R120 000 Lost – From an App downloaded on Google Play

A consumer fell victim to a sophisticated scam, losing R120 000.00, after responding to a social media advert offering discounted airline tickets. After submitting her phone number and email via a link, she was contacted through WhatsApp and instructed to download an app from the Google Play Store to access promo codes. Though the link appeared secure, the app was fraudulent and embedded with malware.

Soon after installation, the consumer's phone began overheating and behaving erratically. The unexpected activation of the camera's green light raised immediate concerns. Upon checking her banking app, she discovered two unauthorised transactions and swiftly reported the incident to both her bank and the South African Police Service (SAPS).

Despite her prompt action—just 27 minutes after the transactions—the bank denied liability, citing that the payments had been authorised via selfie-authentication on her trusted device. The consumer escalated the matter to the National Financial Ombud (NFO), seeking a full refund.

Following investigation, the NFO found that:

- The funds had already been utilised before the fraud was reported, leaving no opportunity for recovery.
- The bank provided evidence that biometric authentication was used to approve the transactions.

Based on the specific facts of the complaint it was evident that the compromise originated from the consumer's interaction with a fraudulent third-party app, which contained malware capable of remote access and biometric simulation.

No proof was provided that the transactions took place as a result of maladministration or safety and security failures on the part of the bank.

By downloading the fraudulent app, the consumer essentially handed over her phone – including all the information stored on her phone – to the criminals and this resulted in the fraud. The NFO accordingly could not conclude that the bank was liable for the consumer's loss.

This type of malware doesn't just steal passwords—it can hijack your device, simulate your identity, and bypass security measures by exploiting biometric systems. That's why downloading apps from unofficial sources—even if they appear secure—is extremely risky.

How to protect yourself from mobile app scams

Be sceptical of social media promotions:

- Verify legitimacy: Check official airline websites or verified social media accounts before engaging.
- Avoid sharing personal info: Never post your phone number or sensitive details publicly.
- If it seems to good to be true, it probably isn't.

Think Twice Before Downloading Apps:

- Use trusted sources: Only download apps from verified developers with strong reviews and a high download count.
- Check permissions: Be wary of apps requesting access to your camera, contacts, or banking apps.

Secure Your Devices and Accounts:

- Enable two-factor authentication on banking and email apps.
- Use strong, unique passwords for each account.
- Install reputable antivirus software to detect and block malicious apps.

Stay Alert for Red Flags:

- Unusual phone behaviour (overheating, camera activation) could signal spyware or malware.
- Pressure tactics or refusal to stop communication are classic scammer behaviours.
- If it has to be now, then it has to be no!

Monitor Your Bank Accounts Closely:

- Check transactions daily, especially after suspicious activity.
- Report fraud immediately to your bank and file a police affidavit if needed.

Trust Your Instincts:

- If something feels off, pause and investigate. Scammers rely on urgency and confusion.

From the files of the National Financial Ombud Scheme (NFO)