Data privacy on mobile applications

Data Privacy is all about confidentiality, availability, and integrity of data. It is all of the practices and processes that are in place to ensure data isn't being used or accessed by unauthorized individuals or parties. The threat is real. Data breaches are happening in all sectors and industries. It can destroy the credibility and reputation of a business environment.

Mobile technology has grown more than any other in the last few years and the IT industry. Due the growing trend, many actors have been attracted by the possibility to exploit the mobile solutions for various purposes. Mobile devices accompany us in our movements, manage our communications and allows us the use of various services such as banking, payments and social networking

Often, the hack or data breach occurs without the consumer's knowledge, And it's not just consumers that criminals target, with the rise of smartphones in the workplace, hackers attempt to attack enterprises through vulnerabilities in mobile devices. Some key reasons that mobile app development is suffering on the security front. Mobile app development projects often place a huge premium on time-to-market. These applications often deal with personally identifiable information, credit card and other sensitive data. In significant numbers of cases, apps have been hacked and uploaded either to capture credentials from users, or to operate maliciously, or to defraud the app's creator by removing adware element.

Analysis found that third-party stores are a significant source of hacked apps. Hacked versions of all of the top 100 paid apps for Android, and 56% of the top 100 paid apps for iOS either on the main store or third-party sites. Hackers will always follow the flow of money, and will focus on the platform with the most users. A recent mobile malware study states that 92% of malware was created for Android, and malware on iOS was not noticeable."

Making sure all company data is private and being used properly can be a near-impossible task that involves multiple layers of security. Fortunately, with the right people, process and technology, you can support your company's data security policy through continual monitoring and visibility into every access point.

AppTrusty brings global experience to the table in understanding technology, the regulatory maze, risks and controls. Our team can work with yours to build and maintain an integrated global framework for data protection, privacy and compliance. Using a scalable, risk-based approach, we'll help you determine what needs to be secured and how to do it, by performing pentesting services.

Penetration testing offers many benefits allowing you to:

- Intelligently manage vulnerabilities
- Avoid the cost of network downtime
- Meet regulatory requirements and avoid fines
- Preserve corporate image and customer loyalty