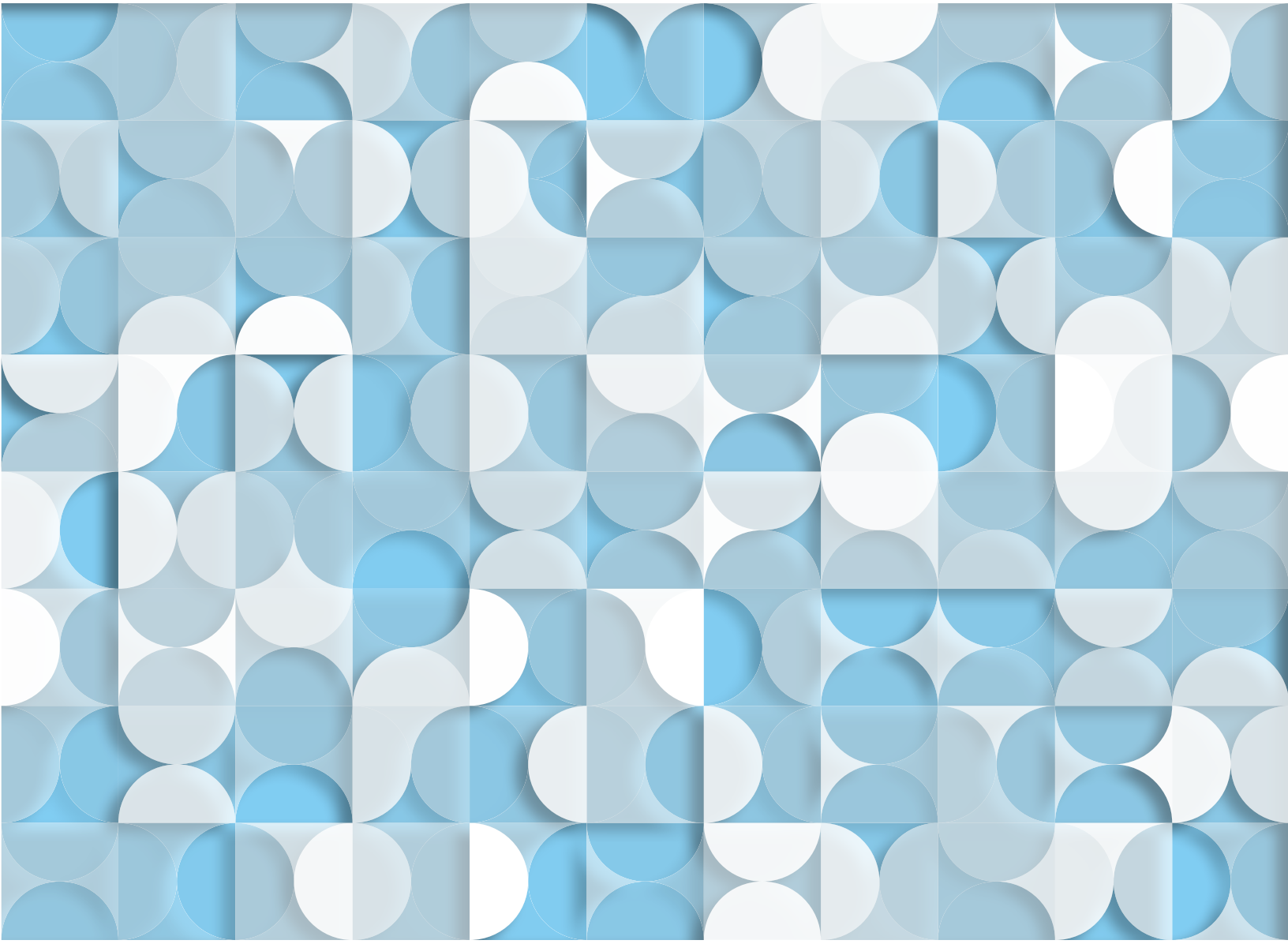
# APPSESSION: IS OUR APPETITE FOR MOBILE APPS PUTTING US AT RISK?

A RiskIQ Mobile Consumer Report
April 2017



RISKIQ®

# EXECUTIVE SUMMARY

Mobile devices have become the undisputed internet platform of choice for consumers, with mobile apps the preferred method of interaction. According to the latest App Annie[1] figures, the number of worldwide app downloads in 2016 increased by 15% to 90 billion and the time spent in mobile apps grew by 25% to 900 billion hours.

With so much of our personal information now flowing through mobile applications, has our security awareness kept pace? Have consumers adopted best practice behaviors or are they leaving themselves vulnerable to cyber attacks?

To better understand consumer behavior, RiskIQ commissioned Ginger Comms[2] to survey 1,000 US and 1,000 UK consumers aged 16 to 60+, specifically focusing on smartphone apps. The survey was conducted between February and March 2017.

Earlier RiskIQ research[3] on mobile apps affiliated with top United Kingdom brands across 150 different app stores, found a 63% increase in the number of apps between 2015 and 2016 and a 131% increase in the number of blacklisted apps. Blacklisted applications are applications linked to nuisance-ware, such as ad servers or malware including ransomware or credential-stealing exploits. With tens of millions of mobile apps and hundreds of different app stores out there, the vastness of the app store ecosystem provides the perfect place for malicious actors to hide, luring smartphone users into believing their apps are official or their affiliation with brands is legitimate. It's easy to see that our acquisition and use of mobile apps needs to be accompanied by better security awareness.

The top line results show that over half of all respondents regularly display behaviors that put themselves at risk:


click on ads promoting apps


click on links in emails, mobile web, and social media promoting apps


rarely or never check the app details before downloading


rarely or never inspect the T&Cs or permissions being requested during app installation


reuse passwords across mobile apps

*...the number of worldwide app downloads in 2016 increased by 15% to 90 billion and the time spent in mobile apps grew by 25% to 900 billion hours.*

[1]https://www.appannie.com/en/insights/market-data/app-annie-2016-retrospective/

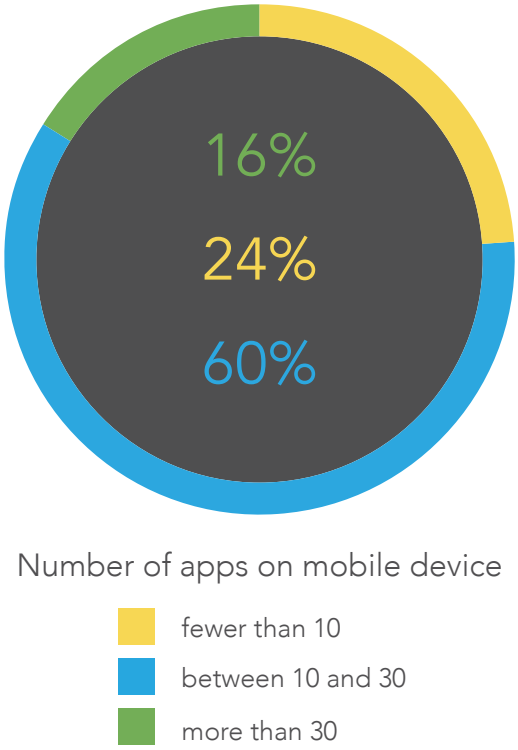
[2]http://www.gingercomms.com/

[3]https://safe.riskiq.com/WC-2015-whos-minding-the-store-the-mobile-app-ecosystem-revealed_minding-the-store-mobile-app-ecosystem-revealed-web-lp-new.html

# A CLOSER LOOK

## According to App Annie research[1], people interact on average with **30 different mobile apps.**

Our survey found that roughly a quarter of users surveyed have fewer than ten applications installed on their phone, 60% have between 10 and 30 applications, and the remaining 16% have 30 or more. Across all age bands, we see that the older the respondent, the fewer apps they are likely to have.




[1]App Annie 2016 Retrospective

# SMARTPHONE MODIFICATION

## Most consumers are happy with their phone as it was configured when they purchased it, but **14%** of respondents have jailbroken or rooted their phone.

The most common reason for jailbreaking their phone is increased freedom in what can be downloaded and installed (67%). Other reasons include the ability to sideload applications (50%), to change services providers (50%), and to customize the look of the operating system (33%). While modifying a phone can allow more choice for the user, it also bypasses many of the security mechanisms put in place by carriers and official app stores. Staying safe requires heightened security awareness on the part of the user.

# ACQUIRING NEW APPS

To gain a better understanding consumers' general security awareness when finding and installing apps, we asked a series of questions on their app discovery and install practices.

The most common way of finding new apps by is looking through the "Top Apps" section in official app stores (58%) followed closely by word of mouth (57%).

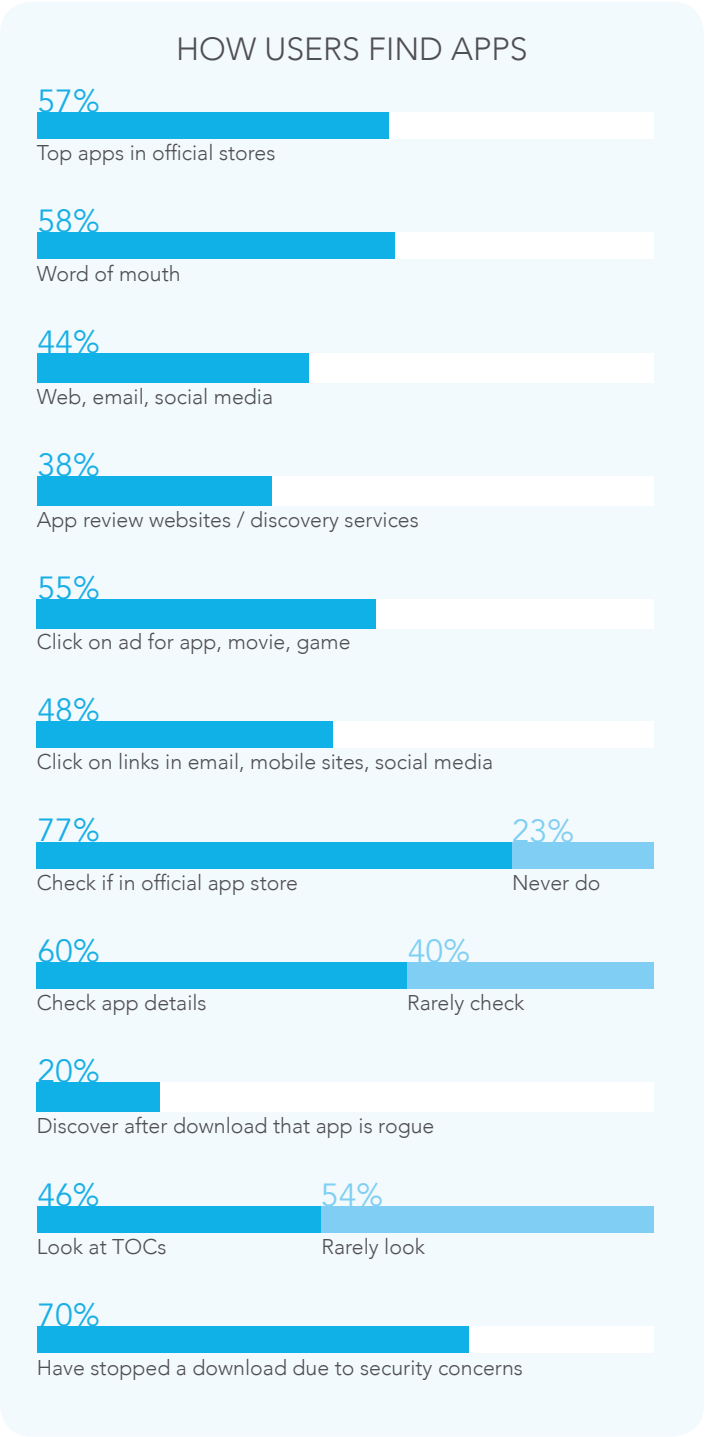
Other ways include ads on web, email, or social media (44%) and app review websites or app discovery services (38%).

Users who stray from the primary app store environment (Google Play, Apple App Store, Windows Store, etc.) to look for new apps or as a result of clicking on links, have an increased risk of downloading counterfeit or compromised apps. Of all survey respondents, 55% have clicked on ads promoting an app, movie, or game and 48% have clicked on links in emails, mobile websites, or social media feeds doing the same. While 77% usually or always check to see that they have been directed to an official app store, 23% rarely or never do.

When selecting an app to download, 60% of respondents usually or always check the app details in the store before downloading. However, 40% rarely or never do and 20% sometimes or frequently download apps only to find that they are not from the brand or organization they expected. Inspecting app details such as description, developer, last version update, the number of downloads, and any posted reviews can help determine if the app is genuine.

During the app installation process, 46% usually or always look at the Terms and Conditions and the permissions being asked for while the majority (54%) rarely or never do. Apps asking for permission to access the camera, microphone, or other features of the phone that are not needed to support the functionality of the app should cause users to think twice before continuing.

To sum up, the app acquisition behavior of consumers, even though 70% say they have stayed away from or stopped an app download because of security or privacy concerns, over half of all respondents regularly display app acquisition behaviors that put themselves at risk.



# SOCIAL MEDIA

According to the App Annie research cited earlier, while all app categories are growing, the most popular mobile apps remain messaging and social media apps. Social media has become a focus area for malicious actors, who impersonate individuals and brands to gain trust with the intent to push users to malicious content.

In our survey, 80% of respondents use social media apps on their phone and 70% of those click on links provided by other users. Of those, 66% of those respondents only click on links from people they know while 34% click on links regardless of source. Clicking on unknown links is sometimes all it takes to get unwanted malware on your phone.

# OTHER CONSIDERATIONS

- Looking at more general security practices, 45% of respondents have installed additional security software or modified their settings to improve security,
- 42% said security was a factor in their decision to buy their phone.
- A less encouraging stat is that 52% reused passwords across their mobile apps, a practice that should be avoided across digital devices, including PC.
- In addition to personal use, 45% use their phone for work purposes. While BYOD (Bring Your Own Device) is common practice in many organizations today, users need to remain vigilant to ensure they are not engaging in behavior that could introduce malware onto their phone, which can then propagate to their corporate network.

# COMPARISONS BETWEEN UK AND US CONSUMERS

The survey results show UK users are more conservative in their smartphone practices than their US counterparts: 36% in the UK use it for work vs. 45% in the US, 7% have jailbroken their phone vs. 20%, and app review websites and app discovery services play a bigger role in the US (41% vs. 23%). More US users have social media apps on their phone (84% vs. 76%) and are more likely to click on links provided by other users (75% vs. 63%). They are also more likely to click on links in ads promoting an app, movie, or game (66% vs. 45%) or emails, mobile websites, and social media feeds doing the same (60% vs. 40%).

However, smartphone security consideration seems to be more ingrained in the US: more have installed security software on their phone or modified their settings to improve security (53% vs. 44%), more said security was a factor in their decision to buy the phone they did (52% vs. 32%), and more inspect the permissions being asked for at app installation time (53% vs. 40%).p

| MOBILE PHONE ACTIVITY | US | UK |
|---|---|---|
| Use SmartPhone for Work | 45% | 36% |
| Jailbroken their phone | 20% | 7% |
| Pay more attention to App Reviews and Discovery Services | 41% | 23% |
| More social media apps on phone | 84% | 76% |
| More likely to click on links by other users | 75% | 63% |
| Click on ads promoting apps, movies or games | 66% | 45% |
| Click on emails, mobile websites & social media feeds | 60% | 40% |
| Installed Security Software | 53% | 44% |
| Said security was a factor in phone choice | 52% | 32% |
| Inspect requested permissions at app installation time | 53% | 40% |

# FINAL THOUGHTS: BAD CONSUMER HABITS MEAN A MAJOR RESPONSIBILITY FOR BUSINESSES

Recently, RiskIQ research* found one in 10 mobile apps out of the 5,315 related to Black Friday in global app stores is blacklisted (unsafe to use) as malicious in our Black Friday eCommerce Blacklist Report, as well as hundreds of fake apps related to romance and dating in our Valentine's Day Mobile Dating App report.

With so many careless users and users lacking mobile security acumen, businesses must take it upon themselves to fight the mobile threat actors fraudulently leveraging their brand. Mobile threat actors developing and hijacking fraudulent and unauthorized apps designed to divert users, distribute malware, and steal customer or company data is a critical security issue that affects almost every organization. A data center-centric, layered security approach needs to be augmented with solutions that monitor your mobile attack surface so they can see it from the outside in—the same way their customers and attackers see it.

**The source of RiskIQ's Blacklists is our collection of internet data, which our collection architecture of virtual users gathers by scanning, crawling, and passive-sensing the internet—including web pages, mobile apps and stores, and a variety of social websites and apps. RiskIQ's crawling technology covers more than 300 million mobile devices, 1.8 billion HTTP sessions, 783 global locations across more than 100 countries, 16 million mobile apps, and 300 million domain records.*

# ABOUT RISKIQ

RiskIQ is a digital threat management company that provides comprehensive coverage across all digital channels—web, social, and mobile—monitoring the digital presence of any organization from a single platform. Through powerful data collection techniques including a worldwide proxy and sensor network with synthetic clients that emulate users, the company maintains robust internet data sets which power its platform and extend digital threat intelligence to customers' existing security and risk-management investments. With RiskIQ, security, compliance, and brand protection teams can proactively hunt, detect, understand, monitor, and mitigate threats originating outside their firewall. Fortune 500 companies rely on RiskIQ to protect their digital attack surface, with over 13,000 security analysts subscribed to the platform. The company is headquartered in San Francisco, California, and backed by Summit Partners, Battery Ventures, Georgian Partners, and MassMutual Ventures.


**riskiq.com** • 22 Battery Street, 10th Floor, San Francisco, CA 94111, USA • 33 Cannon Street, 4th Floor, City of London, EC4M 5SB, UK
sales@riskiq.com • 1.888.415.4447 • 