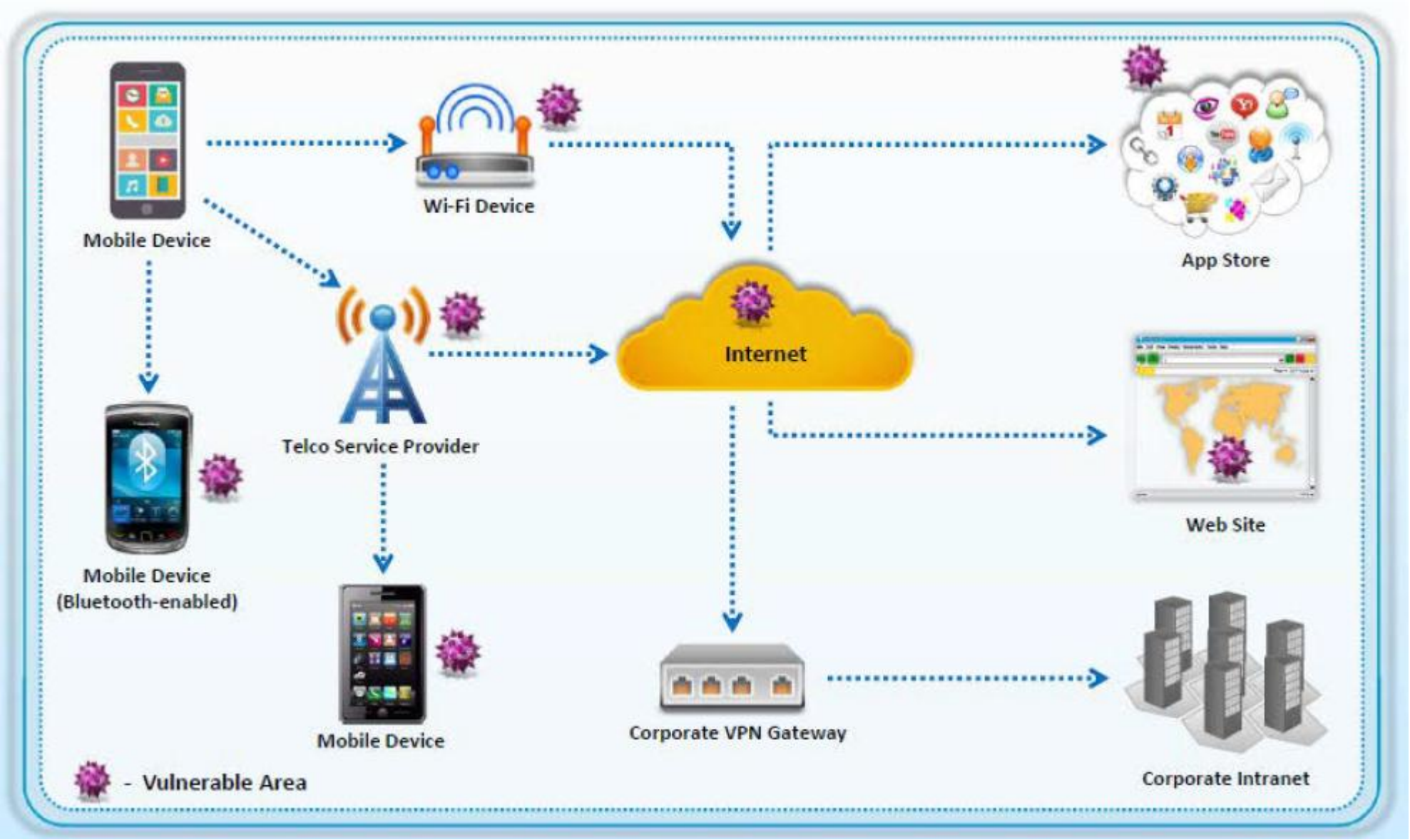
Introduction of Mobile Hacking

Phone hacking is that the practice of manipulating or gaining unauthorized accessto mobile phones, like by intercepting telephone calls or accessing voicemail messages. When the unauthorized access is to the phone user's conversation, it's more commonly mentioned as phone tapping.

The mobile device has become an inseparable a part of life today. The attackers are easily ready to compromise the mobile network due to various vulnerabilities, the bulk of the attacks are due to the untrusted apps. SMS is differently the attackers are gaining access to the mobile devices by sending phishing messages/spam messages to users.

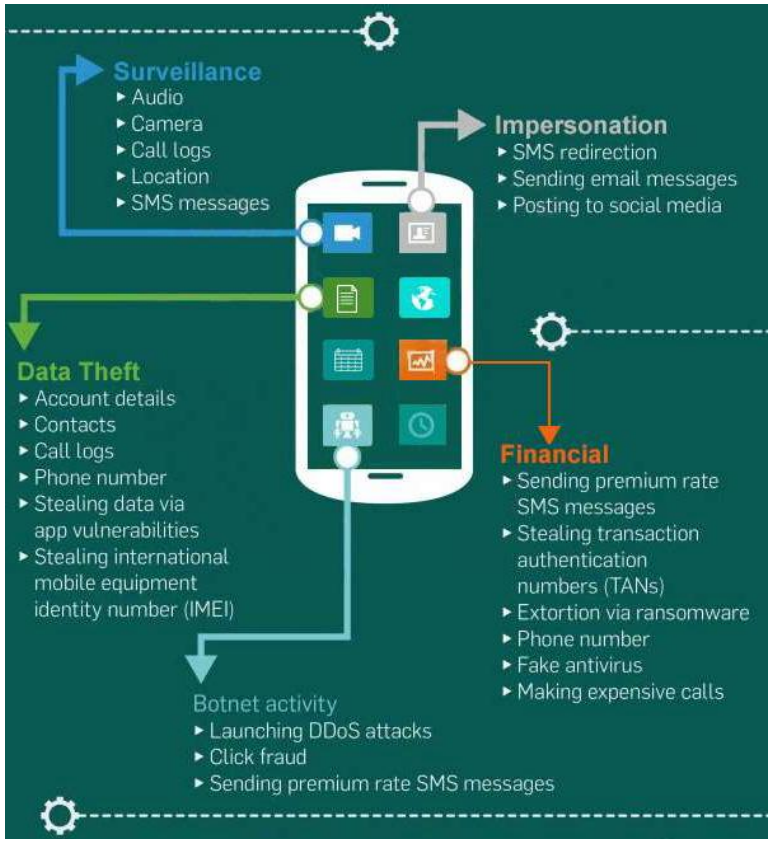
Introduction of Mobile Hacking



Mobile Attack Vector

There are several sorts of threats and attacks on a mobile device. a number of most elementary threats are malware, data loss, and attack on integrity. An attacker may plan to launch attacks through victim's browser by a malicious website. Social engineering attacks, data loss, data theft are the common attacks on mobile technology. Mobile attack vector includes:

- Malware
- Data Loss
- Data Tampering
- Data Exfiltration

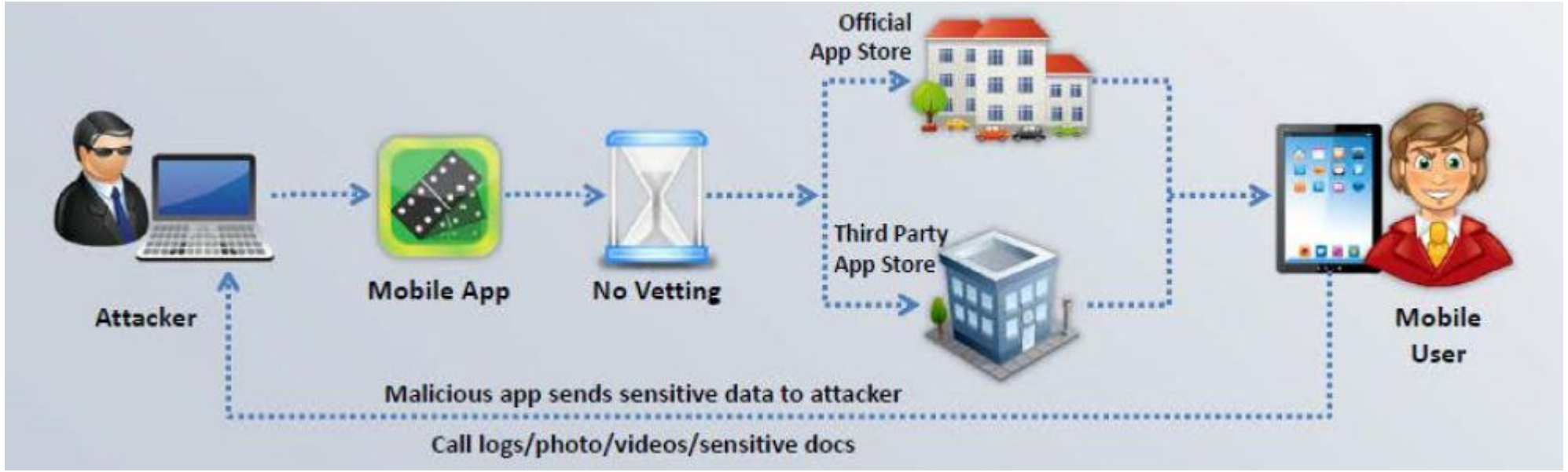


Mobile Platform Vulnerabilities and Risks

- Malicious Apps in Store
- Mobile Malware
- App Sandboxing vulnerabilities
- Weak Device and App Encryption
- OS and App Updates Issues
- Jailbreaking and Rooting
- Mobile Applications Vulnerabilities
- Privacy Issues (Geolocation)
- Weak Data Security
- Excessive Permissions
- Weak Communications Security
- Physical Attacks

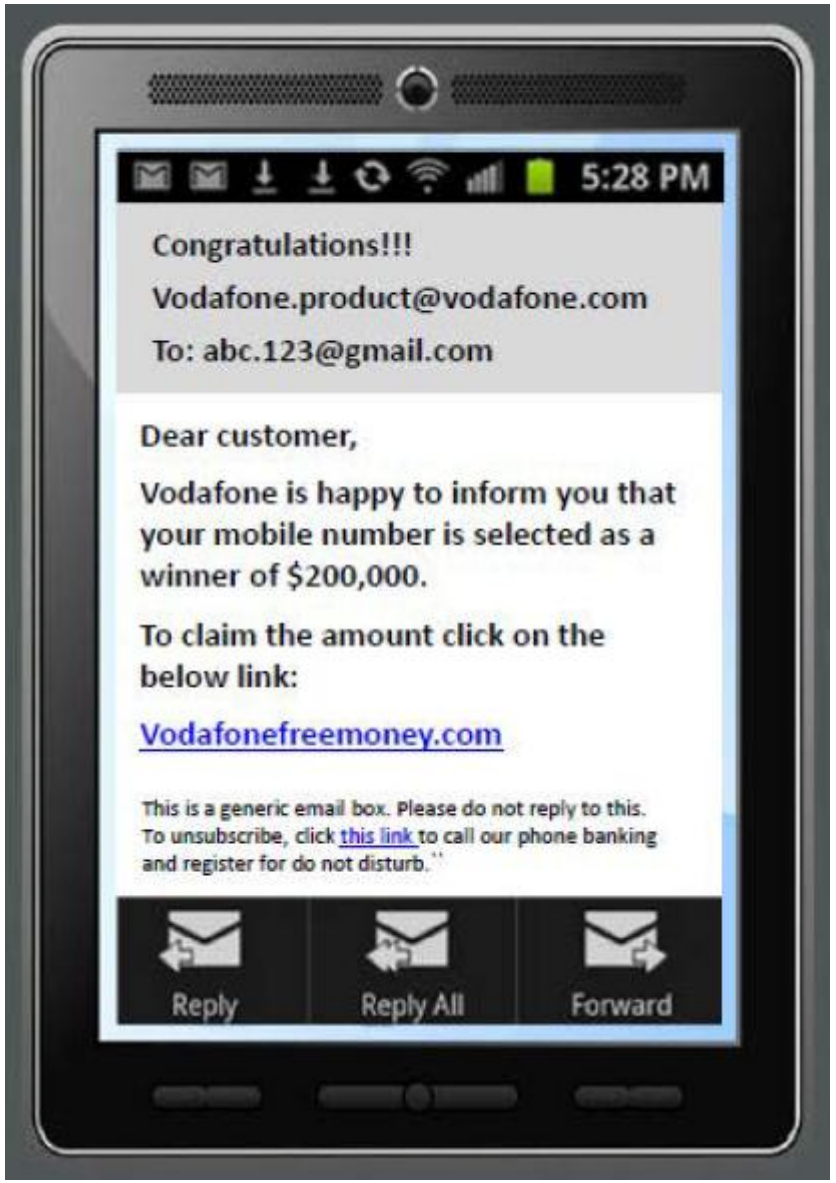
Security Issues Arising from APP Stores

- Insufficient apps leads to malicious and fake apps entering appmarketplace
- App Store are common target for attackers to distribute malware and malicious apps
- Attackers can also social engineer users to download and run apps outside the official app stores
- Malicious apps can damages other applications and data, and send your sensitive data to attackers



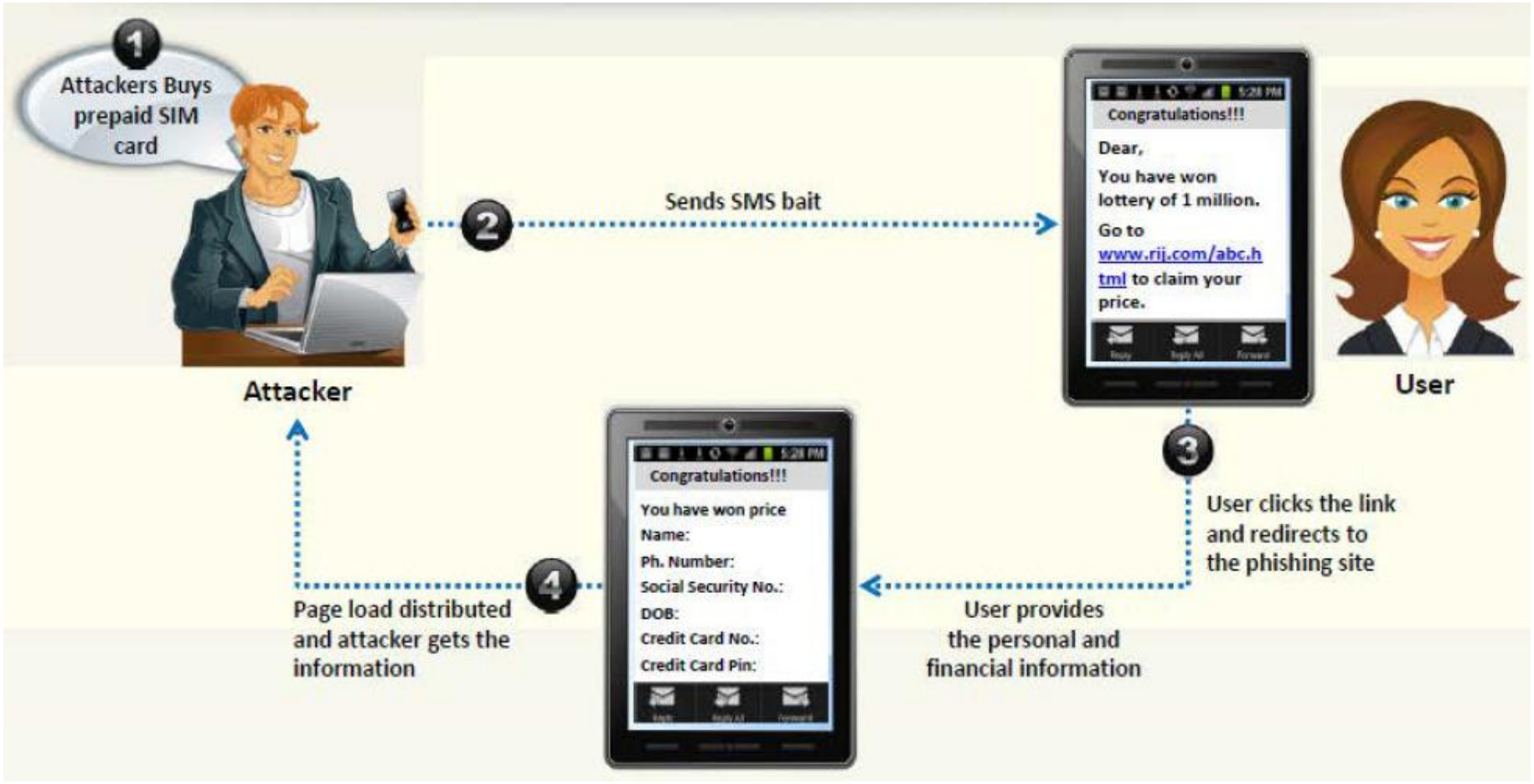
Mobile spam

- Unsolicited text/email messages sent to mobile devices from known/unknown phone number / email ID's
- Spam Messages contain advertisements or malicious links that can trick users to reveal confidential information
- Significant amount of bandwidth is wasted by spam messages
- Spam attacks are done for financial gain



SMS Phishing Attack (SMiShing)

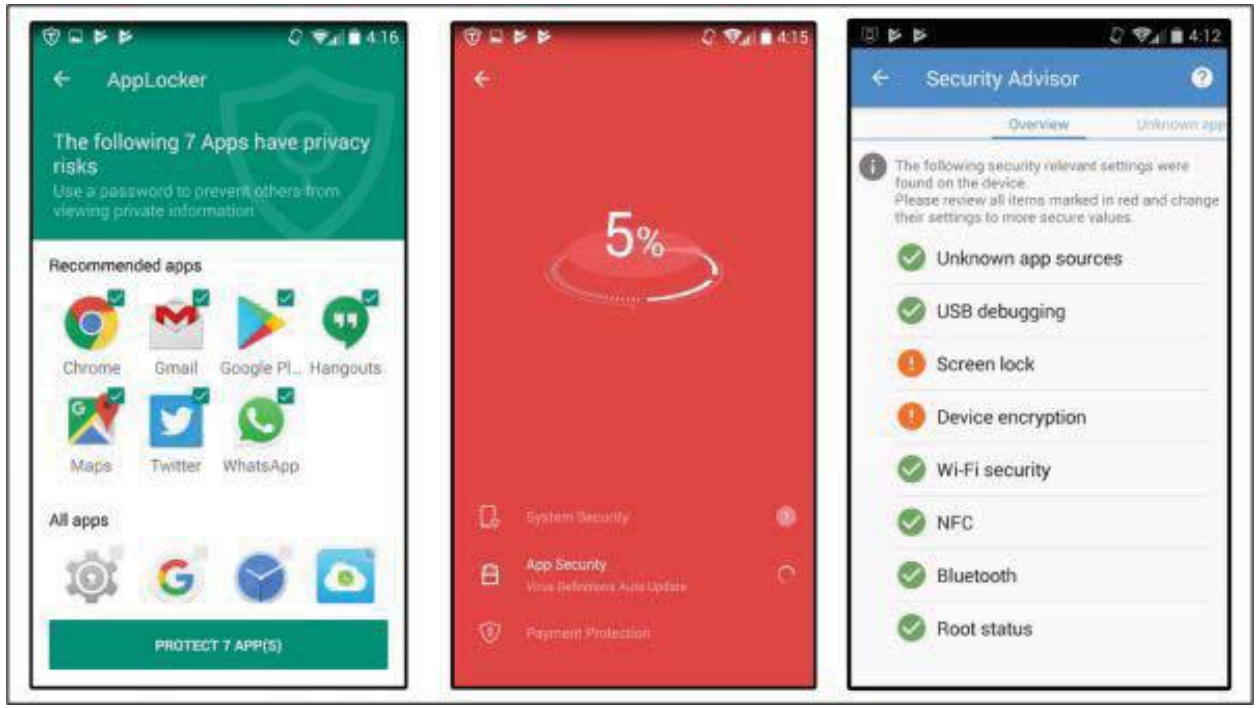
SMS Phishing is the act of trying to acquire personal and financial information by sending SMS (Instant Messages or IM) containing deceptive link.



Android Phone Security Tools

There are many Anti-virus's applications, protection tools, vulnerability scanning tools, Anti-theft, find my phone applications available on the Play Store. These tools include:

- DroidSheep Guard
- TrustGo Mobile Security
- Sophos Mobile Security
- 360 Security
- Avira Antivirus Security
- AVL
- X-ray



Guidelines for Securing IOS Devices

- Use Passcode lock feature for locking iPhone
- Disable Javascript and add-ons from web browser
- Use IOS devices on a Secured and protected Wi-Fi network
- Do not store sensitive data on client-side database
- Deploy only trusted third-party applications on IOS devices
- Change default passwords of iPhone’s root password from alpine
- Do not Jailbreak or root devices if used within enetrprise environments
- Enable jailbreak detection and also protect to iTunes AppleID and Google accounts, which are tired to sensitive data

IOS Device Tracking Tools

Find My iPhone

https://itunes.apple.com

iHound

https://www.ihoundsoftware.com

GadgetTrak iOS Security

http://www.gadgettrak.com

iLocalis

http://ilocalis.com

Mobile Spyware

Mobile Spy
http://www.mobile-spy.com

SpyBubble
http://www.spybubble.com

Mobistealth
http://www.mobistealth.com

FlexiSPY
http://www.flexispy.com

Highster Mobile
http://www.highstermobile.com

SpyPhoneTap
http://www.spyphonetap.com

Spyera
http://spyera.com

PhoneSheriff
http://www.phonesheriff.com

My Mobile Watchdog
https://www.mymobilewatchdog.com

SpyToMobile
http://spytomobile.com

Mobile Protection Tools

McAfee Mobile Security
http://home.mcafee.com

AVG AntiVirus Pro for Android
http://www.avg.com

avast! Mobile Security
http://www.avast.com

Norton Mobile Security
http://us.norton.com

ESET Mobile Security
http://www.eset.com

Kaspersky Internet Security for Android
http://www.kaspersky.com

F-Secure Mobile Security
http://www.f-secure.com

Trend Micro™ Mobile Security
http://www.trendmicro.com

Comodo Mobile Security
http://www.comodo.com

Bitdefender Mobile Security
http://www.bitdefender.com

Countermeasures for Mobile Security

- Avoid auto-upload of files and photos
- Perform security assessment of applications
- Turn Bluetooth off
- Don’t connect to open networks or public networks unless it is necessary
- Install applications from trusted or official stores
- Configure string passwords
- Use Mobile Device Management MDM software’s
- Use Remote Wipe Services
- Update Operating System’s
- Do not allow rooting / jailbreaking
- Encrypt your phone
- Periodic backup
- Filter emails
- Configure application certification rules
- Configure mobile device policies
- Configure auto-Lock