OUCH! October 2024

OUCH!

SANS SECURITY AWARENESS

The Monthly Security Awareness Newsletter for You

Download Danger: How to Outwit Malicious Mobile Apps

The Mysterious App: A Short Cautionary Tale

One lazy Sunday while on social media, Sarah stumbled upon an ad for a new photo editing app, 'PiksPerfect.' Intrigued by its stunning filters, she downloaded it without hesitation. At first, the app worked great, but soon her phone became sluggish, and random ads began popping up. A few days later, Sarah received a call from her bank about suspicious transactions totaling thousands of dollars. In a panic, she checked her bank app and found her savings nearly wiped out. After reporting the fraud and freezing her account, she was left confused and upset.

Her tech-savvy friend discovered the truth: the mobile app was a fake, stealing her personal information, including banking details. It took months to recover, but Sarah became more cautious, researching mobile apps before installing them. She now shares her story to warn others, understanding that a moment of carelessness can have far-reaching consequences.

How Do I Know What Apps are Safe?

Mobile apps are convenient and powerful, enabling us to do just about everything in our lives with the touch of a button. However, cybercriminals are taking advantage of this by creating fake or malicious mobile apps. If you download one of these apps, they can take over your phone and monitor everything you do. The key to protecting yourself is making sure the mobile apps you install on your devices are legitimate and safe.

First and foremost, download mobile apps only from official stores where vendors review the mobile apps, such as the Apple App Store or Google Play Store. This helps reduce the risk of downloading a bad mobile app. Third-party app stores often cannot be trusted and may even be managed by cybercriminals. But even when using a trusted mobile app store, you have to be careful. Here are some additional steps you can take to ensure you are downloading legitimate, safe mobile apps.

1. **Check the Developer's Name**: When looking for a specific mobile app created by a certain company, make sure the app you are downloading is made by that company. A common trick for scammers is to create mobile apps that look very similar to well-known apps. Check the developer's name—is it the same company or a well-known developer or is the app developed by someone you have never heard of? Another option is to visit the official website of the app or developer to find direct links to the mobile app in the app store. This ensures you're downloading the official app.

2. **Read Reviews and Ratings**: Look at user reviews and ratings. A legitimate app will have a significant number of positive reviews and high ratings. Be wary of apps with few reviews, many negative reviews, or overly positive reviews that sound fake.

3. **Examine the Number of Downloads**. Legitimate apps typically have a high number of downloads. An app with a low download count could be a red flag.

4. **Examine Permissions**: Review the permissions the app requests before downloading. Legitimate apps will only request permissions necessary for their functionality. Be wary of apps requesting excessive or irrelevant permissions. For example, does the app really need access to your contacts or always know your location?

5. **Check for Regular Updates**: Legitimate apps are regularly updated to fix bugs and improve performance. Check the app's update history to ensure it receives frequent updates.

6. **Be Cautious with New Apps**: New apps with no reviews or ratings should be approached with caution. If the app is legitimate, it will likely gain positive reviews and ratings over time.

Once you download a mobile app, enable automatic updating. New mistakes and vulnerabilities are constantly found in the code and configurations of mobile apps. By always ensuring you are running the latest version of your mobile apps, you can be sure those vulnerabilities are fixed and you have the latest security features. Also, if you are no longer using a mobile app, delete it from your phone.

Guest Editor

Danielle Strimbu is a Technical Project Manager at Travel Minds Digital Agency, with a background in technology and operations management. As the Events Chair for the WiCyS Colorado Affiliate, she seeks to organize engaging events to help advance women in cybersecurity. She holds a Master's degree in Information Systems Security and a Graduate Certificate in Cybersecurity Management.

Resources

Top Three Ways Cyber Attackers Target You: https://www.sans.org/newsletters/ouch/top-ways-attackers-target-you/
Emotional Triggers – How Cyber Attacks Trick You: https://www.sans.org/newsletters/ouch/emotional-triggers-how-cyber-attackers-trick-you/
All You Need to Know About Background Data: https://www.avast.com/c-what-is-background-data#