12/19/16

By the Council of Better Business Bureaus

This December, scammers are fooling holiday shoppers with a new high tech con. Phony retail apps are popping up in Apple and Android's app stores and stealing shoppers' personal information.

How the Scam Works:

You search in your smartphone's app store for a favorite retailer. Many brands provide apps to make shopping at that store easy and more convenient. Several apps appear, and they all have similar names and brand logo.

Be careful when downloading the new app. Most fake apps are fairly harmless, a way to deliver spammy advertising. But some apps require shoppers to enter credit card information or provide their Facebook password. Sharing this information can open users up to fraud.

This con is notable because it affects so many brands, in both the Apple and Android app stores. Look out for fake apps posing as mall staples, such as Dillard's and Footlocker, online retailers such as Zappos and Overstock, and luxury sellers such as Jimmy Choo. Scammers have snuck these counterfeit apps past Apple's App Store review process, so be careful no matter what type of device you use.

Tips to Protect Yourself From an App Scam

Scammers love to impersonate popular apps. Here's how to spot a con:

Evaluate before downloading. In the app store, look for warning signs such as apps with no reviews and no history of previous versions.

Look out for poor grammar. Most fake apps are developed with little or no quality control. Look for poor grammar, typos, and strange sentences or phrases within the app title, description, or instructions.

Make sure the retailor has an app. Not all retailors have apps, which makes it easier for scammers to pass off fake ones. When in doubt, do a quick search online before downloading.

For More Information

Check out New York Times' coverage of fake retail apps on their website . To report issues with apps, go here for Google Play and here for Apple's App Store.

To report a scam, go to BBB Scam Tracker .