How are scammers using your face to commit fraud?

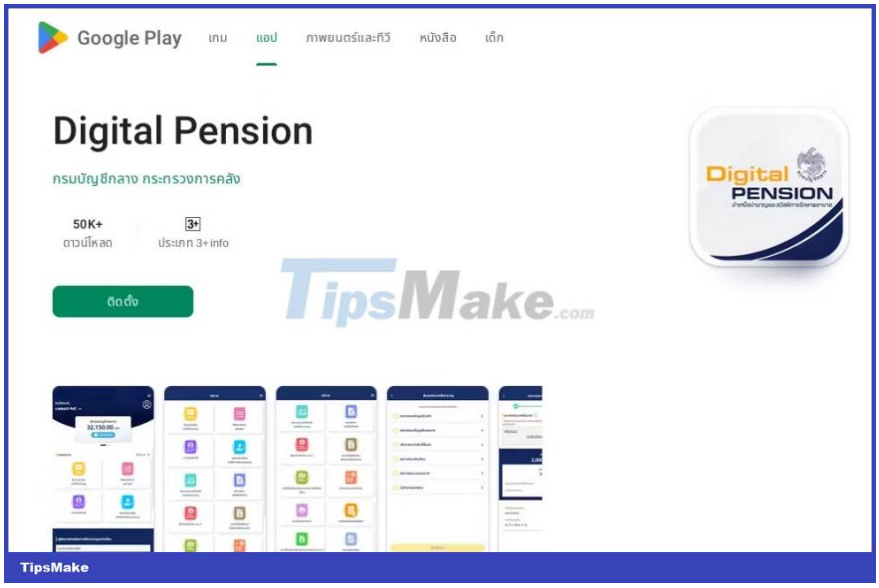
How cautious are you about how your face is used on the Internet? If you do not appreciate the importance of this, you should change it immediately.

Now is a good time to start, because there's a new type of smartphone malware called Gold Pickaxe that's designed to collect your facial data and use it as part of a phishing scam. .

What is Gold Pickaxe?

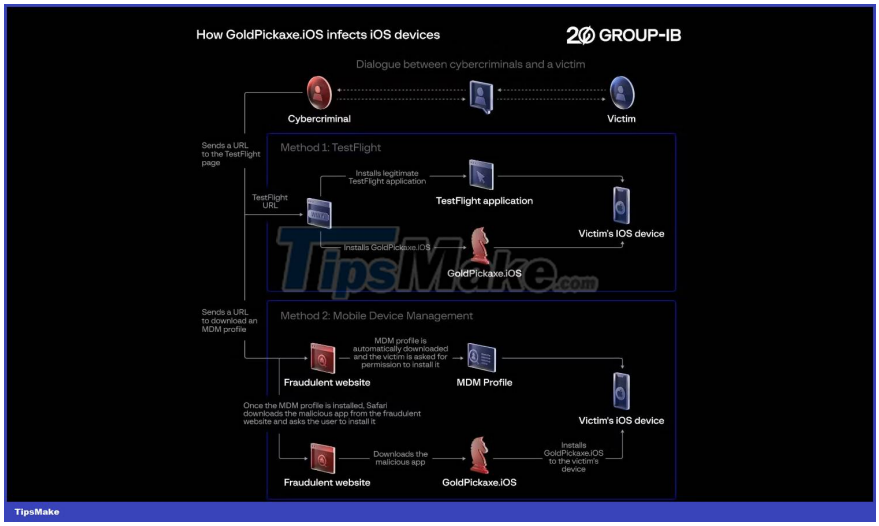
As reported by Bleeping Computer, Gold Pickaxe is a malicious mobile app first discovered by security firm Group-IB, as part of a much larger and long-term malware campaign called Gold Factory. Gold Pickaxe is often disguised as a legitimate application to trick people into downloading it; it is considered as iOS Trojan or Android Trojan.

To increase the number of people downloading the app, Gold Pickaxe operators sent Social Engineering emails impersonating government officials. Emails often push users to download fake apps. In the reported example, the app was disguised as a digital pension manager using a page impersonating the Play Store, the Android app store.



How does Gold Pickaxe work?

Once the victim downloads the infected app to their phone, the app immediately starts collecting data about the user. This includes looking through text messages, scanning web traffic and looking through files. As part of Social Engineering, victims are asked to install a Mobile Device Management (MDM) profile. Once installed, the operator of the Gold Pickaxe malware has almost complete control over the device as MDM grants access to features such as remote wiping, device tracking, and app management. use, etc.



However, they cannot steal banking information immediately, and what sets Gold Pickaxe apart from other malware strains is its primary target. It will attempt to obtain an image of the victim's face, which can be achieved through one of two ways.

The first is by directly asking users to scan their faces. This is why Gold Pickaxe often comes in the form of a government-backed app, as it's not uncommon for these apps to request face scanning through the phone's camera. When a user logs their face through the app, it takes the data and sends it back to the scammer. A more advanced variant of the malware, Gold Pickaxe

The second is to indirectly steal the victim's facial data. In some Gold Pickaxe models, it will continuously take photos through the front camera in the hope of capturing your face. If it can't do that, it can instead send photos saved on the phone to see if they contain your face.

According to Group-IB:

> GoldPickaxe.iOS is the first iOS Trojan discovered by Group-IB, combining the following functions: collection of victim biometric data, ID documents, SMS interception and authorization of traffic through the device of the victim. Its Android cousin has even more functionality than the iOS version due to more limitations and the closed nature of iOS.

It's important to note that the malware does not obtain facial biometric data from services like Face ID. Instead, it tries to take pictures of your face through the camera or in files.

What can scammers do to your face?

It might seem strange that a scammer would try to get a picture of your face, but there are plenty of reasons why scammers would seek out that data.

Gold Pickaxe collects facial data to help hack banking information. Some banks will not allow users to deposit large sums of money without having their face scanned, so obtaining the victim's facial data will allow fraudsters to avoid that restriction.

However, that's not the only way a scammer can use an image of your face. We are seeing a rise in convincing deepfakes that allow people to create a fake version of someone to say whatever they want. These deepfakes can then be used to commit more fraud.

Ultimately, if someone is trying to steal your identity, facial data is a good starting point for fraudsters to begin their fraud. With this data, they can borrow money and create official documents in your name. The scammer will need a little more data than a name and face to do this, but with the way Gold Pickaxe sends tons of data, the scammer can pick out important information from it.

How to stay safe from face scanning attacks

Scary things like Gold Pickaxe rely heavily on someone trusting the initial email and downloading the app from a fake website. So, don't always download apps from suspicious sources and learn how to protect yourself from Social Engineering attacks.

When installing an app, make sure to read all permissions carefully. If an app that doesn't need to see your face or your surroundings requests camera access, handle it with caution. You can also install an antivirus application to remove these malicious applications from your system.

Additionally, on Android devices, do not sideload apps, especially apps you don't know, don't trust, or can't research or check to see where they come from.

And if you're worried about having so many images of your face on the Internet, see if you can enable additional defenses on your sensitive online accounts. For example, if your account supports two-factor authentication (2FA), turning it on adds another layer of protection that scammers need to solve before they get into your data. Setting up and using this feature is also really easy.