MOBILE APPLICATION FRAUDS

Story 1: Cyber-Attacks using Infected Mobile Applications

Samantha and Rohini are resident doctors who use a mobile application to scan medical reports.

Samantha : This app enhances the quality of the photos and combines them in a single PDF file.

Rohini : I can share the reports with senior doctors for their opinion.

Samantha : But I read that this app is infected with malware. It shows intrusive ads and paid subscriptions. It has even been removed from Google Play Store.

Rohini : But I think it will not affect my phone plus this app is very useful for me. I will not uninstall it.

(After a few days)

Rohini notices weird sounds from her phone. She realizes that her phone has started showing intrusive advertisements.

Rohini feels embarrassed to have opened such advertisements in front of her colleagues.

Samantha : Don’t worry, it’s not your mistake. Don’t feel embarrassed.

Rohini : It is. I should have uninstalled this app when I had the chance. This app has also signed me up for paid subscriptions without my notice.

Rohini regrets that she ignored the warnings and continued using an infected mobile application.

TIPS

- Always install mobile applications from official application stores or trusted sources.
- Scrutinize all permission requests thoroughly, especially those involving privileged access, when installing/using mobile applications.
  For example, a photo application may not need microphone access.
- Regularly update software and mobile applications to ensure there are no security gaps.
- Beware of malicious applications or malicious updates in existing applications. Clear all the data related to the malicious application and uninstall it immediately.