

# MOBILE DEVICE SECURITY

at Stanford



**DO YOU USE YOUR PERSONAL MOBILE DEVICE FOR ANY WORK ACTIVITIES?**



**DON'T FORGET! THIS INCLUDES COMMUNICATIONS - LIKE EMAIL, SLACK, OR TEAMS.**

If so, Stanford has important security tools for you to use - for your own safety, and for the university's protection.

**YES**

## **! USING MOBILE DEVICE MANAGEMENT IS REQUIRED.**

If you do any Stanford work on your personal mobile device, such as checking email, you **must have** Mobile Device Management (MDM) active.



**IT'S EASY!  
FOLLOW THE STEPS AT  
[MDM.STANFORD.EDU](https://mdm.stanford.edu)**

At [mdm.stanford.edu](https://mdm.stanford.edu), you'll find instructions for activating MDM for **iOS** and **Android** devices.

## **3 BENEFITS OF SECURING YOUR MOBILE DEVICE WITH MDM:**

MDM applies a bundle of settings that enhance security across multiple Stanford services that you might access on your device, like email, calendar, and VPN. MDM gives you:

**1**

**CONVENIENT ENHANCED PROTECTION**

**2**

**SECURE ACCESS TO LOW, MODERATE, AND HIGH RISK DATA**

**3**

**SELF-SERVICE OPTIONS FOR SECURITY**