

Cybersecurity tips for app development companies

By [Harnil Oza](#)

19 Mar 2019

App development companies that wish to make a name for themselves are in the process of studying every possible sector. While there are some who are looking to assist businesses, there are others who would rather work on apps that are designed with the fun lovers in mind. Any app development companies that are looking to expand their reach are working with a wide range of clients on a variety of projects.



Harnil Oza is the CEO of Hyperlink InfoSystem

No matter what projects app development companies may be working on, there is one aspect of the proceedings that need to be addressed: cybersecurity.

Cybersecurity means many things to many people. For app development companies, it is all about creating an application that can be used without placing the consumer at any level of danger.

Our mobile devices are incredibly useful and thanks to their help, they can do anything at any time. Without proper cybersecurity, our smartphones' ability to assist us is going to be hindered. While this reality may seem frightening to some, there are a few key steps that can be taken.

These helpful pointers will allow for a greater level of cybersecurity to take place and keep users safe each and every step of the way. For app development companies that plan on working with large amounts of data, these tips are especially important.

Be careful about organisational rules

While mobile app development companies can certainly help when it comes to security (we will get to that), organisations that are going to utilise the apps that are being created will also play an important role.



How to go about developing your enterprise app

Peter Scheffel 11 Jan 2018



They must beware of the employees that are going to be bringing their own device to work to use for company purposes. In most instances, giving employees company devices to use instead will go much farther towards reducing potential vulnerabilities.

Protect the devices in the correct manner

The user must also take some level of responsibility for their own actions. Even the most well-designed app is not going to keep a person safe if they are not willing to take certain steps of their own.

The best piece of advice that can be given to users is not to place their faith in a device that has already been jailbroken. This increases the level of vulnerability that the user will experience by forcing them to go without the typical built-in security measures.

Test the software

Mobile app development companies must be willing to test the software that they have chosen to use. This is one of the most pivotal steps in the development process and it cannot be skipped for any reason.

Apps are produced on a daily basis and companies allow themselves to lose sight of the importance of testing as a result. After all, what good is a secure app if your competitors are beating you to the marketplace? Don't worry about the competition. Take the time to test.

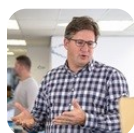
Have the right API security strategy

This is another step that cannot be skipped. Mobile app development and APIs remain closely intertwined. In order to properly secure a mobile app, the API must be secured as well. APIs are responsible for controlling the flow of data between a number of different parties.

If they are not secured, you are essentially setting yourself up for a world of hurt. APIs are a primary conduit and must be treated as such.

Remain mindful of the consumer's data

Mobile apps require a different form of storage than typical web-based apps. This is because there is far more data and code to consider. The more data that is going to be stored, the more vulnerable the device will become.



App development made easy with microservices

Nick Durrant 23 Aug 2018



Mobile app developers must beware of this issue and create apps that are designed to help consumers avoid any unnecessary vulnerabilities. The tactics that have worked well in the past when it comes to web-based applications are not going to be able to be replicated when it comes time to secure a mobile app.

Put the correct measures in place

As any experienced app developer can tell you, the security measures that are going to keep a user safe need to put into place before the app is released to the general public - not after. To that end, the right authentication processes must be considered before the app is provided to the consumer.

Businesses should not be allowing any inexperienced developers to handle this step of the process. Authorisation technology has come a long way and equipping an app with the right identification and authentication tools is what will separate the top notch apps from the apps that end up dying on the vine.

Secure back end network connections

The APIs that the app is going to use will need to access cloud servers. These servers may be yours or they may belong to a third party instead. Protecting data is always important and without the proper back end security on these connections, an app user is placed at risk.

If there are no methods in place that prevent user access that is not fully authorised, you are creating a free for all that will allow anyone and everyone to launch an attack. Sensitive information is going to be passed back and forth on these databases and the right security measures must be taken at all times.

Start from the ground up

Security never stops being important and developers must consider this reality every step of the way. If it is not made a top priority from the very beginning, a number of issues will come into play. Once these issues arise, it is very hard to overcome them.

Preventive medicine is the key in these instances. A sizable percentage of vulnerabilities occur in the source code. Unfortunately, businesses are not always willing to focus their spending accordingly. Developer errors are more likely to take place when firms and businesses do not come together to place the proper level of importance on the early steps of the process.

ABOUT THE AUTHOR

Harnil Oza is the CEO of Hyperlink InfoSystem, a mobile app development company based in the USA and India.

For more, visit: <https://www.bizcommunity.com>