Outlook MONEY

Cyber Fraud: How Fake Ads Freeze Phone And Drain Bank Balance, And What To Do

If you happened to fall prey to digital fraud by clicking a suspicious link, make sure you take the necessary steps after the fraud to safeguard yourself from such fraud-led financial loss

Summary of this article

- Fake ads lure users to download malicious APK files
- Malware hijacks screen and steals banking credentials
- Experts advise isolating the device, scan, and report fraud to cyber cell immediately after realising fraud has happened

A digital arrest, a fake customer service call, a boss scam, investment apps promising high returns, or a fake advertisement link; cyber fraudsters are adopting different ways to trap the innocent. With digital technology, artificial intelligence, apps loaded with new options and features, and different channels to show presence in the virtual world, the digital world is evolving and becoming more nuanced.

Recently, when a Kolkata-based woman lost around Rs 1 lakh after she randomly clicked on an advertisement while checking her Instagram account, her family reported that right after clicking that ad, the phone froze, not even letting them turn it off. By the time they went to a mobile phone shop, which managed to shut it down, the money had already been transferred from their bank account.
It left the family in shock, wondering how clicking a link could freeze the phone and transfer the money from their bank account. Later, they reported the incident to the police and the cyber cell.

But in today's digital world, this incident is terrifying. Is just one click enough to put a person at such a financial risk? How have fraudsters been able to empty the bank account of the victim?

Experts believe the account freeze was just a distraction in this event for them to collect banking and financial data from the phone and execute the money transfer. Let's understand how it could have worked.

How Does Clicking An Ad On Social Media Trigger A Device Freeze And Give Remote Access To Fraudsters?
Harish Kumar, CEO, Quick Heal Technologies, a cybersecurity company, says, "In most such cases, the freeze is not the real event; it is a distraction. The advertisement typically leads to a fake page or prompts the user to download an APK disguised as a reward, cashback, or verification app. Once installed, the malware abuses Android's accessibility permissions to take control of the screen. The "freeze" is often a deliberate overlay: the screen appears hung, but the device is actually being operated in the background. The freeze usually signals that remote-access or screen-control malware has been installed, and every second of inaction is being used against the victim."

It means that it's unlikely for such fraud to take place until an APK file is downloaded on the device. And these fraud-intended APK file links are shown as rewards, prizes, etc., to lure users to click on them.

Ruchin Kumar, Vice President - South Asia, Futurex, an enterprise data protection company, says, "A malicious advertisement or link can redirect the user to a phishing page, attempt to exploit a browser or operating system vulnerability, or persuade the user to download and install a malicious application. Once downloaded, the device may become slow or unresponsive because malicious software is consuming system resources, running background processes, monitoring activity, or establishing communication with an attacker-controlled server."

Does It Mean Fraudster Bypassing PIN Security And No Two-Factor Authentication Security? Harsh says, “Fraudsters rarely 'bypass' UPI security. They hijack it. With accessibility and notification permissions, malicious apps can read incoming OTPs, watch the screen in real time, and simulate taps on the victim's behalf. The PIN is entered by the victim themselves or captured through overlay screens that mimic the genuine payment interface. In effect, the fraudster rides on the user's own authenticated session, so every security check appears legitimate to the bank's systems.”

He cautions users against clicking on random ads and links that offer too good to be true deals, saying that advanced Android banking trojans even stream the screen live and execute transactions in real time. This is why security awareness must extend beyond "never share your PIN". The greater risk today is granting an unverified app the permissions that let it watch, read, and act on your phone.”

So, there is no need to get scared of using a banking platform or an app, but make sure you download it from an authentic source instead of social media links. For a long time, experts have been talking about APK files that can corrupt your device’s system, collect data, or give remote access to fraudsters, leading to financial fraud.

Ruchin emphasises, “It is more accurate to describe these incidents (digital financial fraud) as authentication-factor compromise or device compromise, rather than saying that the attacker has simply bypassed PIN security.” This distinction is important because strong cryptography remains a critical security layer, but it must operate as part of a broader architecture incorporating secure key management, application security, device integrity, transaction monitoring, and fraud detection.

In simple words, two-factor authentication or a PIN is a robust security measure in financial and banking transactions, making it difficult for fraudsters to bypass. But if the device or an app itself is not secure, users become vulnerable to fraud because transactions are done with proper, however stolen, authentication details.

What Should One Do If The Phone Freezes After Clicking A Link?

Ruchin suggests isolating the device and protecting financial accounts before investigating what happened. HE further suggests the following steps:

- Do not enter UPI PINs, bank credentials, or OTPs in the potentially compromised device
- Don’t respond to calls or messages that claim “unlock” or secure your phone

- Check recently installed apps and remove the suspicious ones or revoke unnecessary permissions
- Run a mobile security scan
- Contact the bank and check the transaction history for any unauthorised activity
- Save evidence, such as suspicious URLs, application names, transaction details, and so on, instead of deleting everything

Harsh says that the user may even perform a factory reset if compromise is suspected, and adds, “Always remember: genuine banks or brands never ask you to install an app or share screens to resolve an issue.”

Lastly and more importantly, inform the police or cyber cell at 1930 immediately after realising a fraud has happened, report the incident clearly and lodge the complaint.