CXOtoday.com
IT Perspective for Decision Makers

Quick Heal Technologies Limited Investigates the Growing Threat of Fake App Fraud, Uncovers Alarming Findings

Quick Heal Technologies Limited has uncovered alarming findings on the escalating threat of fake app fraud targeting mobile users across India. According to the researchers at Seqrite Labs, India's largest malware analysis facility, cybercriminals deploy malicious applications disguised as legitimate ones to pilfer sensitive data, drain bank accounts and compromise devices. These deceptive apps, often distributed as APK files via phishing links on WhatsApp, SMS or social media, mimic trusted brands or services to evade detection while embedding spyware, adware or billing exploits that can lead to substantial financial losses.

In a stark illustration of the scale, Apple blocked $1.8 billion in fraudulent transactions on its App Store in 2023 alone, while Indian authorities dismantled scams like a bogus crypto-mining app that defrauded investors of hundreds of crores. Research from Seqrite Labs reveals that attackers now leverage advanced tactics, including AI-generated fake reviews with uniform five-star praise to inflate credibility, deepfake voices and cloned images for social engineering, and hidden malicious code to slip past security scans. Fraudsters frequently pose as banks, delivery services or government schemes, such as a counterfeit "Pradhan Mantri Yojana Loan" app that falsely bore the Indian emblem, to lure victims into sideloading harmful software, resulting in stolen passwords, contacts and one-time passwords that enable rapid account takeovers.

Quick Heal Technologies Limited also points out that human curiosity remains the primary entry point for these threats, affecting everyone from elderly users to enterprises reliant on mobile apps for daily operations. Blended attacks combining social manipulation with obfuscated code have amplified the danger, turning everyday app downloads into potential gateways for identity theft and ransomware. The cybersecurity solutions provider has tracked such incidents

extensively, including over 250 fake dating and social apps in Asia that harvested personal files, and urges immediate adoption of vigilant habits to mitigate exposure.

To safeguard against these deceptions, users should exclusively download apps from official stores like Google Play or the Apple App Store, scrutinising ratings, reviews and developer details for inconsistencies such as generic praise, spelling errors or suspiciously low download counts for popular brands. Avoid installing from unsolicited links, QR codes or third-party sites, and always verify suspicious messages through official channels like a company's website or support email before proceeding. Keeping devices and apps updated ensures access to the latest security patches, while Android's Play Protect feature can flag phishing attempts or app mimicry in real time. If fraud is suspected, activate airplane mode immediately to sever connections, revoke app permissions, uninstall the suspect software and, if necessary, perform a factory reset after backing up essential data – as recommended by police advisories for malicious APK infections.

Quick Heal AntiFraud.AI and version26 stands at the forefront of defence, proactively providing real-time protection against the daily barrage of digital frauds targeting Indian users. The feature blocks fraudulent apps, websites, fake UPI requests, and banking fraud calls with precision. Building on years of analysis, including reports on credential-stealing Facebook apps, wormable malware via social media and auto-launching adware with millions of downloads, the technology empowers users and businesses to neutralise risks before they escalate.

Quick Heal Technologies Ltd. is a global cybersecurity solutions provider. Each Quick Heal product is designed to simplify IT security management across the length and depth of devices and on multiple platforms. They are customized to suit consumers, small businesses, government establishments, and corporate houses. Over a span of nearly 3 decades, the company's R&D has focused on computer and network security solutions.

The current portfolio of cloud-based security and advanced machine learning-enabled solutions stops threats, attacks, and malicious traffic before it strikes. This considerably reduces the system resource usage. The security solutions are indigenously developed in India. Quick Heal Antivirus Solutions, Quick Heal Scan Engine, and the entire range of Quick Heal products are proprietary items of Quick Heal Technologies Ltd. Recently, unveiled Quick Heal pioneers India's first fraud prevention solution, AntiFraud.AI available for Android, iOS and Windows.

For more information, please visit: https://smler.in/UxSeS3n

Seqrite is a leading enterprise cybersecurity solutions provider. With a focus on simplifying cybersecurity, Seqrite delivers comprehensive solutions and services through our patented, AI/ML-powered tech stack to protect businesses against the latest threats by securing devices, applications, networks, cloud, data, and identity. Seqrite is the Enterprise arm of the global cybersecurity brand, Quick Heal Technologies Limited, the only listed cybersecurity products and solutions company in India.