UNIVERSITY
OF MIAMI

Mobile Device Security Configuration FAQ

Mobile Device Security Facts

1. What mobile device security settings are being enforced?
   Response: 1) Device access PIN, 2) Idle-timeout, 3) Tamper wipe, and 4) Remote wipe

2. What is a device access PIN?
   Response: A device access PIN controls access to your mobile device and safeguards data stored on it. Once enforced, you will be prompted to enter a four digit password before being allowed access.

3. What is idle-timeout?
   Response: When your mobile is not used for 5 or more minutes, the device will automatically lock and require the device access PIN before access is allowed.

4. What is tamper wipe?
   Response: Tamper wipe is a proactive protection mechanism that will erase all data and applications on the device after a predetermined number of invalid device access PIN entries. UM has selected a value of 10. Therefore, after 10 unsuccessful device access PIN entries, all data and applications on the mobile will be erased.

5. What can I do to protect my data and applications from tamper wipe?
   Response: Applications purchased from an authorized marketplace such as iTunes or Google will always be available for you to download as needed and do not require additional protections. In order to protect data (contacts, pictures, etc.) it's important to regularly backup your device.

   - For detailed information regarding backing up your iOS based devices please click here.
   - For detailed information on backing up your Android please click here.
   - For detailed information on backing up your Windows Mobile please click here.

6. What is remote wipe?
   Response: Remote wipe is a reactive protection mechanism that will allow an authorized administrator at the University of Miami to remotely delete of all data and applications, should the device be reported lost or stolen. Unlike tamper wipe, that automatically occurs after 10 invalid device access PIN entries, remote wipe must be requested by the device owner and performed by an authorized system administrator.

7. How may a user request a remote wipe?

Response: Time is of the essence and therefore as soon as you realize your device is lost or stolen, immediately contact your respective support service desk as follows:

- Coral Gables Campus: (305) 284-6565
- Medical Campus: (305) 243-5999, Option #1

8. Will devices that are already configured with a device access PIN be affected?
Response: iOS devices that are configured with a device access PIN will **not** be affected. Android devices that are configured with a **pattern** device access PIN will be required to use a numeric PIN instead. To avoid device access issues, users are encouraged to switch to a numeric PIN **BEFORE** the security measures are enforced.

   - For assistance establishing a device access PIN click here.

9. Will I be prompted to reset my device access PIN if I already have one configured?
Response: You will not be prompted to reset your device access PIN at any time. Android users though, leveraging a pattern for device access are encouraged to switch to a numeric PIN **BEFORE** the security measures are enforced.

   - For assistance establishing a device access PIN click here.

10. After the security measures are enforced, when and how may I change my password?
Response: Once the security measures are enforced you may change your password at any time, as often as you'd like.

    - For assistance establishing a device access PIN click here.

11. Are there other security measures that I should consider?
Response: Individuals are encouraged to limit the number of email that is downloaded to their mobile device at any given time. If the device where to become lost or stolen this would minimize data exposure.

    - For assistance minimizing the amount of email on iOS devices refer to the iOS Q&A section.

    - For assistance minimizing the amount of email on Android devices refer to the Android Q&A section.

12. ?
Response:

    - For assistance minimizing the amount of email on Android devices refer to the Android Q&A section.

    -

UNIVERSITY
OF MIAMI

iOS Q&A

1. How may I limit the amount of email that is downloaded to my iOS device?

    - Tap *Settings* on the iPhone *Home* screen.
    - Select *Mail, Contacts, Calendars*.
    - Tap the desired Exchange account under *Accounts*.
    - Now tap *Mail Days to Sync*.

- Pick how many recent days' mail you want to be sent to iPhone Mail automatically.
    - o Choose *No Limit* to synchronize all mail.
    - o Note that there is no way to see or search messages older than the synchronization limit.

Android Q&A

1. May I continue to use a pattern as a devices PIN?
   Response: No. Once the security measures are enforced you will be required to use a numeric PIN.

    - For assistance establishing a device access PIN click here.

2. What if I fail to switch from a pattern to numeric PIN before the security measures are enforced?
   Response: Certain Android devices will prompt the user to change from pattern to numeric PIN but other devices will not prompt and will simply stop synchronizing email. If your device stops synchronizing email, you are encouraged to perform the following:
    - Remove the exchange account from the device
    - Configure a numeric access pin
    - Re-configure exchange access to your University account

    - For assistance establ 

a device access PIN click here.
    - For assistance config your exchange account refer to (link to assistance with configuring access for Android)

3. If your Android device stops synching email after the security measures are enforced what should you do?
   Response: Remove the exchange account entirely and put it back. Then It prompted to change from pattern to PIN lock.

4. How may I limit the amount of email that is downloaded to my Android device?

    - Select the Mail icon
    - Press Menu
    - Select More
    - Select Account List
    - Select the relevant account you'd like to limit email
    - Select Settings
    - Select Send and Receive
    - Select Download options
    - Determine number of days you'd like to have downloaded to your device