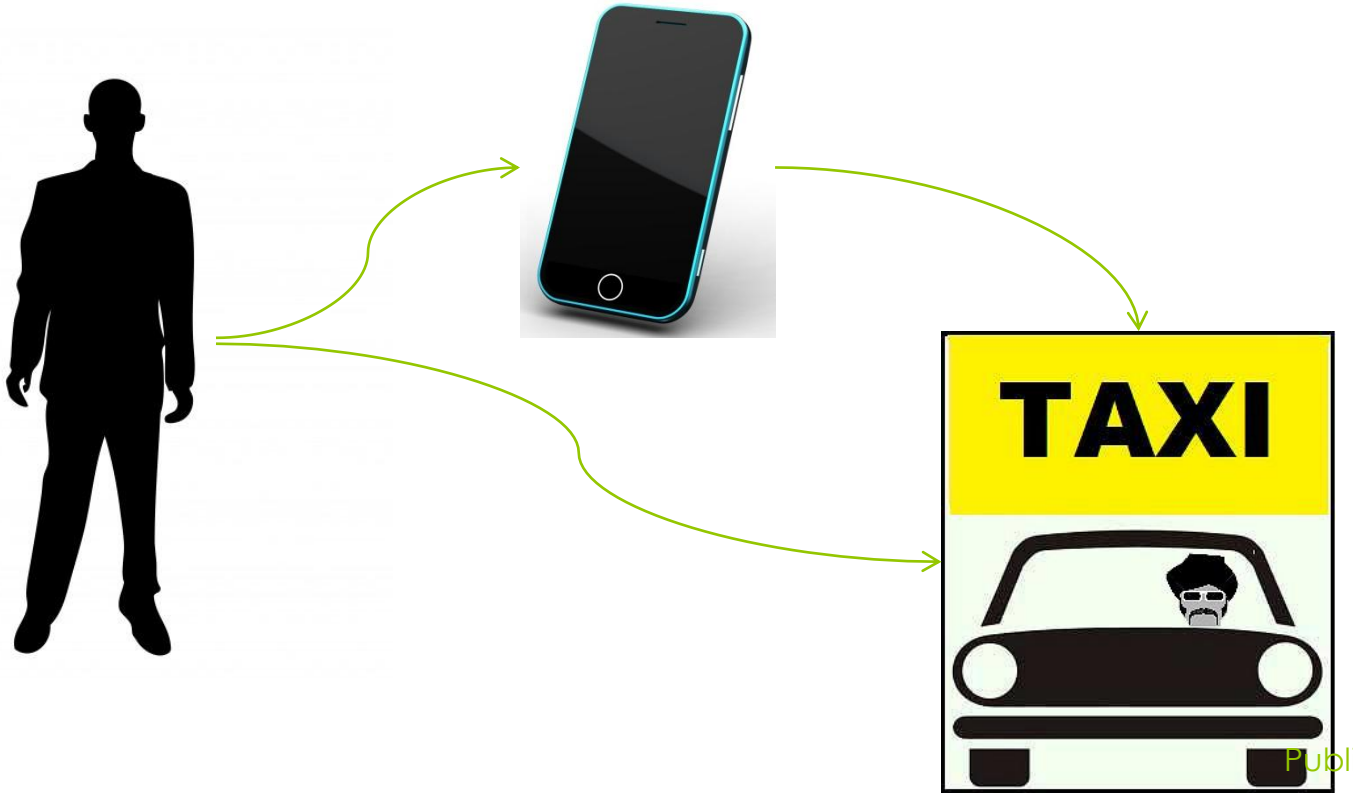
Cyber Security Threats and Risks to Mobile Devices

Public

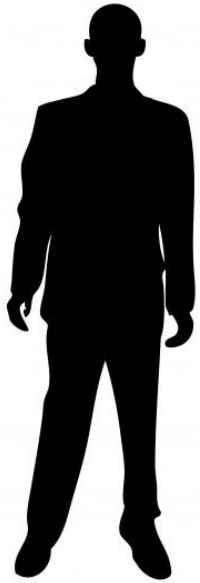
Case Study - 1

Disclaimer: All names and situations used in the case study are fictitious and have no resemblance to any person. These are only being used to give examples.

Jack Walsh, Vice President of Data Mine Pvt. Ltd. was on a business travel and while returning he left his phone in the cab that he used from airport to his house.



What Happened Next Day?



- Fraudulent emails sent from his corporate mailbox
- Sensitive documents leaked
- Credit/Debit cards used for shopping
- Facebook post on his timeline said “You are hacked, Game Over”

Case Study - 2

Disclaimer: All names and situations used in the case study are fictitious and have no resemblance to any person. These are only being used to give examples.

Susan Thomas, Executive at Clark Solutions was sitting in a coffee house when she realized she had missed sending an important mail. She connected to the Free Wi-Fi at the coffee shop and felt relieved after sending that mail. She then used the free Wi-fi to browse her social networking accounts and click on few ads.

Public

What Happened Next Day?

- Office network got affected as a result of “malvertising” and “botnets”
- Sensitive documents leaked
- Portion of corporate database hacked
- Social networking accounts hacked and misused.

Cybersecurity Risks / Threats to Mobile Devices

1. Physical Access
2. Malicious Code
3. Malvertising
4. Device Attacks
5. Communication Interception
6. Insider Threats
7. Productivity Challenges

Next Steps as Individuals…

- Consider security features while buying a phone
- Configure devices to use secure connections
- Choose what apps to install, what links to click, what messages to read
- Set Bluetooth to non-discoverable.
- Say "NO" to Free Wi-Fi
- Do not "root" or "jailbreak" your mobile

Report any loss of mobile immediately and remote wipe data

Next Steps for Enterprise…

- Educate employees
- Controlled use of BYOD
- Secure wireless connections within enterprise
- Consider network access control (NAC)
- Mandate that employee users connect to a virtual private network (VPN)
- Determine data to be exposed to mobiles
- Implement Mobile Device Management (MDM).
- Run Penetration Tests
- Develop a Mobile Security Plan

Think of your Mobile Phone as your Wallet, it probably contains as much personal information and monetary value as your Wallet. Make all attempts to secure it…

Stay Protected!!!

Thank You

Contact Details –

Meetali Sharma
meetalisharma81@gmail.com; meetali.arora@sdgc.com
+91-9971393639