UNIT-2: Cyber Crime

- Mobile and Wireless Devices Introduction
- Proliferation of Mobile and Wireless Devices
- Trends in Mobility
- Credit Card Frauds in Mobile and Wireless Computing Era
- Security Challenges Posed by Mobile Devices
- Registry Settings for Mobile Devices
- Authentication Service Security
- Attacks on Mobile/Cell Phones
- Mobile Devices: Security Implications for Organizations
- Organisational Security Policies and Measures in Mobile Computing Era

Faculty: VIKRAM SHARMA
Vikram1532018@gmail.com

Cyber Security

(BCC301 / BCC401/ BCC301H / BCC401H)

Video Overview:

- Mobile and Wireless Devices Introduction
- Proliferation of Mobile and Wireless Devices
- Trends in Mobility
- Credit Card Frauds in Mobile
- Wireless Computing Era
- Security Challenges Posed by Mobile Devices
- Registry Settings for Mobile Devices
- Authentication Service Security

Faculty: VIKRAM SHARMA
Vikram1532018@gmail.com

UNIT 2

Mobile and Wireless Devices Introduction

Mobile and wireless devices are like digital companions that don't need a physical connection to work. They include smartphones, tablets, and other gadgets that communicate wirelessly, allowing users to stay connected and access information on the go.

Features:

1. **Portability:** These devices are small and easy to carry, allowing users to stay connected wherever they go.
2. **Wireless Connectivity:** They use technologies like Wi-Fi, Bluetooth, and mobile networks to connect to the internet and other devices.
3. **Multifunctionality:** Beyond calls and messages, they serve as cameras, GPS devices, entertainment hubs, and more.

Faculty: VIKRAM SHARMA
Vikram1532018@gmail.com

UNIT 2

Importance of Mobile and Wireless Devices

1. **Communication:** Keeping people connected through calls, messages, and social media.
2. **Information Access:** Providing instant access to the internet for information, news, and enter tainment .
3. **Productivity:** Enabling work and productivity on the go through various apps and functionalities.

UNIT 2

Proliferation of Mobile and Wireless Devices

Proliferation of mobile and wireless devices is like the widespread growth or spread of smartphones, tablets, and other wirelessly connected gadgets. It reflects the increasing number of these devices in our daily lives.

Key Factors:

1. **Technological Advancements:** Continuous improvements in technology make devices more affordable and accessible.
2. **Increased Connectivity:** The rise of high-speed internet and wireless networks enables seamless communication.
3. **Versatility:** Mobile devices offer a variety of functions, from communication to entertainment and productivity.
4. **Consumer Demand:** People increasingly rely on mobile and wireless devices for convenience and on-the-go access.

Faculty: VIKRAM SHARMA
Vikram1532018@gmail.com

UNIT 2

Trends in Mobility

1. **5G Revolution:** The 5G Revolution is like the superhero of internet speed. It's the fifth generation of mobile networks, bringing faster speeds and more reliable connections to mobile and wireless devices.

Impact:

- **High-Speed Connectivity:** Faster internet speeds for quicker downloads and smoother streaming.
- **IoT Advancements:** Enables better connections for the Internet of Things (IoT) devices.

2. **Mobile App Ecosystem:** The Mobile App Ecosystem is like a digital marketplace. It encompasses the diverse range of applications available for download on mobile devices.

Impact:

- **Diverse Applications:** Apps for communication, productivity, entertainment, and more.
- **App Integration:** Seamless integration of apps for a smoother user experience.

UNIT 2

Trends in Mobility

3. Mobile Security Measures: Mobile Security Measures are like digital bodyguards for your devices. With the increasing use of mobile devices, there's a growing focus on ensuring their security.

Impact:

- **Biometric Authentication:** Fingerprint and facial recognition for enhanced device security.
- **Mobile Device Management (MDM):** Tools for businesses to secure and manage mobile devices.

4. Edge Computing: Edge Computing is like having a mini-brain in your device. Instead of relying solely on a centralised server, computations happen closer to the source of data.

Impact:

- **Reduced Latency:** Faster response times for applications and services.
- **Improved Privacy:** Processing sensitive data locally without sending it to a central server.

UNIT 2

Trends in Mobility

5. Augmented Reality (AR) and Virtual Reality (VR): Augmented Reality (AR) and Virtual Reality (VR) are like digital realms overlaying or immersing into the real world, enhancing user experiences.

Impact:

- **Enhanced User Engagement:** AR adds digital elements to the real world, while VR creates immersive environments.
- **Applications in Various Industries:** From gaming to healthcare and education.

6. Remote Work and Collaboration: Remote Work and Collaboration are like the new-age workspaces. With the advancement of mobile technology, working from anywhere and collaborating seamlessly has become a trend.

Impact:

- **Flexibility:** Allows professionals to work from different locations.
- **Virtual Meetings:** Increased reliance on mobile devices for virtual collaboration.

Faculty: VIKRAM SHARMA
Vikram1532018@gmail.com

UNIT 2

Trends in Mobility

7. Sustainable Mobility: Sustainable Mobility is like a green approach to technology. It involves the development and use of mobile solutions that minimise environmental impact.

Impact:

- **Green Technologies:** Focus on eco-friendly materials and energy-efficient designs.
- **Reduced E-Waste:** Efforts to extend the lifespan of devices and promote recycling.

Credit Card Frauds in Mobile

Credit Card Frauds in Mobile are like digital heists targeting your financial information on mobile devices. It involves unauthorised access to credit card details, leading to financial losses and potential identity theft.

Common Techniques:

1. **Phishing:** Fraudsters use fake messages or emails to trick users into revealing credit card information.
2. **Mobile Malware:** Malicious software on mobile devices can capture credit card details.
3. **Fake Apps:** Fraudulent mobile applications mimic legitimate ones to steal credit card information.
4. **Unsecured Wi-Fi:** Conducting transactions on unsecured Wi-Fi networks makes it easier for hackers to intercept data.

UNIT 2

Credit Card Frauds in Mobile

Preventive Measures:

1. **Use Trusted Apps:** Only download apps from official app stores to avoid fake applications.
2. **Secure Wi-Fi:** Avoid sensitive transactions on public Wi-Fi networks; use secure connections.
3. **Two-Factor Authentication:** Enable additional layers of security for mobile transactions.

4 **Regular Monitoring:** Keep a close eye on credit card statements for any unauthorised transactions.

.

Example: Imagine receiving a message that looks like it's from your bank, asking for your credit card details to resolve an issue. If you provide this information, you've fallen victim to Credit Card Frauds in Mobile. It's crucial to stay vigilant, verify messages, and adopt secure practices to protect your financial information on mobile devices.

Faculty: VIKRAM SHARMA
Vikram1532018@gmail.com

UNIT 2

Wireless Computing Era

The Wireless Computing Era is like a technological revolution, marking a shift from traditional wired connections to a world where computing devices communicate and connect wirelessly.

Key Elements:

1. **Wireless Networks:** Use of technologies like Wi-Fi, Bluetooth, and cellular networks for device connectivity.
2. **Mobile Devices:** Proliferation of smartphones, tablets, and wearables, untethered from physical connections.
3. **Cloud Computing:** Storing and accessing data and applications over the internet instead of on local devices.

Faculty: VIKRAM SHARMA
Vikram1532018@gmail.com

UNIT 2

Wireless Computing Era

Characteristics:

1. **Mobility:** Computing devices can be used and moved without the constraints of physical cables.
2. **Instant Connectivity:** Devices can connect to the internet and each other instantly, enhancing communication.

Technological Enablers:

1. **5G Technology:** High-speed, low-latency wireless networks supporting advanced applications.
2. **IoT Integration:** Interconnected devices, from smart homes to industrial sensors, communicating wirelessly.
3. **Edge Computing:** Processing data closer to the source, reducing reliance on centralised servers.

Faculty: VIKRAM SHARMA
Vikram1532018@gmail.com

Wireless Computing Era

Impact on Society:

1. **Digital Transformation:** Changing the way businesses operate, communicate, and deliver services.
2. **Remote Work Revolution:** Allowing individuals to work from anywhere, transforming traditional workspaces.
3. **Smart Living:** Integration of wireless technologies in homes, making them smart and connected.

Example: Imagine a world where you can seamlessly connect to the internet, work, and communicate without any physical constraints. That's the essence of the Wireless Computing Era, where the airwaves carry the pulse of our digital lives, shaping the way we live, work, and connect.

UNIT 2

Security Challenges Posed by Mobile Devices

1. Lost or Stolen Devices: Challenge: Mobile devices are small and portable, making them easy targets for theft or misplacement. If not secured, sensitive information can be accessed.

Mitigation:

- **Strong Passwords or Biometrics:** Protect devices with secure authentication methods.
- **Remote Wipe:** Enable features to remotely erase data in case of loss.

2. Malicious Apps: Challenge: Fake or malicious apps can compromise security by accessing personal information or injecting malware into the device.

Mitigation:

- **Official App Stores:** Download apps only from trusted sources like Google Play or the Apple App Store.
- **App Permissions:** Review and limit app permissions to the essentials.

UNIT 2

Security Challenges Posed by Mobile Devices

3. Phishing Attacks: Challenge: Mobile users may fall victim to phishing attempts through fraudulent emails, messages, or websites seeking personal information.

Mitigation:

- **User Education:** Train users to identify and avoid phishing attempts.
- **Security Software:** Use mobile security apps to detect and block phishing threats.

4. Insecure Wi-Fi Networks: Challenge: Connecting to unsecured Wi-Fi networks exposes mobile devices to potential eavesdropping and data interception.

Mitigation:

- **Use VPNs:** Employ Virtual Private Networks for secure data transmission.
- **Avoid Public Wi-Fi for Sensitive Transactions:** Refrain from conducting financial or sensitive transactions on unsecured networks.

UNIT 2

Security Challenges Posed by Mobile Devices

5. Outdated Software: Challenge: Failure to update operating systems and apps leaves devices vulnerable to known exploits and security flaws.

Mitigation:

- **Regular Updates:** Keep both the operating system and apps up to date.
- **Automatic Updates:** Enable automatic updates for added convenience.

6. Lack of Encryption: Challenge: Unencrypted data transmission and storage can lead to unauthorised access and data breaches.

Mitigation:

- **Enable Encryption:** Encrypt both data at rest and during transmission.
- **Secure Communication Channels:** Use secure protocols for data transfer.

UNIT 2

Security Challenges Posed by Mobile Devices

7. Social Engineering: Challenge: Cybercriminals may exploit human psychology to manipulate users into revealing sensitive information.

Mitigation:

- **User Education:** Train users to recognize and resist social engineering tactics.
- **Multi-Factor Authentication:** Implement additional authentication layers for added security.

8. Insufficient User Awareness: Challenge: Lack of awareness among users about mobile security best practices can lead to risky behaviours.

Mitigation:

- **Training Programs:** Conduct regular security awareness training for users.
- **Communication:** Keep users informed about emerging threats and best practices.

UNIT 2

Registry Setting for Mobile Devices

Mobile devices, especially those running iOS and Android, typically do not have a registry like Windows operating systems. However, they do have settings and configurations that can be managed to enhance security and control device behaviour. Here are some important settings and configurations for mobile devices:

1. iOS (iPhone and iPad)
2. Android

UNIT 2

Registry Setting for Mobile Devices: ISO

1. Device Passcode:

- **Purpose:** Protects the device from unauthorised access.
- **Configuration:** - Settings > Face ID & Passcode (or Touch ID & Passcode) > Turn Passcode On

2. Biometric Authentication:

- **Purpose:** Enhances device security with fingerprint or face recognition.
- **Configuration:** - Settings > Face ID & Passcode (or Touch ID & Passcode)

3. Find My iPhone:

- **Purpose:** Allows tracking and remote wiping of a lost or stolen device.
- **Configuration:** - Settings > [Your Name] > Find My > Find My iPhone

Registry Setting for Mobile Devices: ISO

4. App Permissions:

- **Purpose:** Control which apps have access to sensitive data.
- **Configuration:** - Settings > Privacy > [App Name]

5. Automatic Updates:

- **Purpose:** Ensures the device is running the latest security patches.
- **Configuration:** - Settings > General > Software Update

UNIT 2

Registry Setting for Mobile Devices: Android

1. Screen Lock:

- **Purpose:** Provides an initial layer of security.
- **Configuration:** - Settings > Security > Screen lock

2. Biometric Authentication:

- **Purpose:** Enhances device security with fingerprint or facial recognition.
- **Configuration:** - Settings > Security > Biometrics

3. Find My Device:

- **Purpose:** Allows tracking and remote wiping of a lost or stolen device.
- **Configuration:** - Settings > Security > Find My Device

UNIT 2

Registry Setting for Mobile Devices: Android

4. App Permissions:

- **Purpose:** Control which apps have access to sensitive data.
- **Configuration:** - Settings > Apps & Notifications > [App Name] > Permissions

5. Google Play Protect:

- **Purpose:** Scans apps for malware and provides additional security.
- **Configuration:** - Settings > Google > Security > Play Protect

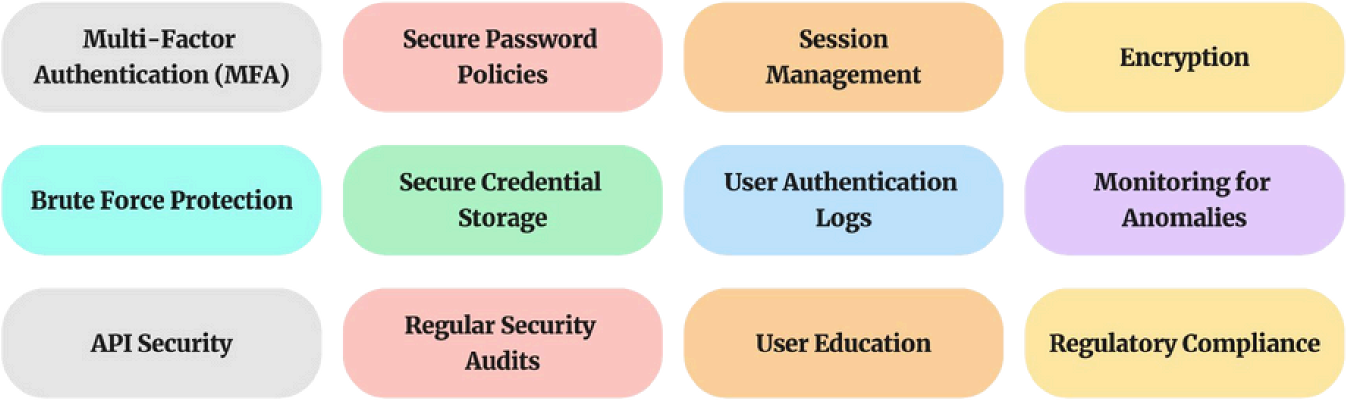
6. Automatic Updates:

- **Purpose:** Ensures the device is running the latest security patches.
- **Configuration:** - Settings > System > Software Update

UNIT 2

Authentication Service Security

Authentication service security is a critical aspect of ensuring that user identities are properly verified and protected. Here are key considerations and measures for enhancing the security of authentication ser vices:



Multi-Factor Authentication (MFA)	Secure Password Policies	Session Management	Encryption
Brute Force Protection	Secure Credential Storage	User Authentication Logs	Monitoring for Anomalies
API Security	Regular Security Audits	User Education	Regulatory Compliance

Authentication Service Security

1. Multi-Factor Authentication (MFA):

Purpose: Adds an extra layer of security by requiring users to provide multiple forms of identification.

Implementation:

- Combine something the user knows (password) with something they have (token, mobile device, fingerprint).

2. Secure Password Policies:

Purpose: Ensures that users create and maintain strong, unique passwords.

Implementation:

- Enforce password complexity (length, special characters).
- Regularly prompt users to update passwords.
- Discourage password reuse.

Authentication Service Security

3. Encryption:

Purpose: Protects sensitive data transmitted between users and authentication servers.

Implementation:

- Use strong encryption protocols (e.g., TLS/SSL) for data in transit.
- Hash and salt passwords before storing them.

4. Session Management:

Purpose: Prevents unauthorised access during an active session.

Implementation:

- Implement session timeout policies.
- Use secure session tokens.
- Provide users the ability to log out remotely.

UNIT 2

Authentication Service Security

5. Brute Force Protection:

Purpose: Mitigates the risk of attackers attempting to guess passwords.

Implementation:

- Implement account lockout policies after a certain number of failed login attempts.
- Use CAPTCHA or similar mechanisms to deter automated attacks.

6. Secure Credential Storage:

Purpose: Ensures that user credentials are stored securely.

Implementation:

- Hash and salt passwords using strong cryptographic algorithms.
- Regularly audit and update credential storage mechanisms.

UNIT 2

Authentication Service Security

7. User Authentication Logs:

Purpose: Monitors and logs authentication events for analysis and auditing.

Implementation:

- Keep detailed logs of authentication attempts, including successful and failed events.
- Regularly review and analyse authentication logs.

8. Monitoring for Anomalies:

Purpose: Detects unusual or suspicious behaviour that may indicate unauthorised access.

Implementation:

- Implement real-time monitoring for unusual login patterns.
- Set up alerts for multiple failed login attempts or other suspicious activities.

Authentication Service Security

9. API Security:

Purpose: Ensures that authentication APIs are secure and not vulnerable to attacks.

Implementation:

- Use secure API authentication methods (e.g., OAuth).
- Regularly test and update API security measures.

10. Regular Security Audits:

Purpose: Identifies vulnerabilities and ensures ongoing compliance with security best practices.

Implementation:

- Conduct regular security audits and penetration testing.
- Address identified vulnerabilities promptly.

UNIT 2

Authentication Service Security

11. User Education:

Purpose: Empowers users to make informed security decisions and recognize phishing attempts.

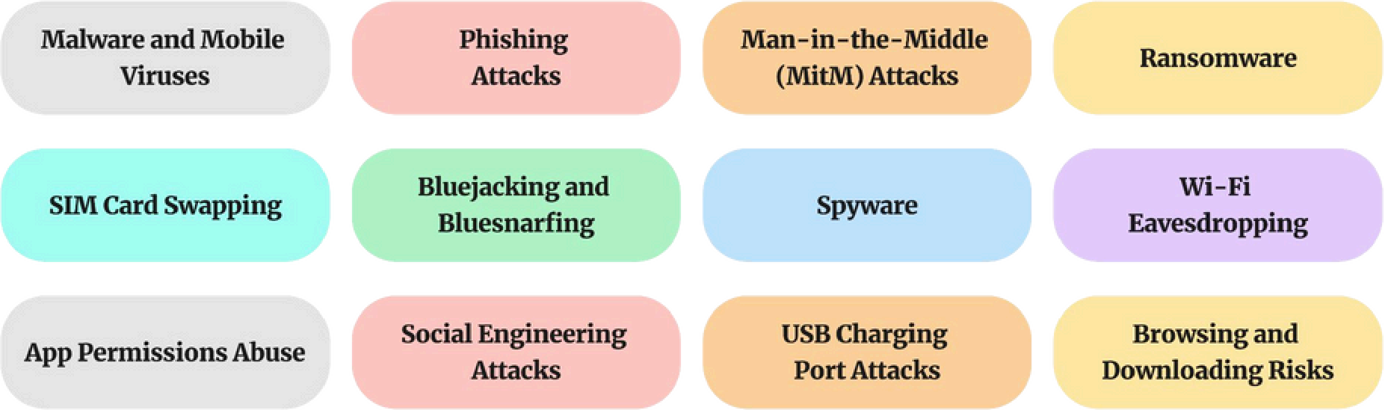
Implementation:

- Provide regular security awareness training.
- Communicate best practices for protecting personal information.

UNIT 2

Attacks on Mobile/Cell Phones

Mobile phones are susceptible to various types of attacks, ranging from traditional malware to more sophisticated social engineering tactics. Here are some common attacks on mobile or cell phones:



- Malware and Mobile Viruses
- Phishing Attacks
- Man-in-the-Middle (MitM) Attacks
- Ransomware
- SIM Card Swapping
- Bluejacking and Bluesnarfing
- Spyware
- Wi-Fi Eavesdropping
- App Permissions Abuse
- Social Engineering Attacks
- USB Charging Port Attacks
- Browsing and Downloading Risks

Faculty: VIKRAM SHARMA
Vikram1532018@gmail.com

UNIT 2

Attacks on Mobile/Cell Phones

1. Malware and Mobile Viruses: Malicious software designed to infect mobile devices and compromise their functionality.

How to Protect:

- Install reputable antivirus and anti-malware apps.
- Download apps only from official app stores.
- Keep the device's operating system and apps updated.

2. Phishing Attacks: Attempts to trick users into revealing sensitive information by posing as a trustworthy entity.

How to Protect:

- Be cautious of unsolicited emails, messages, or calls asking for personal information.
- Verify the legitimacy of websites before entering credentials.

Attacks on Mobile/Cell Phones

3. Man-in-the-Middle (MitM) Attacks: Intercepting and possibly altering communication between two parties without their knowledge.

How to Protect:

- Use secure Wi-Fi connections or VPNs.
- Be cautious when connecting to public Wi-Fi networks.

4. Ransomware: Malware that encrypts data on the device, demanding a ransom for its release.

How to Protect:

- Regularly backup important data.
- Avoid clicking on suspicious links or downloading unknown attachments.

UNIT 2

Attacks on Mobile/Cell Phones

5. SIM Card Swapping: Unauthorised individuals attempt to take control of a user's phone number by swapping the SIM card.

How to Protect:

- Set up a PIN or password for SIM card changes.
- Contact your mobile carrier immediately if you experience unexpected loss of service.

6. Bluejacking and Bluesnarfing: Exploiting Bluetooth connections to send unsolicited messages or gain unauthorised access to a device.

How to Protect:

- Turn off Bluetooth when not in use.
- Set devices to non-discoverable mode in public places.

UNIT 2

Attacks on Mobile/Cell Phones

7. Spyware: Software installed on a device without the user's knowledge to collect information.

How to Protect:

- Regularly review installed apps and permissions.
- Use security software that scans for spyware.

8. Wi-Fi Eavesdropping: Unauthorised individuals intercepting unencrypted Wi-Fi traffic to capture sensitive information.

How to Protect:

- Use secure, encrypted Wi-Fi connections.
- Avoid transmitting sensitive information on public networks.

UNIT 2

Attacks on Mobile/Cell Phones

9. Social Engineering Attacks: Manipulating individuals to divulge confidential information or perform actions that may compromise security.

How to Protect:

- Be sceptical of unsolicited communication asking for sensitive information.
- Educate yourself and others about common social engineering tactics.

10. App Permissions Abuse: Malicious apps exploiting excessive permissions to access and misuse personal data.

How to Protect:

- Review and limit app permissions.
- Only install apps from reputable sources.

UNIT 2

Attacks on Mobile/Cell Phones

11. USB Charging Port Attacks: Malicious USB charging stations or cables that can install malware when connected to a device.

How to Protect:

- Avoid using public charging stations.
- Use only trusted charging cables and adapters.

12. Browsing and Downloading Risks: Visiting malicious websites or downloading apps from untrusted sources.

How to Protect:

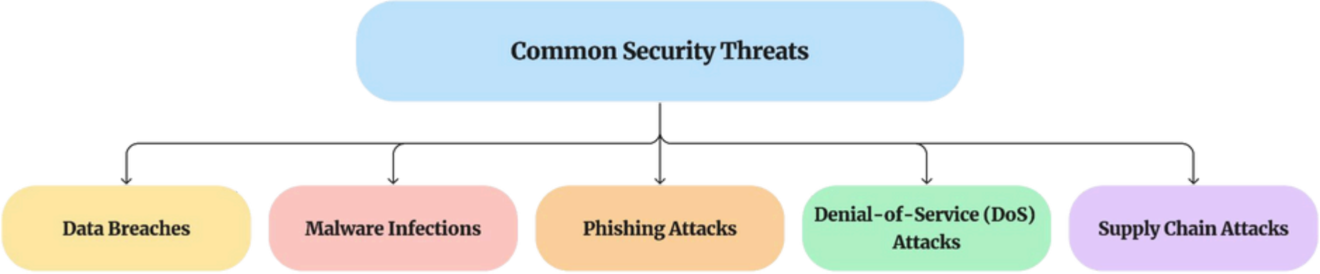
- Use secure and updated browsers.
- Download apps only from official app stores.

Faculty: VIKRAM SHARMA
Vikram1532018@gmail.com

UNIT 2

Security Implications for Organisation

Security is a crucial aspect of any organisation, as it protects sensitive information, systems, and reputation from harm. However, organisations face various security threats that can lead to serious consequences.



Faculty: VIKRAM SHARMA
Vikram1532018@gmail.com

UNIT 2

Common Security Threats

1. **Data Breaches:** Unauthorised access to confidential data like customer records or financial information can be costly and damaging.
2. **Malware Infections:** Malicious software like viruses or ransomware can steal data, disrupt operations, or hold systems hostage.
3. **Phishing Attacks:** Deceptive attempts to trick users into revealing sensitive information like passwords or credit card details.
4. **Denial-of-Service (DoS) Attacks:** Overwhelming a system with traffic to make it unavailable to legitimate users.
5. **Supply Chain Attacks:** Compromising vendors or suppliers to gain access to an organisation's systems and data.

UNIT 2

Mitigating Security Risks

1. **Strong Security Policies:** Establish clear guidelines for IT usage and incident response procedures.

2. **Robust Authentication:** Enforce strong passwords and multi-factor authentication (MFA) for secure account access.

3. **Cybersecurity Awareness Training:** Educate employees on identifying cyber threats and best practices.

4. **Regular Software Updates:** Apply software patches promptly to address vulnerabilities.

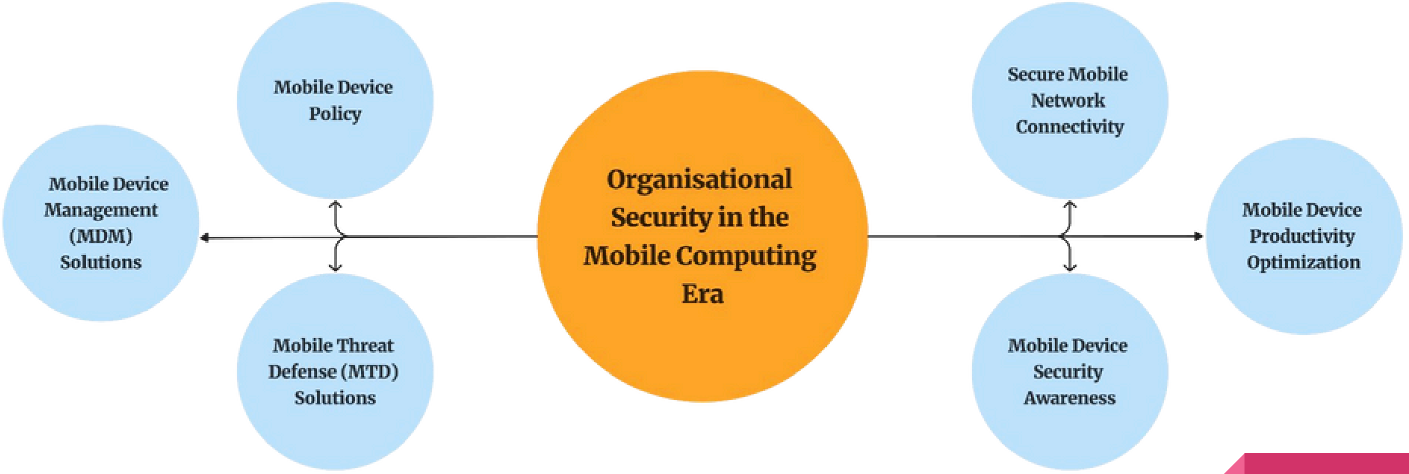
5. **Network Segmentation:** Separate networks to limit the spread of malware and other threats.

6. **Firewalls and Intrusion Detection Systems (IDS):** Implement firewalls to block unauthorised traffic and IDS to monitor for suspicious activity.

UNIT 2

Organisational Security Policies

Organisational Security Policies and Measures in Mobile Computing Era: As mobile devices have become indispensable tools for businesses, organisations need to implement comprehensive security policies and measures to protect their valuable data and maintain operational integrity.



Mobile Device Policy
Mobile Device Management (MDM) Solutions
Mobile Threat Defense (MTD) Solutions
Organisational Security in the Mobile Computing Era
Secure Mobile Network Connectivity
Mobile Device Productivity Optimization
Mobile Device Security Awareness

Faculty: VIKRAM SHARMA
Vikram1532018@gmail.com

UNIT 2

Organisational Security in Mobile Computing Era

1. Mobile Device Management (MDM) Solutions: MDM software provides centralised control over mobile devices, enabling IT administrators to manage and secure devices effectively. Key features of MDM include:

- **Device enrollment and provisioning:** Streamline device setup and ensure consistent configurations.
- **Application management:** Deploy, update, and restrict applications based on organisational needs.
- **Remote access and control:** Remotely wipe or lock devices in case of loss or theft.
- **Security enforcement:** Enforce password policies, data encryption, and other security measures.

UNIT 2

Organisational Security in Mobile Computing Era

2. Mobile Device Policy: A clear and comprehensive mobile device policy outlines acceptable usage guidelines, security requirements, and employee responsibilities. The policy should address:

- **Device usage:** Define permitted and prohibited activities on mobile devices.
- **Data security:** Specify data protection measures and encryption protocols.
- **App installation:** Establish guidelines for installing and using applications.
- **BYOD (Bring Your Own Device) Guidelines:** Set rules for personal devices used for work purposes.
- **Employee training and awareness:** Educate employees on the policy and its implications.

Faculty: VIKRAM SHARMA
Vikram1532018@gmail.com

UNIT 2

Organisational Security in Mobile Computing Era

3. Mobile Threat Defense (MTD) Solutions: MTD software provides real-time protection against mobile threats, such as malware, phishing attacks, and malicious websites. Key features of MTD include:

- **Threat detection and prevention:** Block malicious applications, websites, and phishing attempts.
- **Vulnerability assessment:** Identify and remediate vulnerabilities in mobile devices and applications.
- **Threat intelligence:** Leverage real-time threat intelligence to stay ahead of emerging threats.
- **Data loss prevention (DLP):** Prevent sensitive data from leaving the organization through mobile devices.

UNIT 2

Organisational Security in Mobile Computing Era

4. Secure Mobile Network Connectivity: Organizations should implement secure network access methods for mobile devices, such as:

- **Virtual Private Networks (VPNs):** Encrypt data transmission over public Wi-Fi networks.
- **Mobile Device Management (MDM) integrated VPNs:** Integrate VPN capabilities into MDM solutions for centralized control.
- **Zero Trust Network Access (ZTNA):** Continuously authenticate and verify user identities before granting access to network resources.

UNIT 2

Organisational Security in Mobile Computing Era

5. Mobile Device Security Awareness: Educating employees about mobile security risks and best practices is crucial for preventing human error. Regular training sessions should cover topics such as:

- Identifying and avoiding phishing attacks
- Strong password practices
- Secure app installation and usage
- Reporting suspicious activity

6. Mobile Device Productivity Optimization: Organisations should address mobile device productivity issues to ensure optimal employee performance:

- Optimise applications for mobile usage
- Promote mobile-friendly work practices

Faculty: VIKRAM SHARMA
Vikram1532018@gmail.com