Luxury Daily®

The News and Intelligence You Need on Luxury

LEGAL AND PRIVACY

200 mobile apps, sites leaked personal information last year: report

December 15, 2016

Image courtesy of Citi Bank

By Danny Parisi for Mobile Commerce Daily

Mobile security risks remain a serious concern for marketers and consumers alike now that a new report has shown that more than 200 different mobile applications and Web sites were leaking personally identifiable information over the course of the last year.

The data comes from a new report on data security from Wandera. The report studied mobile apps and sites from 20 different countries and found significant evidence of leaked information.

"Mobile is well and truly the new frontier for data security," said Eldar Tuvey, CEO of Wandera. "It's clear that security and compliance risks are far more formidable threats than previously thought."

Personally identifiable information

With mobile increasingly being the preferred digital medium through which we live our lives, consumers are putting more and more personal information into their mobile apps and mobile Web sites.

With the proliferation of mobile wallets, financial data has now been added to that list. Along with money, other personal information such as addresses, phone numbers, contact information and correspondences all may be subject to leakage or theft.

screen-shot-2016-12-13-at-11-16-44-am

Email addresses were the most likely to be leaked

Wandera wanted to put a rough estimate on how much of this information remains insecure. To do this, the company took a look at nearly four billion requests from across hundreds of thousands of devices in 20 countries.

The results showed that more than 200 different mobile apps and sites were vulnerable to leaked personally identifiable information, or PII.

PII consists of any information that can be used to link digital activity to a specific person. This can be account numbers, email addresses, physical addresses, transaction data or any number of data points that might be tie something to a specific person.

Mobile security

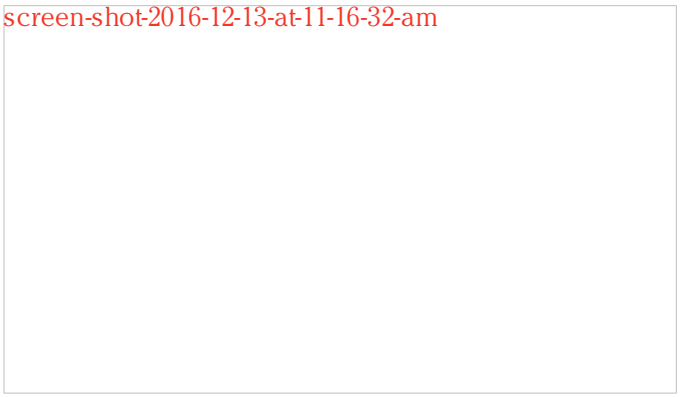
No one industry or category of mobile program is to blame for these vulnerabilities. The leaked data ranged from a wide variety of sources, including news, travel, sports, entertainment and mobile shopping.

Some types of Web sites were more prone to leakage than others. A shocking 80 percent of the top 50 adult Web sites were found to be leaking information.

Almost 60 percent of all leaks came from one of three categories: news/sports, business/industry and shopping.

Another potentially surprising detail is that despite its sharing-oriented nature and outsized popularity compared to other mobile services, social media accounted for only 2 percent of all leaks.

The silver lining is that the most valuable of data things such as credit card information was the least likely to be leaked, accounting for less than 3 percent of all leaks.



This data is important for mobile brands and marketers who want to gauge their audience's response to security concerns.

A recent study found that more consumers would be willing to sacrifice some functionality or convenience for better protection and security (see story).

Taken together, these two reports show that brands and marketers may need to adjust their priorities in the balance between convenience and security to be more in line with consumer desire.

"With the reported cost of remedying a mobile breach in the United States falling between $250,000 to $400,000 in many cases, enterprises need to take concrete steps to routinely monitor the data that flows to and from each individual device, identify potential security gaps and dynamically respond," Mr. Tuvey said.