yubico

Phishing-resistant MFA

to secure Department of Corrections against cyber threats and meet CJIS compliance

Critical need for phishing-resistant MFA across Department of Corrections

State and local governments are key targets for cyber-criminals and the Department of Corrections is no exception. The last few years saw major breaches at the California Department of Corrections and a Georgia correctional facility healthcare provider.

While MFA can be a strong first-line of defense to protect corrections officers and staff, facility workers, contractors and 3rd parties against phishing attacks and account takeovers, not all forms of MFA are created equal. Legacy authentication such as usernames and passwords are easily hacked, and mobile-based authentication such as SMS, OTP codes, and push notifications are highly susceptible to phishing attacks, malware, SIM swaps, and attacker-in-the-middle attacks. Mobile authenticators also create gaps in your MFA strategy across mobile-restricted areas.

Evolving compliance landscape

While the Criminal Justice Information Services (CJIS) Security Policy version 5.9.2 Section 5.6 calls for MFA to secure organizational users, privileged accounts and non-privileged accounts including the use of replay-resistant authenticators, state and local government-focused compliance mandates will evolve to be consistent with Zero Trust and phishing-resistant MFA requirements as outlined in the 2021 White House Executive Order (EO) #14028 on Improving the nation's cybersecurity.

What is phishing-resistant MFA?

Phishing-resistant MFA relies on cryptographic verification between devices or between a device and a domain, making them immune to attempts to compromise or subvert the authentication process. According to the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63, only two forms of authentication currently meet the mark for phishing-resistant MFA: PIV/Smart Card and FIDO2/WebAuthn.

The YubiKey offers phishing-resistant MFA at scale

Yubico offers the YubiKey—a FIPS 140-2 validated hardware security key for phishing-resistant MFA and passwordless authentication at scale. It is the only solution proven to completely eliminate account takeovers in independent research including bulk and targeted attacks[1], meets phishing-resistant MFA requirements in EO#14028, and replay-resistant requirements in the CJIS Security Policy.

The combination of frictionless user experience, data breach prevention, mobile device and service cost savings, and the YubiKeys' versatility providing multi-protocol support results in high ROI for any environment. YubiKeys also enable self-service password resets, eliminating IT support costs related to help desk password-reset requests.

The total economic impact of YubiKeys[2]

Strongest Security
Reduce risk by
99.9%

High Return
Experience ROI of
203%

More Value
Reduce support tickets by
75%

Faster
Decrease time to authenticate by
>4x

> "Given the varied regulatory requirements that state agencies are required to comply with, the Georgia Technology Authority views Yubico's hardware security option, YubiKey, as vital to helping protect mission-critical systems and state data from both external and internal threats, while at the same time doing so in a very cost-effective way."
>
> **Dean Johnson** | Former Chief Operating Officer | Georgia Technology Authority

YubiKeys integrate seamlessly with existing identity and access management (IAM) and identity provider (IDP) solutions such as Microsoft, Okta, GreenRocket, Duo, ForgeRock, and over 1,000 applications and services out-of-the-box with multi-protocol support for Smart Card/PIV, OTP, OpenPGP, FIDO U2F, and FIDO2/WebAuthn, helping bridge to a modern passwordless future without a rip and replace.

YubiKeys are highly suitable for mobile-restricted areas, shared workstations and devices and for users that can't, won't, or don't use mobile authentication. A single YubiKey works across desktops, laptops, mobile, tablets, and notebooks, enabling users to utilize the same key as they navigate between devices. YubiKeys are also easily re-programmed, making them suitable for rotating-shift and temporary workers.

Benefits of the YubiKey

- FIPS 140-2 validated: Meets Authentication Assurance Level 3 requirements (AAL3) of NIST SP800-63B (Certificate #3914)
- Multi-protocol support for Smart Card/PIV, FIDO2/WebAuthn, FIDO U2F, OTP and OpenPGP on the same device
- Portable external authenticator works across all computing devices with options to connect via NFC, USB-A, USB-C, and Lightning
- YubiKeys are tamper proof and require no battery, internet or network connectivity
- Secure United States manufacturing and supply chain processes for trustworthy components and delivery

WATER RESISTANT

CRUSH RESISTANT

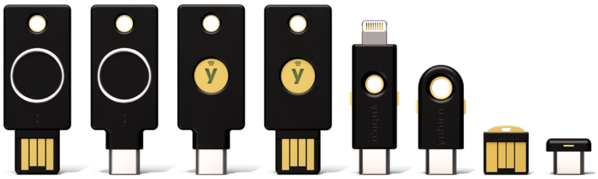
MADE IN USA

Trusted authentication leader

Yubico is the principal inventor of the WebAuthn/FIDO2 and U2F authentication standards adopted by the FIDO alliance and is the first company to produce the U2F security key and a multi-protocol FIDO2 authenticator.

Once **ready to purchase**, Yubico is focused on helping agencies easily access security products and services in a flexible and cost-effective way to heighten security:

- With YubiEnterprise Subscription, agencies receive a service-based and affordable model for purchasing YubiKeys in a way that meets technology and budget requirements, providing priority customer support, easy form factor selection, backup key discounts, and replacement stock benefits
- With YubiEnterprise Delivery, agencies receive turnkey service with shipping, tracking, and returns of Yubico products—all securely handled by logistics experts. It also helps with inventory management with delivery of keys



The YubiKey Family

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

Contact us
yubi.co/contact

Learn more
yubi.co/statelocal

[1] Kurt Thomas and Angelika Moscicki, New research: how effective is basic account hygiene at preventing hijacking, (May 17, 2019)

[2] Forrester, The Total Economic Impact of Yubico YubiKeys, (September 2022)

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.