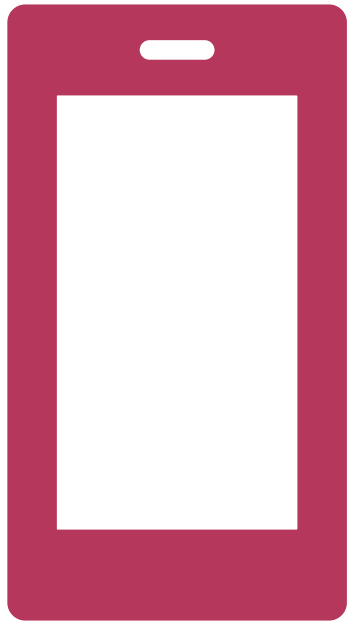
Mobile Cybersecurity

Jordan Patterson

An overview of Mobile Cybersecurity

2024

What is Mobile Cybersecurity?



Mobile Cybersecurity refers to the protection of mobile devices, such as smartphones, tablets, and laptops, as well as the networks they connect to, from various types of cyber threats and vulnerabilities.

The key components of Mobile Cybersecurity are:

- Device Security
- Application Security
- Network Security
- Data Protection
- User Education
- Threat Detection and Response

Mobile Device Management (MDM)

Mobile Device Management platforms are one of the main ways companies uphold Mobile Cybersecurity in the workplace. They are used to enforce policies on mobile devices. These policies may include:

- Text/Call Restrictions and Encrypted Messaging
- Lock Screen Code Requirements
- Mandatory OS and App Updates
- Geofencing / Location Restrictions
- AI/Digital Assistant and Account Restrictions
- Application Restrictions (Restricted and Mandatory apps)
- Data Privacy / Data Loss prevention
- Device Theft / Loss Prevention and Protection

Popular MDM Platforms

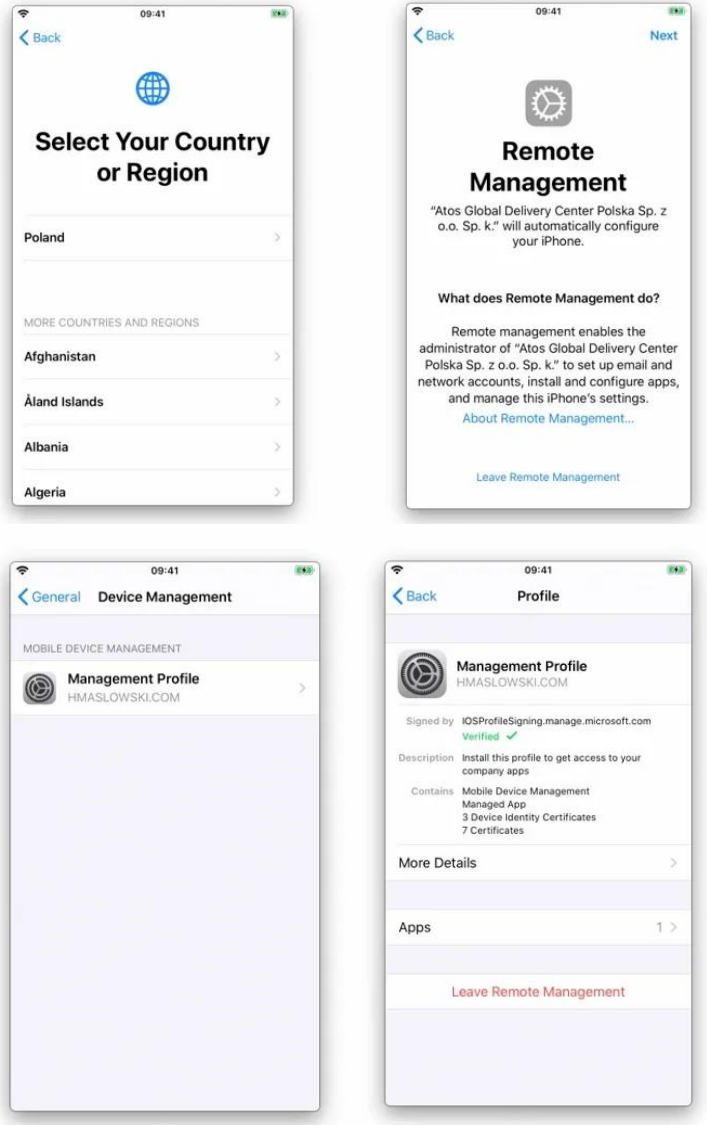
Some common and popular MDM platforms that you may see upon entering the workplace are:

- Microsoft Intune
- Cisco Meraki
- IBM Maas360
- Airwatch by VMWare
- ManageEngine Mobile Device Manager Plus

How is a mobile device added to an MDM?

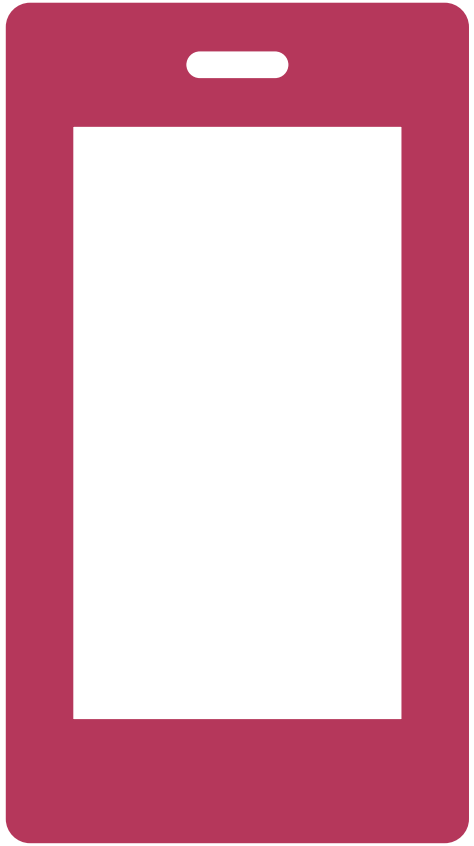
Mobile devices are typically added to an MDM using something called a “Management Profile”. Management profiles can be installed on iOS, Android, Windows, and MacOS devices.

Once added to the MDM, during the mobile device’s setup the management profile will be installed. Once it is installed, the previously mentioned polices will be applied.



What else can we do to ensure that Mobile Cybersecurity is upheld?

- Harden our networks to ensure that data being sent to and from our devices is transmitted securely.
- Avoid public Wi-Fi Networks.
- Ensure the adequate review of any in-house created applications before deployment to prevent the introduction of vulnerabilities.
- Avoid keeping sensitive data stored locally on-device and opt for secure cloud storage instead.
- Provide awareness training to staff regarding phishing / smishing.
- Mandatory OS updates
- Only install applications from trusted sources
- Use a security app such as Lookout for work or ESET



References

- What Is Mobile Security? Definition & Best Practices – Forbes Advisor
- The Best Android Antivirus for 2024 | PCMag
- The Best Mobile Device Management (MDM) Solutions | PCMag
- What Is Mobile Security? Benefits & Threats | Proofpoint US
- What is Mobile Security in Cyber Security? – GeeksforGeeks
- Cyber Security Consumer Tip Sheet: Mobile devices | MediaSmarts
- 9 top mobile security threats and how you can avoid them | ZDNET