Beware of Android scams!

Existing forms of fraud are becoming more and more sophisticated, even on smartphones is a fertile ground for scammers to act. In this article, we will help you be aware of the types of scams on Android like ...

Existing forms of fraud are becoming more and more sophisticated, even on smartphones is a fertile ground for scammers to act. Just a small link, users click to become victims of bad guys, even accidentally become a support for them when we share links or certain information. In this article, we will help you be aware of the types of scams on Android.

1. Phishing by message:

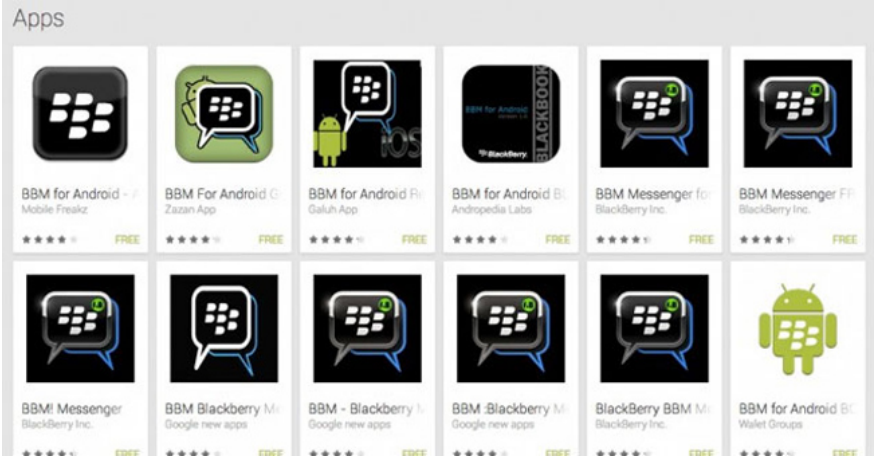
This form in Vietnam appears very much and is now spreading on smartphone devices. Normally, users will receive a message from a strange number asking you to provide personal information, phone number, address . to be able to confirm the prize in a program that you have not participated in. before.

Or you will receive an email informing your personal account at a certain website or Facebook that has been stolen and need you to verify your personal information by re-supplying your password, PIN . to a location. Only the link they sent. A few minutes later, all your personal information has been completely taken over by the bad guys and can be used at any time. With this form you need to be absolutely alert and not believe in any text messages or emails, unless you are sure that it is the phone number or official email message from the website.

2. Fake application:

The fake application once became "exciting" when rampant unknown manufacturers applications. When you search for a link to download some famous software on Google will produce a series of results with many

different download links. Of course, there is only one link to get you to download standard software.



Or some websites when you visit will show that your device is being invaded by viruses, and suggest that you download a piece of virus. All the remaining Apk files you download are actually malware or trojans, if you install them then the personal information will be stolen. In order not to suffer from this situation, you should only install software that has clear origin and is best on the Google Play repository.

3. Fake technical support:

High-tech fraud or phishing technical support has begun to appear in the late 1990s, starting from desktops and spreads to smartphones. There will be a stranger calling you and recognizing yourself from the manufacturer or equipment provider, they claim your computer is infected with the virus and promise to help you as much as you need to pay for first.

They will then entice you to pay money through a fake website and personal information and bank card will be stolen. Whenever you receive such a message or call, do not rush to follow their instructions, then hang up the phone and immediately call the service operator number where you purchased the goods to make sure.

4. Repairing scams:

Some mobile phone shops specialize in replacing components or stealing information when customers send phones to repair. The most easily disconnected components are batteries, monitors, speakers, cameras . Therefore, it is advisable to only send equipment to reputable repair shops or preferably to authorized genuine stores. .

Refer to the following articles:

1. Protect your Android device from the risk of malicious software attacks
1. How to identify Fanpage phishing like sentences on Facebook
1. How to avoid "warranty stamp trapping" laptop?

Hope this article is useful to you!

You finished reading the article "**Beware of Android scams!**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.
