**1.1 What Do You Use and Why?**

**Intro:** This session opens the discussion of mobiles in activism. It includes activities about mobile communication choices. Participants explore their choice of handset, operating system, mobile network operator (MNO), and use of particular apps, and how these factors are or should be influenced by security considerations. The session introduces, but does not discuss in detail, security considerations for particular handsets and operating systems. The activities also function as icebreakers, asking participants to learn how they and others in the group are using mobiles in their work.

**Timing:** 1.5-2 hours

**Equipment Needed:**

* Whiteboard or large sheets of paper and markers to list out participant’s contributions and to take notes.
* Enough physical space for participants to move into several groups.

**Content Outline and Main Topics:**

1. **Exercise (45 minutes):** How do you choose what you use? Participants will self-group by handset, operating system, network, and favorite apps. Trainer will lead a discussion among participants as to why they made those choices and why they prefer (or do not prefer) certain tools.
2. **Bridging Concept (15 minutes):** We already make many choices about our mobile phones. How can we make better choices in terms of security?
3. **Discussion/Instruction (30-45 minutes):** Making choices with security in mind.
   1. Operating Systems
   2. Favorite Apps
   3. Mobile Network Operators (MNOs)
4. **Exercise (30-45 minutes):** Security decision matrix.

**Objectives/Expected Outcomes:**

* Illustrate the range of factors that influence mobile decisions, from choosing handsets to MNOs to apps.
* Help participants integrate security considerations into their decision-making.
* Build connections and community among participants (e.g., participants will be able to share resources with each other.)

**Additional Resources for Participants:**

<https://safermobile.org>

**Content**

**1. Exercise (45 minutes):** How do you choose what you use?

Have participants group themselves by handset, operating system, network, and favorite apps. Depending on the group, this could be:

* Basic phones/feature phones/smart phones
* Basic and feature phones/Android/iPhone/Blackberry

To help participants get to know each other, let them find each other for the groups instead of directing the formation of groups (you can adjust the groups if some are very big or very small).

Ask groups to discuss why they made particular choices, then share in plenary. In addition to phone type, ask about handset type (are particular manufacturers favored, do participants like phones that look a certain way or have certain features), operating system, network, and favorite apps.

Note answers on the board or paper in a series of columns that note the values and logic associated with the decisions. Columns can include the following categories and sample responses:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| TOOL CHOICE | LIKE OR DISLIKE? WHY? | REASON FOR CHOICE | CHOICE RELATED TO SECURITY? HOW? | GOOD CHOICE IN TERMS OF SECURITY? |
| Android Phone | Yes, because of the apps. | Gift from Mom | No | No. (*But tool is good for security because you can run Guardian apps.*) |
| iPhone | Yes, because it’s awesome. But a target for theives. | It was cool | No | No. (*But can now make choices (apps) based on security.*) |
| Blackberry | Yes. | More secure (right?) | Yes | Yes and no. (*Blackberry and its services can be more secure, but it doesn’t guarantee security. But good that security was a consideration when choosing*) |
| *App: Bambuser* | Yes, because it’s a cool tool at an event. But it’s also slow sometimes. | *To stream live videos* | *No* | *Yes and no. (Live streaming can be tagged with identifying information that may increase your security risk. You can turn this feature off. But streaming to let people know where you are if you’re in danger can also assist your security.*  *Uploading media directly to Internet and not saving on your device ensures that your media will be shared even if you lose your device.)* |

Note that there is no right or wrong answer, and many decisions will be made based on happenstance (e.g., handset was a gift or a hand-me-down, an app is chosen because a friend uses it, etc.). In addition, many participants will be uncertain as to why they made or should make certain decisions, and many will not have security-related reasons why they made particular choices. Some choices (like the first example in the table above), will not have been made according to security concerns, but may end up being useful when considering security.

Keep in mind that this exercise is meant to help create an environment of sharing, while getting participants to think about what goes into decisions. At this point, there are no good or bad decisions.

How far you choose to take the discussion of security aspects at this stage is up to you. The italicized answers in the table above are possible results of a combination of class discussion and instruction by the trainer. For example, many participants will not be familiar with the vulnerabilities and “security unknowns” associated with Blackberry; the trainer can refer to examples in [Unit 3.1 The Separation of Phone and State](http://safermobile.org/module/3-1/) to explain that Blackberries do not guarantee security. This example illustrates that whereas the choice was made with security in mind, unfortunately Blackberry isn’t as completely secure as users may have been led to believe.

**2. Bridging Concept (15 minutes):** We already make many choices about our mobile phones. How can we make choices with security in mind?

Based on the preceding exercise (How do you choose what you use?), pull out themes of how participants (currently) make decisions related to mobiles. What were some examples of how participants made choices based on security? What were not? What are some good general guidelines for how they can make good choices to support safer mobile use in the future? Also discuss some of the challenges involved (cost, access, limited options, etc.)

**3. Discussion/Instruction (30-45 minutes):** Making choices with security in mind.

3a. **Operating systems (OSes)**

Discuss in plenary how participants’ mobile technology choices could include security considerations.

* Did you choose your OS or handset first?
* Why did you choose that handset? Do you like it? Why? What does it do that you like?
* Do you like your OS? Why? What does it do that you like? How is it different than other OS you’ve used or seen?
* Did you choose either your handset or OS to be safer in any way? If so, how do they help make your communications more secure?
* Are you aware of specific OS security issues, and if so, how do you mitigate them?
* Is one OS more secure than another?
  + Give brief overview of the security trade-offs for the various OSes. This section should be an overview only, which is tricky because the question covers a lot of ground: mobile software security is complex. One way to deal with this could be to respond to participants’ perceptions of the relative security of different OSes, but leaving detailed discussion until [2.3 Vulnerabilities.](http://www.google.com/url?q=https%3A%2F%2Fdocs.google.com%2Fdocument%2Fd%2F1LWGal0gbDzGKlybs3H5-d0ksfHSnVksX02SunKLWYfg%2Fedit%3Fauthkey%3DCNSI4dMH%26hl%3Den_US%26ndplr%3D1)
  + In general (but this may change depending on events, so please refer to SaferMobile site):
    - **Smartphones** can do things that aren’t possible with feature phones or basic phones, such as run apps and connect to WiFi. This means that they are vulnerable to a greater variety of threats, which exploit their advanced features. However, there are also many more security tools available for smartphones. To secure your smartphone, you need to be willing to dedicate time to learn about security tools.
    - **Blackberry** is sometimes associated with improved security, but this association stems mostly from the ability of corporations to lock down employees’ devices (to prevent installation of apps, for example) and run their own enterprise servers than from any tangible benefit to people who have non-corporate phones for personal use.
    - There are many benefits to **Android** that stem from the variety of apps that can be built and accessed. In particular, many security apps run on Android. If you want to use these apps, you’ll need an Android phone. Secondly, the operating system source code for Android is available, making it harder to hide malicious code at the operating system level. Conversely, the Android marketplace is not as ‘closed’ or controlled as the iPhone app store. There are increasingly more Android marketplaces other than the Android app store, and some apps with malicious code have been downloaded by users and discovered afterward. This is a reminder that whereas it is always recommended that users download apps from trusted (e.g., not pirated) sources, it is not a complete guarantee that apps will be safe. Secondly, with Android overtaking Symbian as the most popular smartphone OS, it will become an increasing target for mobile malware.
    - The **iPhone** iOS has drawbacks because it is a “closed” system, like all Apple products. At the operating system level, it is not possible for users or security researchers to review the code and look for what data is transmitted, for instance. The closed app store puts greater restrictions on what and how apps can be constructed, but it also means that the quality of the apps are more controlled. Apple also tightly controls and vets apps in its app store for security vulnerabilities, which reduces the risk to users. But, similar to Android, the iPhone is increasing in popularity and use, which makes it more vulnerable as a favorable target for malicious apps with malware.

3b**. Favorite Apps**

* Have participants discuss the apps that they currently use. Examples can include social networking apps such as Facebook, task apps, games, etc.
  + What apps do you use the most? Or your favourite apps? Describe what they do, how you use it, and how often you use it.
  + How did you choose it?
  + Why do you like it? Is it helpful for your work? Do you use it in your personal life, in your work, or both?
  + How did you find out about it? Where did you get it from?
  + Does the app make you more insecure in any way? Are there other apps you could use, or other ways to accomplish the same goal?

3c**. Mobile Network Operators (MNOs)**

*Note: this will vary by country. If you are leading a training with participants from a wide variety of countries, you may want to go around the room and ask each participant individually to describe their choices.*

* How did you choose your network?
  + Do you like it? Why? What does it do that you like? How is it different than other networks? Did you switch networks?
  + Did you choose it to be safer in any way? If so, how does it help make your communications more secure? Are you avoiding particular threats that you would be exposed to using other networks? For example, do you think other networks are less secure because they have frequent technical problems? Or because they are controlled by or have a close relationship with a repressive government?

**4. Exercise (30-45 minutes):** Security decision matrix.

Based on the preceding two sections, work with the participants to create a very basic decision matrix for choosing each of the following tools from a security standpoint. (Note: there will not be clear-cut answers to each of these.) In choosing tasks for which you should and should not use your phone, are some communications just too sensitive?

* Choosing a handset and operating system
* Choosing a network
* Choosing apps

**Finally, remind participants that there is no one way to be completely secure when using mobiles. However, we can become safer through examining the choices we make and the way we use the tools we choose.**