Assignment 2: Android Intents

Part 1: Analysis of fake applications in the app market (30 points)

**1. List at least five fake apps that you came across in your analysis**

* Update Whatsapp Messenger(“WhatsApp+Inc%C“WhatsApp+Inc%C2%A0”2%A0”)
* Cooee game (Renan Silva Das Neves)
* MyEtherWallet (Ethereum Wallets)
* Waze Plus (DevTech Inc.)
* Messenger (FORBIS s.r.o)

**2. Based on your analysis - What are some of the potential risks that these fake apps can cause? (briefly explain them)**

* **Malware**.

The malware has been found to exploit known weaknesses in the Android operating system to replace legitimate installed apps on the device with malicious versions without requiring users’ intervention. A malware Agent Smith has been found to leverage its broad access privileges to display fraudulent ads and profit off them.

* **Aggressive Adware**.

A developer, called Pinwheel, which published at least 40 identical fraudulent apps. Some of these apps were named after popular games and movies, such as *Far Cry* and *13 Reasons Why,* to entice users to install them. When launched, these apps show users only an image that’s similar to the Play Store app’s image, with very aggressive advertisement pop-ups. Unbeknownst to the user, the image displayed is not an actual splash screen, but rather a static image.

* **Intercept sensitive data.**

Consumers spent $9.36 billion online over the four-day Black Friday weekend, of which $1.2 billion was driven by mobile shopping. Meanwhile, thousand of apps, blacklisted for being dangerous, are hosted by app stores around the world, even the Apple App Store and Google Play. These apps use the branding of well-known retailers to attempt to fool users into entering credit card information, which opens them up to potential financial fraud. Some fake apps contain malware that can steal personal information or lock the device until the user pays a ransom. Others encourage users to log in using their Facebook or Gmail credentials, potentially exposing sensitive personal information.

* **Malicious activities.** A version of the popular mobile app Facebook has been found to be infected with what we detect as Android/Trojan.Spy.FakePlay.  Facebook Lite is a more compact version of the popular app that uses less data and claims to work in all network conditions. The infected Facebook Lite works as advertised, but with the addition of malicious activities. It contains code that steal personal information and installs additional malicious apps. It contains Code that steals and sends device ID, System Version, MAC address, Phone Model, Location, etc.

**3. What are the steps to eradicate the fake apps? And what are the measures that users can take to stay away from them?**

* **Take a close look at search results.**

If you search the Play Store for the app you want to install, take a few seconds to glance at all the entries—especially if you see the same icon more than once. Fake apps will almost always use the icon from the app they’re trying to mimic, so it should immediately cause suspicion if you see the same icon more than once.

* **Check the App Name and Developer**

If the developer name isn’t an immediate indicator, you should also check their other apps. You can do this on the web by clicking on the developer name on the Play Store listing

* **Check the Download Count.**

If you’re downloading a popular app, always take a quick look at the download number. Let’s say you’re installing the Facebook app—one of the most downloaded apps in Google Play with over a billion installs at the time of writing.

* **Read the Description and Screenshots.**

Most legitimate developers do a good job of providing clear communication as to what their apps do. Most use good, clean formatting in the listing.

* **Read the reviews**

Spend some time reading a few of the reviews. Fake apps will often have fake reviews, but there are also likely to be some legitimate reviews from users who realized the app was bogus after installing it.

* **Keep the android operating system updated**

Any device that isn’t running the latest version of its operating system is more vulnerable to exploits used by fake apps.