



This recent scam is impressively complex. The cyber criminals start by impersonating law enforcement officers. They contact you, claiming that your bank account may have been involved in financial fraud. You're then asked to download a mobile app to help them investigate further. If you download the app, the cyber criminal walks you through the steps to set this scam in motion.

First, you are given a case number. When you search for that number in the app, you'll find legal-looking documents with your name on them. These documents make the scam feel more legitimate. Once your guard is down, the app asks you to select your bank from a list and then enter your account number and other personal information.

The most clever part of this scam is what the app does in the background. When you first install the app, it blocks all incoming calls and text messages. That way, you won't be alerted if your bank attempts to contact you about unusual behavior on your account. If all goes as planned, the cyber criminals will steal your money and sensitive information before you know what happened.

No matter how advanced the app is, you can stay safe from scams like this by following the tips below.

- Only download apps from trusted publishers. Anyone can publish an app on official app stores or sites—including cybercriminals.
- Be cautious of scare tactics that play with your emotions. Cyberattacks are designed to catch you off guard and trigger you to reveal sensitive information.
- If you're contacted by someone claiming to be in a position of authority, like law enforcement, ask them to confirm their identity. Real officials will understand your concerns and can provide information that doesn't require you to download an app.