

There's an app for that (but it might be fake)

December 22, 2016

by Ari Lazarus

Consumer Education Specialist, FTC

As more and more consumers are shopping with mobile apps, fraudsters are following the money. There are fake phone apps popping up that impersonate well-known retailers in order to steal your personal information. Their names are similar to well-known brands, and their descriptions promise enticing deals or features.

But these fraudulent apps can take your credit card or bank information. Some fake apps may even install malware onto your phone and demand money from you to unlock it.

Here are some tips to avoid downloading fraudulent apps:

- Not sure if a shopping app is legit? Go directly to the retailer's website and see if they promote it. If they do have an app, they will direct you to the app store where you can download it.
- On the web, you can search a brand name, plus "fake app" to see if the company has reported its brand being spoofed.
- Look for reviews of the app before you download – both in the app stores and on the web. If the app has no reviews, it was likely created recently, and could be a fake. Real apps for big retailers often have thousands of reviews.
- Don't download apps with misspelled words in their description. Many fake apps were created in a hurry. On the other hand, some fake apps look almost like the real thing.

If you're using apps for shopping, keep records of your transactions. Screenshot or save the product description and price, the online receipt, and the emails you send and receive from the seller.

Monitor your credit card statements frequently; be on the lookout for charges that you don't recognize.

For more tips on safely using apps on your phone, check out our ["Understanding Mobile Apps"](#) article.

External Link Disclosure: By accessing links in this article, you will be leaving Itasca Bank's website and entering a website hosted by another party. Although Itasca Bank has approved this as a reliable partner site, please be advised that you will no longer be subject to, or under the protection of, the privacy and security policies of the Bank's website. The other party is solely responsible for the content of its website. We encourage you to read and evaluate the privacy and security policies on the site you are entering, which may be different than those of the Bank.)