguishes each personnel. YubiKeys can be uniquely associated and are extremely portable, ensuring that only people who are authorized to access a specific system, application or even function will be able to. This protects against external cyber threats and even insider threats when implemented with prudent access policies.

4. Leverage modern MFA in mobile-restricted environments

In environments not conducive to mobile-phones, do not default to weak forms of authentication. Call centers and devices across mobile-restricted environments need authentication that is highly secure, compliant and simple to use. YubiKeys provide secure authentication where people can't, won't, or don't use mobile phones.

YubiKeys provide you with always-on available phishing-resistant authentication. They don't require a battery or internet connection, are highly durable, crush-resistant, and water-resistant. Even technicians servicing remote locations will always have a form of secure MFA readily available.



5. Drive compliance to industry regulations and authentication standards

Global regulations like NIS2 Directive, Essential Eight, PCI DSS 4.0.1, SOC2, OMB M-22-09, and others continue to highlight the importance of how customer data, payment data and critical digital infrastructure are secured. The U.S. Federal Communications Commission (FCC) continues to hold telecommunication providers accountable to safeguard sensitive customer information, and to provide customers with the tools needed to protect themselves in the event that their data is compromised. The YubiKey bolsters Zero Trust and for regulated telco 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.

For regulated telco 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.

Easily procure and distribute phishing-resistant security at scale

To make it easy to deploy passwordless authentication at scale, Yubico offers YubiKey as a Service and YubiEnterprise Delivery for easy procurement and delivery of YubiKeys.

With YubiKey as a Service, organizations receive a service-based and affordable model for purchasing YubiKeys in a way that meets their technology and budget requirements. This service also provides priority customer support, ease of form factor selection, backup key discounts, and replacement stock benefits.

With YubiEnterprise Delivery, organizations receive a cloud-based service that streamlines the distribution of YubiKeys to end-users, serving both domestic and international locations including residential addresses.

Yubico also offers the Yubico Enrollment Suite, delivering a complete registration experience for easy enrollment of YubiKeys on behalf of users, with support for Microsoft and Okta currently, and additional Identity Provider (IdP) support planned to come on board.

YubiKeys meet you where you are on your MFA journey

YubiKeys act as a bridge to a passwordless future, allowing you to leverage existing OTP authentication as you progress all the way to modern phishing-resistant authentication by using either FIDO2 or Smart Card—all on one key. YubiKeys future-proof security and empower you to focus on providing exceptional quality of service to your customers. Embrace the YubiKey with confidence knowing that you have a solution to prevent account takeovers.

The YubiKey Family

The YubiKey is available in multiple form factors for desktop, laptops and mobile devices.

WATER RESISTANT | CRUSH RESISTANT | MADE IN US & SWEDEN

Contact us
yubi.co/contact

Learn more
yubi.co/telco

[1] Darkface, 2025 The State of Cybersecurity in the Global Telecommunications Sector

[2] Google, How effective is basic account hygiene at preventing account takeovers

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 AB
Kungsgatan 44
2nd floor
SE-111 35 Stockholm
Sweden

Yubico Inc.
5201 Great America Pkwy, #122
Santa Clara, CA 95054, USA
844-205-6787 (toll free)
650-285-0088