



Scam of the Week: Malicious Mobile Apps in Disguise

Google recently removed a number of dangerous mobile applications (apps) from the Google Play store. These were disguised as generic VPN and audio control apps that appeared to be safe, but once installed, they tricked victims into allowing downloads from untrusted sources.

If you download a disguised app and fall victim to this scam, a dangerous piece of malicious software (malware) is installed on your device. The malware adds malicious code into your financial apps, giving the bad guys access to your banking and credit card accounts. Over time, cybercriminals use this malware to gain complete control over your device and use it however they please.

This is not the first time that malicious apps were found on Google Play or on the Apple app store—and it won't be the last. When you download applications, remember these tips:

- Read reviews and ratings for the app. Look for reviews that are critical or reviews with three stars or less, as these are less likely to be fake.
- Avoid apps with few or no reviews and apps that have a low number of downloads.
- Only download apps from trusted publishers. Remember, anyone can publish an app on official app stores—including cybercriminals.

Stop, Look, and Think. *Don't be fooled.*

The KnowBe4 Security Team

KnowBe4.com