yubico

Fortifying Europe’s Cyber Defences with Phishing-Resistant MFA

As Europe enters an era of unprecedented strategic investment in its defence and armed forces[1], the importance of building cyber resilience cannot be neglected. Information operations is the fifth domain of warfare[2]—European critical infrastructure, vital intelligence and communications are constant targets for sophisticated state-sponsored cyber attacks, where the weakest link is often human credentials.

The Imperative for Phishing-Resistant MFA

Traditional Multi-Factor Authentication (MFA) methods, such as SMS codes or app-based OTPs, are no longer sufficient. Formidable adversaries, including groups like the Russian GRU (APT28) and other state-sponsored actors, routinely employ advanced phishing techniques to bypass these defences, in conjunction with generative AI tools to automate and amplify the threat. High-profile breaches demonstrate how **a single compromised credential can lead to catastrophic consequences** well beyond intellectual property theft and operational disruption.

Phishing-resistant MFA, powered by FIDO passkey or Smart Card technology, is the only robust answer to these and other escalating threats. It fundamentally changes authentication by eliminating shared secrets (like passwords or OTPs) that can be intercepted or stolen, instead leveraging public key cryptography, where unique private keys are securely bound to hardware devices or cloud services.

YubiKey: Modernizing PIV and Delivering Phishing-Resistance

YubiKeys are hardware security keys purpose-built for security, providing phishing-resistance though both **FIDO passkey** and **Smart Card (PIV)** protocols. Seamlessly integrating with existing Smart Card Credential Management Systems (CMS), as well as hundreds of enterprise applications and services, including Microsoft Entra ID and Google Workspace, YubiKeys work with legacy systems on day one while supporting a migration to modern infrastructure over time.

YubiKeys’ USB and NFC connectivity offers plug-and-play functionality across devices, with no need for embedded Smart Card readers or additional hardware. A single YubiKey can store up to **100 passkeys** and **24 PIV certificates**, including RSA-3072 and RSA-4096 encryption, allowing powerful flexibility for privileged users.

[1] The Hague Summit Declaration

[2] European Council Cyber Defence Policy

Optimised for Operational Environments

This is underscored by real-world adoption in the most demanding environments, with YubiKeys deployed globally in armed forces, government defence agencies and their contractors. These entities recognise the unparalleled security offered by hardware security keys in protecting sensitive data and critical systems, particularly in enabling secure remote access and thwarting sophisticated credential-based attacks that bypass traditional MFA.

YubiKeys are uniquely suited for **air-gapped or mobile-restricted environments and areas with no network connectivity**. Unlike software or mobile-based MFA, YubiKeys require no internet, mobile reception or battery for authentication, providing reliable access where traditional methods fail—essential for tactical and highly secure operations.

IP68-rated for both water and dust resistance, YubiKeys are also crush-resistant, ensuring unparalleled durability and dependable authentication even in harsh conditions encountered by defence personnel.

Developed, **manufactured and programmed in Sweden**, Yubico's secure, reliable European supply chain provides governments and military partners the verified trust and transparency required for their most sensitive operations.

Beyond User Access: Securing Cryptographic Keys

Today's armed forces are faced with adversaries that are increasingly sophisticated. It's critical that sensitive and classified information is secured while in transit and at rest across the supply chain. The YubiHSM 2 is a hardware security module built in a portable nano form factor with low power usage for secure generation and storage of private key data for rugged computers and devices at the tactical edge.

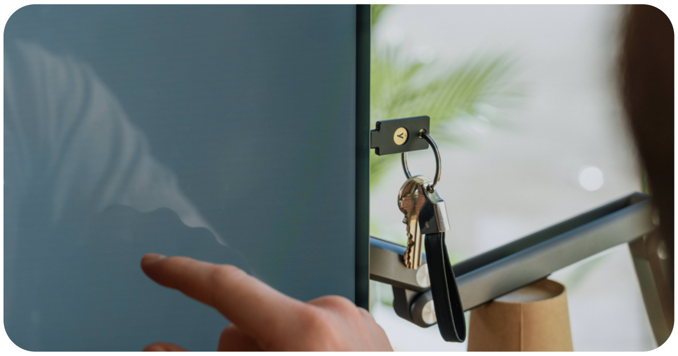
Meeting NATO Standards

Phishing-resistant MFA aligns directly with NATO's operational necessity to protect classified networks, secure remote access for personnel and maintain supply chain integrity. The YubiKey is included in NATO Communications and Information Agency's Product Catalogue.

Meeting European Compliance & Security Mandates

YubiKeys directly address the requirements of key European regulations and standards, providing a clear path to compliance.

- ✓ **NIS2:** YubiKeys meet strong multi-factor authentication and access control policies mandated by the NIS2 Directive for critical infrastructure.
- ✓ **GDPR:** By preventing credential theft—a leading cause of data breaches—phishing-resistant MFA is a critical technical measure to protect personal data and demonstrate GDPR compliance.
- ✓ **FIPS:** YubiKey 5 FIPS Series has FIPS 140-2 validation (FIPS 140-3 pending), enabling US government agencies and global partner agencies to meet the highest authenticator assurance level 3 (AAL3) requirements from NIST SP800-63B guidance.



Contact us
yubi.co/contact

Learn more
yubi.co/yk5

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.