Rising cyber attacks on financial platforms: How to protect your money and data

Security firms are reporting a sharp rise in malware attacks, fake mobile applications, and identity theft through commonly-used communication platforms. The fake apps are often distributed via social media or influencer promotions.

Cyber frauds targeting financial data and digital transactions are becoming more complex. Security firms are reporting a sharp rise in malware attacks, fake mobile applications, and identity theft through commonly-used communication platforms.

Surge in malware and fake applications

Quick Heal Technologies recorded over 369 million malware detections in 2024 through its research arm Seqrite Labs, covering 8.44 million users.

Trojans made up 43% of these threats, according to CEO Vishal Salvi.

Seqrite Labs also noted a sharp increase in behaviour-based malware detections, which rose from five million in 2021 to 53.73 million in 2024 — a 975% increase.

Salvi stated that attackers are using malicious APK files distributed via platforms like WhatsApp. These files are often disguised as government or banking applications and belong to the RewardSteal malware family.

Other reported threats include fake traffic department alerts and fraudulent government apps.

As more users adopt mobile-based trading and cryptocurrency platforms, Salvi cautioned that fake investment apps may increase.

These apps are often distributed via social media or influencer promotions.

Threats to communication infrastructure

Infobip, a global cloud communications platform, has observed threats like artificially inflated traffic (AIT). Bots generate high volumes of one-time password (OTP) requests to exploit telecom systems.

Harsha Solanki, VP GM Asia at Infobip, noted other threats such as Flubot malware, smishing (SMS phishing), and grey routes. These exploit telecom infrastructure and affect both communication and user data.

Infobip has implemented real-time threat detection through its SMS firewall and Infobip Signals platform. The company works with over 120 mobile network operators, covering 1.1 billion users.

Human error and insider risks

Insider threats remain a key risk. Salvi estimated that up to 50% of cyber incidents could be linked to human error. Basic actions like clicking unknown links or downloading files from unverified sources can lead to phishing or data breaches.

Risks to infrastructure and new technologies

Cyber attackers are also targeting critical infrastructure such as healthcare, finance, and energy sectors. Salvi added that malware could begin targeting augmented reality (AR) features on Android devices. Malicious AR apps may collect user data or compromise digital interactions.

Key measures for users

To reduce the risk of financial and data-related frauds, users can take the following actions:

- Download apps only from verified sources or official stores.
- Avoid clicking on links received through SMS or messaging platforms.
- Enable two-factor authentication (2FA) and update passwords regularly.
- Install antivirus software with real-time scanning.
- Verify legitimacy of investment platforms and apps before use.
- Do not respond to unsolicited OTP requests or financial offers.