Skycure
Mobile Threat Defense

Mobile Threat Intelligence Report

Q3 2016

HOLIDAY SHOPPING ADVISORY

EXECUTIVE SUMMARY

As we enter the 2016 holiday shopping season, it is important for people to understand the new and increased risks introduced into this jolly season by way of their smartphones and other mobile devices. These devices are making our lives so much easier in many ways - easier to communicate, easier to manage and access information, and easier to shop. Unfortunately, cyber criminals are making all of these activities more risky every year, constantly finding creative ways to steal and expose sensitive data, and exploit that information for their own gain.

Risks abound, whether shopping online or in retail stores. According to industry statistics, **90 percent** of people admit to using their smartphones while in brick and mortar stores, to check online reviews, compare prices and evaluate competitive products. That means shoppers are also looking for Wi-Fi networks to connect their phones to in order to save on their data plans. While many stores and malls offer Wi-Fi for their customers, so do cyber criminals.

When shopping online, often performed on mobile devices today, shoppers may use store apps or look for online bargains and coupons. Hackers know this and will offer repackaged versions of your favorite store app, or even create new apps that promise deals and rewards. When much of our attention is on the task of shopping, especially during the frantic holiday season, please don't overlook the risks.

Note: This investigation is based on tens of millions of security tests from July through September 2016.

Skycure

ATTENTION: SHOPPING MAY BE HAZARDOUS TO YOUR MOBILE DEVICE

Hackers target frantic shoppers

While out shopping this holiday season, beware of joining risky Wi-Fi networks. Many are simply misconfigured and may expose your communications to anyone who may be interested in viewing them, while others are being monitored or even set up by cyber criminals specifically to steal your data. The most popular data to steal is user names and passwords - with those a hacker can break into your cloud accounts, corporate email and other systems, long after your visit to the mall.

Cyber criminals converge where there are lots of people, and malls are among the leading locations where people gather and attempt to connect to available Wi-Fi hotspots. Add the timing of Black Friday, and not only will there be an order of magnitude more people in these locations, but they will have many things on their minds other than mobile security. Under these circumstances, cyber criminals are bound to catch many devices connecting to unsafe or malicious networks. Skycure Research evaluated millions of network scans to identify that Fashion Show mall in Las Vegas is the most risky for mobile shoppers, where 14 Wi-Fi networks were found to be malicious or risky to connect to. Every mall in the top 10 has at least 5 risky networks to avoid.

Other malls with multiple networks to avoid include: South Coast Plaza in Costa Mesa, CA; NorthPark Center in Dallas, TX; Mall of Georgia in Buford, GA; and Hanes Mall in Winston-Salem, NC.

TOP 10 SHOPPING MALLS FOR RISKY WI-FI NETWORKS

1. Fashion Show, Las Vegas, NV
2. Tysons Corner Center, McLean, VA
3. Yorktown Center, Lombard, IL
4. Town Center at Boca Raton, Boca Raton, FL
5. Sawgrass Mills, Sunrise, FL
6. Mall of America, Bloomington, MN
7. Houston Galleria, Houston, TX
8. King of Prussia Mall, King of Prussia, PA
9. Westfield Garden State, Paramus, NJ
10. Memorial City Mall, Houston, TX

Skycure

Wi-Fi designed to deceive

Many of the Wi-Fi networks flagged as risky are set up by businesses with good intentions, but are simply misconfigured, and as such will be easy for hackers or even laymen to observe your communications that should be confidential. Other Wi-Fi networks are set up by cyber criminals specifically to lure victims and their devices to connect and give up their secrets.

The methods cyber criminals use to hack mobile devices through Wi-Fi networks vary, but there are two primary strategies hackers utilize:

1. Find misconfigured or poorly secured networks that legitimate organizations have set up, like coffee shops, stores and malls, and set up a Man-in-the-Middle (MitM) exploit. In this scenario, the hacker can either observe unencrypted traffic, stealing data and account credentials, or manipulate the content the victim sees to redirect to a malicious website or download malware.

2. Set up a fake Wi-Fi network to trick the victim or the device into connecting. By mimicking a legitimate network, using the same name, a user may connect thinking it is legitimate and safe. If the device has previously been connected to the official version, it will often connect without any action by the user. Alternatively, the hacker may set up a network and use the term "free" in the name to lure victims.

Both of these scenarios can be dangerous and put mobile shoppers and their data and online accounts at risk. Even a short exposure to a malicious network may give hackers enough information to later access bank accounts, social media accounts and corporate accounts. When shopping, pay attention to these things. Skycure research has determined that almost 10% of malicious Wi-Fi hotspots use the term "free" in the name, such as "FreePublicWiFi", so make sure the network is one you trust. Also, if you see a familiar network, like Starbucks or Apple Store, make sure you are actually nearby that establishment. Otherwise it is probably a fake. Skycure researchers found the following examples of fake Wi-Fi networks at popular shopping centers.

- **Macysfreewifi** - in Park Meadows mall Denver, the Waterfront mall Pittsburgh as well as in places where there's no Macy's store
- **Belk_Guest** - in Columbiana center NC
- **Apple Store** - multiple instances where there's no Apple Store
- **Bloomingdalesfreewifi** - at Liberty Place, Philadelphia
- **officedepot** - In Magnolia Shoppes near Miami
- **Panera** - near Baltimore

If you see a Wi-Fi that is named as if it is hosted by a store, but that store is nowhere nearby, don't connect.

Skycure

Commerce Apps to avoid on Cyber Monday - or any other day

Black Friday network threats are not the only risk shoppers face this year. On Cyber Monday, bargain hunters will be using their mobile devices to access the apps from their favorite retail stores to search for sales and deals online. One-third of all ecommerce purchases during the 2015 holiday season were made on a smartphone, and hackers know that people are shopping for bargains around the holidays, and there are many ways to lure people by promising savings or convenience. One way is to offer apps that look like they are from your favorite stores, either designed to make shopping easier, or to offer discounts or rewards.

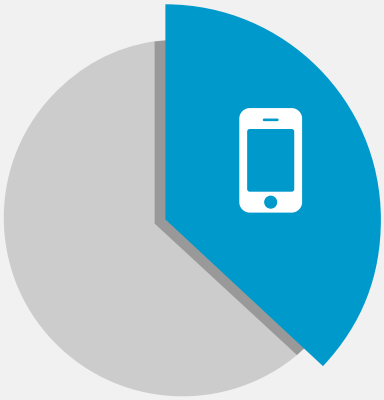
Skycure Research has identified two types of apps to be wary of:

1. Repackaged Apps: The first type of app looks exactly like the official apps offered by your favorite retailers, but have a small amount of malicious code added in. These are called repackaged apps and will look and behave exactly like the original app, except that it will also do bad things in the background without your knowledge, like steal your data or spy on you by observing communications or recording audio and/or video. An example of this that was discovered in the research was a repackaged version of the Starbucks app. Avoid this hazard by only installing apps from the official Apple and Google app stores.

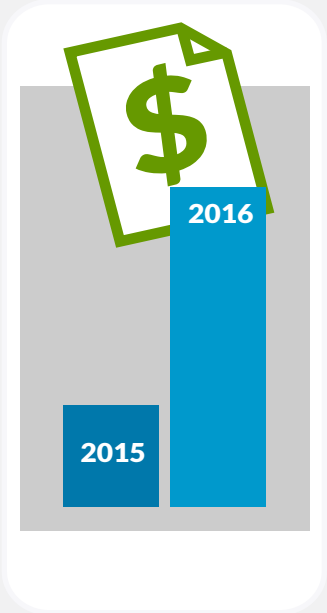
2. Fake Apps: The second type of shopping app to avoid are apps that are created from scratch to deceive bargain-hunting victims. Some hacker created an app called Amazon Rewards, yet no such app exists in the official app stores. By promising “rewards” people are more likely to download this, even though it will not appear on the official app stores, because the desire to save money this time of year is at its highest. In the case of this app, it is actually a trojan that spreads using SMS messages with fake Amazon vouchers and a link to a fake website. It accesses the user’s contact list so that it can send SMS messages to even more people.

WHY CYBER CRIMINALS ARE LOOKING FORWARD TO THIS HOLIDAY SEASON

$656 BILLION
IN RETAIL SALES PROJECTED
IN THE 2016 HOLIDAY SHOPPING SEASON



37%
OF WEBSITE VISITS IN 2015 WERE GENERATED BY MOBILE WEB BROWSERS



90%
OF SMARTPHONE USERS CONSULT THEIR PHONE DURING SHOPPING IN A PHYSICAL LOCATION

18%
OF NORTH AMERICANS USE MOBILE PAYMENTS REGULARLY

$27.05 BILLION
ESTIMATED MOBILE PAYMENTS IN 2016 *(3X THAT OF 2015)*

$40.241 BILLION
ESTIMATED AD SPEND IN 2016 (41% INCREASE OVER 2015)

50%
OF CLICKS ON MOBILE ADS WERE ACCIDENTAL

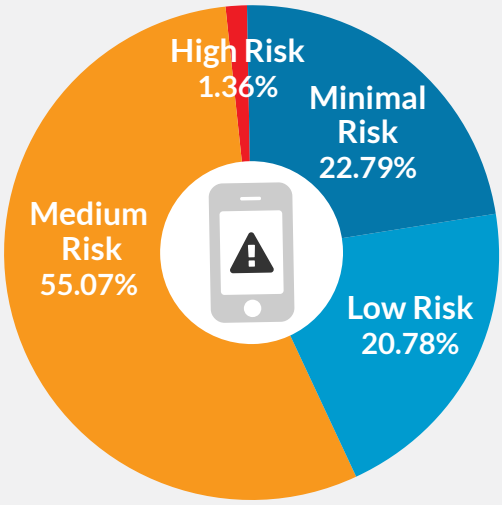
Credits: StatCounter, Accenture, eMarketer, GoldSpot Media

Skycure

OTHER MOBILE RISKS

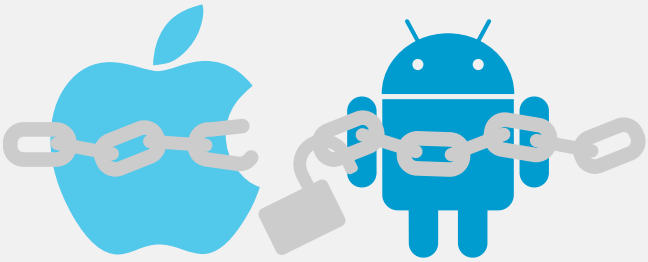
Over half of all devices are risky

About 56 percent of all mobile devices are rated as medium-to-high risk according to the Skycure Mobile Threat Risk Score. The percentage of high risk devices dropped slightly in Q3 2016 from 1.7 to 1.4 percent. These devices have either already been compromised or are currently under attack. The Skycure risk score takes into account recent threats the device was exposed to, device vulnerabilities, configuration and user behavior.



Jailbroken & Rooted

Rooting an Android device, or Jailbreaking an iOS device, is a way for the user to gain greater control over the device, allowing better access to system files and enabling greater personalization and functionality of the device that wouldn't otherwise be allowed by the operating system as designed. Users will do this to their own phones to improve their productivity or enjoyment of the device, but this continues to decrease in popularity as newer operating systems naturally allow some of the functionality that could previously only be achieved through rooting or jailbreaking.



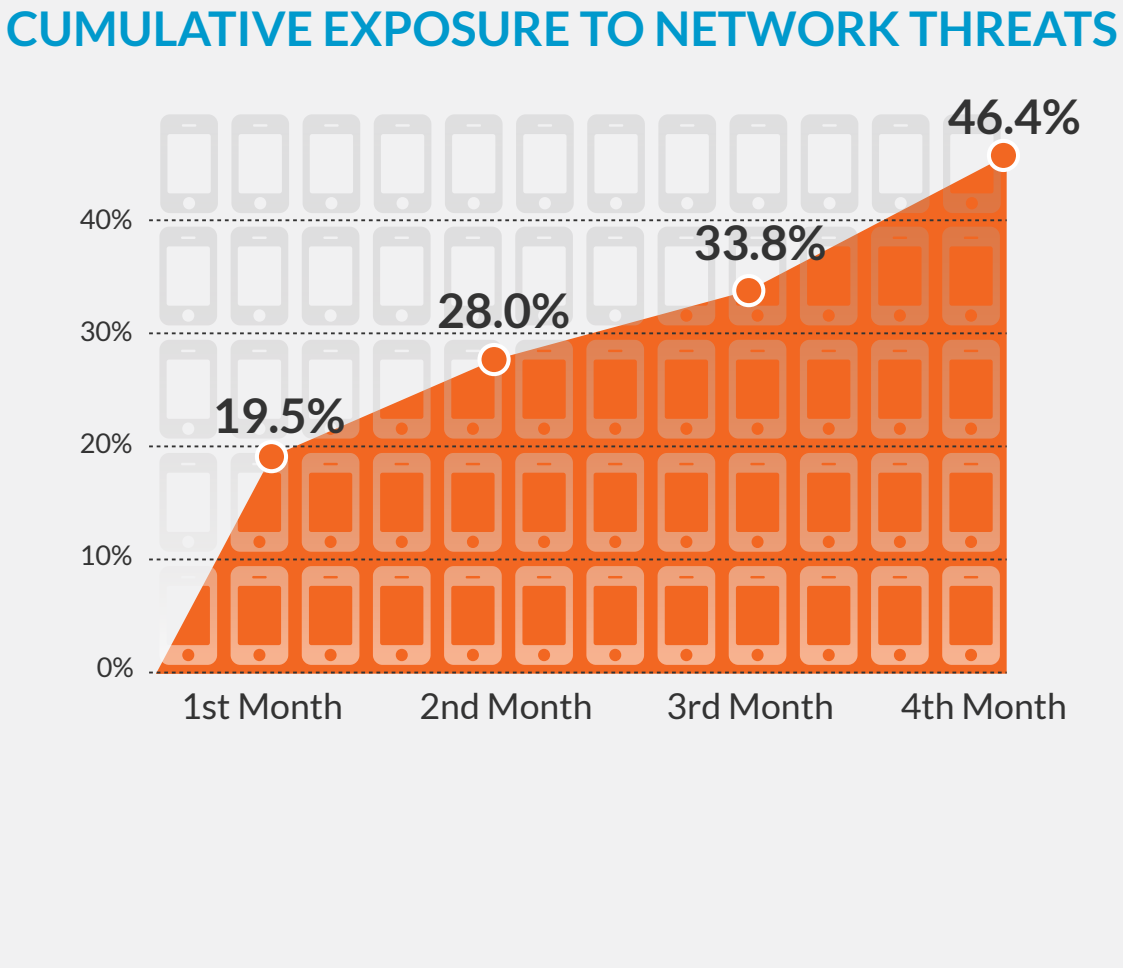
Enterprise Managed	0.01%	0.32%
Self Managed	0.35%	2.07%

Because of the greater control over the device that this affords, it is a common goal of hackers to figure out ways to root or jailbreak devices, and alware is a common way to do that. A user that roots or jailbreaks their own device should be aware that they may be simply making it easier for hackers to exploit, so it is not generally recommended. Fortunately, these rates are trending down over time.

Skycure

Devices exposed to network threats over time

In any typical organization, about 20% of the mobile devices will be exposed to a network threat in the first month of security monitoring. This number goes to 46% over the next 3 months. A network threat may be a malicious Man in the Middle (MitM) attack that decrypts SSL traffic or manipulates content in transit to or from the device. It can also be a simple misconfigured router that exposes otherwise encrypted data for anyone to view. Regardless of how malicious the intent of the network threat is, individuals and organizations would be wise to avoid any network that does not accurately and securely perform the connection services originally requested by the user and the device.



Skycure

SAFETY TIPS FOR SHOPPERS

1. Avoid "Free Wi-Fi" networks (10 percent of malicious networks have the word "Free" in their name).
2. If you see a Wi-Fi that is named as if it is hosted by a store, but that store is nowhere nearby, don't connect. Skycure found multiple networks named "Apple Store" or "Macysfreewifi" where the named stores were nowhere nearby. Remember that mobile devices automatically join "known" Wi-Fi networks without any user intervention.
3. Check for top mobile threats in any destination by visiting https://maps.skycure.com
4. Only download mobile apps from reputable app stores such as the Google Play store and Apple's App Store.
5. Read the warnings on your device and don't click "Continue" if you don't understand the exposure.
6. Update your device to the most current operating system.
7. Disconnect from the network if your phone behaves strangely (e.g. frequent crashes) or you receive a warning notification.
8. If you see a suspicious app, text, or Wi-Fi network, or your device acts strangely, report it to security@skycure.com
9. Protect your device with a mobile security app like Skycure.

Download the free mobile threat defense app from Skycure,

which detects and alerts you to malicious network attacks, suspicious networks, malware and vulnerability exploits. To download Skycure, go to: https://apps.skycure.com on your iOS or Android device, or go to the App Store or Google Play store and search for "Skycure". **IT SECURITY ADMINS USE SKYCURE TO PROTECT FROM SHOPPING HAZARDS.**

Available on the App Store

Available on Google play

FREE ENTERPRISE TRIAL

About the Mobile Threat Intelligence Report

The Skycure Mobile Threat Intelligence Report reviews worldwide threat intelligence data. For the shopping mall report, Skycure researched mobile threats and high-risk networks for the top shopping malls based on Travel & Leisure's Most-Visited Shopping Malls list. Other information in today's report is based on millions of monthly security tests conducted by Skycure from August through October 2016 and includes both unmanaged devices and those under security management in enterprise organizations. Data includes Skycure's proprietary Mobile Threat Risk Score, which acts as a credit score to measure the risk of threat exposure for mobile devices. For organizations, Skycure condenses millions of data points to calculate a risk score so that IT can quickly discern the state of the overall system and the risk to each device. Skycure analyzes more than a million apps and more than 1.5 million unique networks worldwide every year.

About Skycure

Skycure is the leader in mobile threat defense. Skycure's platform offers unparalleled depth of threat intelligence to predict, detect and protect against the broadest range of existing and unknown threats. Skycure's predictive technology uses a layered approach that leverages massive crowd-sourced threat intelligence, in addition to both device- and server-based analysis, to proactively protect mobile devices from malware, network threats, and app/OS vulnerability exploits. Skycure Research Labs have identified some of the most-discussed mobile device vulnerabilities of the past few years, including Accessibility Clickjacking, No iOS Zone, Malicious Profiles, Invisible Malicious Profiles, WifiGate and LinkedOut. The company is backed by Foundation Capital, Shasta Ventures, Pitango Venture Capital, New York Life, Mike Weider, Peter McKay, Lane Bess, and other strategic investors.

Skycure