TATA

TATA ADVANCED SYSTEMS

CYBER SECURITY PRACTICE

MOBILE SECURITY

A GROWING CONCERN FOR BUSINESSES & THE IMPACT OF PANDEMICS

#Areyoucybersecure

Follow us: @tataadvanced

"Mobile device productivity comes at a price – increased security risks." As mobile security threats are escalating in number as well as evolving in scope, both individuals and enterprises need to understand common threat vectors and prepare for the next generation of malicious activities. Presently, there are more than 6.8 billion smartphone users in the world. As our dependency on mobile devices increases over time, so does the data security and thus, the motivation for cybercriminals.

The rapidly growing global momentum of mobile usage has made "mobile security" more critical than ever. It is astonishing to know that mobile accounts for approximately half of the web traffic across the globe. In the fourth quarter of 2019, mobile devices (not including tablets) generated 52.6% of global website traffic. And, if we talk about India, it is estimated that there will be 829 million smartphone users by the end of 2022, according to Cisco's 13th annual Visual Networking Index (VNI). Additionally, in Myanmar, there were approximately 61.14 million mobile subscriptions in 2018.

As per the combined report submitted by US tech giant Google, Singapore wealth fund Temasek and consultancy firm Bain & Co, Southeast Asians are the most engaged mobile Internet users in the world. The region's Internet economy has reached $100 billion in sales in 2019 and is ready to hit a mark of $300 billion in 2025. Also, the adoption rate of digital payments has grown at an exceptional speed and the market is expected to cross a mark of $1 trillion by 2025.

From the security point of view, these numbers are good enough to draw cybercriminals' attention. More users mean more vulnerable endpoints for hackers to exploit. Lack of awareness of device vulnerability is one of the main reasons for increasing cyber threats targeting mobile devices.

As per Symantec, India (after the US) was the top country for mobile malware (23.6%) in 2018. Phishing attacks, malicious applications, data leakage, malware-infected files, etc. are some of the troubles that each organization is struggling to fight with. Mobile applications create another path to enter into organizations' networks, allowing hackers and swindlers to transmit malicious code. This could further lead to data breaches, public disclosure of sensitive information, or compliance violations. Whereby most organizations have now recognized mobile device threats and vulnerabilities, and understood that they need proper security protection.

"As per the report from Verizon, 87% of financial services companies said that cybercriminals see them as a more lucrative target than other sectors."

If we take an example of the BFSI industry, mobile banking has completely transformed the banking sector. According to RBI's report 2017-2018, mobile banking services increased to 92.6% from 88.9% in the previous year.

But with that growth come a whole new set of threats (or possible risks). Third-party mobile banking applications, unsecured wireless networks, mobile malware, and risky user behaviour are some of the risks that have created a concern for security officials. A report from Kaspersky Lab reveals that mobile banking malware is increasing at an alarming rate. In the first quarter (Q1) of 2019, it detected around 30000 installation packages for mobile banking Trojans, which was 11,000 more than in Q4 of 2018.

How Pandemic Impacts Mobile Security

"Not everything is under human control."

Since COVID-19 has been declared a pandemic by the World Health Organization, hackers are using the hype and fear connected to this deadly virus. They are well aware of the fact that people are struggling to carry out basic essential transactions and visit their nearest banks. The situation has strained people to use alternative methods like internet banking, mobile wallets, UPI, etc. for making payments, which has significantly increased the number of electronic transactions made per day worldwide. The cybercriminals are viewing the current outbreak as an opportunity to launch malicious campaigns and infiltrate mobile devices to steal critical user data like credit/debit card information and banking credentials.

In a recent analysis, performed by Domain Tools (a threat intelligence firm), it was revealed that hackers have been deploying Android ransomware known as CovidLock, which appears to be a COVID-19 information tracker but is intended to lock targets' screens until they pay a ransom.

Also, the researchers from Avast have issued an alert regarding an increase in COVID-19 themed mobile malware. They said, *"attackers are releasing malicious applications that claim to be genuine, but actually they are fake."*

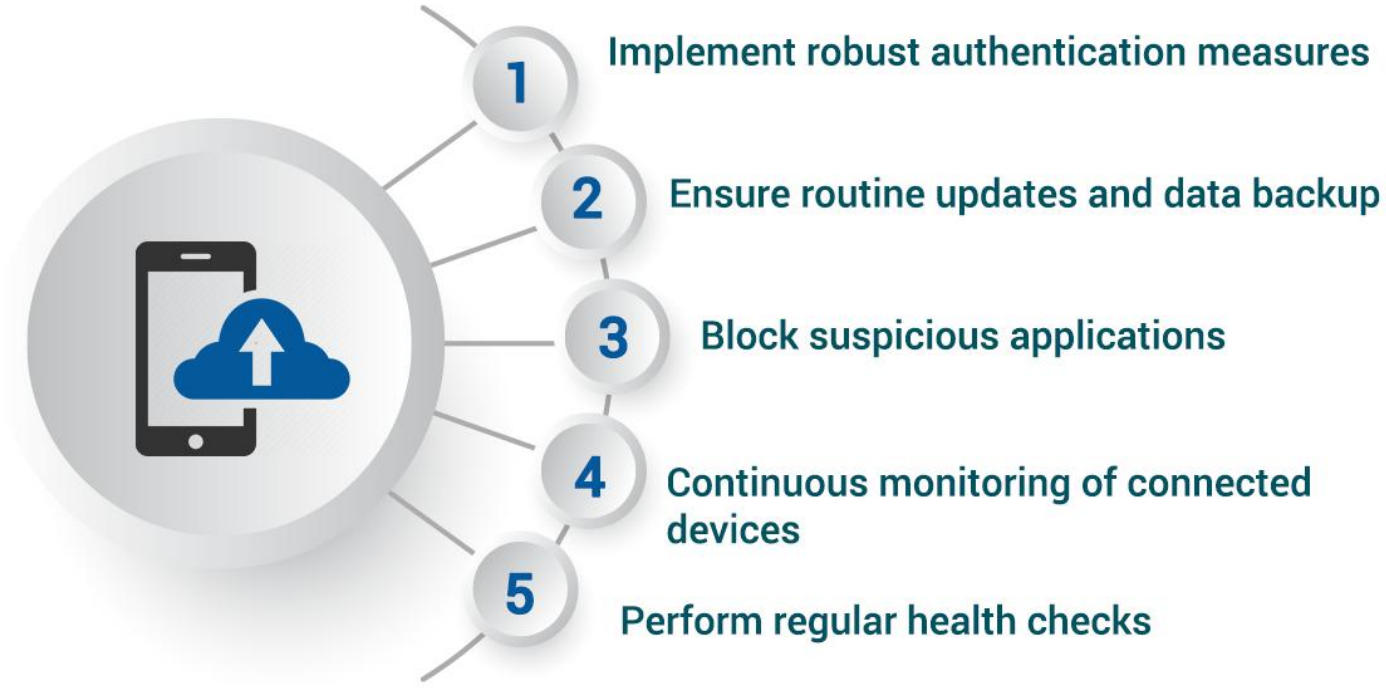
TATA

TATA ADVANCED SYSTEMS

CYBER SECURITY PRACTICE

How Enterprises Can Ensure Mobile Security

Let's have a look at some of the recommended security practices that every enterprise can follow to ensure mobile security and protect business-critical data against unauthorized users.



Tata Advanced Systems Limited (TASL) is a managed security service provider with over a decade of experience and trusted by leading organizations. Currently, TASL is actively servicing satisfied clients while continuing to truly transform the customer experience, with IT security as their top priority.

At TASL, we help organizations to ensure mobile security through our wide portfolio of services such as Mobile Device Management (MDM), Mobile Application Access (MAA), Data Leakage Protection (DLP) and Identity Right Management (IRM).

To know more about our mobile security services, mail us at
contactcs@tataadvancedsystems.com

Follow us: @tataadvanced