yubico

Embracing critical infrastructure security and resilience

SRMA's your business case to phishing-resistance

Safeguarding against cyber threats

Protecting critical infrastructure from cyber attacks is complex as it heavily relies on securing both information technology (IT) as well as operational technology (OT). Each poses unique challenges such as protecting legacy/existing infrastructure, managing third-party business risk, and ensuring the CIA triad (confidentiality, integrity, and availability of information) is upheld.

Phishing should be considered a top risk as the threats are evolving, and critical infrastructure including manufacturing has been the number one target for these kinds of attacks for the past three years.[1] Additionally, there has been a 71% year-over-year increase in cyberattacks that used stolen or compromised credentials.[2] Further advancements in generative text may make it harder to discern phishing attempts from genuine communication. Once accounts are breached, malicious actors can steal data, damage critical systems or wreak havoc using ransomware. With the concept of zero trust, the legacy method of using perimeter oriented approaches is no longer good enough.

Impact of NSM-22

A reaffirming step forward was taken by the United States releasing the National Security Memorandum on Critical Infrastructure Security and Resilience (NSM-22). The Cybersecurity and Infrastructure Security Agency (CISA) identifies 16 sectors whose assets, systems, and networks, whether physical or virtual, are considered vital. It outlines in the memo that Sector Risk Management Agencies (SRMAs) shall serve as day-to-day Federal interfaces for their designated critical infrastructure sector and conduct sector-specific risk management and resilience activities by collaborating closely with owners and operators.

Connecting the dots

A few years ago the Office of Management and Budget (OMB) M-22-09 memorandum shared the importance of phishing-resistant MFA. The reason for this mandate is that sophisticated attackers can intercept legacy forms of authentication, such as mobile-based authenticators, that are highly susceptible to phishing, malware, SIM swaps, and attacker-in-the-middle attacks. Further, Enduring Security Framework (ESF) calls for identity and access management best practices recommending phishing-resistant MFA for all critical infrastructure sectors.

Achieving phishing-resistance

To mitigate this cyber risk, leverage phishing-resistant technologies. Currently there are only two phishing-resistant approaches to MFA that can defend against these attacks:

- The Federal Government's Personal Identity Verification (PIV) standard that smart cards are built on, which has long been used to provide access to on-premises environments via government issued Common Access Cards (CACs)' and is widely supported.
- The WebAuthn/FIDO2 standard that is supported today by nearly every major consumer device, and an increasing number of popular cloud services. FIDO2 is the overarching term for FIDO Alliance's set of specifications, of which WebAuthn is a key specification. WebAuthn can be used in combination with a FIDO2 security key for phishing-resistant MFA. PIV and WebAuthn/FIDO2 are the proven standards offering phishing-resistant MFA. Passkeys are a new name for FIDO2 passwordless-enabled credentials.

> “FIDO stands for “Fast IDentity Online” and is considered the gold standard of multi-factor authentication.
>
> **CISA**

The YubiKey 5 FIPS Series

The YubiKey 5 FIPS Series is the first FIPS validated FIDO2/WebAuthn, multi-protocol authenticator lineup. From left to right: YubiKey 5C NFC FIPS, YubiKey 5 NFC FIPS, YubiKey 5Ci FIPS, YubiKey 5C FIPS, YubiKey 5 Nano FIPS and YubiKey 5C Nano FIPS.

Creating phishing-resistant users

Yubico offers the YubiKey—the best available security against phishing attacks and account takeovers with PIV and WebAuthn modules on the same key. With the YubiKey deploy the most secure passkey strategy: device-bound that is purpose-built for security. YubiKeys are FIPS 140-2 validated to meet the highest authentication assurance level 3 requirements (AAL3) of NIST SP800-63B guidelines. YubiKeys are DFARS/NIST SP 800-171 compliant, and are approved for use in DOD Non-Classified and Secret Classified Environments. Phishing-resistant users create phishing-resistant enterprises.

The YubiKey is simple to deploy and use—YubiKeys can be used across legacy and modern applications, services, and devices, with multi-protocol support for SmartCard, OTP, OpenPGP, FIDO U2F and WebAuthn/FIDO2 on a single key. YubiKeys are supported natively by leading identity, credential and access management (ICAM) solutions such as Axiad, Duo, Google Cloud, Entra ID, Okta Workforce Identity, OneLogin, Ping Identity platform, and RSA SecurID® Suite, and provide highest-assurance security for non CAC eligible employees and contractors, teleworkers, cloud services, isolated/closed networks, digital citizen services, and mobile device users. The YubiKey enables you to cultivate phishing-resistant users, providing authentication that moves effortlessly with users no matter how they work and across the entire authentication lifecycle.

Phishing-resistant authentication options

Access points		Supports login with WebAuthn	Supports login with PIV/Smart Card	YubiKey (WebAuthn/FIDO and/or PIV)
On premise (active directory)	Windows 10+ Login	✓ / 3rd party	✓	✓
	Earlier versions of Windows login	3rd party	✓	✓
	macOS login on a Windows domain	3rd party	✓	✓
	VPN Access	Varies	✓	✓
	Secure Proxy Gateways	✓	Varies	✓
Cloud platforms	Microsoft Azure	✓	✓ / Federation	✓
	Amazon Web Services (AWS)	✓	Federation	✓
	Google Cloud	✓	Federation	✓
	Oracle Cloud	✓	Federation	✓
	IBM Cloud	✓	Federation	✓
IDPs	Okta	✓	✓	✓
	Ping Identity	✓	✓	✓
	Duo	✓	N/A	✓
	EntraID	✓	✓	✓

The total economic impact of YubiKeys[3]

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

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 organizations easily access security products and services in a flexible and cost-effective way to heighten security:

- With YubiKey as a Service, organizations 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, organizations receive turnkey service with shipping—serving both domestic and international locations including residential addresses, tracking, inventory management, and returns of Yubico products—all securely handled by logistics experts.

We're trusted by regulatory bodies, government agencies and many of the most security-conscious organizations, individuals and industries.

Key takeaways

The importance of securing critical infrastructure is felt around the world. We can strengthen the security and resilience of critical infrastructure by engaging international partners and allies.

Creating a secure and resilient nation for generations to come depends on what is enacted today.

Making the business case for phishing-resistant technology has never been more important to secure critical infrastructure in this interconnected world.

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

Contact us
yubi.co/contact

Learn more
yubi.co/YKSvc

[1] Smart Industry, Manufacturing leads in cyberattacks for a third straight year, so what are some defenses, (May 2024)

[2] IBM Security, X-Force Threat Intelligence Index, (February 2024)

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