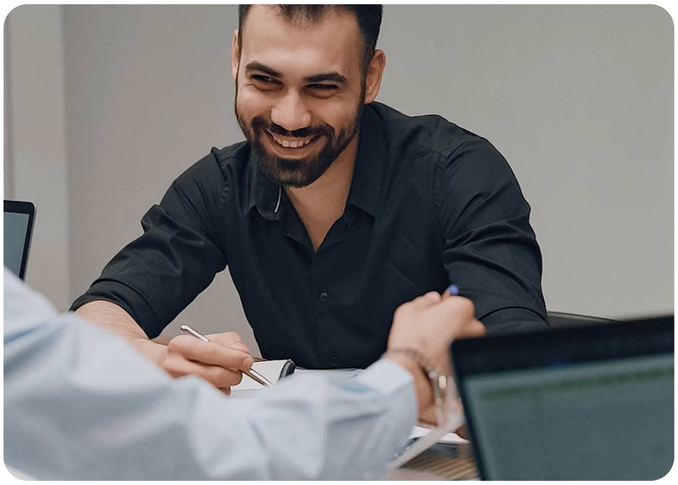
yubico

Keeping financial services organizations in the United Arab Emirates ahead of modern cyber threats

Why Banks Need Stronger MFA— And How YubiKey Leads the Way



The Need for Cyber Resilience Amid Escalating Digital Fraud

The United Arab Emirates is globally recognized as a leading financial and technological hub, actively driving innovation through initiatives like the UAE Digital Economy Strategy. This rapid digitalization, while fostering unparalleled growth in banking and financial services, has also created an irresistible venue for high-level cyberattacks.

As the volume of digital transactions soars, so too does the risk of fraud. This surge primarily affects virtual banking cards, which have become more frequent targets than traditional ATM cards, marking a significant shift in the cybercrime landscape.

Key figures[1]

56%	of the UAE population receives a scam attempt once a month (mostly via instant messaging platforms)
73%	increase in digital banking fraud complaints during the first five months of 2025 compared to the same period in 2024
27%	of victims reported losing money from account takeover tactics like phishing and social engineering
$2,2≈	$2,194 average reported loss from phishing, social engineering, and other account takeover scams

Regulatory mandate from the Central Bank of the UAE

This has spurred a significant regulatory response. The Central Bank of the UAE (CBUAE) has issued a definitive directive to modernize authentication mechanisms across the financial sector. Recognizing the inherent and escalating vulnerabilities of traditional one-time passwords (OTPs), the CBUAE has mandated the phasing out of SMS and email OTPs as primary forms of multi-factor authentication by 2026.

This regulatory push requires financial institutions to adopt stronger, more resilient methods to meet the new security and anti-fraud requirements. This marks a critical turning point for banks in the UAE, moving toward a security posture rooted in phishing-resistant authentication standards.

Securing financial enterprises with hardware passkeys

The main objective of the CBUAE mandate is customer security in online transactions. However, customers also require assurance that financial assets entrusted to banks are fully protected.

Consequently, banks need to invest in their internal cybersecurity infrastructure, particularly for employee access, as compromised employee credentials remain the most common vector for major enterprise breaches.

Software-based authentication meets the immediate regulatory need for customer authentication, but leaves organisations vulnerable to sophisticated phishing attacks. To ensure cyber resilience and reduce risks related to business continuity, banks should deploy truly phishing-resistant authentication methods, such as passkeys stored on security keys. This is especially important for securing internal IT, cloud and operational environments.

By adopting security keys for their workforce, banks in the UAE can achieve the highest level of phishing-resistance, solidify compliance with the CBUAE directive and proactively secure their core assets against cyberthreats.

[1] Sources

https://www.netsweeper.com/government/the-rising-threat-of-scams-in-the-uae#:~:text=Key%20Statistics%20from%20the%202024,completed%20by%201%2C964%20UAE%20citizens.

https://www.gasa.org/_files/ugd/beb5f3_da5ba21562114b4f951c4578c8ddfd81.pdf

Driving a turning point in the UAE's digital banking evolution

Why Financial Institutions Choose Yubico

- **Proven across regulated markets**
  Used by major U.S. and E.U. banks to comply with NIST, PSD2, and GDPR
- **Battle-tested resilience**
  Stops phishing, SIM swap, and credential theft
- **Seamless deployment**
  No network changes, fast onboarding, and low support overhead
- **Trusted brand**
  Used by Google, T-Mobile, Hyatt, Cloudflare and many of the world's most security-conscious enterprises

The YubiKey Advantage: Phishing-Resistant MFA at Scale

- **Hardware-based, phishing-resistant authentication**
  No shared secrets, no phishing window
- **Simplified distribution**
  Ready for scale across distributed users including delivery to residential addresses
- **Fast and seamless UX**
  Google research found YubiKeys allow 4x faster login than mobile 2FA codes[2]
- **Increased operational efficiency**
  Drive productivity and deliver immediate ROI by reducing login times and eliminating IT password reset requests

Modern security for the modern enterprise

The YubiKey is a modern hardware security key offering phishing-resistant multi-factor and passwordless authentication. A single YubiKey can store up to **100 passkeys** and **24 PIV (Smart Card) certificates**. Unlike synced passkeys, passkeys stored on YubiKeys are hardware-bound.

A user simply has to touch or tap the YubiKey to authenticate. This required human presence, ensuring that any remote attack is stopped immediately. The YubiKey Bio allows for fingerprint authentication, offering the additional convenience of even faster authentication.

YubiKeys: Modern security that stops phishing scams and online fraud—fast and easy login security across desktops, laptops and mobile devices

A Call to Action for banks in the UAE

The time for strategic security transformation is now. While the CBUAE mandate primarily addresses customer authentication, financial institutions must lead the cultural shift towards a security-first culture. Banks can encourage the widespread adoption of physical passkeys by immediately deploying YubiKeys within their internal operational environments.

By embracing this technology, banks in the UAE will align themselves with leading global practices in Asia's financial sectors, including countries like Singapore and the Philippines, which are already leveraging YubiKeys to future-proof their digital ecosystems. This ensures compliance with the CBUAE directive and positions the institution as a market leader in digital trust.

Yubico is ready to help your institution:

- Deploy phishing-resistant MFA with hardware-bound passkeys
- Achieve compliance with new FSA guidelines and regulations
- Reduce fraud, operational burden, and liability risk

Let's protect your customers—and your reputation.

Contact us
yubi.co/contact

Learn more
yubi.co/yk5

[2] Google Research, Security Keys: Practical Cryptographic Second Factors for the Modern Web

About Yubico 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.