Singtel

OTP authentication is broken. It's time for telco-backed verification.

Still trusting OTPs? Here's why you shouldn't.

Phishing sites now mimic legitimate login pages down to the pixel.

SIM swap attacks reroute messages before users notice.

Deepfakes can trick voice- or video-based verification systems into granting access.

For businesses and users alike, traditional security measures are no longer sufficient. Relying on outdated systems leaves sensitive data vulnerable, especially as threats become more sophisticated.

Cracks in the system

Hackers have adapted. OTPs haven't. They weren't built to detect deepfakes, outsmart phishing kits, or survive a SIM swap. And attackers know that.

Easily intercepted
SIM swap fraud and phishing attacks can hijack OTPs in seconds.

False sense of control
OTPs are predictable, static, and reactive.

No match for AI
Deepfakes and generative impersonations are bypassing even multi-layered OTP systems.

The rise of identity fraud in the AI era

76% **surge** in phishing attempts in 2025[1]

70% **of businesses** are concerned about AI-powered fraud[1]

Consumers face identity scams **34+** **times a year**[2]

$47B+ in combined losses from fraud and scams in 2024 (18M+ victims)[3]

194% **YoY increase** in deepfake fraud in APAC[4]

Global: Deepfake scams occur **every 5 minutes**; doc forgeries up **244% YoY**[5]

Closer to home, in **Singapore**

A finance director nearly lost **SGD 670,000** to a deepfake video scam[5]

A **$55 million dollar** document forgery scandal at a Singapore-based family office[5]

Traditional authentication is hurting business confidence

Forward-thinking businesses are recognising that traditional authentication methods like OTPs are no longer enough and they come with a cost.

- Reputational damage, compliance breaches, and user churn
- Regulatory pressure to secure onboarding and transaction flows
- Growing customer expectations for seamless yet secure digital interactions

As customer expectations evolve toward seamless and secure experiences, leading organisations are already taking steps to modernise their security strategies.

Seamless, secure, and smarter authentication with SingVerify

SingVerify offers seamless, real-time user authentication by leveraging telco data and silent network authentication. Unlike outdated OTPs, SingVerify works in the background, verifying users without interrupting their experience, ensuring security and convenience.

Aligned with the GSMA Open Gateway framework, SingVerify is designed for seamless deployment and broad accessibility across diverse mobile networks. This enables businesses and service providers to tap into its robust security features, broadening the scope of protection.

How it works

- **Authenticates users in real-time**
- **Supports secure onboarding, payments, logins, and other use cases**
- **Helps businesses stop suspicious activities in real-time**
- **Defends against cyber scams while keeping the user experience frictionless**

APIs

Number Verify
Real-time, secure authentication to prevent 2FA/MFA hijacking

Device Location
Real-time location verification to prevent unauthorised access

Scam Sniffer
Proactive scam detection through integrated blacklist analytics

Rethink authentication with SingVerify. **Contact us**

References

[1] SDX Central, AuthenticID report reveals surge in identity-based fraud across businesses, 2025
[2] BusinessWire, AuthenticID annual report reveals surge in identity-based fraud across businesses, 2025
[3] Javelin, Compromised today, exploited tomorrow: innovation can stop the fraud cycle, 2025
[4] FintechNews, When US$1,000 can cause US$2.5 million in monthly business losses from fraud, 2025