Mobile Ministry 9

Security: Understanding the Risks

TOPIC

Whether through movies or our own life experiences, many of us have ideas about some of the risks of using mobiles today. What can people really find out about you? Should you really carry a “burner phone”? Should you not use a mobile phone at all? These are all good questions to consider when we begin to think about being more active using our mobiles personally and for ministry.

OBJECTIVES

In this first of a two-part lesson, we will be looking at the risks of using mobile devices. By the end of this lesson, participants will be aware of the different types of risks and be equipped to evaluate how significant these risks are for them and those they serve.

PREREQUISITES

Completion of Mobile Ministry 1: Why Mobile Matters would be helpful but is not required for this lesson.

RESOURCES

Presentation

PowerPoint Presentation

Student Materials

Power Guide Handout

Preparation

The following are not required reading but, rather, links to materials that were used in the preparation of this lesson plan and which you, the trainer, might find of value if you have extra time and an interest in digging deeper into the subject

General Security- Overall

- Communicating with Others
- NICAR18: Digital Security Tip Sheet for Journalists
- Cybersecurity Report

General Security- Mobile

- Smartphone Security
- Why You Need New Mobile Security Best Practices for Business Travel
- Mobile Tips

Threat Recognition- General

- Assessing Your Risks
- What's Your ICT4D Cyber Threat Model?
- World Watch List
- Appendix 4: Religious Restrictions Index Scores by Region (the higher the score the worse the restrictions)
- How Tech Companies Mislead You Into Making Bad Privacy Choices

Threat Recognition- Mobile

- How Does My Mobile Phone Put Me at Risk?
- The top 5 mobile security threats
- The Problem with Mobile Phones
- 7 Shifty Ways Your Smartphone Is Violating Your Privacy

If you have any questions or suggestions for changes, please contact info@mobileministryforum.org.

TEACHING CONTENT

If possible, lead with a personal story that involves mobiles and security, such as a time you misplaced your phone or something that happened to you or someone you know when their phone was compromised. If you do not have a story, ask the class if anyone has ever misplaced their phone. If so, ask them to briefly describe what happened, how this made him/her feel, and what they learned from the experience.

1. Before we talk about the different kinds of risks, there are two disclaimers to keep in mind:
    a. There is no such thing as “secure” - only “more secure” and “less secure.” Perfect security isn’t possible. The goal in talking about this is to move you from wherever you are today to being more secure in your use of mobiles.
    b. Mobile security is just one part of the security puzzle. At a recent ministry conference on technology and media, security was taken so seriously that all participants had to leave their phones and computers in their room or have a special I.T. team disable features on the devices to safeguard against any personal risks. One day during the conference, after a coffee break, someone asked a question: “We understand the need for security and the risks of having our phones and computers with us. Thank you for doing everything you’ve done to secure them. However, we have hotel staff coming in and out of our meeting area. They can easily see who is here, possibly record things they see, or even hide a bug (listening device). Has anyone thought about these things?” Sometimes we get so anxious about digital security risks that we forget that there are many, many different ways that our security can be compromised.

So with those two disclaimers, let’s now talk about risks when using mobiles. We will not talk about solutions to these risks yet. That will happen in the next session.

2. Compromised Phone: Your phone can be compromised if it is stolen, lost, or confiscated. Our phones now contain so much valuable data – our contacts, photos, emails, banking info, etc. – that they are popular targets. It is very possible that authorities will confiscate your phone and seek to access your data if they have reason to suspect you of anything. This has happened to missionaries and local believers. Having a passcode is a great first step, but it is still possible that your passcode gets cracked or that you are forced to divulge it.

3. Data Interception: In general, just about anything being transmitted from your phone can be intercepted (captured between your phone and the person or service you are communicating with). This includes voice, text, and data (including app traffic). As an example, it has been reported that in Iran, all text messages are searched for certain keywords. Messages that are deemed offensive, critical of the government, etc. are automatically gathered/stored (and probably used to build a profile on the sender and recipient). While this sounds very scary – and it is - in general, you would need to be a person of high interest to the government for this to be a major issue. With that said, it is a very real issue, especially for data that may have low or no encryption such as voice calls, SMS texts and some e-mail.

4. Location Tracking: If you Google "location tracking", you might find yourself feeling a bit uneasy. All of those spy movies that show agents tracking the bad guys – well – that technology is real. A politician in Germany obtained phone logs from his cellular provider that provided all of the location tracking detail from his mobile phone. He used that to put together a map and make a video that detailed his movements for a 1-month period. Occasionally there were gaps – these were the times that he was on a plane traveling and had his phone turned off or in airplane mode. Location tracking can work in different ways…
    a. Many of us are now aware of geo-tagging. Since our phones have both cameras AND GPS (Sat-Nav) chips, location data can be easily captured & embedded in our photos. In fact, this typically happens by default unless we've disabled it.
    b. Many popular apps today encourage voluntary location sharing. Such apps allow us to "check in" when we've arrived at our destination so others know we are there. Some people regularly share their locations in social media posts (Facebook, Twitter, Instagram, etc.).
    c. The type of location tracking that is least known about is done by cellular providers. Mobile networks operate using a network of towers that carry cellular signals. As you move around town, or around the world, your phone is always making contact with the nearest cell tower so that it has service. Every time a tower is "pinged", it gets logged with the phone's unique identification number. Your location can also be determined when you connect to a particular internet wi-fi signal.
    d. There are also apps that can be installed on phones – with or without your knowledge – that can constantly communicate your location. Some parents use such apps to keep track of their children just in case

something happens to them, but it doesn't take our imaginations long to think of all of the ways such apps could be exploited.

There are wonderful applications for all of these location tracking services, but they can also pose obvious security risks. Consider how dangerous it might be for people to be able to track your movements, see patterns in your schedule, know the places you visit and when, know when you are at home or away, see when groups of people are meeting together, etc. If any of these possibilities concern you, then you will want to consider appropriate steps to minimize location tracking.

5. Social Media: Social Media presents a variety of potential risks that cannot be adequately addressed in this lesson, but it is important to consider this aspect of mobile security. Consider the various types of social tools that you use and do a Google search to learn about their specific security concerns. Just two specific risks associated with social media are (a) "guilty by association" - who you are friends with or follow on social media can tell others a great deal about you and may put you at risk even if you don't say or do anything that is troubling; and (b) facial recognition – technology gets more and more accurate at identifying people in photos using facial recognition. Even if you don't post anything about where you were at a certain time, if someone else posts a photo that includes you (or mentions you by name), that photo could identify you and allow the social tool to know more things about you.

6. When it comes to mobile security, one of the best ways to protect *ourselves* is to educate *others* – your friends, family, co-workers and others – about the risks. The more they practice good safety with their mobiles, the safer you will be also.

LEARNING ACTIVITIES

Discuss: Which of these types of mobile risks concerns you the most? Does God want us to take risks? If so, how much?

FOLLOW-UP REVIEW/ASSESSMENT

Finish the lesson by asking if anyone has any comments or questions. Feel free to say if you don't have the answer. No one has all of the answers! But if possible, see if you can help the person get their questions answered later.

In part two of this lesson, ask students if they have any new questions about this lesson.