


# How to talk to patrons about: *Securing A Mobile Device*


- Your phone likely has a lot of sensitive information on it (email, banking apps, etc.) so you want to make sure that strangers can't access it.
- Make sure you lock the phone through a PIN, fingerprint, or Face ID. Most phones let you make the PIN longer (4 digits might be the default, so you might want to increase to 6 or 8 digits).
- See if you can add PINs to your most sensitive accounts (e.g., banking apps). This way, even if someone gets access to your phone, they shouldn't be able to access everything.







*"Your phone probably has more sensitive information on it than any other device you own, so you want to make sure you protect that information!"*



## Securing Your Mobile Device

Your cell phone contains a lot of sensitive information in your emails, text messages, and apps. These are some tips to make sure your data is protected.



-  Whenever possible, connect to secure WiFi.
-  Password protect your phone! Use a PIN, fingerprint, or face ID to prevent random people from accessing your phone.
-  Regularly update your phone's operating system (OS).
-  Only download apps from authorized app stores (e.g., Google Play, Apple's App Store).
-  Turn off location services unless the app needs your location to work (e.g., Google Maps, Uber, Lyft).
-  Add passwords to apps that contain sensitive information like banks.

For more information, visit <https://safedata.umd.edu>