



THE JOURNALIST SURVIVAL GUIDE





AN ANIMATED VIDEO GUIDE

Lesson 14

A guide to mobile security



Mobile Security Survival | Internet at Liberty 2012
@safermobile | www.safermobile.org

-  Understand how mobile phones work
-  Learn about mobile phone risk
-  Improve your mobile security
-  Know where to go for more

Mobile communications are far **less secure** than the Internet but are relied upon more by activists, organizers, and journalists.

Mobile technology is increasingly used as an **attack vector** by repressive regimes.

Even tech-savvy individuals are extremely underprepared to deal with new mobile threats. So, **how do we protect ourselves?**

Mobile Networks

How do they work?



The Network: SIM Card

The SIM card has a unique number - the **IMSI** - that is stored as a 64-bit field in the SIM inside the phone and is sent by the phone to the network.



The Network: Handset

Your handset has a unique number, the **IMEI**



The Network: Cell Tower

Cell towers relay information from your phone to the Mobile Network Operator (MNO)



The Network: Cell Towers

Cell towers “triangulate” your location and relay data to/from your phone



The Network: Transmitting Information



The Network:

Mobile Network Operators (MNOs):

- ✓ Sells you a **SIM card**
- ✓ Owns or leases **cell towers**
- ✓ Relays data to/from your **phone**
- ✓ Stores your **data** (call logs, SMSs, triangulation)
- ✓ Charges you

What is a **vulnerability**?

A weakness in the process of communicating with your mobile device that can be exploited by others.

Your phone holds lots of data about you:

- ✓ Contacts
- ✓ SMSs
- ✓ Pictures and Video
- ✓ Emails
- ✓ Account information

What Does an Adversary Know?

- ✓ **Where you are**
- ✓ **Who you are**
- ✓ **Who you talk to**
- ✓ **What you say**

Threats: Surveillance



A quick demo

Threat: Shutdown



Threat: SMS Filtering



Threat: Location Tracking

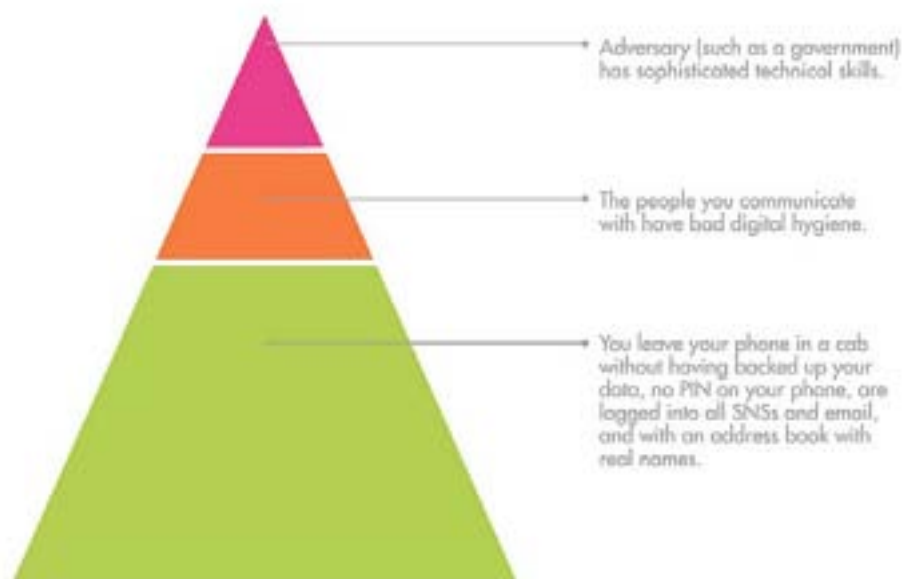


Risk

Risk = Probability of a **Threat**
Targeting a **Vulnerability**

Risk

Likelihood that someone will take advantage of Vulnerabilities



What do I do now??


Threat Mitigation

Threat Mitigation for mobile phones

Legend

 Don'ts




 Do's

 Smartphone specific
(any brand)

Threat: Shutdown



Shutdown Some Mitigation Tactics




If a network shutdown is possible, make sure you have alternate communications and coordinations plans.		Don't assume that phones will be working when you get to a protest
		Set up meeting places in advance in case of network
		shutdown Exchange land line numbers with your close network

Threat: You are identified





Case Study - Syria

The Syrian government has reportedly sentenced a citizen journalist to death after he gave a series of interviews to Al-Jazeera. Mohammed Abdelmawla al-Hariri was found guilty of "high treason and contacts with foreign parties".




Identification *Who are you ?*

<p>Make sure they cannot be linked to your Identity. All mobile actions and moves are traceable.</p>		Keep SIM anonymous (pay in cash, don't give personal details, change SIM often)
		Use foreign SIMs, but with caution.
		Don't give real name or address on phone or via SMS.



Identification *Who did you talk to ?*

<p>If opponent access to the network operator:</p>		Have everybody use anonymous SIMs
		Use more than one phone and SIM
		Use smartphones for secure internet calls
<p>To deter a 'random person':</p>		Clear Call logs





Identification *Who else is in your network?*

Network operator		Don't swap and reuse phones and anonymous SIMs in your network
		Store sensitive contacts on paper, scrambled
Random person		Purge socialmedia apps Never store passwords





Surveillance *What did you say?*

If surveillance is a threat, practice countersurveillance		Don't communicate sensitive information over mobile networks.
		Use secure Internet based voice services
		Use code language





Phone as Bug *What is going on around you?*

If you fear constant surveillance , then consider your phone as the perfect bug...		Don't lend your phone or accept phone as a gift
		Lock your phone well
		Take out batteries & put in noisy place during sensitive meetings
		Know your apps!






Tracking: *Where are you, Where were you?*

Make it harder for your adversaries to track your movements.		Don't keep your phone on and with you all day
		Take your phone battery out before traveling to sensitive meetings
		Use more than one phone
		Disable Location service and remove GPS antenna





Seizure *What were you doing ?*

Make it harder for your adversaries to track your movements.		Don't keep your phone on and with you all day
		Take your phone battery out before traveling to sensitive meetings
		Use more than one phone
		Disable Location service and remove GPS antenna

Seizure *What were you doing ?*

Make it harder for a random person to see your data		Don't store sensitive data, photos, passwords
		Use a strong passcode
		Delete logs, data ASAP
		Prepare remote or panic Wipe
		Encrypt your phone

Seizure *What were you doing ?*

Mobile phones have very low security standards. Forensics can recover ... pretty much everything		Most passcodes can be unlocked
		Deleted data may still be present
		Overwritten files may still be present
		Most encryption mechanisms are flawed

Seizure *What were you doing ?*

Mobile phones have very low security standards. Forensics can recover ... pretty much everything		Don't store sensitive data, photos, passwords
		Only wiped encrypted data is safe

Threat: Remote Information Theft

On the Internet, Smartphone are just computers....with fewer defenses

Produced by:

The SKeyes Center for Media and Cultural Freedom at the Samir Kassir Foundation

The content of the video was prepared with the pro bono assistance of:

The ICT team at the National Democratic Institute

Executive producer: **Maroun Sfeir**

Storyboard creation and animation: **kook creative studio**

Video Consultant: **Andrew Codd**

Translation: **Nour El-Assaad**

Voice over - Arabic: **Rima Khaddaj**

Voice over - English: **Andrew Codd**

Sound recording: **Creative Impact**

Music: **“Mining by Moonlight” by Kevin MacLeod**

This project has been made possible thanks to the support of the **National Endowment for Democracy**.

You are free to share, copy, distribute, and transmit this work under the condition that you attribute the work to the Samir Kassir Foundation, but without suggesting in any way that the Samir Kassir Foundation endorses you or your use of the work. You may not use this work for commercial purposes. You may not alter, transform, or build upon this work.