yubico

Phishing-resistant MFA for Telecoms

Modern security with the YubiKey to bolster existing security approaches

The critical need for modern security

In such a digitally-driven and always-connected world, telecommunication organizations are a critical infrastructure that consumers and businesses heavily rely upon. The 2021 SpyCloud report on Telecommunications Industry Credential Exposure found that in exposed assets per company, telecom exceeds every other industry including high-risk sectors—finance, technology, health care and defense. A big cause for the industry's vulnerability is its high rate of password reuse across multiple accounts[1] and stolen credentials are the leading cause of account takeovers and data breaches.[2] Not only are breaches costly, but they can greatly damage brand reputation and customer loyalty.

To protect against the ever-evolving sophistication of cyber attacks, strong multi-factor authentication (MFA) needs to be a foundational part of your holistic security strategy. This would ensure that no person or device is allowed into your network, unless vetted. 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.

Safeguard people, technology, and data with the YubiKey

To protect against modern cyber threats, Yubico offers the YubiKey—a hardware security key for phishing-resistant two-factor (2FA), MFA, and passwordless authentication at scale. It is the only solution proven to completely eliminate account takeovers in independent research.[4] The YubiKey is helping telecom organizations secure their employees and customers against cyber threats, while driving regulatory compliance.

This modern security solution can bolster existing security approaches—if you are using mobile-based MFA, it can be complemented with the YubiKey, for an additional phishing-proof layer of protection. 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 protects telecom organizations from modern cyber threats:

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 hundreds of applications and services, eliminating any rip or replace of existing solutions. Users get protected in minutes right out-of-the-box.

The impact of legacy authentication in the telecom industry

76%

of telecom employees are reusing passwords[1]

82%

of breaches tied to the human element social attacks, errors, misuse, credential theft[2]

$4.91 million +

average cost of data breach with phishing as initial attack[3]

[1] Spycloud, 2021 Special Report Telecommunications Industry Credential Exposure

[2] Verizon, 2022 Data Breach Investigations Report

[3] IBM, Cost of a Data Breach Report 2022

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

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.

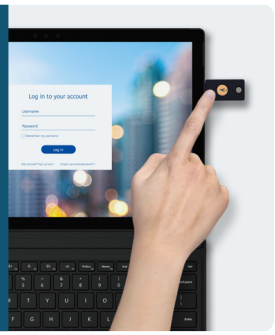
3. Secure shared workstations

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 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

In January 2022, the U.S. Federal Communications Commission (FCC) proposed new rules for the telecom industry: eliminate the mandatory seven-business-day waiting period for customers to be notified of a breach, expand consumer protections and require the carrier to notify key organizations. The purpose is to accommodate the evolving nature of breaches and their impact. Additionally, the Office of Management and Budget (OMB) Memo M-22-09 provides actionable strategies, in response to the Executive Order 14028 to strengthen cyber security across state, local, and corporate levels. The YubiKey meets and surpasses the Zero Trust and phishing-resistant MFA recommendations outlined in the OMB Memo.

Seamlessly procure and distribute YubiKeys at scale

Yubico offers flexible and cost-effective enterprise plans that help organizations with 500 users or more move away from legacy and broken MFA and accelerate towards phishing-resistant authentication at scale.

YubiEnterprise Subscription

YubiEnterprise Delivery

With YubiEnterprise Subscription, organizations can benefit from a predictable OPEX model, the flexibility to meet user preferences with choice of any YubiKey, upgrades to the latest YubiKeys, and faster rollouts with easy access to Deployment Services, Priority Support and a dedicated Customer Success Manager.

Subscription customers are also eligible to purchase additional services and product offerings, such as YubiEnterprise Delivery, a global turnkey hardware key distribution service to residential and office locations across 49 countries.

Yubico's Professional Services team can also help streamline your YubiKey implementation and rollout with services mapped to your needs.

YubiKeys provide the gold standard for phishing-resistant MFA

YubiKeys meet you where you are today on your MFA journey by acting 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 smartcard—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.

Contact the Yubico sales today to be a cyber security leader in telecommunication with the YubiKey.

The YubiKey Family

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

[5] Customers outside of North America should contact their local Yubico rep for details

About Yubico As the inventor of the YubiKey, Yubico makes secure login easy. As a leader in setting global standards for secure access to computers, mobile devices, and more, Yubico is also a creator and core contributor to the FIDO2, WebAuthn, and FIDO Universal 2nd Factor (U2F), and open authentication standards. For more information, please visit: 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