yubico

Keeping Indian financial services organisations ahead of modern cyber threats

Why Indian Banks Need Stronger MFA—And How Yubico Leads the Way

Escalating cyber risks in the Indian financial sector

India's massive digital boom, powered by digital payments, cloud computing and government e-services, has fundamentally reshaped both business and daily life. However, the explosive growth has outpaced cybersecurity infrastructure and regulations, resulting in vulnerabilities.

In 2023 alone, India experienced approximately 5.3 million compromised digital accounts. Further, according to the Data Security Council of India (DSCI), 72.5% of organisations do not report when they experience cyberattacks, suggesting the actual scale of the problem is considerably larger.

Currently, the majority of digital transactions in India rely on SMS One-Time Passwords (OTPs) for payment authentication. However, SMS OTPs are inherently vulnerable and can be easily intercepted by sophisticated cybercriminals. Given that India accounts for 48.5% of global real-time payments, this landscape presents an extremely attractive target for malicious actors.

48.5% of global real-time payments are from India[2]

135,000+ phishing incidents reported from January to June 2024[3]

$2.18 million The average cost of data breaches in India in 2023[4]

₹22,845.73 crore Total losses from finance-related cybercrime in India in 2024[5]

Regulatory response from the Reserve Bank of India (RBI)

In response to this pervasive threat landscape, in September 2025 the Reserve Bank of India (RBI) formally released a framework on new authentication mechanisms. These guidelines are designed to achieve several critical objectives: protecting financial institutions and customers, mitigating fraud, strengthening customer trust, and ensuring India aligns with global security standards.

Effective April 2026, the RBI mandates that all digital payments must be secured by a minimum of two distinct factors of authentication, with the requirement that at least one factor must be unique to each transaction. The RBI recommends moving away from OTPs and looking instead at adding stronger authentication—such as hardware security keys.

Financial institutions will have the flexibility to select authentication methods that are most appropriate for their specific operational context and risk profile, moving away from a rigid, one-size-fits-all mandate. Therefore, the required level of security can be risk-adaptive, differing, for example, between a simple system login and a high-value financial transfer.

Implications and strategic imperatives for banks

This regulatory shift requires a proactive and strategic response from the banking sector. Financial institutions must:

- **Recalibrate risk engines.** Banks must ensure accurate prediction of financial risk and to maintain full compliance with the new guidelines by the April 2026 deadline.
- **Explore advanced authentication methods.** Banks are tasked with exploring and adopting alternative, more resilient authentication methods. This will require the implementation of robust customer communication strategies to inform account holders about the upcoming changes to security processes.
- **Strengthen internal security posture.** Enhancing internal cybersecurity is paramount. The security of customer data is dependent on the security of the bank's internal systems. By securing employee access to an institution's operational infrastructure, banks are, in effect, directly safeguarding their customers.

The flexibility offered to banks allows for the adoption of innovative, higher assurance authentication methods beyond traditional OTPs. This presents a unique opportunity to deploy advanced solutions, such as hardware security keys, to meet the RBI's strong authentication requirements.

[1] Alarming 73% of organizations fail to report cyber attacks: DSCI survey

[2] Ibid.

[3] Phishing attacks on financial sectors soar in India, increasing by 175% in 2024: Report

[4] RBI Report on Cybersecurity

[5] India's cyber fraud losses soar 206% to ₹2,845 crore from 2024

Modern security for the modern enterprise

The YubiKey is a modern hardware security key offering phishing-resistant multi-factor and passwordless authentication. A user simply has to touch or tap the YubiKey to ensure that any remote attack is stopped immediately. The YubiKey Bio allows for fingerprint authentication, offering the additional convenience of even faster authentication.

A single YubiKey can store up to **100 passkeys** and **24 PIV (Smart Card) certificates**. Compared to synced passkeys, which can be copied and shared, passkeys on YubiKeys are hardware-bound, and so enforce human presence as a requirement when submitting credentials for authentication.

Yubico is ready to help your institution:

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

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, Mitsubishi Electric 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
- **No software installs or batteries**
  Plug-and-play simplicity across devices and platforms
- **Lower total cost of ownership**
  Proven to cut help desk calls by up to 75% and reduce account recovery friction

Driving a turning point in India's digital banking evolution

The RBI recommends implementing phishing-resistant MFA for all digital transactions. However, banks are only as secure as their own employees, so we recommend banks also adopt YubiKeys across their internal workforce to strengthen their compliance and security posture.

A common starting point is securing privileged users (e.g., IT administrators, risk managers) who have access to the most sensitive systems and data. This protects the bank's core infrastructure and also establishes a phishing-resistant operational environment.

This strategy can then be expanded to include employees in critical operational areas, such as customer support call centers, where the handling of confidential information necessitates the highest level of assurance and often restricts the use of mobile phones for authentication.

Finally, the greater vision for digital security in India involves the widespread adoption of device-bound passkeys by the general public to safeguard their digital transactions, in alignment with the RBI's new directive. At the same time as securing their internal infrastructure, banks can recommend the use of modern hardware security keys to customers, beginning with high-net-worth individual (HNI) accounts, cto prevent financial fraud caused by phishing attacks.

Ultimately, deploying phishing-resistant authentication is the most direct pathway to creating a phishing-resistant bank, thereby protecting customer assets and fortifying institutional reputation.

A Call to Action for Financial Institutions

The time for strategic security transformation is now. Financial institutions must lead this cultural shift. Banks can kickstart this security-first culture internally by immediately deploying YubiKeys within their operational environments.

By embracing this technology, Indian banks will align themselves with leading global practices in Asia's financial sectors, including countries like Singapore and the Philippines, which are already leveraging phishing-resistant MFA to future-proof their digital ecosystems. This not only ensures full compliance with the RBI's additional factors of authentication (AFA) directive but also positions the institution as a market leader in digital trust.

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

Let's protect your customers— and your reputation.

Contact us
yubi.co/contact

Learn more
yubi.co/yk5