How to make money by finding security issues in Android apps

If you are an Android app developer who is able to find security issues, you can make money by showing your talents to Google.

If you are an Android app developer who is able to find security issues, you can make money by showing your talents to Google. Hackers have brought malware-infected applications to the Google Play Store, some of which have been downloaded millions of times.

In response, Google launched the Bug Bounty program, which rewards users for discovering vulnerabilities, allowing developers to find security issues in many common applications. Previously only a few applications were included. Now, all popular Play Store apps are part of the program. The cash rewards program for developers to find and report security issues.

Find security issues in Android apps - Your chance to make money from Google

1. Why did Google create the Bug Bounty program?
2. How to participate in the Bug Bounty program?
3. Earn bonuses for detecting data abuse by the app itself
4. What are the rewards for finding specific errors?

Why did Google create the Bug Bounty program?

Google has had a Bug Bounty program for its own applications for a long time. Like many companies, Google awards developers for discovering problems in their websites. It also awards rewards for finding bugs on its Chrome browser or Chrome operating system. But recently, Google has taken the leap forward, by offering rewards for bugs found in many other companies' applications.

The first step of the Bug Bounty program on the Play Store only applies to a very small number of top apps. Now, Google has expanded the program to cover any app in the Play Store with over 100 million installs. This means that there are more chances for bug hunters to find problems in the Play Store app and be rewarded for reporting them, even if the app developer doesn't publish Bug programs. Bounty of their own.

Google said it introduced the program in the hope of encouraging the community to join hands to improve security for everyone. Therefore, Google encourages bug hunters to find problems and report them to app developers as well as Google. This gives root app developers the opportunity to fix bugs quickly. And that

means better security for all Android app users.

How to participate in the Bug Bounty program?

The Bug Bounty program on the Play Store is called the **Google Play Security Reward Program (GPSRP)** . Google invites security researchers and application developers to participate. The first step is to fill out an application form to join the program. You can look for security issues in any eligible Play Store app after being approved.

There are 3 types of vulnerabilities that participants seek. Firstly, Remote Code Execution vulnerabilities (remote code execution) are vulnerabilities that allow hackers to access a user's device and make changes. These are very serious security issues.

The second is the issue of non-confidential data privacy. This is where a vulnerability allows hackers to steal personal information such as login information, web history or contact lists.

The third is access to protected application components. This refers to applications that perform functions for which they are not authorized. For example, an application sends SMS messages even if the application does not have the user's permission to do so.

The program does not include some security issues. For example, phishing attacks, though potentially very dangerous, are not eligible for the program. The reason is that they work by cheating users, not by running malicious code. The program also does not include attacks that require physical access to the device.

When you discover an error, you should contact the application developer to let them know. You can then work together with that developer to fix the problem. Once the vulnerability has been resolved, you can claim a cash reward from Google.

Earn bonuses for detecting data abuse by the app itself

Not only does Google reward rewards for finding security bugs. The company is also trying to "crack down" applications stealing user data. Recently, the company launched the **Developer Data Protection Reward Program (DDPRP)** , which provides similar rewards for developers who detect data misuse by applications.

The types of data abuse the program is looking for are applications that collect and sell user data in a way that opposes Google's privacy policy. For example, this could be an application that collects data from users' contact books, such as metadata indicating who, when and when they called, without being protected as sensitive data. cold.

The program will also include apps that violate permission rules, such as apps with access to SMS, but use this to collect data about SMS users and sell it to third parties. father. In addition, it also involves an application requesting access to contact data and then reusing that data for an unrelated application.

For more precise details on the types of data abuse eligible for the program, you can look on the DDPRP website. As with the Bug Bounty program, any app on the Play Store with over 100 million installs is eligible.

What are the rewards for finding specific errors?

There is a cash reward given in both the bug detection and data abuse program. The amount paid for any report depends on the severity of the problem. It also depends on the quality of the report sent to Google.

The rewards for the Google Play Security Reward Program range from $ 5,000 to $ 20,000 for remote code execution errors, from $ 1,000 to $ 3,000 for unsecured private data theft errors, and from $ 1,000 to $ 3,000 for access errors. Application part is protected. In addition, there are rewards for detecting vulnerabilities for application developers responsibly. This gives developers the opportunity to fix the problem.

The rewards for the Developer Data Protection Reward Program range from $ 100 to $ 1000. To receive the reward, you need to submit a report. You should write down information about which data policy is violated, how the data was abused, and a list of the number of times the application violated the policy.

Google's data collection and error detection programs give you the opportunity to make money. They also allow you to jointly improve the security of applications distributed through the Play Store. If you're interested in more opportunities to hunt for bugs, you can also check out other companies' programs.

Good luck!

for similar articles on tips and guides. Thank you for reading and for following us regularly.