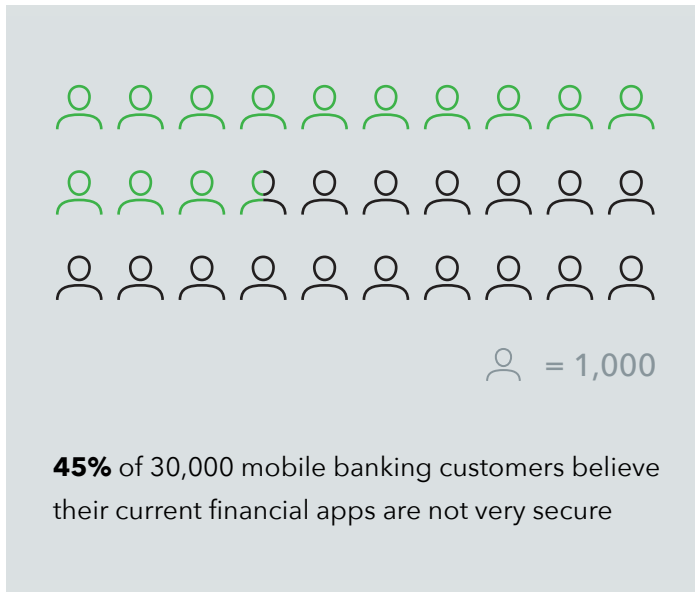# Financial services mobile apps are under attack

Mobile banking is quickly changing the face of the financial services industry.

Your customers are savvy and they want to know they're protected. Lookout surveyed over 30,000 mobile banking customers, including your customers, and found that 45% of respondents believe their current financial service apps are not very secure.
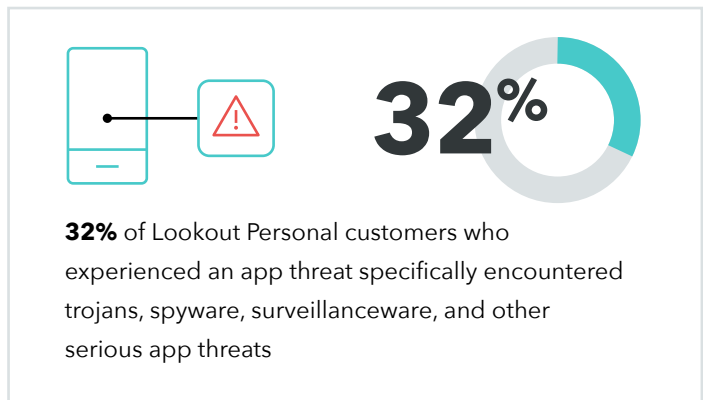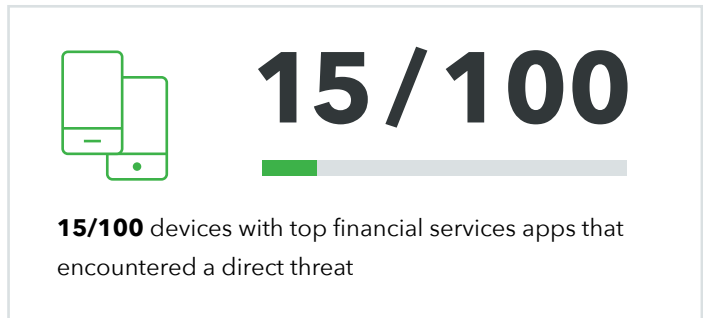

= 1,000

45% of 30,000 mobile banking customers believe their current financial apps are not very secure

Nearly 100% of users say this is Very Important to them – especially as active threats continue to multiply.

While today's banking customers enjoy 24/7 accessibility, financial institutions benefit from increased customer engagement, improved brand recognition, and a reduced cost of service.

Yet, with all the advantages mobile banking offers, it has also introduced significant risk. From trojans that steal login information to rogue versions of legitimate banking apps, customer privacy and security are under attack.

Financial-industry focused mobile threats are active now

15/100

15/100 devices with top financial services apps that encountered a direct threat

32%

32% of Lookout Personal customers who experienced an app threat specifically encountered trojans, spyware, surveillanceware, and other serious app threats

Motivation

At Lookout, we're seeing an increase in the number and sophistication of actual threats targeted directly at finserv apps, including:

- **BancaMarStealer and TauSpy** – Intercepts customer login credentials

- **PlayBanker** – Sends push notifications for rogue versions of legitimate banking apps

- **Shunbad** – Impersonates banking apps and steals SMS and contact data

- **SvPeng** – Overlays fake logins on legitimate apps to steal victim's banking credentials
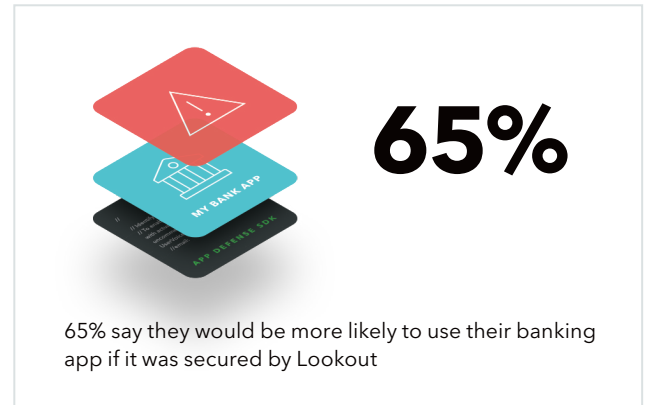
BancaMarStealer: a mobile banking trojan stealing customer login credentials

The BancaMarStealer malware family is an Android mobile banking trojan first seen in May 2013. It is currently very active with over 7,500 samples being seen to date. BancaMarStealer lures victims into unknowingly entering their credit card details by displaying legitimate looking overlays that are carefully designed to imitate the login portal of a victim's bank. It can be configured to target specific banks, communicate to certain command and control servers, and supports a wide range of remote commands. Impacted banks include Bank of America, Discover, CitiBank, JPMorgan Chase, and others.

Why Lookout App Defense

On average, nearly 65 percent of respondents said they'd be more likely to use their banking app if it was secured by Lookout.

65%

65% say they would be more likely to use their banking app if it was secured by Lookout

Lookout App Defense provides financial services firms with proactive mobile app security by preventing data compromise of customer-facing mobile apps. Lookout detects mobile risks that can lead to account takeover and prevents malicious threats from accessing customer data and financial transactions via your mobile app.

You will receive:

- Our cloud-first architecture allows us to deploy instant threat protection without app updates, making security seamless for app developers and consumers.

- Quick and easy deployment through our SDK format.

- Security at consumer scale - With over 150 million mobile devices running Lookout, you can have confidence your app security will scale with your customers.

Learn more about how App Defense can protect your organization today at lookout.com/products/app-defense