

Identity Theft? There's an App for That



Smartphones are among the most important innovations of our time. We rely on their increasingly sophisticated technology as it gives us “on-the-go” access to anything, anywhere, with the touch of a finger. But in our zeal to acquire the latest and greatest applications promising to increase our productivity and up our fun factor, we can open ourselves up to wolves in sheep’s clothing.

According to a recent [Symantec Intelligence Quarterly](#) report, cybercriminals are launching more targeted attacks with more sophisticated malware than ever before and their favorite target is currently the Android phone.

With its vulnerabilities (Symantec documented [163](#) in mobile devices in 2010) and the open, community-policed Android Market, cybercriminals are becoming more creative in their battle to gain full or partial control of your device. One method they’re employing goes to the heart of a smartphone’s functionality: its applications.

Whether they develop malicious apps from scratch or insert malicious logic into legitimate applications, attackers are distributing more Trojan programs than ever before. Telling the difference between safe and infected applications can be difficult so we’ve put together a list of tips from industry leaders.

1. Check the rating. If the app receives four or five stars it’s probably safe. If there’s no rating, do more research.
2. Read the comments and reviews. Before you download anything, make sure you read multiple opinions of the various users who have gone before you. If there aren’t any comments, try the Android user forum search.

3. Check the permissions. Before installing an app, you should read the alerts that tell you what information the app will access. If you feel uncomfortable in any way with the level of disclosure, cease the installation. No application should require access to contacts or passwords.
4. Check Android user forums. Search the Android user forums for the app name or post a question for other users to answer. Community members can offer you a wealth of information and your question could, in turn, help someone else.
5. Check the developer's website. What does it look like? Is it professional? Does it seem like there is a real person on the other end of the digital line? Note: Even a malicious operation can have a professional-looking website, so you should engage in other checks as well.
6. Post your own comments. The more information available on the products in the marketplace, the safer they become.
7. When in doubt, don't download. If you still don't feel comfortable, move on to the next app. The beauty of this ever-changing, ever-evolving landscape is that developers are constantly coming out with new ways to make your life easier and more fun.