MOBILE APP USAGE EXPLODES IN 2016

There were
90 BILLION
mobile apps
worldwide

15%
increase
over 2015

Survey Shows Mobile Users' Risky Behaviors:

48%
click on links in emails, mobile web and social media promoting apps

55%
of click on ads promoting apps

This behavior increases the risk of downloading counterfeit or compromised apps.

40%
rarely or never check the app details before downloading

&

54%
rarely or never inspect the T&C's or permissions being requested during app

Applications that ask for suspicious permissions, like access to contacts, text messages, administrative features, stored passwords, or credit card are usually up to no good -- there is an elevated risk of the app being fraudulent.

14%
of respondents have jailbroken or routed their phone...

a practice that bypasses security mechanisms established by carriers and official app stores.

App Annie's Retrospective Report Showed:

People spent

900 BILLION
HOURS using mobile apps

25%
increase
over 2015

44%
of online retail traffic was on mobile devices

accounting for

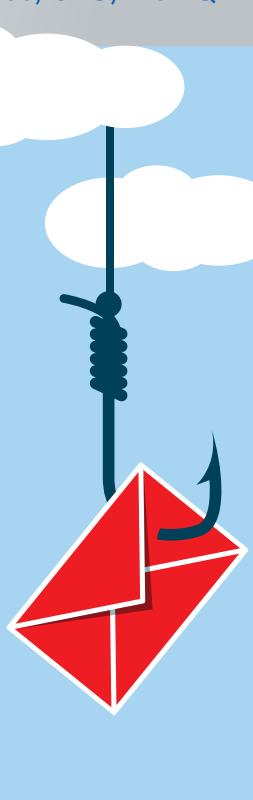
31% of their online sales

"Unfortunately, most companies are blind to all the outdated, unauthorized, modified and malicious mobile apps affecting their business and customer."

- Elias Manousos, CEO, RiskIQ

HOW DOES MOBILE EXPLOSION THREATEN YOUR SECURITY?

Here are just a few reasons the explosion of mobile is a threat to any organization's security:

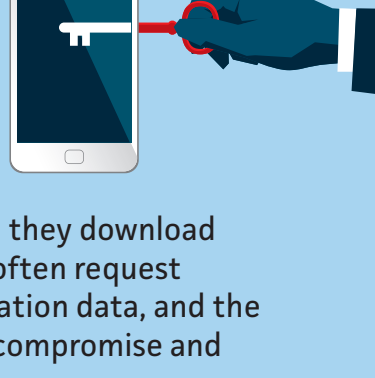


☒ Phishing Attacks:

Mobile devices are the front line of phishing attacks. Mobile users often first see legitimate-looking emails on mobile first, take the bait and click. And, the small size of the mobile screen makes it even harder for the user to verify URLs or closely monitor the email and its associated pages. And, Fake apps also phish for information

☒ Use of Unsecured Wi-Fi:

Mobile users will often gravitate to the free wi-fi to save on their own cell data limits. But, these are usually unsecured and open them to hacking and data theft.



☒ Jailbroken Phones:

A surprising amount of mobile users have jailbroken phones, which enable them to sideload potentially malicious apps and other unsanctioned programs.

☒ Overly Nosey Apps:

Many app users ignore the permissions that are requested when they download and run an application for the first time. Malicious applications often request permissions to items like your text messages, phone call log, location data, and the ability to post to social media networks. These permissions can compromise and expose user data.

Download the full Mobile Consumer Research Report March 2017.

App Annie's Retrospective 2016 report

* RiskIQ commissioned Ginger Comms2 to survey 1,000 U.S. and 1,000 U.K consumers aged 16 to 60+, specifically focusing on smartphone and mobile app usage.

RISKIQ