Fake finance apps on Google Play target users from around the world

By Lukas Stefanko

Archived: 2026-04-05 15:07:15 UTC

Scams

Cybercrooks use bogus apps to phish six online banks and a cryptocurrency exchange

19 Sep 2018 • , 3 min. read

Another set of fake finance apps has found its way into the official Google Play store. This time, the apps have impersonated six banks from New Zealand, Australia, the United Kingdom, Switzerland and Poland, and the Austrian cryptocurrency exchange Bitpanda. Using bogus forms, the malicious fakes phish for credit card details and/or login credentials to the impersonated legitimate services.

NetBank mobile

LogCorp Books & Reference

★★★★☆ 4

3+

Add to Wishlist Install

GoMoney

First Green Development Books & Reference

★★★★★ 3

Everyone

Add to Wishlist Install

Online Money

EuropeUnitedGroup Books & Reference

Everyone

Add to Wishlist Install

Post Finance

System Technologies Apps Books & Reference

Everyone

Add to Wishlist Install

WBK Zachodni mobile

bzwbsz wbk Dla firm

★★★☆☆ 7

PEGI 3

Aplikacja jest zgodna z niektórymi Twoimi urządzeniami.

Dodaj do listy życzeń Zainstaluj

Bitpanda Viewer

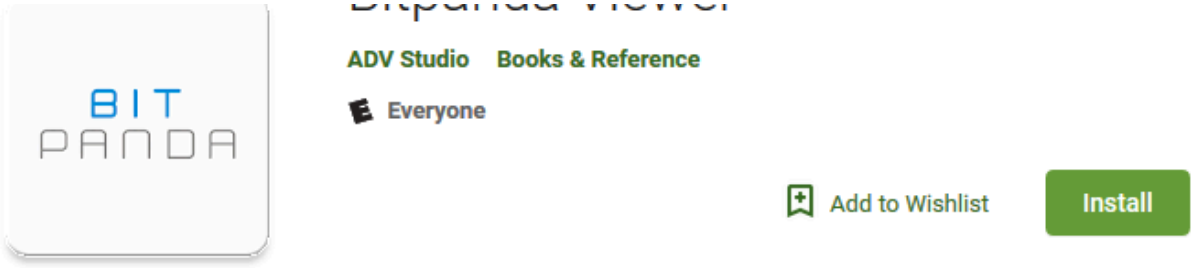

Figure 1 – Six of the malicious apps found on Google Play

The malicious fakes were uploaded to Google Play in June 2018 and were installed more than a thousand times before being taken down by Google. The apps were uploaded under different developer names, each using a different guise; code similarities, however, suggest the apps are the work of a single attacker. The apps use obfuscation, which might have contributed to their slipping into the Store undetected.

The sole purpose of these malicious apps is to obtain sensitive information from unsuspecting users. Some of the apps take advantage of the absence of an official mobile app for the targeted service (such as Bitpanda), while others attempt to fool users by impersonating existing official apps. The full list of targeted banks and services can be found at the end of this article.

How do the apps operate?

While the apps don't follow one common procedure, upon launch they all display forms requesting credit card details and/or login credentials to the targeted bank or service (examples can be seen in Figure 2). If users fill out such a form, the submitted data is sent to the attacker's server. The apps then present their victims with a "Congratulations" or "Thank you" message (an example can be seen in Figure 3), which is where their functionality ends.

PostFinance

REGISTER

AUTHORIZE

Please provide additional information so we can ensure that this request is being made by you

Card number

Card expiry (MM/YY)

CVV/CVC Code

SecureCode

VERIFY

ANZ

GoMoney

Hi and welcome to ANZ GoMoney!
If you're an existing ANZ Australia customer, you're just a few taps away from managing your account in one easy place.

To start, please register your device.

Log in to ANZ Internet Banking

Customer Registration Number

Password

Log in

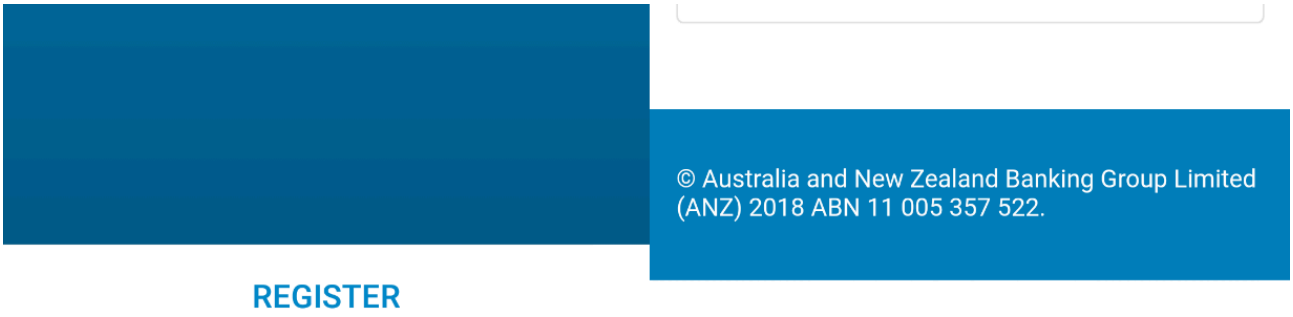

Figure 2 – Bogus forms phishing for credit card details and internet banking login credentials

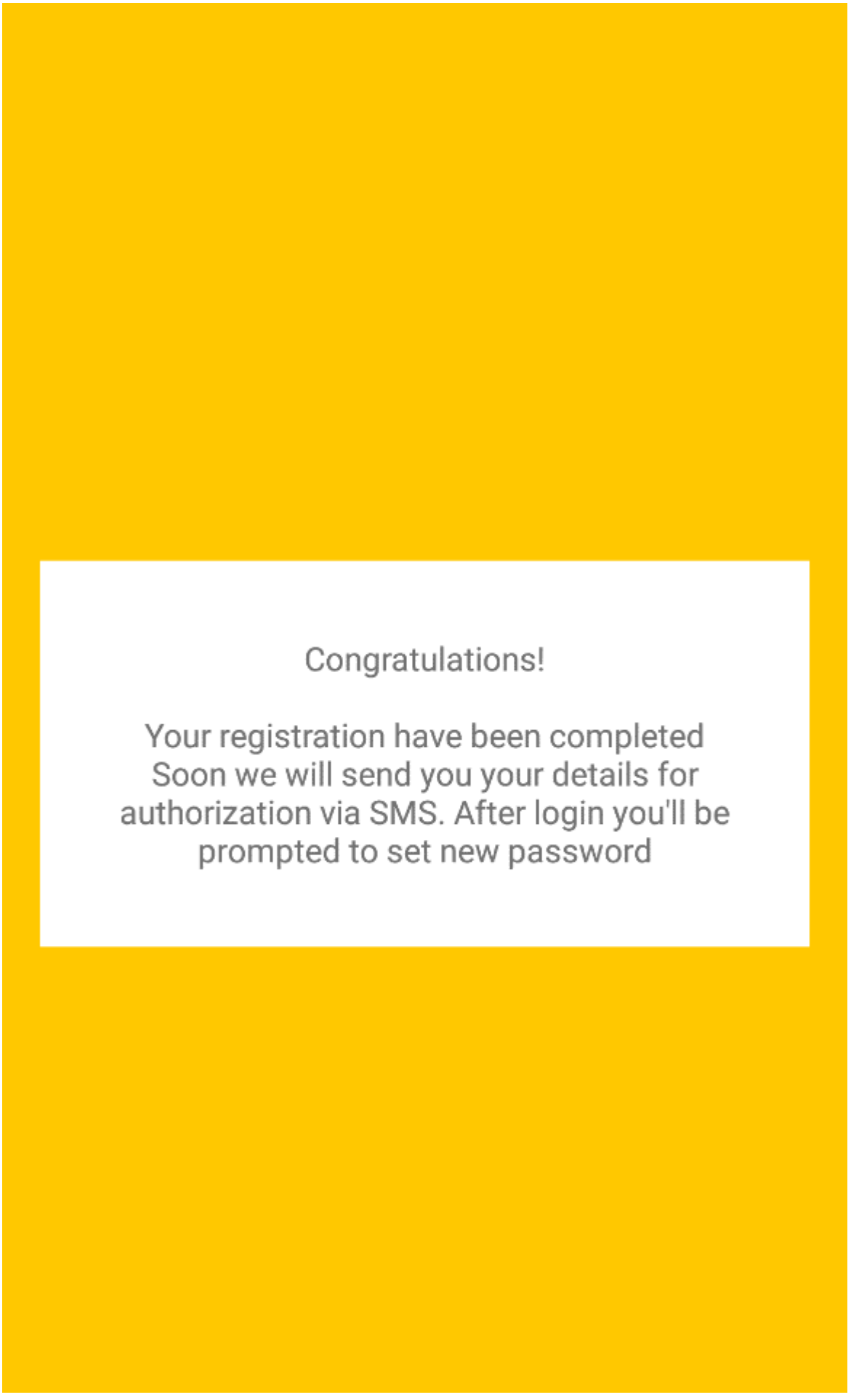
Congratulations!
Your registration have been completed
Soon we will send you your details for
authorization via SMS. After login you'll be
prompted to set new password

Figure 3 – Final screen displayed by one of the malicious apps

How to stay safe

If you suspect that you have installed and used one of these malicious apps, we advise you to uninstall it immediately.

Also, change your credit card PIN codes as well as internet banking passwords and check your bank accounts for suspicious activity. If there have been unusual transactions, contact your bank. Users of the Bitpanda cryptocurrency exchange who think they have installed the fake mobile app are advised to check their accounts for suspicious activity and change their passwords.

To avoid falling victim to phishing and other fake financial apps, we recommend that you:

- Only trust mobile banking and other finance apps if they are linked from the official website of your bank or the financial service
- Only download apps from Google Play; this does not ensure the app is not malicious, but apps like these are much more common on third-party app stores and are rarely removed once uncovered, unlike on Google Play
- Pay attention to the number of downloads, app ratings and reviews when downloading apps from Google Play
- Only enter your sensitive information into online forms if you are sure of their security and legitimacy
- Keep your Android device updated and use a reliable mobile security solution; ESET products detect and block these malicious apps as Android/Spy.Banker.AIF, Android/Spy.Banker.AIE and Android/Spy.Banker.AIP

Targeted banks and services

Australia and New Zealand

Commonwealth Bank of Australia (CommBank)
The Australia and New Zealand Banking Group Limited (ANZ)
ASB Bank

The United Kingdom
TSB Bank

Switzerland
PostFinance

Poland
Bank Zachodni WBK (renamed to Santander Bank Polska SA in September 2018)

Austria
Bitpanda

Indicators of Compromise (IoCs)

Package name	Hash	Detection
cw.cwnbm.mobile	651A3734103472297A2C65C81757FB5820AD2AB7	Android/Spy.Banker.AIF
au.money.go	DE09F03C401141BEB05F229515ABB64811DDB853	Android/Spy.Banker.AIF
asb.ezy.pay	B6D70983C28B8A0059B454065D599B4E18E8097C	Android/Spy.Banker.AIF
uk.mobile.tsb	91692607FB529218ADF00F256D5D1862DF90DAAF	Android/Spy.Banker.AIF
ch.post.finance	FE1B2799B65D36F19484930FAF0DA17A0DBE9868	Android/Spy.Banker.AIF
pl.mblzch	C43E7A28E1B807225F1E188C6DA51D24DCC54F5F	Android/Spy.Banker.AIE
www.bit.panda	7D80158C8C893E46DC15E6D92ED2FECFDB12BF9F	Android/Spy.Banker.AIP