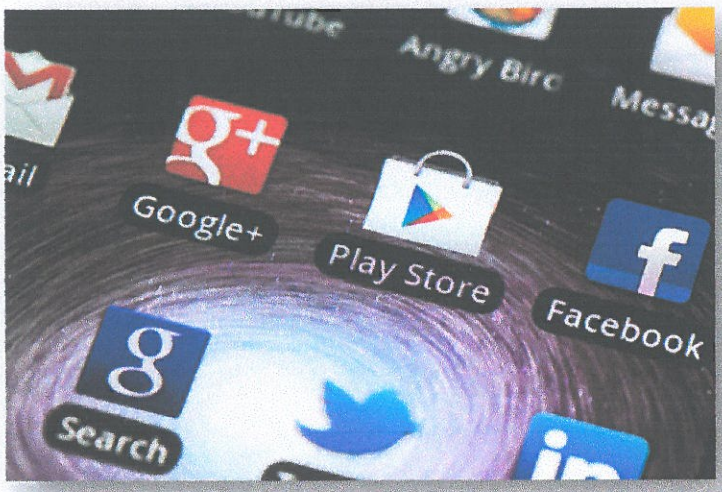
GENERAL HEADQUARTERS
ARMED FORCES OF THE PHILIPPINES
OFFICE OF THE DEPUTY CHIEF OF STAFF FOR COMMUNICATIONS, ELECTRONICS AND INFORMATION SYSTEMS, J6
Camp General Emilio Aguinaldo, Quezon City

CMD

CYBERSECURITY BULLETIN

Cybersecurity Bulletin: 2016–15

How to Spot a Fake Android App



Malware on mobile devices is rampant. CNN reports that 55% of Internet traffic in January was on mobile devices, so it seems natural that cybercriminals target mobile, often devising scams using the apps that are most familiar to users.

Just because an app is in the Google Play Store doesn't mean that it is a legitimate app. Google is constantly removing fraudulent apps from the Android marketplace, such as fake antivirus, browsers, and games. Recently, Symantec discovered cyber scammers attempted to impersonate Norton products, and, while imitation is the sincerest form of flattery, we recommend that you use caution when downloading apps from app markets.

Besides Google Play, and other app markets, there are many other ways that fake apps can get onto your Android device. Scammers will try any means necessary to trick you into installing a fake app. Criminals use emails and SMS messages that appear to be from your bank, credit card company or other brands to trick people into downloading applications that will compromise their data. Sometimes fake apps will pose as security updates, and clicking on the links may also lead to your information being stolen.

If you're an Android user and you receive an unexpected SMS, a strange alert or notification, or unusual requests from what may seem to be your bank or other familiar brand, beware: criminals may be trying to rip you off.

What can you do to protect yourself?

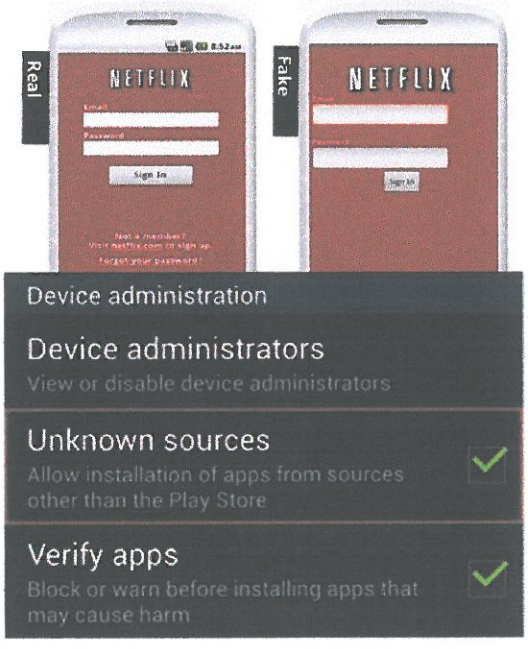
Unsolicited texts, emails, or sudden notifications that appear to be from a bank, retailer, or other known institution may not always be what they seem. Use caution with any link delivered to you and always read the message first. Instead of using the link supplied in the message, go directly to the website in question and log into your account the way you would normally. If the message seems particularly worrisome, call the company directly to verify the information before acting online.

Also, only download Android apps from official sources, such as the Google Play Store. Before downloading any app, do some research. How many times the app has been downloaded? A wildly popular app is a telltale sign of a good app. Read app reviews, look at the developer, and do a search online. There could be more information coming from other users who have previously been duped. Cybercriminals may try to fool you with fake reviews that are often short and generic, so be sure to check out any other apps made by the developer. The more apps that developer has created, the higher the chance that the developer is the real deal.

Security or software update notifications can be a bit trickier to decipher. Often users receive a prompt to install an urgent security update. Your best action in this scenario would be to search online to find out information about that update. If there are multiple discussions online about that specific security update, that can confirm if it is genuine.

There are also clear visual things that stick out if you want to identify fake Android apps. Spelling errors, shoddy logos, and unbalanced or poorly formatted interfaces are clues the app may be fake.

Recently, there was a fake Netflix app floating around. The visual cues were all there- the fake app had the login fields way off to the left of the screen and used a smaller, more awkward sign-in button.



Always remember to think before you click. Even though there may be a sense of urgency to one-click and install, it is better to take the time and remind yourself of all the signs an app may be fake.

An easy protection step everybody should take is to visit your Android settings and make sure you do not allow third-party app downloads from untrusted sites.

In case of any cyber-related incidents, report immediately to the AFP Computer Security Incidents Response Team (AFPCSIRT), Cyberspace Security Group, CEISSAFP, at AFPTSN 911-6001 local 5873.

Reference:

This was cross posted from:
https://community.norton.com/en/blogs/norton-protection-blog/how-spot-fake-android-appjp as referenced by CMB, G6, PA Cyber Security Bulletin #67 with minor additions/modifications.