



As the Remote Workforce now takes a permanent foothold here in the United States, there is going to be one common denominator: People will use their smartphones more than ever before, to conduct both personal and work-related matters. Notably, there will even be more reliance on mobile apps. Consider these statistics:

- At the present time, there are well over 3.2 billion smartphone users on a global basis. This number is only expected to increase in the future, as more companies adopt a Cloud-based infrastructure. In fact, technology gurus estimate that the total number of smartphone users will surpass 7 billion by 2025.
- The mobile app market is expected to reach a whopping \$100 billion by the year 2024.

Mobile App Usage By Market Sector

Here are some statistics on mobile app usage by industry:

At the present time, the two dominate mobile app players are:

- The App Store: More than 2 million mobile apps;
- The Google Play: 3.4 million mobile apps.

Here is how the mobile app market breaks out by market sector:

- The Financial Industry: Mobile apps in this sector have been downloaded 4.6 billion times on a global basis, with an annual growth rate of 15%.
- The Hospitality Industry: Mobile apps have been downloaded 400 million times, and this represents a growth rate of 20% year over year.
- The Travel Industry: Almost 11 million apps have been recently downloaded, which represents an astonishing growth rate of 81%. This number is only expected to grow as the COVID-19 restrictions start to ease up worldwide.

But it's not just the mobile apps themselves that are gaining in popularity; the advertising revenue that is generated from mobile apps is tremendous. Consider these statistics:

- On a global basis, mobile advertising revenue reached \$276 billion.
- In the US, ad revenue has reached \$113 billion.
- The ad revenue for Facebook was around \$84 billion.
- The ad revenue for Google was at \$147 billion.

(Sources 1, 2)

What might stop the growth rate for mobile apps?

There is one thing that might stop these numbers from growing exponentially: the Cyber Threat Landscape. The Cyber Threat Landscape is becoming more complex and stealthier every day, and the mobile app is a favorite target of today's Cyberattacker.

There are many ways for a hacker to penetrate into a mobile app and deliver a malicious payload. But one of the more pronounced avenues in which they can find their way in are the mistakes that mobile app developers make during the development process.

While insecure source code design can be a common culprit, other factors in the app development process also come into play. This will be examined in the next article in this series, as we take a closer look at what can be done to correct these weaknesses, so that the mobile app industry can continue to grow.

Source:

- https://intersog.com/blog/mobile-app-development-statistics/
- https://clearbridgemobile.com/stats-for-mobile-app-growth-and-success/



As the first article in this series explained, the mobile app market is growing exponentially. However, continued success of this market depends on app developers avoiding some common mistakes.

Before we delve into the top mistakes mobile app developers make, we should provide some insight as to why users decide to uninstall a mobile app. The illustration below outlines those reasons.

What makes Users Uninstall an App



(Source 1)

The top mistakes mobile app developers make

The following are some of the chief reasons why mobile apps fail in the first place, at the holistic level.

- Not meeting the needs of the end-user. One of the most basic rules in business is that you must meet the needs of your customers. If you don't, they simply won't buy from you. Whether you agree with it or not, the customer is always right, especially when it comes to using your mobile app. So, this is the point at which you really need to sit down with your client to make sure you understand what they need. *This can be one of the hardest and longest phases of the mobile app development lifecycle*. If you're client is getting impatient with how much time it is taking, tell them that it would be far costlier to make any changes at the end rather than addressing all of their needs and requirements at the very beginning. Also, as the mobile app is being developed, keep your client informed with mockups so they can get a firsthand view of what is happening. That way, if there are any changes to be made, or new requirements that need to be met, it is far easier to do it by embracing this modular approach, rather than waiting until the very end. Also, keep things simple. Mobile app users are not enamored with bells and whistles; they just want to use the app right away and have it do what they want it to do..
- Creating for too many platforms. In this regard, the top three sources for mobile app downloads are Google, Apple, and Microsoft. While your ultimate goal is to have your app on every app store possible (apart from these three), you need to take a slow and cautious approach to this. If you are developing an app for a specific customer, then this point of consideration does not need to much of attention. But if you are developing an app for the masses, then this is of utmost importance to you. It is highly recommended that you first start with one store, such as Apple. Develop your app, thoroughly test it in a sandbox environment, then upload it for the public. Keep in mind that Apple has one of the most stringent security requirements when it comes to this process. Once you get a gauge as to how your mobile app is doing, then proceed in creating for Google Play, then Windows, etc. This is also serves as a Cybersecurity advantage, because this phased-in approach, your mobile app will not catch the direct attention of a hacker. But if you attempt to upload your app to every app store out there, this will definitely grab the attention of Cyberattackers who will try to break your product as much as possible.
- Not having enough tools to help the user. While most mobile app users are intuitive and can figure out pretty quickly how to use an app, others will need a helping hand. There is no need to write a 100-page manual, but rather, as your customer goes through it, you should add visual cues coupled with some text to demonstrate how that specific function works. You want your customers to understand that feature and benefit quickly. Here are tips on how to do this:
 - Create a simple and clean design. This goes back to the principles of User Interface and User Experience (also known as "UI/UX"). At this point, you should consider working with a web designer to get this right the first time around.
 - Make sure that the language in the text is appropriate to the culture of the people who'll be using your mobile app. Simply put, once you have determined the target market, make sure that the tempo and lingo of the text fits that group, so that they can understand things easily.
- Overloading the app. This goes back to our first point, and that is why it is so important. Give the customer exactly what they want
 the first time, and as you continue with updates to the mobile app, then add more to it. Start with a few top-notch features first that
 dazzle your customer. From there, it's virtually guaranteed that they will want more from you, which of course means repeat business
 —and more revenue for your bottom line.

In addition to the design issues reviewed in the last section, mobile app developers fail to consider the **Cybersecurity issues** related to what they are developing. This can result in the end user becoming a victim instead of a happy customer. Here are the key Cybersecurity factors that are often overlooked:

- Not using encryption. This is one of the biggest buzzwords being thrown around today in the world of Cyber; simply put, encryption is merely the scrambling of data at the point of origination and unscrambling of the data at the destination point. Many mobile app developers do not take this into consideration during the creation process. They have the mindset that their job is to only to develop the app, and nothing more. Keep in mind that end users today use their mobile apps more than ever to make online purchases. If their personal data is not encrypted (primarily their credit card number and social security number), they could easily become the victim of identity theft, or other threat variants, such as Man In The Middle Attacks. All it takes for a Cyberattacker to intercept the data packets coming from a smartphone is to use a basic network sniffer.
- Using inexperienced mobile app developers. This comes down to a matter of whether to outsource your mobile app development or not, and the primary driver is cost. Thus, you want to make sure that your mobile app developer is also well versed in the latest programming languages, such as Python. Remember, developing your mobile app is, at its very core, also a software development process. Therefore, you may even want to incorporate the principles of DevSecOps (which was examined a previous article). The bottom line is that in the end, you get what you pay for, and it may be wiser to get an experienced development team involved in the process.
- Not keeping a coherent structure. It is imperative that the mobile developer stick with a consistent formatting. This simply means that any comments that are required to put into the source code are included, and that they are comprehensible, so that anybody on the team can understand them. Commenting is a very important component to have, especially when it's time to come out with subsequent releases. In a rush to launch, mobile app developers often write and compile the code any which way they can, without paying any attention to how it looks structurally. This is crucial, as having source code that this written in a clean, organized structure will make it far easier to go back and make corrections, if necessary.
- Not testing the code. This is by far the most overlooked area in mobile app development. The source code is hardly ever tested, and if it is, at best it is done at the very end, when it is often too late. In fact, for a long time, software developers in general have escaped the eyes of Cybersecurity—until now. According to the latest Verizon Security Breach report, Web application security is becoming a prime concern today, and this is coming from the source that has not been evaluated. Quality Assurance (QA) testing needs to be done as well but is often ignored. Therefore, it is highly recommended that both of types of testing take place at a modular level, so that any flaws do not have a cascading effect in other parts of the mobile app development process. This kind of approach can be seen in the diagram below:



(Source 2).

- Using APIs from open-source libraries. In the world of mobile app development, developers often like to use what are known as "APIs." These are merely lines of code that have been created (much like a script in PERL or Python) that can be used to bridge the front end (the user interface) and the backend (the database) of the mobile app. The beauty of this approach is that the code in the APIs can be used to modify to fit the needs and requirements of the project, without having to write the code from scratch. This of course can save a lot of time and money. But the problem here is that mobile app developers use APIs from open-source libraries that have not kept their products up- to-date with the latest patches and upgrades. This can be a serious security flaw and can have detrimental consequences down the road if they are not checked before they are first used.
- Not implementing other protocols. Many mobile app developers fail to implement what are known as Authentication and Authorization protocols into the source code. The former refers to the 100% confirmation of the end user, and the latter refers to the permissions granted to access the mobile app (the primary example here is the password). In fact, the world today is moving towards what is known as the "Zero Trust Framework." This is the situation where at least three or more layers of authentication and authorization are used. Mobile app developers need to factor this heavily at the very beginning stages of the mobile app creation, and make sure that it has been included into the source code as it evolves over time.

Up Next: Best practices for mobile app development

This article has detailed the top mistakes to avoid when developing a mobile app, and the next article in this series will take a proactive stance by outlining the best practices for mobile app developers to follow.

Sources:

- 1. https://techspective.net/2021/12/07/10-common-security-mistakes-that-mobile-app-developers-make/
- 2. https://rebit.org.in/blogs/strategic-benefits-of-secure-software-development-lifecycle-ssdlc-approach

https://www.appventurez.com/blog/mobile-application-development-mistakes-to-avoid/



The first two articles in this series focused on the rapid growth and common pitfalls of mobile app development, as well as the top mistakes mobile app developers make. This third and final article in the series puts a more positive spin on the topic by laying out a set of best practices to follow when creating a mobile app, inclusive also of the other categories covered in this article:

- Keep the navigation easy. It is only human nature to think that by making something more complex, it will have a wider appeal to
 the customer, because you are showing off what you can do. But this is not true. Mobile app users want something that is easy to
 navigate and get to where they want in seconds. If the navigation is complex, they will likely discard your mobile app in search of
 something else. In fact, 60% of mobile app users say that they will get rid of the app if it does not load in three seconds or less.
 (Source 1)
- Choose the right technology to create the app. You need to select the right programming language to create the mobile app in the most efficient way possible. Here is a sampling of languages that are heavily used to create mobile apps:
 - Ruby
 - ASP.NET
 - AJAX
 - Objective-C
 - Python
 - Perl
 - C
 - C#
 - C++
 - HTML
 - ∘ Java
 - ∘ SQL
 - ∘ PHP
 - Swift
 - TypeScript

(Source 1)

- **The Thumb Rule.** This is a critical area in the UI/UX process. This simply means that the mobile app should be easily accessed and used by the customer using a thumb only. Think about it when you use your smartphone next time: You are using your thumb to navigate through everything. The mobile app should be made so that it is both thumb scrolling and thumb interactive friendly.
- Keep up the testing. As noted earlier in this series, the testing process should be repeated over and over again to make sure you have a secure product and that your end user will be happy when new releases come out. However, there are other testing procedures that you may want to consider, such as:
 - Localization testing
 - UI/UX testing
 - Memory leak testing
 - Platform and device testing.
- Break it down into smaller tasks. Although creating a mobile app is a fun process, it can also be quite complex, depending on the needs and requirements of your client. Therefore, use the principles of Project Management and break down actions into smaller chunks that are much more digestible and consumable. You should never take the approach of creating a mobile app by chopping down a tree all at once. Rather, you need to cut each branch at a time, and from there, go to the root.
- Follow the guidelines from the beginning of the process. As described earlier, the two main venues for uploading your mobile apps are Google and Apple. Therefore, you will want to review their app development requirements and guidelines *before* you embark upon the development process.

- The Google Requirements doc can be seen here: https://developer.android.com/guide
- The Apple Requirements doc can be seen here: https://developer.apple.com/programs/
- Stay engaged with the metrics. Once you have developed your first mobile app for the masses, you will want to keep a keen eye on these specific metrics:
 - The level of User Engagement
 - The rate of Adoption
 - The overall rate of Customer Retention
 - The rate of Customer Retention in your target markets.

By keeping track of these metrics, you will have a better idea of the functionalities and tools you need to put into future releases of the app.

Conclusions

This article has examined the trends in mobile apps and their development, where the development process goes wrong, and a list of best practices to follow. Technically speaking, mobile app development does not really take too long – but if you want to market your brand and get new prospects and customers, this process can take ten times longer. But in the end, the effort will be well worth it.

Source:

https://www.designveloper.com/blog/mobile-development-best-practices/