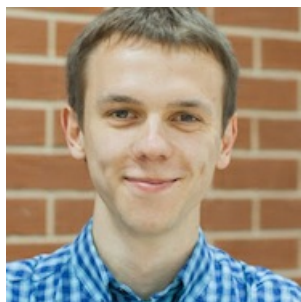


COLUMNS

Building engaging and secure mobile apps

August 9, 2016



Pavel Novik is QA unit manager and head of the Mobile Testing Center of Excellence at AIQA

By **Pavel Novik**

Subscribe to **Luxury Daily**
Plus: Just released
State of Luxury 2019 **Save \$246 ▶**

We live in the era of Big Data, where the Internet of Things and smartphones are ubiquitous. Each month we adopt new applications that require us to enter personal information, share our geo-coordinates, or ask to observe our browsing habits. Obviously, the main goal that marketers are pursuing is to collect social profile data and improve user acquisition.

The more personal data that marketers obtain, the better they can serve their users. However, users do not typically have much desire to help them.

Sharing is scaring?

According to the Global Consumer Trust Report 2016, the number of mobile users who feel comfortable with the idea of sharing information has decreased.

In 2013, 21 percent of the respondents said they would eagerly share with the application. By 2015, this number has fallen to 6 percent.

The scope of "reluctant sharers" who share data only because they have no other choice if they want to use the app has leapt to 41 percent from 2014's 33 percent.

This data should serve as a wake-up call to the mobile industry to collaborate and do more to instill consumer trust in mobile services.

There are a number of practices on asking users for more information such as social sign-in options and bonuses in the exchange for extra data.

No matter which of them you adhere to, one thing remains constant: you need to be sound clear and reliable. Obviously, a good marketer should be aware of the security issues relevant to its app.

Users must feel confident installing the app and using it wherever they might want to. However, most public Wi-Fi networks lack security. So it would be a wise choice to disable automatic connectivity to such networks to prevent loss of important data.

Data leaks are the concern where users are expected to sync data to the cloud. The vendor's protection mechanisms cannot be controlled even if the company's security policies comply with best practices. To tackle this issue, it is recommended to ensure a different password for every app or service.

However, most of the security shortcomings are to be tested beforehand, on the development and testing stages of the security lifecycle. And it is hardly possible that marketers will be involved when making decisions of this kind.

By design

One of the main contacts for mobile marketers should be user experience specialists, both designers and testers.

Marketers might be willing to ask endless questions to the users, but it is up to the user experience design (UX) experts to consider them all and, in turn, deliver comfortable and easy solutions to satisfy both marketers and users.

Sometimes it will be necessary to limit the number of data-gathering questions, sometimes it will be vital to prepare a prototype and implement a user-friendly screen or a new pop-up window with progress bars to let users know that they will eventually reach a conclusion.

This is why any mobile marketer should know the difference between user experience and usability, and know how main UX facets can be measured.

UX specialists will also consult on the choice of the words to overcome the ambiguity and communicate the right question when asking users to provide their data.

TO SUCCEED in delivering engaging and secure software over the long term, the whole team must take responsibility for quality, planning and the execution of testing activities.

It is imperative to build quality in from the start. That means testers, programmers, designers, product experts and marketers everyone must collaborate continuously.

The "Three Amigos" talk, which is one of the most valuable agile approaches, can be adjusted so that marketers could also have a voice to improve the software that they will have to promote.

Pavel Novik is QA unit manager and head of the Mobile Testing Center of Excellence at [AIQA](#), Lakewood, CO. Reach him at p.novik@aiqa.com.