Octal0g1k
ANSWERING YOUR CYBER CHALLENGES

Cybersecurity risk in the Mobile World

The global mobile market is expected to reach $1351.8 billion by 2025. The combined count of apps available on the Apple App Store and Google Play Store is over 5 million. The low cost of internet and the explosion of the number of mobile applications every day have not only escalated the cyber security risks for mobile applications but also created new cyber security risks. According to a research report by Gartner, more than 75 percent of the mobile apps fail the basic security tests.

Technological advancements have made the smart phones cheaper, more powerful, and thus the number of global smart phone users are on the rise and have crossed 3.8 billion with the total number of mobile phones set to cross the 5 billion mark in 2021. Smartphones have become the new utility tool and have made portability of accessing mobile banking, office applications, gaming, and utility payments on our fingertips. The mobile has also opened a new and comfortable space for cyber criminals. They are stealing data, leaking sensitive information in the public domain, and trying to cripple the whole ecosystem of smartphones.

The increase in the number of mobile applications utilising multiple platforms and with increasing number of downloads from users, the cyber criminals could not have asked for a better time to flourish as the number of mobile app downloads is increasing exponentially. Most critical user data including banking, contact details, and passwords are readily available to hackers via smartphones. In addition, for a lowly secure smartphone, accessing credit cards, emails, and personal information is becoming the new target of hackers. Mobile phones have become more prone to sophisticated cyber-attacks and a single smartphone cyber attack is enough to cripple one's business and personal life.

The following are some of the key cyber-security attacks that take place on smartphone platforms.

1. **Cross-Device Cyber Threat**: Cross-device threats occur when apps let smartphone users download the application from the computer first and later to a smartphone device.
2. **App Store Security:** More than 90 percent of mobile apps are prone to cyber-security threats. All types of mobile gadgets are prone to such cyber-attacks as they cater to a massive range of devices, operating system needs, and app store checks. The need is to control all the hardware and software, which is not possible in the current age of mobile devices.
3. **IoT Hardware:** IoT devices are meant to collect user data and leverage it for smart decision making. However, mobile phones allow itself to establish connections with other operating systems. This process increases security risks and can get out of hand at any point in time.
4. **Mobile Malware:** Mobile gadgets are always prone to Trojan attacks, spy-wares, viruses, and malware. These are straightforward means for hackers to steal the data and best ways is via email and links downloads.
5. **Illegal Access:** Unauthorised access to digital accounts, including bank, social media, email, and other applications.
6. **Single Device for Multiple Purposes:** People at the corporate level always deal with sensitive and private information. Thus, high-risk data is always susceptible to the risk of getting mixed with personal data if employees do everything on the same device.

Any kind of breach in the mobile app's security can be catastrophic for business owners, developers, and individuals. Hence, one needs to be on alert, trained and made cyber threat aware to tackle advanced cyber-security threats to keep one's mobile applications safe from hackers.

Ways to protect ones Mobile Applications Against Cybersecurity threats

1. **Making sure that Mobile Applications are secure by design:**
   - **a.** To ensure end-to-end security of any application, there is a requirement to undertake the security at the heart of development by preparing the threat model from the start. The best approach is to brainstorm and engage ethical hackers to identify all the shortcomings. It will help in enforcing ironclad security measures. It is highly recommended to take the assistance of professional cyber security experts to test the level of security and identify all the vulnerabilities of the application
   - **b.** The security of the app becomes even more critical if the application is used to run an eCommerce website or business. As the possibility of a breach in the application would lead into loss of sensitive user data, including phone number, bank account numbers, and credit details. The safeguarding and protection of personally identifiable information (PII) should be the top priority for any mobile based eCommerce application.
2. **Mobile Device Management (MDM)**
   - **a.** Online security of the applications is very much dependent upon the type of mobile device in use and the protection that comes along with that device. Most smartphones are either iOS or Android based and as both operating systems behave differently – one needs to understand the approach both these operating systems undertake at ensuring mobile device security. Data accumulated on any device can cause a security breach and thus leading into loss of information.
   - **b.** Encryptions are the best way of managing mobile devices. Encryption methods such as 256-bit Advanced Encryption Standard, are a welcome start point. The higher the encryption, the better the security measures against cyber criminals. Data security is fundamentally linked to encryption methods employed and used on a mobile device. Moreover, while finalizing the mobile applications cyber-security, it is imperative to consider encryption key management.
   - **c.** User awareness and mobile use best practices should be made everyday use, such as before installing any mobile application, a proper understanding of the application and what it does should be made aware or the security of the mobile device would be easily breached.
3. **App Wrapping**
   - **a.** App Wrapping segregates your mobile application from the remaining devices by capturing it in a safe zone. Developers who are using MDM provider get this option automatically. By setting a few parameters, you can segment the app without writing any code.
4. **Secured User Authentication**
   - **a.** Deploying secured user authentication and authorization is essential for any mobile application's security. It is crucial to establish the fact that a genuine user is running the app to prevent its access from hackers and malware. Most of the cyber security crimes happen via malware coming in form of a message, email, or download. User identification of these spam messages is necessary and now a must at minimising cyber attacks on mobile phones.
   - **b.** While setting up the user authentication, a user must ensure including all the essential privacy points, identity, session management, and mobile security features. 2FA (two- factor authentication) or an MFA (multi-factor authentication) should be enforced for stronger user authentication.

5. **Hardening the Operating System:**
    a. There are several methods to harden the operating system for added security of your
    b. mobile app. For example, installing regular hardware updates help better the security architecture of the mobile phone. In addition, users must keep pace with patches released for greater security of mobile phones and stay updated about the latest code samples and understand static code commercial tools.
6. **Application Program Interface or APIs security:**
    a. It is rewarding and provides greater safety if APIs handle all the data and business logic of the mobile applications. APIs ensure the security of data at any state including at transit or when in static. It is one of the most favourable security features of any mobile application.
    b. It is recommended to deploy secure sockets layer (SSL) (a computing protocol ensuring security by encryption) with 256-bit encryption to ensure the security of data in transit. And for data at rest, one can secure the origin and device both. Ensuring the deployment of APIs having an app-level authentication is a step up in mobile cyber security. Keep sensitive data gated to the memory and ensure the authorized person is only using the services.
7. **Getting expert services by Cyber experts**
    a. It is recommended that for the safety of mobile devices and professional applications, hiring a cybersecurity professional is a good start at understanding and mitigating cyber-threats from the start point. Most credible cyber-security experts have a Master Certificate in Cyber Security and could be useful at subverting the major security threats, although yes, it is best recommended for an organisation, as cyber security experts are mostly expensive and thus is a good solution approach for an organisation wide engagement.

Conclusion:

The need for securing the smartphone is imminent and would become a high priority risk in the future as more and more business applications and work-related information become compatible on mobile devices. Now a days many of the organisations are integrating a lot of in-house applications into smartphones for easier access to employees, thus it become critical that organisations take extra care at securing mobile apps against dangerous cyber security threats. In addition, it is critical to identify the potential threats that one is expected to face and understand to identify the threat and undertake measures to mitigate the risks. Individuals are required to become cyber-tech savvy in operating and storing critical data and must get self-trained at identification of a cyber risk and the right way of addressing the problem.

Once you identify the security threats plaguing your mobile app, it will be decidedly easier for you to tackle the real threat. Failing to follow a recommended set of practices at securing data and important information on a smartphone is of grave significance and lead mobile security breaches that might cost an individual and an organisation heavy loss both professionally and personally. It is high time, that mobile cyber security is taken seriously as part of the day to day practice and we work together at subverting cybercrimes today.