WHY DO I NEED MOBILE DEVICE SECURITY?

Mobile Device Security refers to the measures designed to protect sensitive information stored on and transmitted by laptops, smartphones, tablets, wearables, and other portable devices. At the root of mobile device security is the goal of keeping unauthorized users from accessing the enterprise network. It is one aspect of a complete enterprise security plan.

WHY IS MOBILE DEVICE SECURITY IMPORTANT?

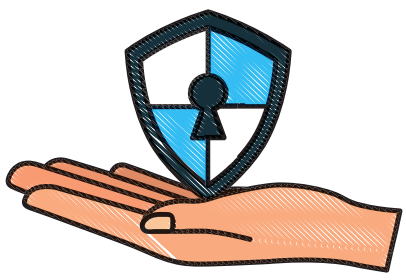
With more than half of business PCs now mobile, portable devices present distinct challenges to network security, which must account for all of the locations and uses that employees require of the company network.

Potential threats to devices include malicious mobile apps, phishing scams, data leakage, spyware, and unsecure Wi-Fi networks. On top of that, enterprises have to account for the possibility of an employee losing a mobile device or the device being stolen. To avoid a security breach, companies should take clear, preventative steps to reduce the risk.

WHAT ARE THE BENEFITS OF MOBILE DEVICE SECURITY?

Mobile device security, or mobile device management, provides the following:

- Regulatory compliance
- Security policy enforcement
- Support of “bring your own device” (BYOD)
- Remote control of device updates
- Application control
- Automated device registration
- Data backup
- Above all, mobile device security protects an enterprise from unknown or malicious outsiders being able to access sensitive company data.



Davichi