WHY APP DEVELOPERS IN THE UK CHOOSE IOS

FOR ENTERPRISE APPLICATION DESIGN

With the rapid growth of smartphone adoption, their users, app developers and manufacturers have faced a new major challenge - the fear of losing a phone or having it compromised has given birth to a new fear: someone stealing your personal data stored on the device.

Security has always been a matter of a holy war between Android and iOS opponents. But which operating system is more secure when it comes down to protecting enterprise data?

Millions of new mobile phones pour into businesses on a monthly basis, and it is really important to know the risks these devices can bring to your company in terms of enterprise apps and data security.When just looking at statistics, it is clear that an overwhelming majority of corporations prefer iOS to Android - according to various reports, the enterprise market share of iOS comes up to 64% (see the full report here). But what are the reasons of its popularity and why has iOS app design become the top priority for UK enterprise app developers?

Open vs Closed

To start with, let us make sense of some key terms. Android is an open operating system because it is based on a code from the Android Open Source Project, which is open to the public. That means that you or any of your company's employees can access the code and change it to your liking. Moreover, mobile phone manufacturers can do exactly the same - they customize Android source code to create a new software with unique aesthetics, features and functionality. On the contrary, iOS is a closed source system. No one can make changes to it. Such a lack of freedom is absolutely justified, as it provides a uniform experience across all devices in your company running on iOS. In other words, all the iPhones and iPads of every member of your staff have exactly the same system configurations and interfaces. However, it does not mean that iOS is invulnerable - one of the latest reports demonstrates that 375 flaws were discovered in Apple’s mobile operating system.

On the other hand, it is impossible to provide the same statistics for Android. But how can that be? This is due to the fact that device manufacturers enjoy a certain number of liberties when they design Android devices. All the changes made to the OS, its default applications and interface add more vulnerability. Such companies as Samsung, HTC, Motorola and others are free to update Android whenever they like - daily, monthly, annually or even never (such as when you have an older smartphone). The main exception is Google Nexus phones - they are updated immediately from the source, similar to Apple's products.

iOS & Android: Guarding Against Malware

The fact that Android is open and iOS is closed affects you and your company's employees at different levels. One of the major problems of an open source platform is that it enables you to run third-party applications on corporate devices. This option exposes your devices to various risks posed by unofficial app stores and applications that have not undergone security checks, as it is impossible to track all the applications employees install on their smartphones or tablets. On top of that, Android's open nature enables developers to build malicious apps that can be very harmful, whereas when speaking of iOS, its closed nature grants protection from intruders and ensures corporate data safety, much like if the system were surrounded by a force field. All iOS applications pass strict security examinations before they are approved and published in the App Store. There is no way you can download and install a third-party app on an iOS device, unless you jailbreak it.

Enterprise App Design Management

Over time iOS has become a top platform for enterprise **app developers,** penetrating workplaces not only in the UK, but all around the globe. Meanwhile Android is still trying to catch up. The two platforms have their unique mobile device management (MDM) specifications, which are crucial to understand if you want to create a secure and productive enterprise application.

The general purposes of MDM are:

- Monitoring mobile devices within corporate infrastructure;
- Enabling employees to work anyplace and anytime;
- Managing app distribution across a company; and
- Securely managing data and configuration settings on all corporate and personal devices.

The major difference between Android and iOS MDM strategies comes down to this: iOS MDM enables the administrator to stream commands to all iOS devices at a time, while Android MDM commands are developed by different manufacturers (HTC, Samsung, Motorola, etc.) and cannot be applied to all Android devices at once. As a result, Android's security features depend heavily on hardware and vary from one smartphone to another. To summarise, iOS is the clear winner, as it provides instant support to every personal and enterprise device and has a more secure protocol that relies on security certificates for authentication.

If security is a top concern for your enterprise - and it should be without doubt - iOS is the best choice. While Android is struggling to improve, it still has a long way to go before catching Apple’s mobile operating system, which boasts higher safety and provides regular security updates for all devices.