**Exercise 2: Lockdown Guides**

**Intro:** This section aims to teach participants how they can mitigate against some risks just by familiarizing themselves with the components of the phone and adjusting the built-in settings. During the activity, everyone creates a password for their SIM and device.

**Timing: 30 minutes-1 hour**

**Equipment Needed:**

* Participants’ phones, including any manuals, software, and cables that came with the phone, which they should bring to all hands-on sessions.
* Have printouts of [SaferMobile lockdown guides](http://www.google.com/url?q=http%3A%2F%2Fmobileactive.org%2Fsafermobile-lockdown&sa=D&sntz=1&usg=AFQjCNHQ2Gdw7UIxnjm1mlxzwbJcVgAEqQ) for various devices to hand out to participants. (As part of training prep, use pre-training questionnaire to see how many have guides for various phones and have a few extra copies for each device type.)

**Content Outline and Main Topics:**

1. **Discussion:** Threats to your phone and the information on it.
2. **Exercise/Instruction:** Lock it down!
   1. Lock your phone.
   2. Use a strong password.
   3. Avoid the most common passcodes.
   4. Be aware of widely available code hacks.
   5. Examples of easily accessible master code hacks.
3. **Homework:** Other lockdown modifications

**Objectives/Expected Outcomes:**

* Participants will have one of the most useful tools available for their devices: passcodes to lock down their phones.
* They will also learn how to avoid the most common passcodes, and understand that locking your mobile doesn’t completely prevent access.
* If interested and if time allows, participants can walk through using additional settings described in the lockdown guides.

**Additional Resources for Trainers and Participants:**

[SaferMobile 1-pager lockdown guides](http://mobileactive.org/safermobile-lockdown)

[SaferMobile Vulnerabilities Module](https://docs.google.com/a/mobileactive.org/document/d/1LWGal0gbDzGKlybs3H5-d0ksfHSnVksX02SunKLWYfg/edit?authkey=CNSI4dMH&hl=en_US)

[WSJ Voicemail lockdown guide](http://blogs.wsj.com/digits/2011/07/11/how-to-make-your-mobile-phone-a-bit-safer/)

##### Content

**1. Discussion:** Threats to your phone and the information on it.

* What are the risks you are most concerned about with your mobile security?
* Do you face **device threats** such as physical threat of confiscation or destruction?
* Is your service at risk of interruption or shutdown?
* Do you face **information threats** (from Assessment and Module 2),
  + Listening, modifying, spoofing, identifying, interrupting.
* Do you face **human network threats** (such as other people who have access to your phone or with whom you communicate)?

**2. Exercise/Instruction:** Lock it down!

Have participants group by phone type. Phone settings are likely to be similar among phones made by the same manufacturer, so in these groups, participants can assist each other and you can instruct more efficiently.

Lead groups through the lockdown tactics below, pausing to let everyone try this on their own phone. When introducing a tactic, ask if anyone does this, and if so, ask them to explain why.

2a. **Lock your phone**

* Risks mitigated against:
  + unauthorized use of your device or service.
  + unauthorized access to your device, account, and data.
* Creating a lock passcode for your phone is a good “frontline” defense against having the information on your phone quickly read by third parties when you leave your phone unattended. If your phone is stolen or confiscated, it will make a third party work harder to access your phone information, but unfortunately, eventual access isn’t impossible, especially if they have access to advanced resources.
* You can lock both your SIM card and your device
  + Device locking prevents use of any feature of your device without the access code. This is commonly done by setting a PIN, and should be done on all phones.
  + SIM blacklisting prevents use of your SIM card, and should be done as soon as your phone is lost or stolen.
* [Mobile Phone Lock-Gown Guides Online](http://www.mobileactive.org/safermobile-lockdown)
* Some phones (usually smartphones) have remote lock via SMS or remote wipe functions. If your phone has this functionality, learn how to use it. For more information see MobileActive’s guide to Backup, Data Deletion and Remote Wipe apps //LINK//.
* Note that **locking isn’t an ultimate failsafe for protecting your data**. Some password systems are relatively easy to bypass, while others require the advanced data retrieval/reconstruction capabilities of law enforcement. Locking will deter a casual observer, and buy you time to block the phone or wipe it remotely.
* There are usually several options for how your phone locks (i.e. stops accepting input), especially for smartphones. Encourage participants to set their phones to autolock after the briefest amount of time.

2b. **Use a strong password.**

A strong password is one that is:

* Not a single dictionary word. Consider using a short phrase.
* Not easily guessed by someone with access to your personal details. For example, don’t use your name, the name of a family member, your birth date, address, or hometown.
* Ideally, contains letters and numbers.
* Not re-used for other accounts on different websites.

2c. **Avoid the most common passcodes.**

When users have created their passcodes, ask who has created the most common ones (“Did any of you use 1234? How about 1111?”). List out the most commonly used and created passcodes on phones and advise users **not** to use them. Also remind them of set default passcodes on most phones (also 0000, 1234, etc.).

[For iPhones](http://www.eweek.com/c/a/Security/Top-10-PIN-Codes-Picked-by-iPhone-Users-637446/?kc=EWKTS06152011AB) (and probably most 4-digit passcodes) the most common codes found in a study were: 1234, 0000, 2580, 1111, 5555, 5683, 0852, 2222, 1212 and 1998.

2d. **Be aware of widely available code hacks.**

Because of the need for phone manufacturers, retailers, and thieves/resellers to be able to access phones when a passcode is unknown or forgotten by the user, there are a number of ways to bypass a user’s passcode with various codes created by the handset manufacturer, using only the IMEI for a handset. **We recommend that you scratch out or remove the IMEI on your phone in order to make these hacks more difficult for third parties.** That way, if your phone is locked when in the hands of a third party, they cannot enter the code for IMEI to have it displayed on the screen. Neither can they simply look at where it is physically posted on the device (usually on the phone underneath the battery).

2e. **Examples of easily accessible master code hacks.**

*Nokia:* With a phone’s 15-digit IMEI (obtainable by entering \*#06# on the standby screen of your device, or on the phone itself, usually underneath the battery), you can enter your IMEI on [this site](http://www.nokialockcode.com/calculate.php) to obtain your phone’s “master code” to override any passcode you may have for your phone. This is a great tool in case you forget your passcode, but it’s a dangerous one for a malicious third party who hacks your passcode to access the data on your phone.

**3. Homework:** Other lockdown modifications

For each lockdown action, ask what risks these tactics will mitigate. As time allows, choose tactics that participants find most useful and lead them through setting these or assign as homework for the night and compare the following day.

* Set a password for your voicemail. Remember, no common codes!
* Make sure you know how to silence your ringer.
* Have a piece of tape handy to cover your phone’s camera in instances where you are concerned about surveillance.
* Do you know how to clear your messages and call log?
* Can you find a setting to limit the number of messages saved on the phone, and prevent outgoing messages being saved?
* WiFi/Bluetooth
  + Do you use these features? Turn off these features if and when not using. Set to only be in use if connecting to trusted networks.