# Mobile and Network Security

# Cyber Security

## Third Stage

**Assistant Lecturer: Anfal mahmood ahmed**

# Lecture 1

- **Mobile security definition**
- **The importance of mobile security**
- **Components of mobile security**
- **The challenges of mobile security**

## Mobile security definition

Mobile security is the strategy, infrastructure, and software used to protect any device that travels with users, including smartphones, tablets, and laptops. Cybersecurity for mobile devices includes protecting data on the local device and the device-connected endpoints and networking equipment. As mobile devices continue to be a user preference over desktops, they will be bigger targets for attackers.

The goal of mobile security is to ensure the confidentiality, integrity and availability of data stored or transmitted by mobile devices. Mobile security is typically part of an organization's comprehensive security strategy.

## The importance of mobile security

As more users travel and work from home, mobile devices have become increasingly more integrated into their everyday lives, including corporate employees. Internet browsing activity used to be limited to desktops, and employees that traveled were the only ones with laptops. Now, mobile devices are the preferred way to browse the internet, and traffic from these devices has become the dominant form of web browsing over desktops.

Mobile devices have a much bigger attack surface than desktops, making them a more significant threat to corporate security. A desktop is immobile with threats mainly from outside attackers, but mobile devices are vulnerable to physical and virtual attacks. Users carry mobile devices with them wherever they go, so administrators must worry about more physical attacks (e.g., theft and loss) and virtual threats from third-party applications and Wi-Fi hotspots (e.g., man-in-the-middle attacks). Stationary desktops don't move from the corporate network, making it easier for administrators to control network and endpoint security. With mobile devices, users can root them, add any app, and physically lose them.

For many of these reasons and more, corporations have a lot more overhead when creating strategies surrounding mobile devices. Even with the overhead, it's a critical part of cybersecurity as mobile devices pose significant threats to data integrity.

## Mobile security is important for the following reasons:

- Protects sensitive data. Mobile devices contain a large amount of personal data and sensitive information, such as contact lists, emails, passwords and financial data. It's imperative that mobile security protects this data from illegal access and potential misuse.

- Prevents data breaches. Cybercriminals are increasingly targeting mobile devices as potential entry points for illegal access to corporate networks and sensitive data. Setting up comprehensive mobile security measures helps prevent data breaches and the potential financial and reputational damage they can cause.
- Mitigates mobile-specific attacks. Mobile devices are vulnerable to specific security threats, such as malware, phishing schemes, vishing attacks, SIM swap attacks and network vulnerabilities. Mobile security helps protect data integrity and confidentiality by recognizing and minimizing threats specific to mobile devices.
- Protects business assets. Mobile devices are frequently used in the workplace to access business apps, sensitive data and confidential information. Securing mobile devices protects these valuable company assets from illegal access or compromise.
- Ensures regulatory compliance. Many companies must ensure they follow specific regulations and compliance regarding the security of sensitive data. Businesses that use mobile security can follow these requirements while avoiding financial and legal penalties.

- Provides user privacy and trust. When using mobile apps and services, users anticipate that their personal information will be secure. By giving mobile security priority, businesses can win over the trust of their customers and show that they're committed to protecting their privacy.

## Components of mobile security

Organizations that use mobile devices have several options to protect them from attackers. Components in mobile security can be used to define cybersecurity strategies surrounding mobile devices. In addition to the infrastructure added to corporate strategy, it's also important to create BYOD and mobile device policies that instruct users what can and cannot be installed on the device.

The following components will help any organization protect from attacks directed towards mobile devices:

- **Penetration scanners:** Automated scanning services can be used to find vulnerabilities in endpoints. While this is not the only cybersecurity that should be used on endpoints, it's the first step in finding authentication and authorization issues that could be used to compromise data.
- **Virtual Private Network (VPN):** Users connecting to the network from a remote location should always use VPN. VPN services

and always on VPN alternatives installed on a mobile device will encrypt data from the device to the endpoint or from the device to the internal network. Plenty of third-party services are set up specifically for protecting corporate traffic from a mobile device to the internal network.

- **Auditing and device control:** While administrators can't remote control a smartphone or tablet, they can require users to install remote wiping capabilities and tracking services. GPS can be used to locate a stolen device, and remote wiping software will remove all critical data should it be stolen.
- **Email security:** Phishing is one of the biggest threats to all organizations. Email services are usually added to a mobile device so that users can obtain their email messages. Any phishing messages could target mobile devices with malicious links or attachments. Email filters should block messages that contain suspicious links and attachments.

## The challenges of mobile security

Due to the evolving nature of technology and the widespread use of mobile technology, mobile devices and communications face the following security challenges:

- **Diverse ecosystem.** One of the biggest challenges to mobile device security is the sheer variety of devices that employees potentially

use. There are countless makes and models of smartphones, tablets and other mobile devices. MDM software generally supports the more popular devices and the latest mobile OSes, but not all security policy settings work on all devices.

- **Evolving threats.** Another challenge to mobile device security is the constantly evolving threat landscape. At one time, there were relatively few mobile threats for organizations to worry about. As devices became more widely adopted, however, cybercriminals began increasingly targeting mobile platforms. Hackers are always coming up with new techniques to exploit vulnerabilities in mobile devices and applications. They often use malware, phishing or social engineering attacks to gain unauthorized access to sensitive information.
- **Bring your own device (BYOD).** Many organizations practice BYOD and let employees use their personal devices for work, creating a challenge for IT to secure a mix of devices with varying security postures. Managing and securing these diverse devices can be complex.
- **Data leakage.** Data leakage and disclosure of sensitive information from mobile devices can occur from a variety of sources, including misplaced or stolen devices, unsecured wireless networks and illegal access to cloud storage.

- **Human factor.** Users are frequently the weakest link in mobile security. Lack of awareness, bad password practices and vulnerability to phishing attacks all contribute to security flaws.
- **Internet of things (IoT) integration.** The integration of mobile devices with IoT can create new security challenges because the interconnection of devices increases the attack surface, necessitating complex security measures.
- **App store vulnerabilities.** Malicious apps can sometimes get past security measures and into authorized app marketplaces by using techniques such as versioning and disguising themselves as harmless beta versions. This can cause users to inadvertently download and install harmful applications, exposing their mobile devices to potential security threats.