



# Mobile Users at Risk



Allot MobileTrends Report H1/2016



# Contents

<b>Executive Summary</b>	<b>1</b>
<b>Who is at risk for malware?</b>	<b>2</b>
<b>Research and Methodology</b>	<b>2</b>
<b>Findings</b>	<b>3</b>
Every mobile user is at risk for malware	3
Some Apps and Websites are riskier than others	4
Risk increases as usage increases	6
Online behavior significantly affects potential for malware risk	8
Sharing is a risky business	9
Profiling mobile behaviors at risk for malware	10
<b>Protecting mobile users at risk</b>	<b>12</b>
<b>Key Take Aways</b>	<b>12</b>
<b>Further Reading</b>	

## Executive Summary



Malware is spreading with increasing frequency into the mobile realm, transmitted through URLs that we use every day and even more through mobile Apps. Some regulators already require mobile operators to provide basic security measures to protect data users, but most don't yet. Mobile operators have a real opportunity to be proactive and profitable by offering network-based security services to protect users at risk.

While every mobile user is at risk to a certain extent, not every mobile user is alike. To determine the potential for malware risk, we correlated the online behavior of specific user profiles with the potentially risky Apps and URLs that they use on a daily basis.

Our findings reveal that:

- Malware risk is affected more by online behavior of the user than by the App or URL itself. In other words, it's not just the App; it's how you use it.
- Business people have the riskiest online behavior. 79% of businessmen and 67% of businesswomen use potentially risky Apps.
- 65% of Youth and Millennials use potentially risky Apps.
- While mobile App downloads are often protected, their ongoing use is not protected, making certain user behaviors vulnerable to malware threats.

Rather than providing security per App, it makes sense to safeguard users at the network level where the security measures can provide a protective umbrella for all online activity. Mobile operators are uniquely positioned to provide this level of protection for consumers and businesses. Our report suggests how mobile operators can identify and reach out to customers who are at risk, targeting them with personalized Security as a Service from their network or cloud.

# Who is at risk for malware?



The mobile Internet continues to increase dramatically, with hundreds of millions of people using mobile browsers and Apps to access the online content and services they want. Naturally, mobile Apps and URLs have become an attractive target for malware to wreak its havoc on mobile devices and personal data. Many studies focus on the nature of Apps and URLs, ranking them by their vulnerability to malware infection. Others focus on coding methods that reduce malware's ability to exploit mobile Apps and

browsers as a vehicle for intrusion. However, little is known about the end users who are exposed to malware threats every day. Is everyone at risk? Are some mobile users more at risk than others? Routine Activities Theory suggests that since our daily activities have migrated to the Web, the criteria for determining the risk of becoming a victim can also be applied to online behavior.<sup>1</sup> This edition of Allot MobileTrends sheds light on different user profiles and the online behaviors that put them at risk.

## Methodology



To determine the potential for malware risk, we revisited the user demographics and behavior profiles that we identified in the previous Allot MobileTrends Report<sup>2</sup> i.e., Male, Female, Youth, Millennials, Generation X, Baby Boomers, Business Users, and Digitally Hooked. We analyzed these profiles in relation to the potential riskiness of the mobile Apps and URLs they use. As in our previous report, user demographics and profiles were defined by distinctive and recurring patterns of online behavior in relation to volume of data consumed, as well as specific App and browsing activity.

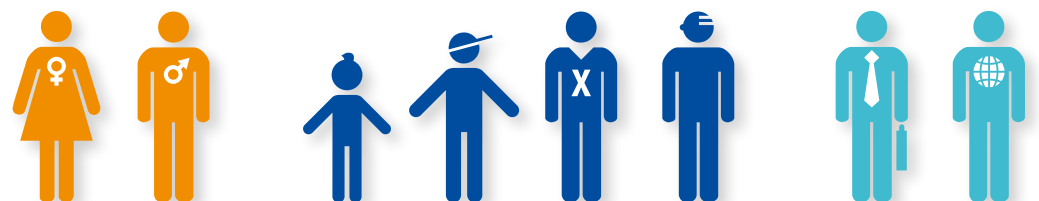
Our analysis was based on mobile data records from a random sample of 500,000 mobile users during a 7-day period, using Android, iOS and Windows Phone operating systems. We identified the 500 Apps and 500 URLs that were most popular with our user sample, ranked them according to their potential for malware risk, and categorized each one as "safe" or "potentially risky."

The experts at Kaspersky Lab assisted us in grouping the URLs into relevant content categories. Similar categories were used for grouping Apps.

Next we correlated safe and potentially risky Apps and URLs with each user demographic and behavioral profile. First level analysis correlated App/URL use with simple demographic profiles (e.g., Male). Deeper analysis correlated App/URL use with composite profiles that incorporate the online behavior of the user (e.g., Male, Generation X, Business User).

Our findings reveal that online behavior can play a determining role in identifying who is at risk for malware. Let's take a closer look.

Type	Groups
Gender	Female Male
Age	Youth (<14), Millennial (15-25), Generation X (25-60) Baby Boomer (60+)
Use Type	Business User Digitally Hooked



<sup>1</sup> Theorizing Cyber Crime: Applying Routine Activities Theory, Micah-Sage Bolden and Mahesh Nalla, CJ 801, Spring 2014  
<sup>2</sup> Allot MobileTrends H2/2105, 5+1 CSP Touch Triggers for Monetizing Customer Engagement

## Findings

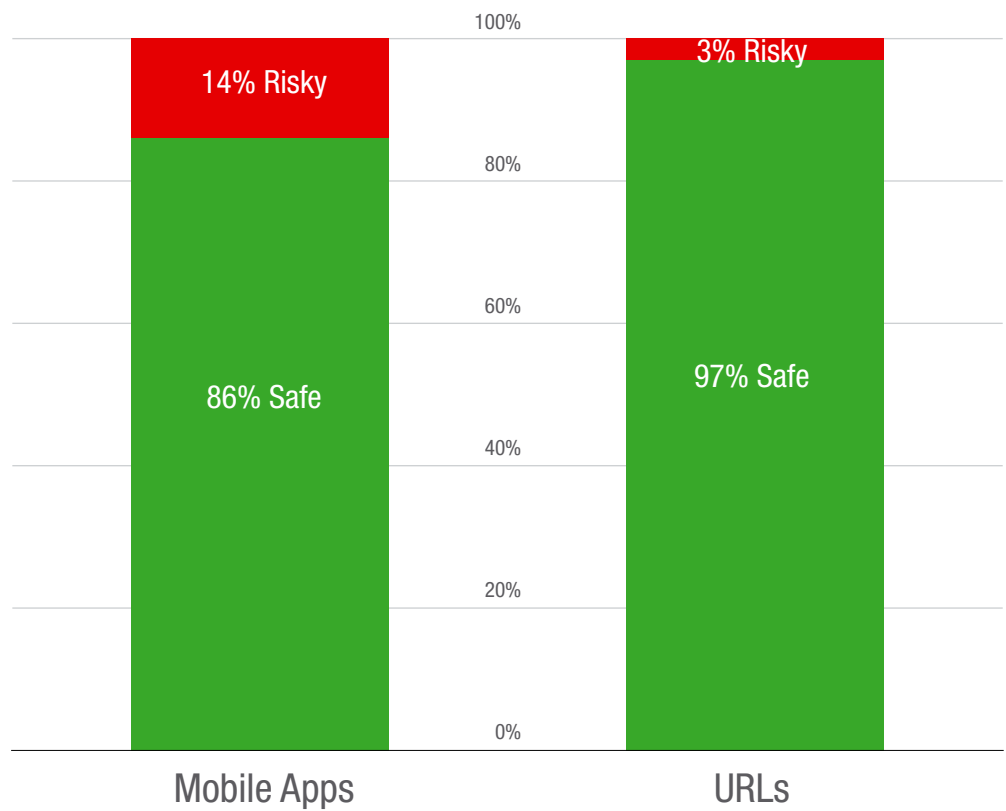


### Every mobile user is at risk for malware

Smartphones and tablets have become “real” mobile PCs, equipped with fast Internet connectivity and the ability to install an endless variety of new Apps on demand. It is not surprising that mobile Apps and browsers have become attractive vehicles for cybercriminals who want to spread their malware, exposing mobile users to

infection and its debilitating consequences. Our findings presented in Graph 1 show that about 1 in every 30 mobile browsing transactions is potentially risky, and 1 in every 7 mobile App sessions is risky. Clearly, every mobile user is at risk to some extent.

**Graph 1: Percent of safe and potentially risky Apps and URL transactions per day**





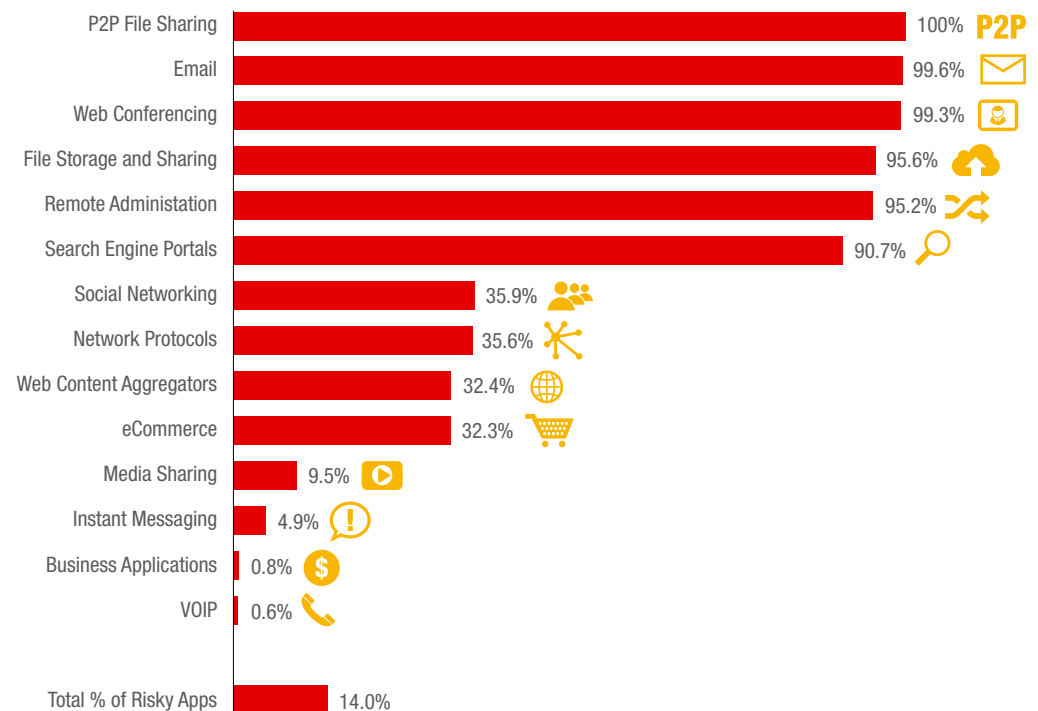
## Some Apps and Websites are potentially riskier than others

The digital experience is driven by millions of mobile Apps with new ones popping up all the time. Moreover, millions of people use mobile browsers to search, find and consume an endless variety of content and services online. The digital lifestyle invites and encourages us to share information, content and experiences via email, social networks, online storage, and other Apps, which often become a vehicle for malware to spread. Without knowing, mobile users click malicious links, forward infected content and download infected files, putting themselves and their online contacts at risk.

Graphs 2a and 2b summarize our findings regarding the potential riskiness of Apps and URLs that were scored individually and then categorized, resulting in a risk score per category.

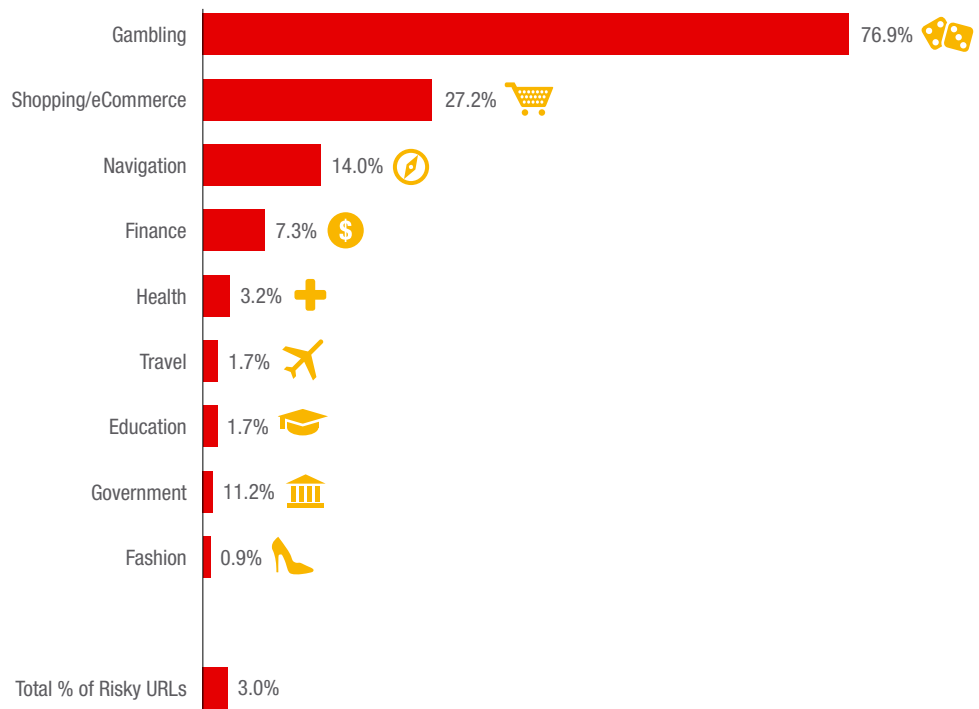
- More than 90% of the Apps in these categories are potentially risky: P2P File Sharing, Web Conferencing, File Storage and Sharing, Remote Administration, and Search Portals
- 23%-36% of the Apps in these categories are potentially risky: Social Networking, Network Protocols, Web Content Aggregators, and eCommerce
- 5%-10% of the Apps in these categories are potentially risky: Media Sharing and Instant Messaging

**Graph 2a: Percent of potentially risky Apps per content category**



In contrast to Apps, browsing activity appears to be riskiest when it involves monetary transactions, with Gambling (77%), Shopping/e-commerce (27%) and Finance (7.3%) in the top four categories of potential risk. While most eCommerce websites use encryption to assure privacy, encryption is also a common evasion technique for hackers, making these web sites (URLs) an attractive target for injecting malware and keeping it hidden.

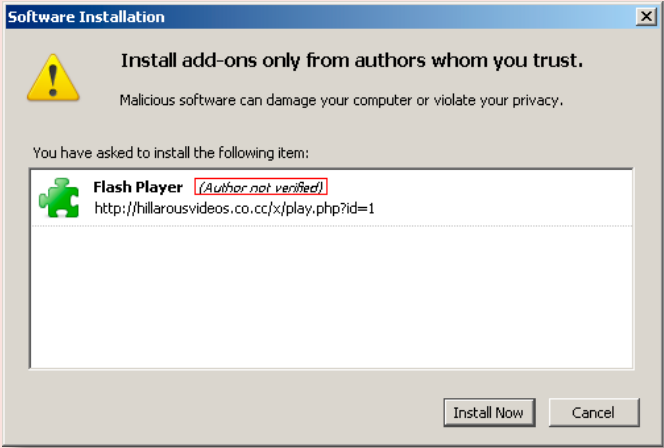
**Graph 2b: Percent of potentially risky URLs per content category**






## Risk increases as usage increases

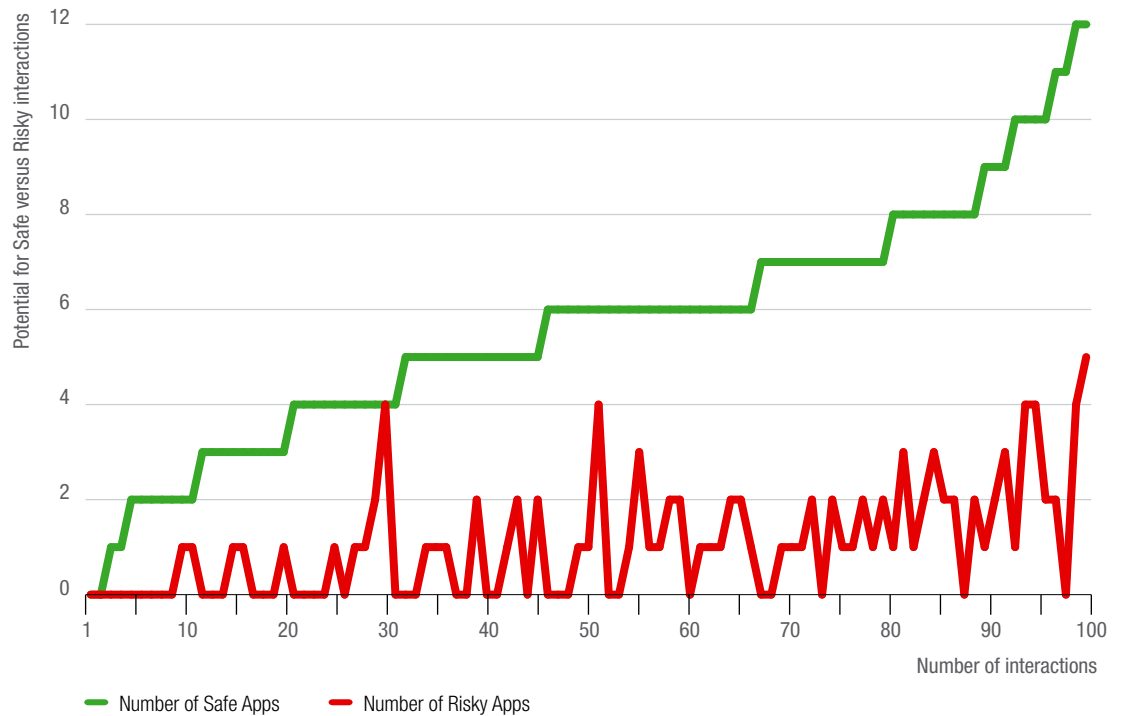
Mobile users at risk are not necessarily people who use only or even mostly potentially risky Apps and websites. In fact, our research shows that malware risk increases as online activity increases in general. Graphs 3a and 3b examine the correlation between routine use of safe and risky Apps. The findings show that as the number of safe browsing or App sessions increases, the number of potentially risky browsing or App sessions will also increase.



**Spreading Viruses via Social Networks**  
Unsuspecting Facebook users click to update their Flash player and get malware instead.

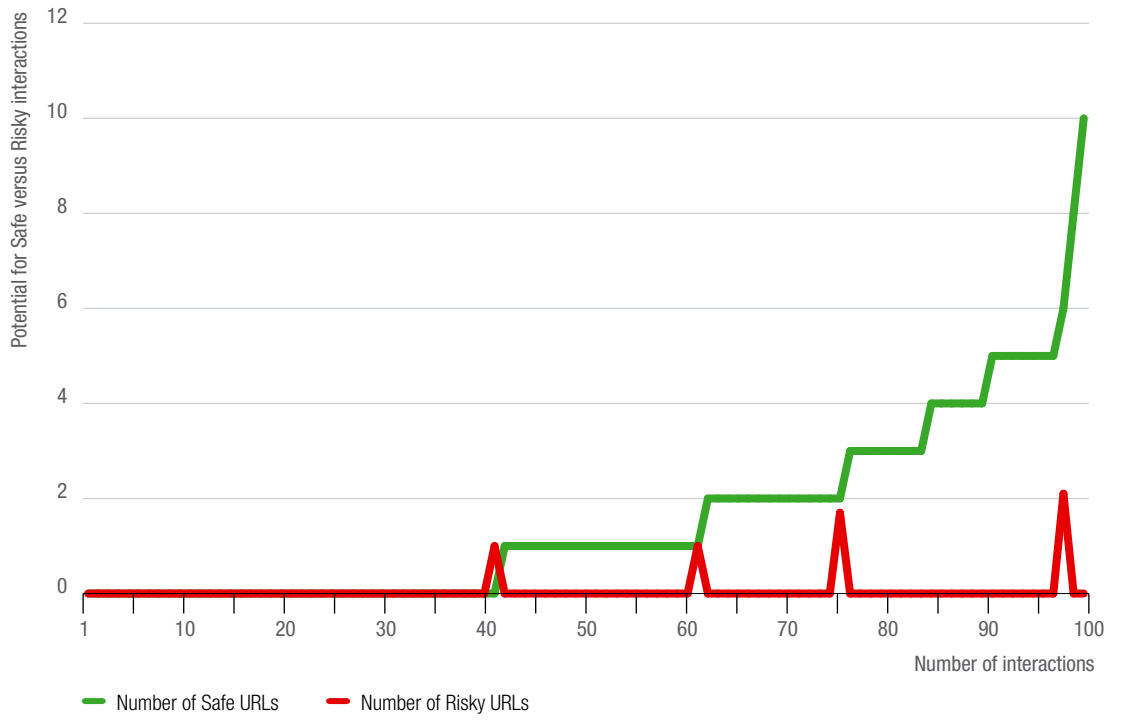


Graph 3a: Correlation between safe and potentially risky App activity





**Graph 3b: Correlation between safe and potentially risky browsing activity**



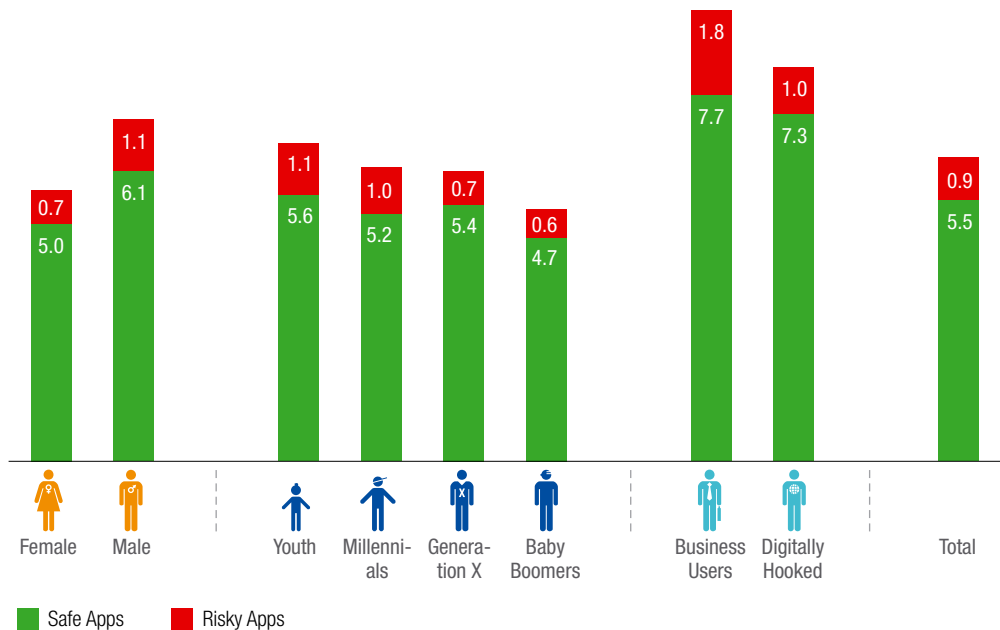


## Online behavior significantly affects potential for malware risk

While every mobile user is at risk for malware, some users are more vulnerable than others. Our analysis shows that online behavior is a significant indicator of malware risk, even more than the potential riskiness of the App or website itself. These findings are summarized in the following graphs.

In charting the number of safe and risky App sessions per day for each user demographic and behavior profile, Graph 4a shows that Males use more potentially risky Apps than Females; Youth use more potentially risky Apps than all other age groups; and among heavy Internet users Business People use more potentially risky Apps than the Digitally Hooked. This last finding is probably due to the particularly heavy use of video and music streaming by the Digitally Hooked whereas Business People tend to use a wider range of mobile App and URL categories, including email, online storage, web conferencing and remote administration.

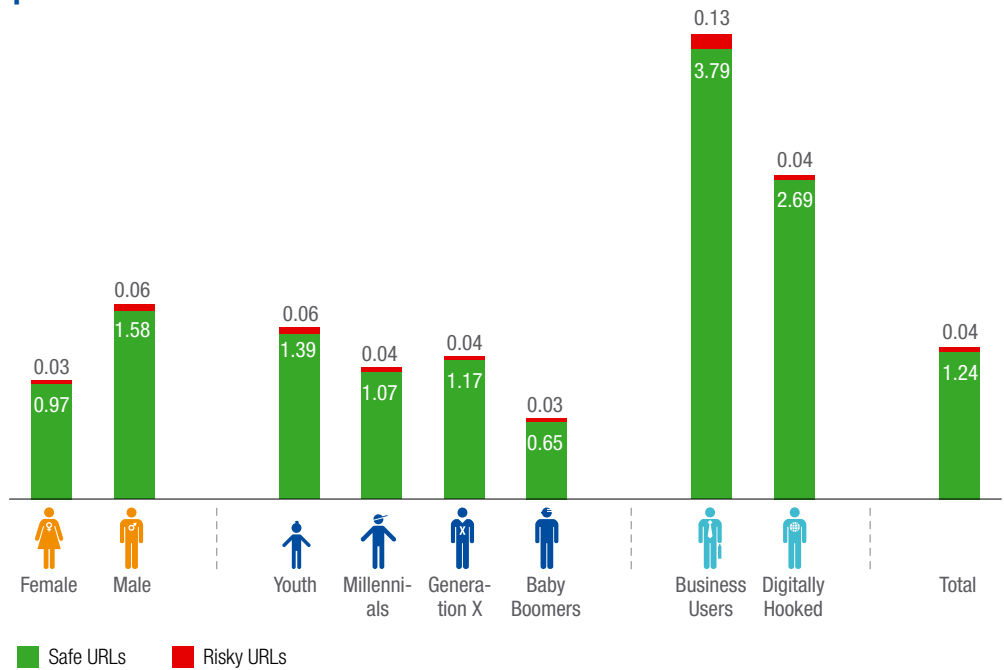
**Graph 4a: Number of safe and potentially risky Apps used per day by customer profile**



As we see in Graph 4a, Business People have more safe and more risky App sessions than any other group - 20% of their daily activity is with potentially risky Apps. When we consider URLs shown in Graph 4b, Business Users are 30% more at risk than other behavioral profiles. This could be fueled by the tendency for Business People to use smartphones and tablets for both business activities and personal use, increasing the variety of content and number of transactions they engage in regularly. Often, their security demarcations are blurred.

Unlike business PCs and laptops where software installation and use is scanned and controlled, smartphone users can download and use any App they choose, and often, they can browse to URLs that are blocked on the company network. This freedom exposes Business People to more cyber risk and can open a backdoor for malware to infect business networks.

**Graph 4b: Number of safe and potentially risky URLs used per day by customer profile**



## Sharing is a risky business

When an App allows file-sharing of any sort, there is more potential for malware risk because it introduces the human factor into the security equation. Mobile users readily share files and links over social networks, email and online storage apps to name just a few. And mobile users readily click to view photos, videos, documents, and other files because they come from trusted friends and colleagues. Cybercriminals are well aware of the “human factor” when it comes to file-sharing and they exploit this vulnerability to spread malware.



Mobile users are tempted to click links which are shared on social media and in talkbacks and look authentic





## Profiling mobile behaviors at risk for malware

When we analyze composite demographics and behavior profiles, the influence of individual behavior in determining malware risk comes into sharp focus. Branching out from our Male/Female demographic, we took a closer look at several composite behavioral profiles and their use of potentially risky Apps during a 24-hour period.

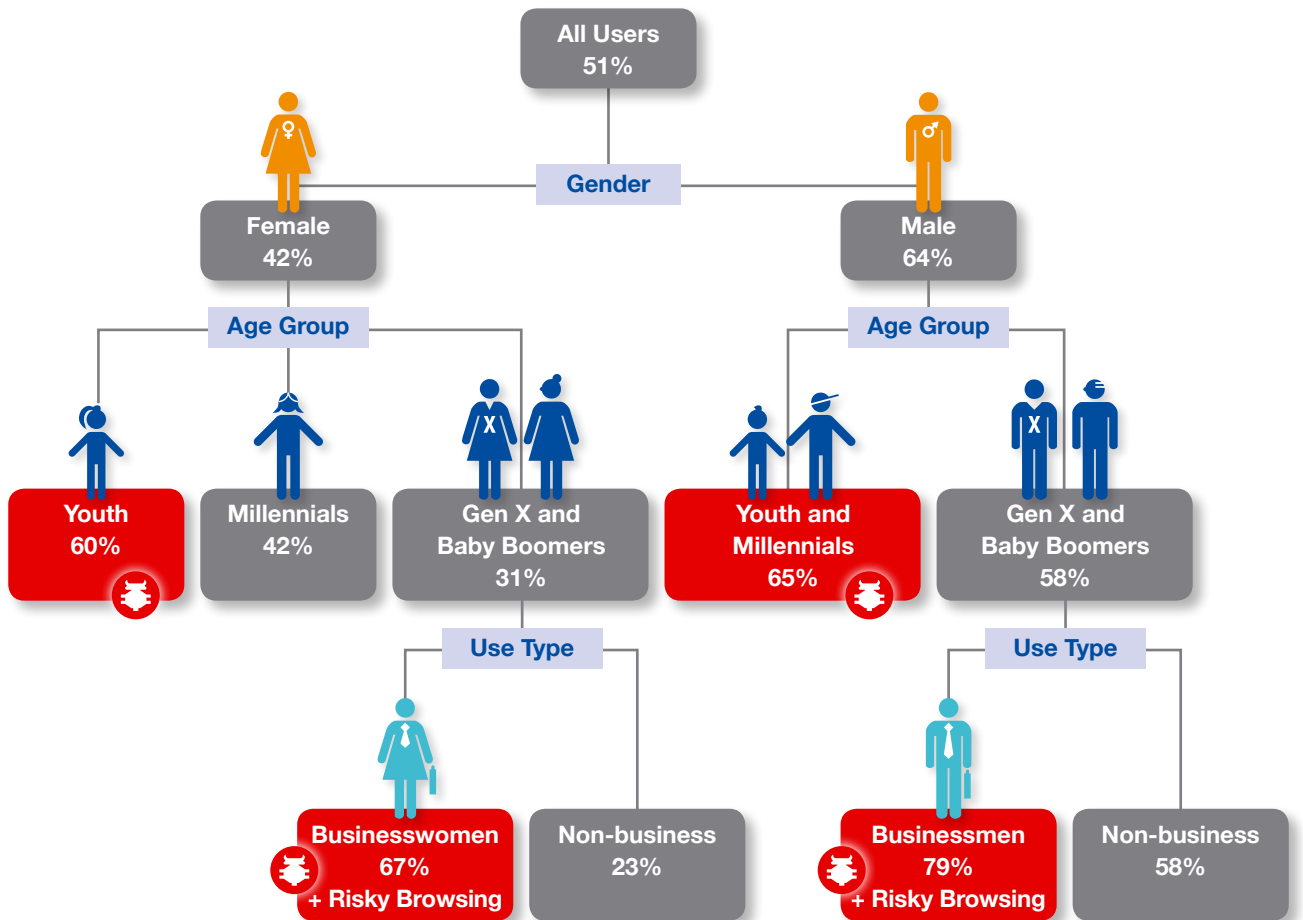
Our findings show that Business People have the riskiest online behavior, with 79% of businessmen and 67% of businesswomen using potentially risky Apps at least once in 24 hours.

Close on their heels are 65% of Male Youth and Male Millennials, and 63% of Female Youth who used potentially risky Apps at least once in a 24-hour period.

To a lesser but still very significant extent, Generation X and Baby Boomer Males also exhibit risky online behavior with 58% of them using potentially risky Apps.

Digitally Hooked users are heavy data consumers of primarily streaming video and music. Due to their routine use of mostly safe Apps, we did not perform further analysis of this segment.

### Percent of behavioral profiles using potentially risky Apps at least once in 24 hours



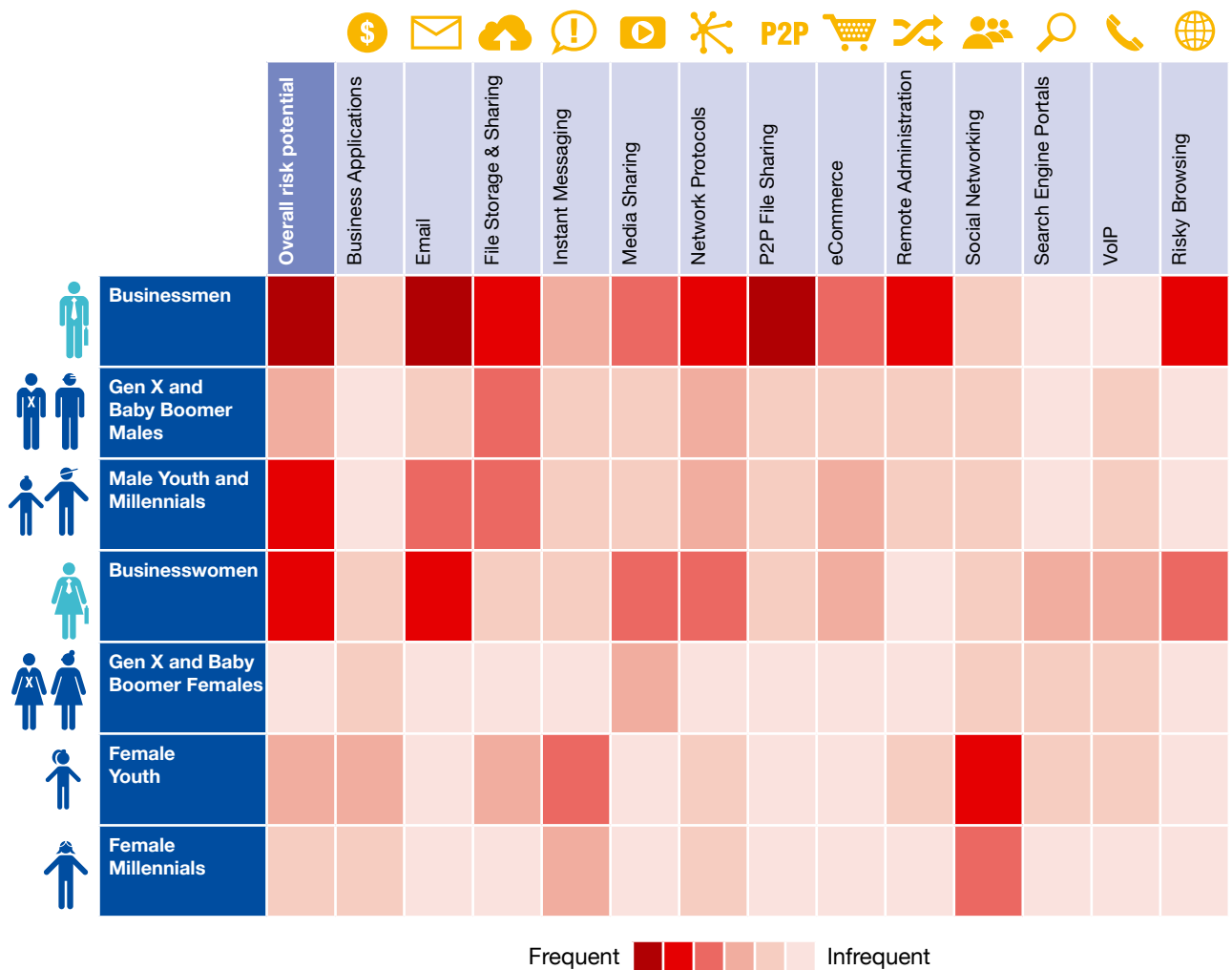
The Risk Assessment Chart below uses heat map methodology to illustrate the potential for malware risk according to the App categories which characterize the online behavior of our composite user profiles and how often they used potentially risky Apps in a 24-hour period.

The chart clearly shows that the online behavior of **Business Users** – both men and women – results in the highest potential risk for malware. In our data sample, we see that Businessmen in particular are not only heavy consumers of data, they frequently browse to a wide variety of websites and use several different Apps. For example, we found that Businessmen use Dropbox and other OTT storage services 57% more often than any other profile. They also had the most transactions with travel-related services – 3 times more on average than other profiles. Moreover, they routinely use remote administration Apps to access email servers and databases, and thereby incur higher potential risk.

In contrast, **Female Youth** are heavy users of social networking Apps. Their online activity is far less diverse than Business Users, focusing primarily on chats, instant messaging, and social networking Apps like Facebook. We noticed that the younger the profile, the greater the tendency to socialize online. While social networking Apps encourage file-sharing, which is potentially risky, this narrow realm of activity incurs much less risk than profiles who use a wider variety of Apps.

### Risk Assessment Chart

Frequency and variety of App and Browsing activity identifies mobile users at risk







## Protecting mobile users at risk



Even though they may be at risk for malware, mobile users will not stop browsing or using popular Apps. But they will be eager to protect their devices and personal data from cyber threats. This is where mobile operators can play an important role in securing the digital experience.

In light of our findings, it makes sense to safeguard users at the network level where the security measures provide a protective umbrella for all online activity and all devices. Our report findings strongly suggest that mobile CSPs can identify and reach out to consumer and business customers who are at risk, targeting them with personalized Security as a Service from their network or cloud. The table below suggests a number of engagement opportunities for CSPs.

	Behavioral Profile	Percent at risk	Engagement Opportunity
	Businessmen	79%	Engage Businesses with a comprehensive Security as a Service package or à la carte services
	Businesswomen	67%	
	Youth (Male and Female)	60-65%	Engage Parents with anti-malware, parental controls, quiet time, and ads blocker in a Security as a Service family package
	Millennial Males	65%	Engage Consumers with anti-malware and ads blocker bundled into data packages to increase their value

## Key Take Aways



**All mobile users are at risk for malware to some extent.** While some Apps and URLs are riskier than others, the potential for malware is pervasive. Therefore, it makes sense to implement security measures at the network level, and not only at the the level of the App store or website.

While **mobile Apps** may be safe to download, they are **potentially risky to use**. And the heavier the use, the greater the risk because frequent users are more exposed to malicious links and files that are shared via email, social networks, online storage, etc.

**Online behavior is a significant indicator of the potential for malware risk** – even more than the App or URL itself. While the cyber security industry develops better tools

and methods for fighting malware, it has no control over individual behavior which often aids and abets the cybercriminal, albeit unwittingly. The desire to click a link or play a video sent by a friend or colleague is just too tempting. Mobile operators are in a unique position to offer effective protection from malware vulnerabilities.

This report suggests a method for mobile operators to **leverage their own network data** to analyze subscriber online browsing and App activity and to gain insight into behavioral profiles who are at risk and would benefit from network-based security services.

## Further Reading



- 1. Malware hidden in desktop and mobile ads is one of the biggest security threats in 2015**  
<http://www.firstpost.com/business/malware-hidden-desktop-mobile-ads-one-biggest-security-threats-2015-2300848.html>
- 2. Malware Spreads through Facebook Tag Scam.** By Diwakar Dinkar on May 18, 2015  
<https://blogs.mcafee.com/mcafee-labs/malware-spreads-facebook-tag-scam/>
- 3. One Million Android Users Infected With Facebook Hacking Malware Apps.** By Farzan Hussain on July 12, 2015  
<https://www.hackread.com/android-malware-Apps-hacking-facebook/>
- 4. Snapchat Warns Users of Third-Party Apps**  
<http://www.securityweek.com/snapchat-warns-users-third-party-Apps>
- 5. Analysis on Maliciousness for Mobile Applications**  
[http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=6296843&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxppls%2Fabs\\_all.jsp%3Farnumber%3D6296843](http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=6296843&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxppls%2Fabs_all.jsp%3Farnumber%3D6296843)
- 6. Differences between peer victimization in cyber and physical settings and associated psychosocial adjustment in early adolescence**  
<http://onlinelibrary.wiley.com/doi/10.1002/pits.20437/abstract;jsessionid=79D6A71E44028ECA50729C67495253EB.f03t03>
- 7. Apps continue to dominate the mobile web**  
<http://www.businessinsider.com/mobile-web-vs-App-usage-statistics-2014-4>



## Allot MobileTrends Report

H1/2016

## About Allot Communications

Allot Communications (NASDAQ, TASE: ALLT) is a leading provider of security and monetization solutions that enable service providers to protect and personalize the digital experience. Allot's flexible and highly scalable service delivery framework leverages the intelligence in data networks, enabling service providers to get closer to their customers, safeguard network assets and users, and accelerate time-to-revenue for value-added services. We employ innovative technology, proven know-how and a collaborative approach to provide the right solution for every network environment. Allot solutions are currently deployed at 5 of the top 10 global mobile operators and in thousands of CSP and enterprise networks worldwide.

[www.allot.com](http://www.allot.com) [info@allot.com](mailto:info@allot.com)

- **Americas:** 300 TradeCenter, Suite 4680, Woburn, MA 01801 USA · Tel: (781) 939-9300 · Toll free: 877-255-6826 · Fax: (781) 939-9393
- **Europe:** NCI – Les Centres d’Affaires Village d’Entreprises ‘Green Side’, 400 Avenue Roumanille, BP309, 06906 Sophia Antipolis Cedex, France · Tel: 33 (0) 4-93-001160 · Fax: 33 (0) 4-93-001165
- **Asia Pacific:** 25 Tai Seng Avenue, #03-03, Scorpio East Building, Singapore 534104 Tel: +65 67490213 Fax: +65 68481015
- **Japan:** 4-2-3-301 Kanda Surugadai, Chiyoda-ku, Tokyo 101-0062 · Tel: 81 (3) 5297-7668 · Fax: 81(3) 5297-7669
- **Middle East and Africa:** 22 Hanagar Street, Industrial Zone B, Hod-Hasharon, 4501317, Israel · Tel: 972 (9) 761-9200 · Fax: 972 (9) 744-3626

