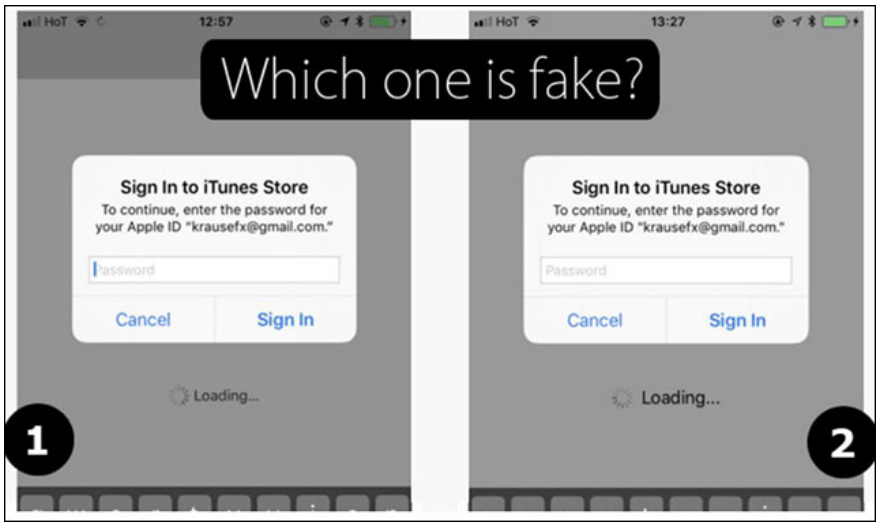
Watch out for phishing attacks that can steal Apple ID passwords very hard to detect

Felix Krause, the iOS developer and founder of Fastlane.Tools, describes a nearly undetectable phishing attack, explaining how iOS apps poisoned to steal Apple ID passwords to access iCloud accounts and personal data.

Looking at the 2 images of the iCloud password asking iPhone users below, you can distinguish what is real, what is fake?



The screen requires entering iCloud password

At first glance, these two screens are identical, but the pop-up shown on the second picture is just a fake - a perfect attack is used to trick those who are not careful.

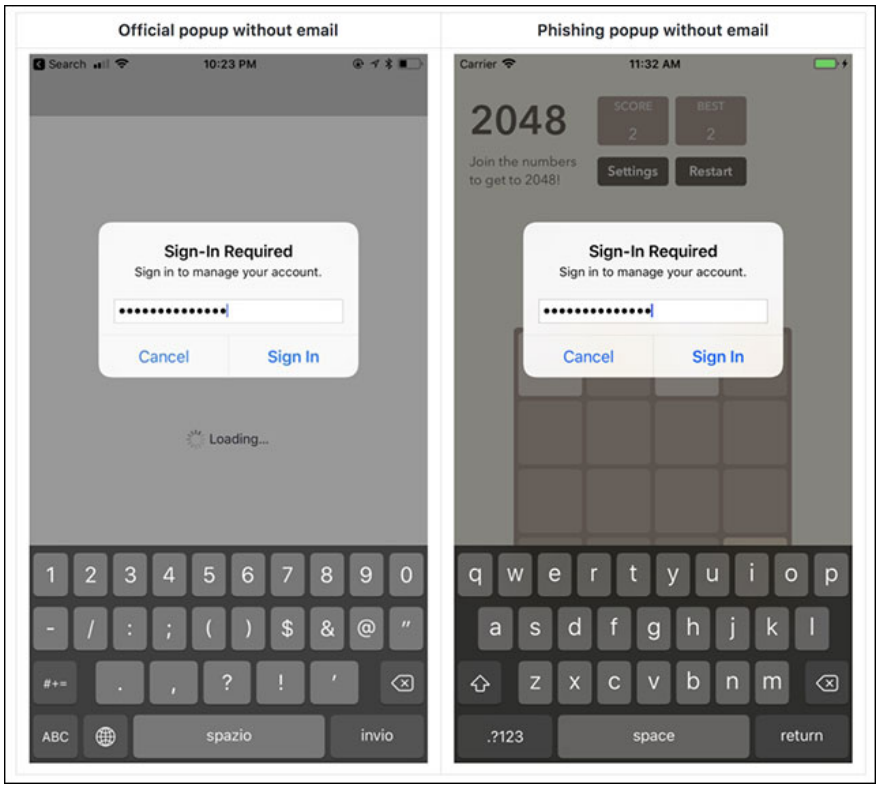
Felix Krause, the iOS developer and founder of Fastlane.Tools, describes a nearly undetectable phishing attack, explaining how iOS apps poisoned to steal Apple ID passwords to access iCloud accounts and personal data.

According to Krause's post, the iOS app only needs to use UIAlertController to display a fake dialog, mimicking the look and language that Apple uses. This makes it easier for hackers to persuade users to give Apple ID passwords without a doubt.

> 'iOS can ask users for iTunes passwords for a variety of reasons, most commonly updating iOS operating systems or applications. At that time, users often enter their Apple ID password without question, 'Krause said. 'However, these pop-ups are not only displayed on the lock screen, Home but

also in the app, for example when accessing iCloud, Game Center or IAP'.

The app developer can also create fake alerts without knowing the user's email because sometimes Apple does the same as shown below.



Login without user email

Although there is no evidence of an attacker exploiting this trick, Krause says that it is easy to copy the system notification dialog, any standalone application can do it. For security reasons, he did not give the actual source of pop-ups when describing this attack.

This is how to prevent this type of smart phishing attack

Krause advises users to press the Home button when suspicious dialog boxes appear. If this operation closes the application and the dialog box is a scam. If both the dialog and the application are still there, that's true Apple.

'The reason is that the system dialog is running on another process, not part of the iOS app'.

Krause also recommends that users avoid entering information into any pop-ups, instead opening Settings and filling in them, as well as how users are encouraged not to click on the link received via email and then visit the website itself.

Even more important is the use of two-factor authentication, even when a password is available, the attacker does not get an OTP.

and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.