Vidyalankar Institute of Technology

Electronics & Telecommunication Department

Orientation Program : Academic Year 2023 – 2024

Subject: ILO1016 - Cyber Security and Laws

Semester: VII

Subject Teacher

Prof. Harshada Rajale

VIT | Vidyalankar Institute of Technology

Accredited A+ by NAAC

University of Mumbai

Module 2: Cyber offenses & Cybercrime

By Prof. Harshada Rajale

OUTLINE

- Attacks on Mobile/Cell Phones
- Mobile Devices: Security Implications for Organizations
- Organizational Measures for Handling Mobile
- Devices-Related Security Issues
- Organizational Security Policies and Measures in Mobile Computing Era
- Laptops

13 Attack on mobile /cell phone

- Attackers have been exploiting the mobile phones by using old techniques along with the new ones.
- The three prime targets:
  - Data
  - Identity
  - Availability

13.1 Mobile Phone Theft

- Due to growing popularity- mobile phones are becoming favorite target of thieves.

- Some security features of mobile include
  - Access Control using unique code
  - Tracing location
  - Wiping data or locking handset
  - Function to display home or lock screen
  - Prevent thief from resetting

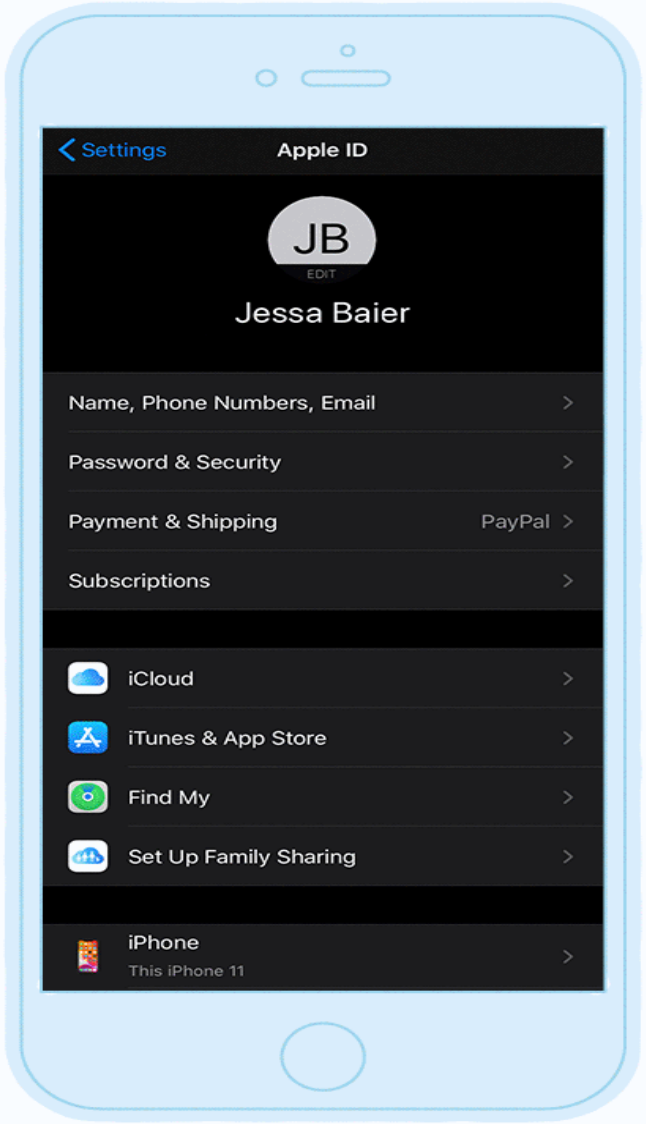
13.1 Mobile Phone Theft

- Some generalized safety tips to secure all kinds of mobile phone include
  - Always keep phone details
  - Keep it out of sight when not in use
  - Do not leave it unattended
  - Be alert and aware of surrounding
  - Be aware in vehicle
  - Ensure it has PIN activated
  - Contact network provider to disable SIM Card
  - Report theft to police
  - Change account credentials
  - Install find your phone application
  - Install anti-theft software
  - Wipe out phone

13.2 Mobile Virus

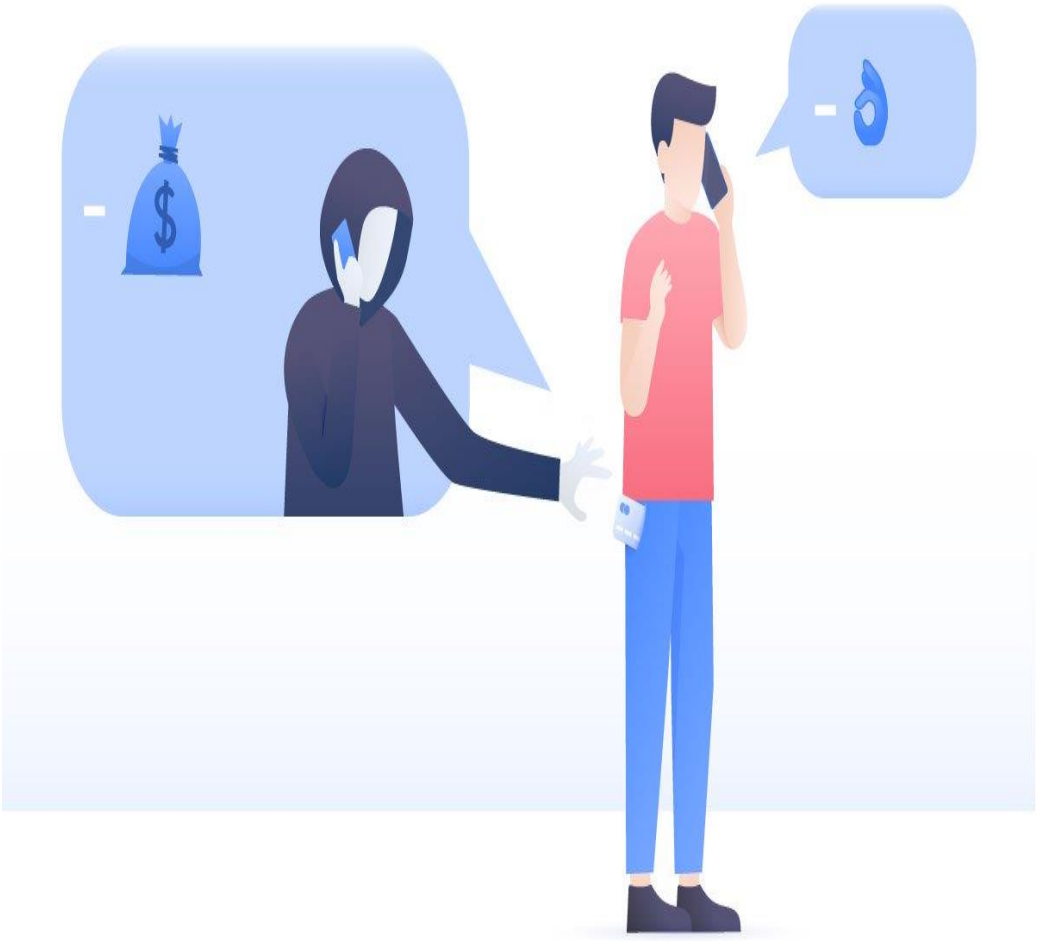
- Mobile virus are very much like Computer virus
- It primarily spreads by three ways:
  - Internet downloads
  - Bluetooth wireless connection
  - Multimedia messaging services (MMS)
- The first mobile virus – Mosquito by Ojam

13.2 Mobile Virus



- Protecting mobile phones from virus
  - Maintain up to date system and software
  - Install anti –virus software
  - Enable PIN or password
  - Read and understand permissions while installing
  - Encrypt personal and sensitive data
  - Disable Bluetooth, infrared, Wi-Fi when not in use
  - Always set Bluetooth enabled devices non discoverable
  - Use caution when opening email or message attachment
  - Never join unknown public Wi-Fi network
  - Delete all information prior discarding the device

13.3 Vishing



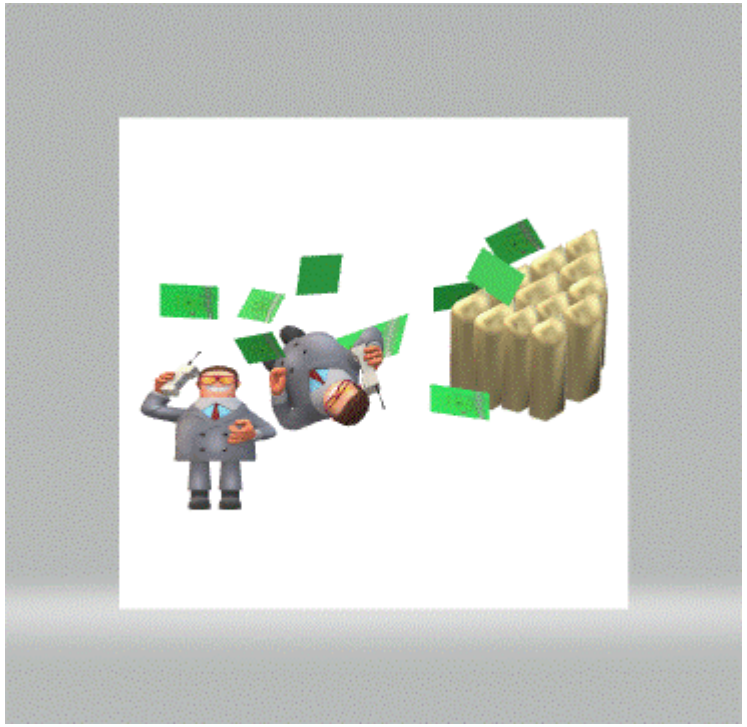
- Vishing is a criminal practice of using the telephone system to gain access to the personal and financial information of customers for the purpose of committing fraud.

- Fraudsters make use of PBX to connect to VoIP services and perform auto dialing to thousands of people in an hour.

- Vishing attack includes
  - ID theft.
  - Purchasing money / funds.
  - Transferring money /funds.
  - Monitoring the victims's bank account.
  - making application for loan and credit card.

13.3 Vishing

- Typical process involves following steps:
  - War dialler is used to call numbers in a given region
  - Automated recording customer user regarding fraudulent activity
  - Instructs the customer to place a call to the bank and provides false number
  - When the victim calls, automated instructions requests him/her to enter credit card or bank account detail using keypad along with PIN, expiration date, CVV, DOB
  - The fraudster gets the necessary information to make fraudulent use of the information
  - Some attacks combine Vishing and traditional phishing



13.3 Vishing

Beware of vishing scam!

Banks or any other institutions will never ask for personal information like bank details, card number, CVV and OTP over the phone

13.3 Vishing

- Technical and pro-active steps to avoid vishing
  - Never answer a call from an unknown person
  - Never share personal information over phone
  - Do not completely trust caller ID
  - Avoid automated calls
  - Report the incident

13.3 Vishing

Beware of that friendly 'customer care' exec

Kingpin | Ram Kumar Mandal
Age | 35
Education | Matriculate; trained in cellphone repairing
Location | Jharkhand

ASSOCIATES

Surendra Singh (22) from Rajasthan. Singh couldn't clear the Class X hurdle while the other two got no education

Shabir Ali (27) from Rajasthan

Purnanand Kumar Tiwari alias Mukesh (22) from Jharkhand

What is Vishing

It's voice phishing by which cyber crooks take your money out by asking for your account/card details posing as bank staff

Modus operandi

STEP 1 | Crooks call up unsuspecting people posing as bank officials and ask for one-time password, credit/debit card number, CVV number, expiry date, secure password, ATM PIN, internet banking login ID and password. Reasons given are reactivation of account/card, redemption of reward points, linking account with Aadhaar, etc

STEP 2 | Details are then used to conduct online transactions

How to stay safe

- Never divulge your account and card details to anyone
- Banks never ask for such details whether online or offline
- If duped, lodge an FIR with local police or Cyber Cell of Crime Branch
- Log on to www.cybercelldelhi.in and lodge a complaint
- Change passwords/PINs often
- Avoid using cyber cafes for net-banking
- If in doubt, call on phone banking number of your bank
- Never provide identity proof to anyone without genuine reason
- Never click on any link in any email to access bank's site; always type down the URL of the bank in your browser

13.3 Vishing

generators than MCG estimates | 3

'New Jamtara' op: Simultaneous raids at 14 Nuh villages for a day

Searches Planned For A Month, Cops Underwent Four-Day Training

Shankar Mukherjee | TNN

Gurgaon: Haryana Police mapped villages across Punhana, Firangwan, Firozpur Jhirka and Nuhber and carried out recces to determine hotspots while planning its massive operation against cyber fraud.

"Police personnel from the entire state were involved in the operation. We launched the raids at the same time on Thursday morning," DIG (special task force) Simardeep Singh said.

The Nuh villages where raids were carried out are Khedla, Lohinga Khurd, Lohinga Kalan, Gokalpur, Godhola, Aminabad, Mahu, Gulalta, Jaimat, Jakhopur, Nai, Tirwara, Mamlka and Papda.

Nuh SP Varun Singla led the operation. He was assisted by six additional SPs and 14 DSPs. Singla told TOI that the police conducted a training programme in Bhondsi from April 4 to 8 to prepare personnel for the operation. Cops were given an outline of the raids and details of the intelligence they had gathered.

"The highest number of suspects was detained in Nai village, followed by 25 from Lohinga Kalan village, 20 each from Jaimat and Jakhopur, 17 each from Khedla and Tirwara, and 11 from Aminabad. We also recovered mobile phones, ATM cards and other equipment. We also nabbed one criminal who had a reward of Rs 10,000 for his arrest," Singla said.

Two ATM card racke...

chines and Aadhaar-enabled payment system (AEPS) machines were also found. In addition, seven country-made pistols, two cartridges, two cars, four tractor-trolleys and 22 motorcycles were recovered.

"All the 125 men who were detained are in the 18 to 30 age group. We are checking their records," the Nuh SP said. Over the last one year, Haryana Police's cybercrime cell has blocked almost 5 lakh SIM cards in 40 villages of Nuh as these numbers were allegedly being used to facilitate cyber frauds.

Though the crackdown would have made a dent, challenges remain. A police officer who was part of the raids said the key problem is that of numbers. "Catching one scammer doesn't end the problem as hitchers pop up. This is so popular among youngsters in the region that it has predominantly become a leaderless racket. There are no kingpins, and just a smartphone and a SIM card is needed," the officer said.

Cybercrimes have risen manifold in recent years. From April last year to March 2023, over two lakh complaints have been registered over the cybercrime help-

Future t... for forei...

RAIDS LASTED FOR 20 HOURS

UNDER SCANNER

The triJunction of Nuh (Haryana), Mathura (UP) and Bharatpur (Rajasthan) has been an emerging hotspot for cybercrimes, earning it the sobriquet 'New Jamtara' based on the Jharkhand village famous for such cons

LIKELY IMPACT

> Cops say they expect to get leads on fraudsters across other states

> Raids will have dented the network of cyber cons

ABOUT THE OPERATION

Began on April 27, last 20 hours till April 28

5,000 Haryana cops divided into 102 teams carried out coordinated raids

300 spots across 14 villages in Nuh were under scanner

125 suspects detained, FIRs to be filed

CYBER FRAUDS

Gangs and cyber cons try to target online users in myriad ways, from sending links to seeking OTPs

• Spots raided in Nuh

"Some raids were deeper into the district

International Journal of Research in Engineering, Science and Management
Volume-1, Issue-12, December-2018
www.ijresm.com | ISSN (Online): 2581-5792

A Survey Report on the Cyber Crime Growing Vigorously in Jamtara, Jharkhand (India)

Sweta Kumari Barnwal
Assistant Professor, Dept of Electronics and Communication Engg., Arka Jain University, Jamshedpur, India

***Abstract*: This Modern Technology is almost inspirable from our daily life. Since its beginning in the 1990s, the internet has a vast electronic network. This network consists of millions of devices which is hyper-connected to each other. With the rapid technological developments, our life is becoming more digitalized. Be it business, education, shopping or banking transactions everything is on the cyber space. There are some threats posed by this incredible rise in digitization which is creating a new set of global concern called as cyber crime. It is easy to fall prey to such unethical way of hacking and penetrating into personal life which is feasible at a click of a button. Cyber crimes thereby take place in many forms like illegal access and theft of data, intrusion into devices and fraud which is a big concern amongst all the users. In a major revelation, Jamtara in Jharkhand has been identified as a new cyber hub for crime. More than fifty per cent of cyber crimes in India are traced back to this sleepy town of Jharkhand. The revelation was made by Union Home Secretary Rajiv Gauba who himself is a 1982 batch IAS officer from Jharkhand. When we hear about "Cyber crime" Our focus is gone on "cyber Security". This paper, gives detailed information regarding cybercrime and how it's affecting the life of we all. With increasing use of information technology (IT) enabled services such as e-governance, online business and electronic transactions protection of personal and sensitive data have assumed paramount importance. The economic growth of any nation and its internal security depends on how well is its cyberspace secured and protected.**

***Keywords*: Cyber Crime, Information Security, Cyber threats, Hacking, Phishing, Cyber Safety, Digital Data, Technology.**

1. Introduction

Social Media can be defined an individual or agency to communicate interactively and exchange of user generated content and it is explained by a number of tools, which includes blogs, wikis, discussion forums, micro-blogs, twitter and social networking sites. So many advantages of social media but there are threat to internal security in different forms like Cyber crime, Cyber Terrorism, Fraud, spreading violence, etc. National Security's Importance (NSI) for any nation maintained peace and harmony. Internal security challenges and Social Media act as the platform for nations face numerous. Social media is not security threat in itself but the users of these services can pose the threats by their anti-social Endeavour's.

"Jamtara is a sleepy town in the tribal region of Santhal Pargana. It still continues to be an obscure town. But has gained notoriety as cybercrime hub," Gauba said while addressing a conference on internal security. More than half of India's crimes committed by fraudsters posing as bank managers were traced back to this town. Expressing concern over the new age crime, the government is still not ready to tackle the increasing rate of cyber crimes.

2. Discussions

In these parts – Karmatand and elsewhere in the villages of Jamtara, Madhupur, and Dumka of eastern Jharkhand – the frequently-used "cyber" in Hindi and Bengali refers to cybercrime and those dabbling in cybercrime, both petty and serious. There are thousands of "cyber" in this area, about 250 km northeast of Kolkata.

When we met there a localized, he told "they guys do their cybercrime there, pointing to this area".

Fig. 1. Cyber criminals do their crimes from barren fields & nearby forests

Among the millions-strong generation of boys and young men in their teens and early 20s in Jharkhand, a state that is rich in mineral wealth (it accounts for some 40% of the country's natural resources) but counts 39 of its 100 people living in poverty. Amidst the malnutrition and poverty, smart phones make the world a less unequal place for the Jamtara's youth involved in cybercrime. With more than half of India's cyber crimes, mostly committed by fraudsters posing as bank managers and traced back to Jharkhand, this belt is clearly digital India's underbelly. This estimate comes from police officials in Jharkhand and Karnataka. To be sure, Jharkhand ranks 13th in terms of cyber crime rates in 2016, the latest year for which data is available the National Crime Records Bureau (NCRB), and 14th in terms of incidents and the percentage share of overall reported cyber crimes for the same year. But, that's primarily because most of the victims targeted by the

Smishing

(SMS-Phishing)

ed to steal
nal information

It's a type of
Social Engineering

That targets
mobile devices

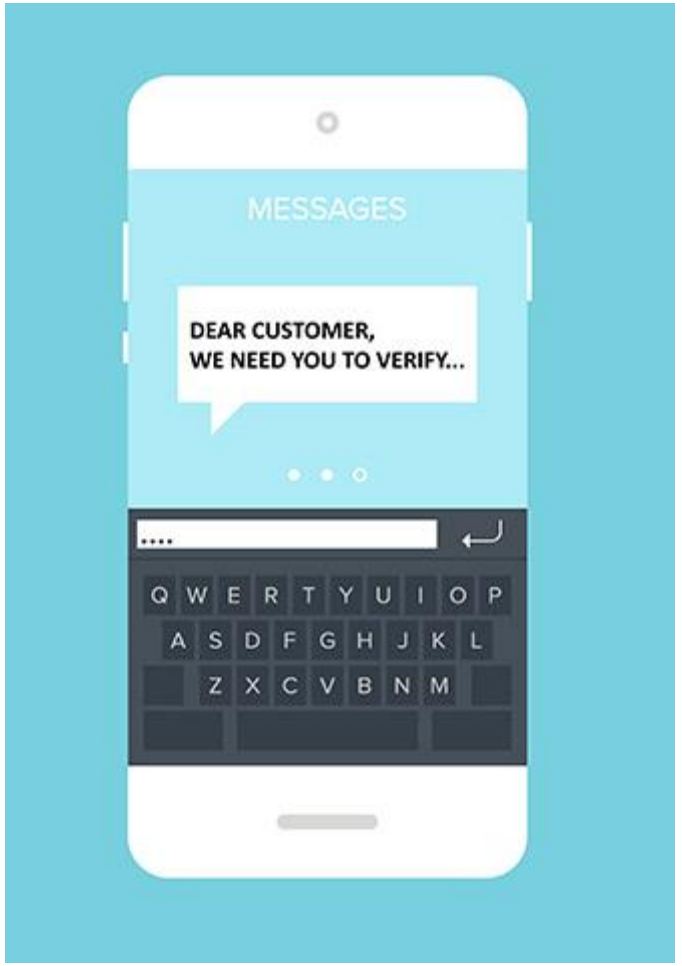
13.4 Smishing

- Smishing or SMS Phishing is a technique where a text message is sent to the individual's mobile phone to get him/her divulge personal information.

- The two most common types involves:
  - Person receives text message directs him/her to call a phone number
  - Person receives text message directs him/her to visit a website

- Smishing has become more attractive alternative to phishing

- Most attack target banks and financial institutions



13.4 Smishing

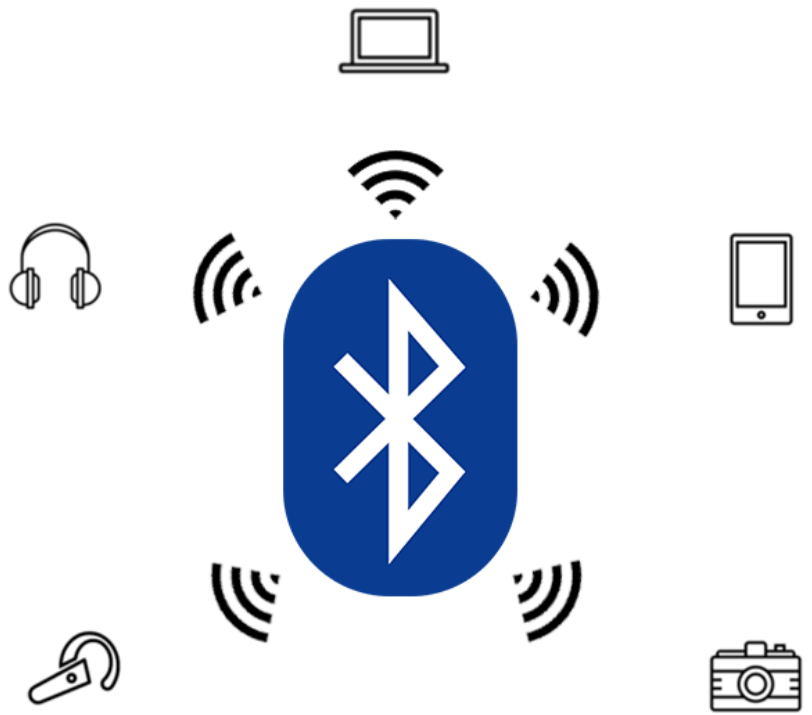
- To protect mobile devices from Smishing attacks, users from any organizations should follow:

1. Add mobile security
2. Create and implement IT policy
3. Perform threat modelling
4. Train application developers in secure coding
5. Limit sensitive data transfer
6. Utilize mobile device Management software
7. Perform technical security assessment
8. Establish program that continually evaluates new and emerging threats
9. Increase monitoring control
10. Assess classic threats

13.5 Hacking Bluetooth

- Bluetooth has become solution to problems like driving and talking on a cell phone and introduced new and interesting marketing opportunities for attacks.

- Bluetooth devices are connected through pairing
- Once pairing is complete the devices bond with one another
- PIN is required



13.5 Hacking Bluetooth

- Some common attacks for hacking Bluetooth are:
    - Bluejacking
    - Bluesnarfing
    - Bluebugging
    - Car Whisperer

13.5.1 Bluejacking

- Bluejacking : (Bluetooth and jacking :"hijack").

- Attacker send unsolicited message to bluetooth enable device.

- Most common form of Bluetooth hacking
- Harmless
- Prank people
- Does not give hacker access to your phone or information in it

- Keep Bluetooth setting to invisible or non discoverable
- Ignore messages if you receive them

13.5.2 Bluesnarfing

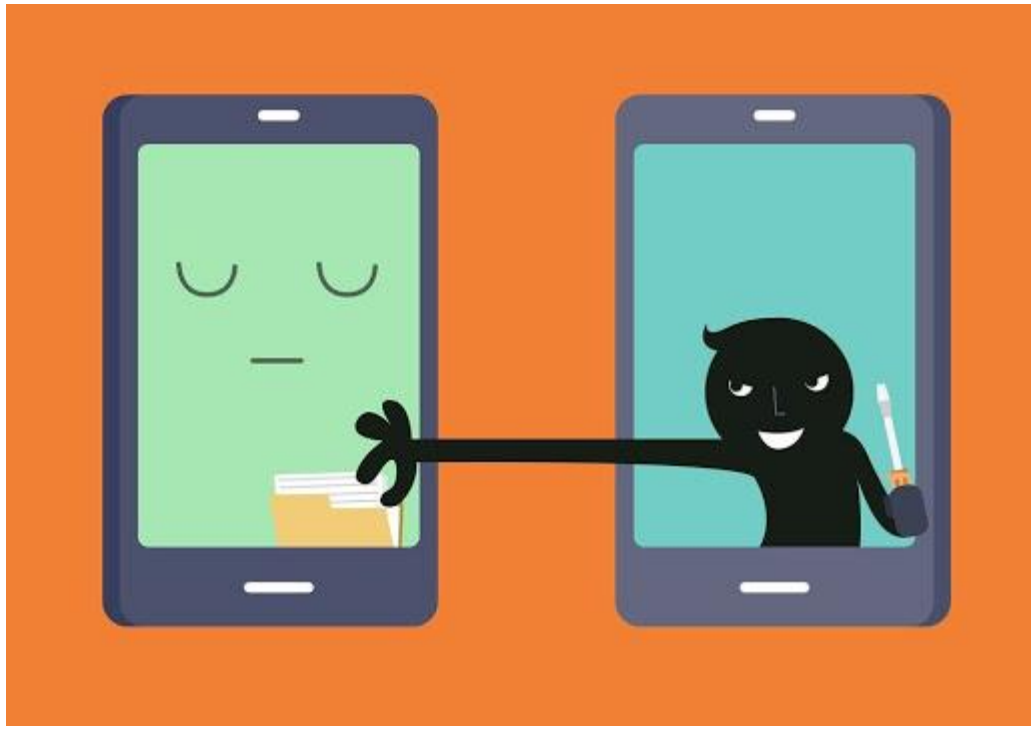
- More serious than Bluejacking
- Can leave open some of the private information stored on your smart phone
- Hacker may purchase a software
- Can happen when device is set to invisible or non discoverable

- The information stolen can be important to you but not as precious as banking information
- Data can be accessed by hacking your device through Bluebugging

13.5.3 Bluebugging

- Hacker gains complete access and control of your device
- Hacker is capable of accessing all information including photos, apps, contacts, etc
- Can happen when device is set to invisible or non discoverable
- Much harder than Bluejacking and Bluesnarfing

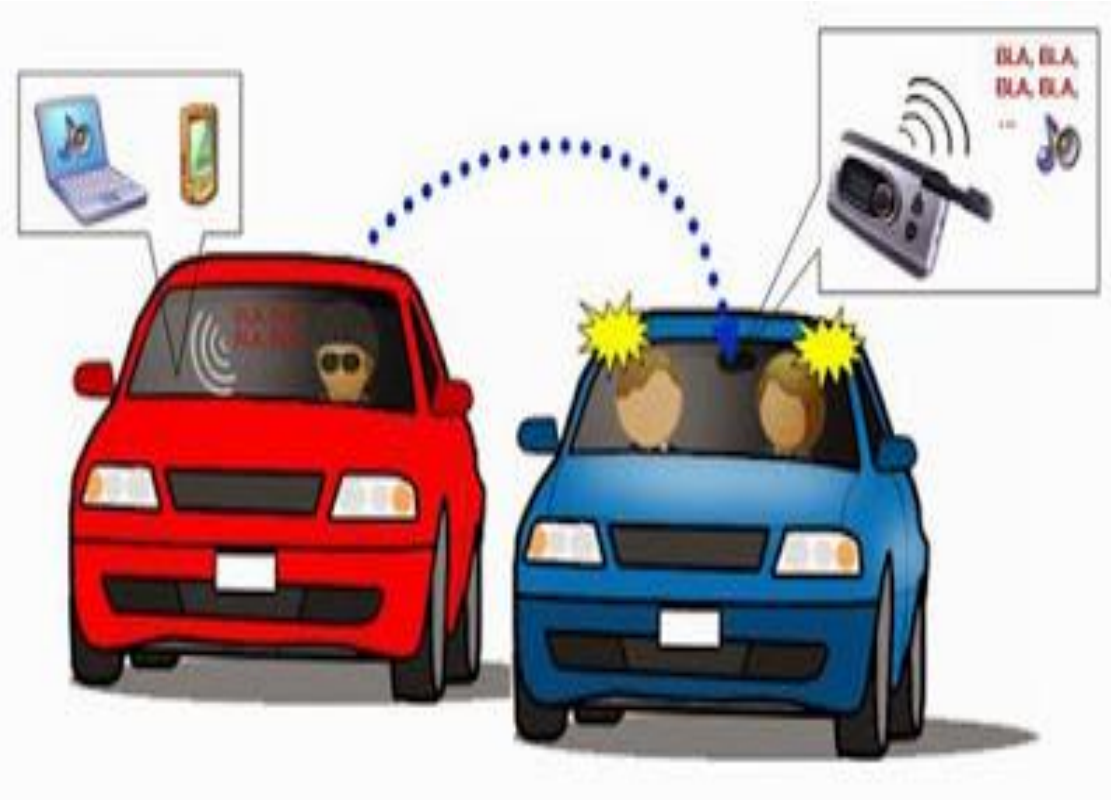
- Only feasible on older phones



13.5.4 Car Whisperer

- Can be used by attackers to hack hands free Bluetooth in a car system
- Connect to the system to inject audio or record audio from a bypassing car
- Easily used by attackers to invade privacy and listen to the conversation
- Bluetooth system in cars need simple 4 digit security key

- Experts could not confirm yet if this attack can be used to disable air bags or breaks



13.5 Hacking Bluetooth

- Simple tips to protect from Bluetooth hacking:
  - Update all software
  - Turn the Bluetooth services off when not in use
  - Never use public Wi-Fi networks
  - Consider a virtual protected network

- Man In Middle attack

https://www.youtube.com/watch?v=fTBmD2t3p90

- SMS Phishing

https://www.youtube.com/watch?v=_dj_90TnVbo

- Credit Card Fraud

https://www.youtube.com/watch?v=E3gxA5HD-nQ

- Technical Support Phone Scam

https://www.youtube.com/watch?v=WhV6rIgyQ-s

- Fake IRS Phone and Phishing Scams

https://www.youtube.com/watch?v=dq0TNFnc4nY

- How to hack usernames and passwords

https://www.youtube.com/watch?v=js78vXfWX3s

- Hacking Tip: Password Cracking with Cain & Abel

https://www.youtube.com/watch?v=RyQL9AdxHqY

OUTLINE

- Attacks on Mobile/Cell Phones
- Mobile Devices: Security Implications for Organizations
- Organizational Measures for Handling Mobile
- Devices-Related Security Issues
- Organizational Security Policies and Measures in Mobile Computing Era
- Laptops

14 Mobile Devices: Security Implications for Organizations

- Mobile technology is current used not only for calling but also used in business
- Cell phones untethered employees from landline phones and laptops revolutionised the ability of employees to work remotely.

14 Mobile Devices: Security Implications for Organizations

- The evolving mobile device technology can, if properly utilized, enable the enterprise to achieve several significant benefits

  - Improved Workforce productivity
  - Improved customer service
  - Improved business process efficiency
  - Employee security and safety
  - Employee retention

14 Mobile Devices: Security Implications for Organizations

- If proper and strong security policies are not enforced, there is a huge risk of data loss, theft, or misuse of confidential information available on mobile devices.

- All mobile devices can be victim of cyber attacks through the use of malicious applications, spams, and phishing schemes.

- Jailbreak software
  - Hijack a device and access all its information
  - Inserting zombies
  - Controlling device
  - Turning on Bluetooth and Wi Fi automatically

14 Mobile Devices: Security Implications for Organizations

- Mobile devices could pose a risk that can be categorized into 5 areas:

1. Physical access
2. Malicious code
3. Device attacks
4. Communication interception
5. Insider threats

14 Mobile Devices: Security Implications for Organizations

1. Physical access

- Small, easily portable and extremely lightweight
- Easy to steal or leave behind
- Cleverest intrusion detection system or anti virus are useless if attacker is having physical access
- Circumventing password or accessing encrypted data is possible
- Not only corporate data but other passwords (iPhone keychain, VPN)
- Forensic data retrieval software

14 Mobile Devices: Security Implications for Organizations

2. Malicious code

- Socially engineered and tricking the user into accepting what the hacker is selling
- Spam, weaponized links and applications
- Mobile ads – Malvertising
- Android devices
- Mobile malware trojans – Sent through SMS
- Once the user clicks- trojan is delivered by the way of application
- These applications can transmit information

14 Mobile Devices: Security Implications for Organizations

3. Device attacks

- Similar to PC attacks
- Browser based attacks, browser overflow attacks are possible
- SMS and MMS – used by hackers
- Designed to gain control of device and access data or DDoS

14 Mobile Devices: Security Implications for Organizations

4. Communication interception

- Technology to hack into wireless networks – online
- Wi Fi hacking, Man-in-the-middle attacks
- Cellular data transmission – intercepted and decrypted
- Weaknesses in the WiFi and cellular data transmission protocols
- Companies providing Free Wi Fi
- Personal social networking login and enterprise system

14 Mobile Devices: Security Implications for Organizations

5. Insider threats

- Downloading of applications
- Can access enterprise assets
- Misuse of personal cloud use
- Smart phones can be used

14 Mobile Devices: Security Implications for Organizations

- Mobile security threats will continue to advance
- Users need to understand the implications of faulty mobile security practices

15. Organizational Measures for Handling Mobile Devices-Related Security Issues

- Four questions need to be addressed when developing a mobile security strategy:

1. How do we deny access to unauthorized users?
2. What is our plan if a personal device gets lost or stolen?
3. Ho w do we remove corporate data from a personal device whose owner is leaving the company?
4. How do we keep prying eyes away from the confidential files?

15. Organizational Measures for Handling Mobile Devices-Related Security Issues

- Some of the most common security features used to protect mobile assets are:
  - Enforced authentication
  - Over the air data encryption
  - Over the air provisioning
  - Remote wipe and data fading
  - Full disk encryption
  - Separation of personal and enterprise information
  - User access rights and security policies
  - Network filters

16. Organizational Security Policies and Measures in Mobile Computing Era

- An organization should adhere the following rules for effective mobile device management

1. Identify all mobile devices on the network
2. Know which back-office systems employee need to access
3. Formalise your user types and set policies
4. Be ready to block access
5. Add password and encryption policies plus remote wipe
6. Consider separating personal data from business data
7. Enable user to be self sufficient

16. Organizational Security Policies and Measures in Mobile Computing Era

- Effective remote management and data protection tools and policies
- Preventing sensitive information on mobile devices
- Providing bullet-proof strategy
- Steps to secure an organization’s mobile devices are :

16. Organizational Security Policies and Measures in Mobile Computing Era

- Steps to secure an organization's mobile devices are :

1. Configure mobile devices securely
   a) Auto lock
   b) Password protection
   c) Avoid auto-complete features
   d) Browser security setting
   e) Remote wipe
   f) SSL protection

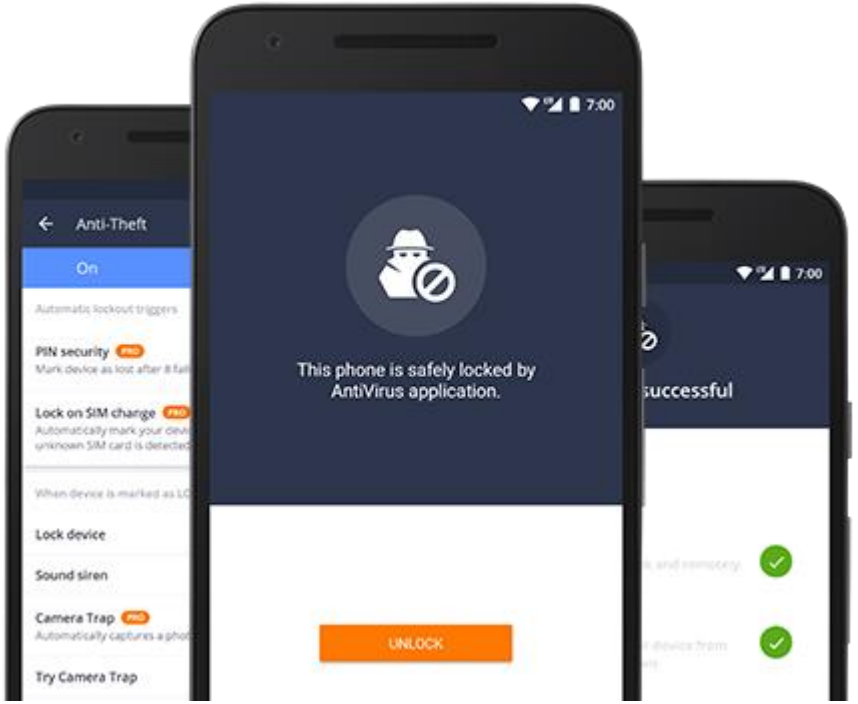
16. Organizational Security Policies and Measures in Mobile Computing Era

- Steps to secure an organization’s mobile devices are :

2. Disable Bluetooth, infrared or WiFi when not in use

3. Update mobile devices frequently

4. Utilise anti virus programs



16. Organizational Security Policies and Measures in Mobile Computing Era

- Steps to secure an organization’s mobile devices are :

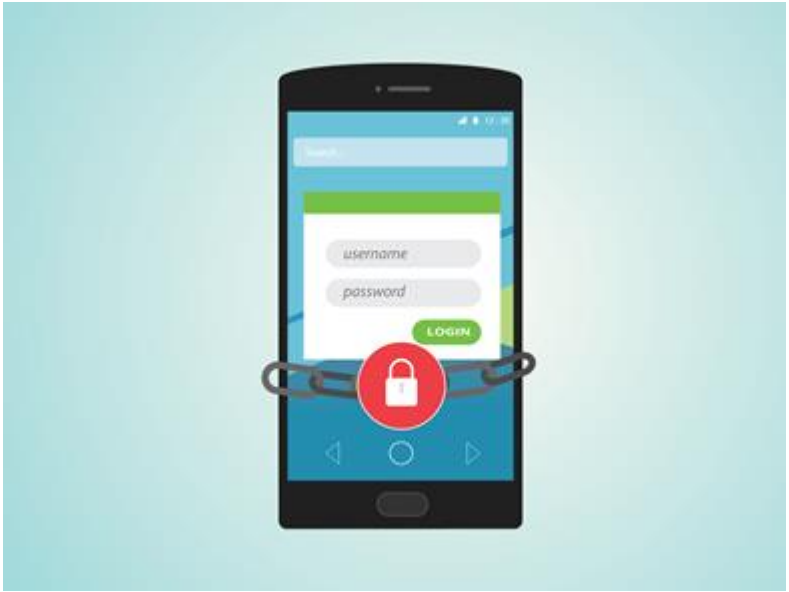
5. Use an encryption solution

a) Data protection
b) Do assessment
c) Data is centrally and securely maintained
d) Educate users

16. Organizational Security Policies and Measures in Mobile Computing Era

- Steps to secure an organization’s mobile devices are :

6. Use digital certificates



16. Organizational Security Policies and Measures in Mobile Computing Era

- Steps to secure an organization's mobile devices are :

7. Take physical security methods

a) Cable locks
b) Tracking and tracing software
c) Never leave device unattended
d) Report lost or stolen
e) Back up data

16. Organizational Security Policies and Measures in Mobile Computing Era

- Steps to secure an organization’s mobile devices are :

8. Appropriate disposal procedures

9. Develop appropriate policies and guidelines

16. Organizational Security Policies and Measures in Mobile Computing Era

- Steps to secure an organization's mobile devices are :

10. Educate employees about mobile device security

a) Cautious when opening email and text message
b) Aware of links, attachments and downloads
c) Aware of current threats affecting mobile

16. Organizational Security Policies and Measures in Mobile Computing Era

- Every organization needs to frame a comprehensive yet flexible mobile device policy
- Enforce it
- Centrally managed
- Security policy must be auditable

16. Organizational Security Policies and Measures in Mobile Computing Era

- Audit procedures are as follows:

1. Policy
2. Antivirus updates
3. Encryption
4. Secure transmission
5. Device management
6. Access control
7. Awareness training
8. risk

17. Laptops

- Laptops enhance the business functions as they give mobile access to information anytime and anywhere, but they have serious threat of being stolen.
- 2 counter measures
  - Physical Access Control (Physical security measures)
  - Logical Access Control

17. Laptops

Physical Access Control

1. Cables and hardwired locks

2. Laptop safes

3. Motion sensors and alarms

4. Warning labels and stamps
5. Other measures

17. Laptops

Logical Access Control

1. Protecting from malicious programs/ attackers/ social engineering
2. Avoid weak passwords/ open access
3. Monitoring application security and scanning for vulnerabilities
4. Proper handling of removable drives/ storage mediums/ unnecessary ports
5. Password protection through appropriate rules and use of strong passwords
6. 6. Regularly installing security patches and updates

17. Laptops

7. Installing antivirus software/ firewalls/ intrusion detection system (IDS)

8. Encrypting critical file systems

9. Choosing secure Operating system

10. Registering the laptop with laptop manufacturer to track down incase of theft

11. Disabling unnecessary user accounts and renaming the administrator account

12. Disabling the display of the last logged in username in the login dialog box

13. Backing up data on a regular basis

17. Laptops

- Some basic security principles for laptops

1. Choose a secure operating system and lock it down
2. Enable strong BIOS password
3. Engrave the laptop
4. Register the laptop with the manufacturer
5. Get a cable lock and use it
6. Use a docking station
7. Lockup your PCMCIS cards
8. Use a personal firewall on your laptop
9. Use a tracking software to have your laptop call home

University Questions from Module 2

1. Compare Vishing, Phishing and Smishing in cyber security.

2. What is Bluetooth hacking? Explain Bluetooth hacking tools in brief.

3. Discuss basic precautions to be taken to safeguard laptops and wireless devices.

Join **CSL** on MS Teams:

Team Name:

Code:

••••

THANK YOU

HARSHADA ARUN RAJALE

+91 9594146413

Harshada.Rajale@vit.edu.in