The New York Times | http://nyti.ms/2edFLyF

TECHNOLOGY

Beware, iPhone Users: Fake Retail Apps Are Surging Before Holidays

By VINDU GOEL NOV. 6, 2016

SAN FRANCISCO — Hundreds of fake retail and product apps have popped up in Apple's App Store in recent weeks — just in time to deceive holiday shoppers.

The counterfeiters have masqueraded as retail chains like Dollar Tree and Foot Locker, big department stores like Dillard's and Nordstrom, online product bazaars like Zappos.com and Polyvore, and luxury-goods makers like Jimmy Choo, Christian Dior and Salvatore Ferragamo.

"We're seeing a barrage of fake apps," said Chris Mason, chief executive of Branding Brand, a Pittsburgh company that helps retailers build and maintain apps. He said his company constantly tracks new shopping apps, and this was the first time it had seen so many counterfeit iPhone apps emerge in a short period of time.

Some of them appeared to be relatively harmless — essentially junk apps that served up annoying pop-up ads, he said.

But there are serious risks to using a fake app. Entering credit card information opens a customer to potential financial fraud. Some fake apps contain malware that can steal personal information or even lock the phone until the user pays a ransom. And some fakes encourage users to log in using their Facebook credentials, potentially exposing sensitive personal information.

The rogue apps, most of which came from developers in China, slipped through Apple's process for reviewing every app before it is published.

That scrutiny, which Apple markets as an advantage over Google's less restrictive Android smartphone platform, is supposed to stop any software that is deceitful, that improperly uses another company's intellectual property or that poses harm to consumers.

In practice, however, Apple focuses more on blocking malicious software and does not routinely examine the thousands of apps submitted to the iTunes store every day to see if they are legitimately associated with the brand names listed on them.

With apps becoming more popular as a way to shop, it is up to brands and developers themselves to watch for fakes and report them, much as they scan for fake websites, said Ben Reubenstein, chief executive of Possible Mobile, a Denver company that makes apps for JetBlue Airways, the PGA Tour and the Pokémon Company, among others.

"It's important that brands monitor how their name is being used," he said.

Apple removed hundreds of fake apps on Thursday night after The New York Times inquired about the specific app vendors that created many of them. Other apps were removed after a New York Post article last week drew attention to some of the counterfeits.

"We strive to offer customers the best experience possible, and we take their security very seriously," said an Apple spokesman, Tom Neumayr. "We've set up ways for customers and developers to flag fraudulent or suspicious apps, which we promptly investigate to ensure the App Store is safe and secure. We've removed these offending apps and will continue to be vigilant about looking for apps that might put our users at risk."

In September, Apple also embarked on a campaign to review all two million apps in the App Store and remove "apps that no longer function as intended, don't follow current review guidelines or are outdated." The company says that a significant number of apps have been removed and that the review is continuing.

Despite Apple's efforts, new fake apps appear every day. In some cases, developers change the content of an app after it has been approved by Apple's monitors. In other instances, the counterfeiters change their names and credentials, and resubmit similar apps after one round of fakes is discovered.

"It's a game of Whac-a-Mole," Mr. Mason of Branding Brand said.

On Friday, for example, an entity calling itself Overstock Inc. — an apparent attempt to confuse shoppers looking for the online retailer Overstock.com — was peddling Ugg boots and apparel through a fake app that was nearly identical to one banished by Apple on Thursday.

The same Chinese app developer, Cloaker Apps, created both fake Ugg apps on behalf of Chinese clients.

Jack Lin, who identified himself as the head of Cloaker, said in a phone interview in China that his company provides the back-end technology for thousands of apps but does not investigate its clients.

"We hope that our clients are all official sellers," he said. "If they are using these brands, we need some kind of authorization, then we will provide services."

Mr. Lin said Cloaker charged about 20,000 renminbi — about $3,000 — for an app written in English.

But like so many of the apps his company produces, Cloaker is not what it purports to be. Its website is filled with dubious claims, such as the location of its headquarters, which it says is at an address smack in the middle of Facebook's campus in Menlo Park, Calif.

In the interview, Mr. Lin at first said he had offices only in China and Japan. When asked about the California office, he then claimed to have "tens of employees" at the Facebook address.

China is by far the biggest source of fake apps, according to security experts.

Many of the fake retail apps have red flags signaling that they are not real, such as nonsensical menus written in butchered English, no reviews and no history of previous versions. In one fake New Balance app, for example, the tab for phone support did not list a phone number and said, “Our angents are available over the hone Monday-Firday.”

Data from Apptopia show that some of the fake apps have been downloaded thousands of times, although it is unclear how many people have actually used them. Reviews posted on some of the apps indicated that at least some people tried them and became frustrated. “Would give zero stars if possible,” wrote one reviewer of the fake Dollar Tree app. “Constantly gets stuck in menus and closes what you were doing and makes you start over.”

Mr. Mason says consumers want to shop online and they search for apps from their favorite stores and brands.

“The retailers who are most exposed are the ones with no app at all,” he said. Dollar Tree and Dillard’s, for example, have no official iPhone apps, which made it easier to lure their customers to the fake apps.

But the counterfeiters have also mimicked companies that do have an official presence in the App Store, hoping to capitalize on consumer confusion about which ones are real.

The shoe retailer Foot Locker Inc., for example, has three iPhone apps. But that did not stop an entity calling itself Footlocke Sports Co. Ltd. from offering 16 shoe and clothing apps in the App Store — including one purporting to be from a Foot Locker rival, Famous Footwear.

Similarly, the supermarket chain Kroger Company has 20 iPhone apps, reflecting the various retail chains in its empire. An entity calling itself The Kroger Inc. had 19 apps, purporting to sell things as diverse as an $80 pair of Asics sneakers and a $688 bottle of Dior perfume.

Some of the fake apps have even used Apple’s new paid search ads to propel them to the top of the results screen when customers search for specific brands in

the App Store.

Jon Clay, director of global threat communications for Trend Micro, an internet security firm, said Apple's tight control over the iPhone had historically kept malicious apps out of its App Store. Fake apps appeared more often on Google's Android platform or on third-party app stores, he said.

But that is beginning to change. Shortly after the Pokémon Go game was released in the United States in July, for example, a spate of fake iPhone apps related to the game appeared, especially in countries where the game was not yet available.

"The criminals are going to take advantage of whatever is hot," Mr. Clay said.

Emily Feng contributed reporting from Beijing.

A version of this article appears in print on November 7, 2016, on page B1 of the New York edition with the headline: A Surge of Deceptive Apps for iPhones Arrives in Time for Holiday Shopping.
