**2.1 What is Information Security for Mobiles?**

**Intro:** This section introduces participants to concepts of security. It includes discussions to help participants understand mobile security as one part of information security and engages participants in a discussion on what is and is not sensitive data in their own work.

**Timing:** 1 hour

**Equipment Needed:**

* Whiteboard or large sheets of paper and markers to list out participant’s contributions and take notes.

**Content Outline and Main topics:**

1. **Instruction (20 minutes)**: Overview of information security and introduction to mobile security.
2. **Discussion (30 minutes):** Share experiences of security breaches and measures taken by participants.
3. **Discussion/Instruction (15 minutes):** Mobile phones are never entirely safe/secure.

**Objectives/Expected Outcomes:**

* Will help participants begin to distinguish, understand, and identify threats, vulnerabilities, and risk.
* Participants will get a sense of shared risks in their own environment via shared stories and will learn how others have mitigated risk.
* Participants will begin to build skills for risk assessments and security planning.

**Additional Resources for Trainers and Participants:**

[Guide to Mobile Security Risk Assessment](http://mobileactive.org/risk-assessment)

[Mobile Security Risks: A Primer](http://www.mobileactive.org/howtos/mobile-security-risks)

<http://www.mobileactive.org/howtos/mobile-security-risks>

**Content**

**1. Instruction (20 minutes)**: Overview of information security and introduction to mobile security.

* Conduct a brief discussion about what security means to participants in the context of information. Some tasks to prompt discussion:
  + Define security: of yourself, of your possessions, and of your communications.
  + Define information. What forms can it take? How is it communicated? For example, information could be data stored on a phone or PC, physical documents, or the contents of a conversation with someone, communicated in person, via email, phone, or mass media.
  + Define information security. How do you store and communicate information securely?
  + Discuss what tools you currently use to increase the security of your communications. This can be for online security, such as secure Gmail, mobile apps, or rules you and your contacts follow for phone use or face-to-face communication.
* With a group that already does a lot of work online it is likely that concepts and principles such as “privacy” and “anonymity,” and tools such as “encryption” and “secure browsing/SSL” will come up. With groups that do not have this experience, are there codes used to communicate certain things? How do you handle sensitive information? Use this discussion to gauge your group’s experience with security, and to point out that security is about policies and procedures as much as it is about technologies and tools.
* Try to highlight that in many ways, the word “security” is not terribly helpful because it is so vague, context-specific, and means different things to all of us.
* Begin a discussion about how information is defined as sensitive. It is the perceived value or impact this information can have that gives it significance. Some data is public and widely known. Other data isn’t public, but it wouldn’t have much effect if it were known. Other information, for example the name of a confidential source for a high-profile article, or your bank account card PIN number, can be extremely sensitive and put people and things we value at risk if they fall into the wrong hands.
* Information is now being communicated and shared in many forms and through many channels. Our tools are evolving so rapidly, we are struggling to keep up with the communication itself, let alone who or how it may be lost or seen by others. Remember, Youtube has only been around since 2005!
* Information security means systematically working to increase awareness of risks to sensitive information by mapping out:
  + What information is important.
  + How it is vulnerable in all the ways we now communicate and transmit it.
  + What or who may put that information “at risk.”
  + How we can help make that information more secure, or *mitigate* that risk.
* Remember that people and communications do not exist in isolation. The information you send and receive goes over the air, through online networks, and is stored in a wide variety of devices and virtual spaces.
  + The information you share and receive from others is probably also passing through and stored in *their* multiple networks, systems, and devices.
  + Because of how we communicate, share, and store information throughout our networks, we now may have access to manage information that is extremely sensitive to *others.* Therefore we must constantly keep in mind that our information security and even our personal security is highly interdependent across multiple systems and channels of communications, but also throughout and across vast human networks as well.
  + Because of the nature of the work that many activists, journalists, and rights defenders do, we must adjust our understanding of information security to match this increasing level of responsibility to others who put their trust in us to manage information that may be sensitive in their eyes.
  + **Optional discussion questions for participants:** How have they adjusted their understanding, approach, and behaviors towards information security over the past 5-10 years as communications have changed so rapidly and dramatically? How can we continue to adjust our habits and behaviors?
* The mobile phone is becoming a central hub for information. Consider what passes through your mobile: voice, email, online activities, media and content creation, and more. So when we discuss mobile security, we’re discussing a “point” in the network that is part of a vast web of people and nodes of information and data. Mobile security is by no means the only thing at play, but we have to remember how it is a point in a larger web of security concerns and issues and think about how management of mobile security can affect other parts of this web of people and information systems**.**

**2. Discussion (30-45 minutes):** Share experiences of security breaches and measures taken by participants.

Begin this section by asking participants for stories of when they thought their security had been compromised and what steps they took to address those situations. These can be stories of online, computer, mobile, or physical security breaches.

The goal here is to get participants sharing stories in a supportive environment. Rather than feeling bad about past mistakes, encourage them to think about what they learned from these experiences, and how they might apply this to thinking systemically about security risks and responses. It is sometimes helpful for the trainer(s) to kick off this exercise with their own story or a situation they observed directly.

Keep in mind that participants may be embarrassed or self-conscious of perceived security failures. Try to create an supportive environment of learning and sharing so individuals do not feel “singled out” for past mistakes. There also may not *be* any (or many) stories to share, or participants may start to ask a number of questions as to whether or not a particular incident was a security breach. Put these in the grab-bag space on your whiteboard or chalkboard to use as cases to deconstruct later under the assessment section when participants have gained better risk assessment and incident identification skills further in the training(s).

**Questions to ask:**

* When has your security been compromised and what steps did you take to address the situation?
  + Examples: Has your phone ever been taken? Have you ever had your email hacked? Has anyone ever gained access to your online accounts (banking, social media, etc.)? Have you ever needed to change the locks at your home or workplace?
* What did you do?
* What resources did you have with which to respond?
* What do you wish you would have known before that experience occurred?
* How have you used what you learned in that experience since then?
* What questions do you still have? There will probably be a list of questions as to what could have been or caused a security breach and what they “should have done.” Note these and table them in a side list on the board.
* Has anyone else had the same experience? In many communities, shared security threats and similar anecdotes may arise during this exercise. As a trainer, take note of the most common and try to keep a sustained low level of focus on them. You may make them an example centerpiece throughout your training, but at the very least make sure participants will have the tools to understand and address them after the entire training is complete.

**Things to highlight:**

* What participants have learned from their experiences.
* How responses can be creative, but also systematic (e.g. creating a policy after an incident to ensure that it doesn’t happen again).
* The need to depend on human networks to help us identify and address security threats.
* How security breaches can affect a number of people at once, especially if confidential or identifying information on a network of individuals is compromised.
* How challenging information security is (remind participants that large companies like Google and Sony struggle to keep their systems secure and their information private).
* How complex and inter-related our communications are now, with the large number of services, devices, and channels of communications we now use on a daily basis in our personal and professional lives.

**3. Discussion/Instruction (15 minutes):** Mobile phones are never entirely safe or secure.

Remind participants that mobiles, like any other technology, are never “completely” secure. However, through a combination of increased awareness, safer behaviors, tactics, and tools, participants can make their mobile usage safer. The motto here is: **The more you know, the more you can make smart choices regarding your mobile communications.**