Cybersecurity issues have become a major challenge for businesses now. Latest trends and cybersecurity statistics show a huge increase in breached data from sources being commonly used such as *mobile and IoT devices*. An increase in the number of mobile app security threats attacks due to mobile devices has been reported in the last few years.

In a survey conducted by Dell, 63 % of companies said their data was potentially compromised within the last twelve months due to a hardware- or silicon-level security breach.

This increase in the number of mobile app risks calls for the need of strict measures to be taken to protect data loss. This is why enterprises these days are looking for ways to strengthen their cyber security. With the advent of advanced technologies such as Machine Learning, Artificial Intelligence, Blockchain, and more these days, companies can ensure the security of their data.

Major Mobile Application Threats!

Moreover, recent security research *suggests that most companies have unprotected data. They are implementing poor cybersecurity practices which makes them vulnerable to data loss. To successfully fight against malicious intent, it's imperative that companies make cybersecurity awareness, prevention and security best practices a part of their culture.*
In order to fight against mobile app risks, it's important to be aware of these.

Here in this blog, I have discussed some of the major mobile app security threats that you need to be aware of so as to prevent cyber attacks and malicious activities.

Overall, in 2017, 27% of malicious apps were found in the Lifestyle category. Next in line: Music & Audio, with 20 percent, followed by Books & Reference, with 10 percent.

Source

Social Networking and eCommerce Apps!

You can do a number of activities with the help of your smartphones such as sending emails, storing contact information, passwords, and other vital data. Moreover, smartphones are one of the most commonly used devices for social networking.

Thus, mobile applications for social networking sites running on your smartphones offers a breeding ground for cyber attackers so as to get access to confidential data. Since social networking sites are a store of huge data. This is why malicious applications use social networking sites to steal data and affect data security. Accessing eCommerce sites via mobile phones is one of the major mobile app risks that cause serious issues for the users now.

With the increase in the number of mobile application threats, it's important for companies to build secured mobile apps for their users. You can hire a mobile app developer to create apps with enhanced security features.

Good Read: [Cybersecurity Is An Asset, Not A Nuisance!]

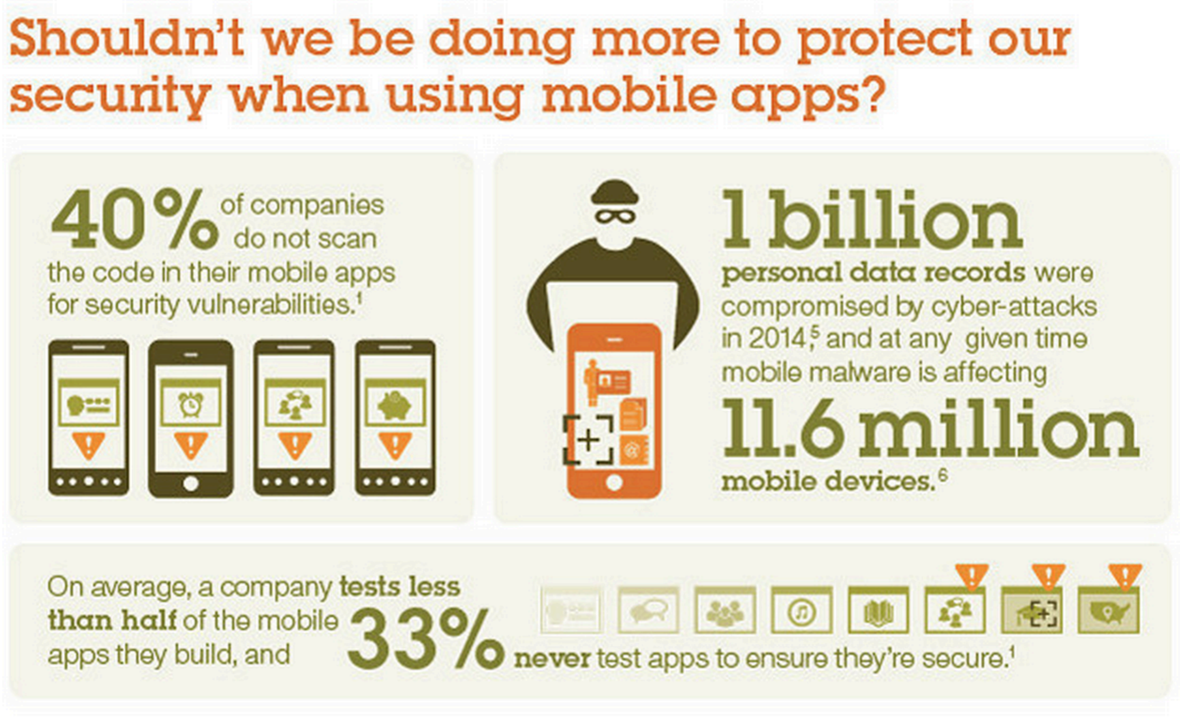
Smartphones Permissions!

Smartphones use a permission mechanism in order to determine what users are allowed to do in applications. However, using these smart permission mechanisms can cause serious issues in your mobile applications and can harm your data security. Let’s see how.

The permissions are granted through the “*manifest permission*” that allows these applications to access your data. In turn, this process allows the application to run independently.

However, allowing external applications to seek permission can be harmful for the smartphones because it creates an opportunity for malware to exploit the ability to access sensitive data on Android handsets and thus install malicious software. So, be cautious when you grant permission to a software application to avoid risks.

To ensure the growth of your business, you need to create secured apps that suit your business requirements. Here are some alluring mobile ideas that you can consult for building alluring mobile apps for your business specifics.



Shouldn’t we be doing more to protect our security when using mobile apps?

40% of companies do not scan the code in their mobile apps for security vulnerabilities.[1]

1 billion personal data records were compromised by cyber-attacks in 2014,[5] and at any given time mobile malware is affecting 11.6 million mobile devices.[6]

On average, a company tests less than half of the mobile apps they build, and 33% never test apps to ensure they’re secure.[1]

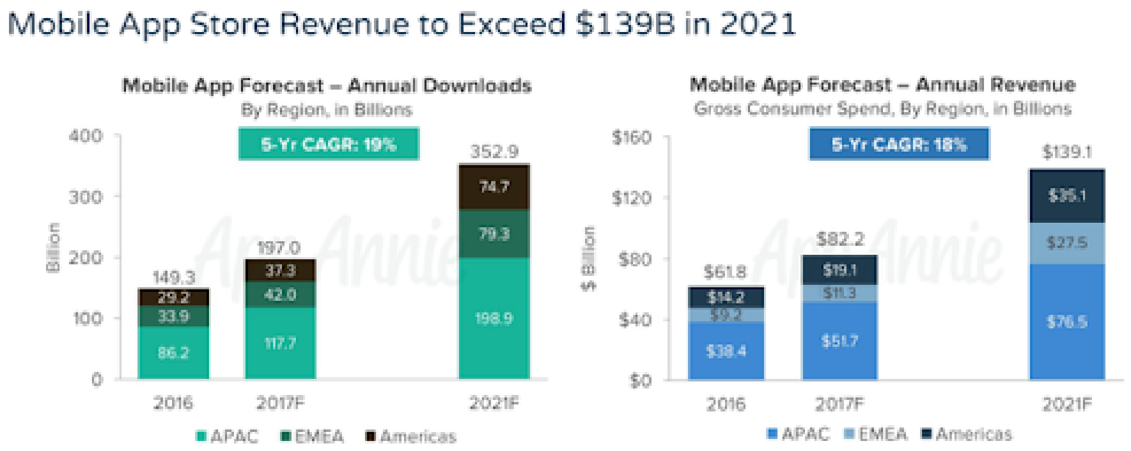
Source

Smart Mobile Web Browsers!

Everyone today uses a web browser to access sites on the internet. Using a web browser, you can surf different sites and drive useful information. But did you know that accessing these web browsers to gain information can cause serious threats to your cyber security. Accessing browsers on smartphones is one of the greatest mobile app security threats.
Web browsers are vulnerable to cyberthreats.

The chances of being attacked by malicious entities increases when you access any site using these.When you visit these sites consisting of malicious entities, cyber criminals may get access to your personal data which might pose a great threat to your system.

This is surely one of the major mobile app risks that can affect your security. You can hire a react native developer to create a secured mobile application for your business.



[Source](#)

Wi-fi Interference!

Wi-fi interference can create serious mobile application threats to your system. An unsecured public wireless network combined with unsecured file-sharing allows malicious users to access any directories and files that you might have made available for sharing.

'***All wifi networks' are vulnerable to hacking, security expert discovers.WPA2 protocol used by vast majority of wifi connections has been broken by Belgian researchers, highlighting potential for internet traffic to be exposed,*** [says](#) **a report.** By gaining access to a public wireless network, they can have unrestricted access to all of your data.

Malware!

Malware has been an old problem in the IT world. It is a problem in the mobile world too. Malware can cause serious damage to data security. They are one of the biggest mobile application threats that can cause huge data loss.
As long as mobile apps will exist in the app stores, malware will continue to cause serious damage to data.

According to a 2018 online survey by The Harris Poll, nearly 60 million Americans have been affected by identity theft.

The Bottomline

By now, I am pretty sure that you have a clear idea of the major application threats that can damage the security of your system. With increase in the use of smartphones now, the number of malware-related attacks through mobile devices have increased too.

Malicious software, also known as malware, is taking aim at your mobile devices. Things like spyware, ransomware, and viruses used to focus on your laptop or desktop computer. But now they access data through mobile devices.

It's important now for companies to consider strict measures to prevent their system from malicious cyber attacks and mobile application threats.