

Mobile Literacy Curriculum – Kenya Curriculum

Module 2: Mobile Security and Information Sharing

Stacey Wedlake

Lauren Holstein

March 2018

# TASCHA_logo_stacked_black

ABSTRACT (100–150 WORDS)

As millions of people come online across the globe through mobile devices, mobile information literacy is vital for those who have leapfrogged from traditional media to digital devices that provide instant access to information. Mobile information literacy is necessary to help people learn how to find and evaluate the quality and credibility of information obtained online, understand how to create and share online information effectively, and participate safely and securely. Mobile information literacy is critical to help people better consume, generate, and disseminate trustworthy information through both digital and traditional media. Most information and digital literacy curricula were designed for a PC age, and public and private organizations around the world have used these curricula to help newcomers use computers and the internet effectively and safely. The central question for this project is: what are the relevant skills, concepts, and attitudes for people using mobiles, not PCs, to access the internet?

140-CHARACTER SUMMARY

What are the relevant skills, concepts, and attitudes for people using mobile devices, not PCs, to access the internet & information?

KEYWORDS

mobile information literacy, information literacy, digital information literacy, digital literacy, mobile-centric, mobile-first, mobile phones, smart phones, Kenya, ICTs, libraries, curriculum, training, training of trainers

RECOMMENDED CITATION

Wedlake, S & Holstein, L. (2018). Mobile Information Literacy – Kenya Curriculum. Seattle: Technology & Social Change Group, University of Washington Information School.

ABOUT THE AUTHOR

**Stacey Wedlake** is a Research Coordinator at the Technology and Social Change Group.

**Lauren Holstein** is a graduate of the University of Washington Evans School of Public Policy & Governance.

ACKNOWLEDGEMENTS

First, the authors would like to acknowledge the work of the original Mobile Information Literacy Curriculum developed for Myanmar. Our work builds upon your research and curriculum. The development of this curriculum also received valuable input and direction from Ramune Petuchovaite, Ugne Lipeikaite, and Susan Schnuer of EIFL. Raymond Chepkwony and Juliana Muchai from the Kenya National Library Service (KNLS) helped with development and adaptation to the Kenya Public Library Context. Many thanks to the inspiring KNLS public librarians and library staff TASCHA researchers met on both of our trips to Kenya. Last but not least, thank you to the TASCHA Researchers and staff that provided important behind-the-scenes work to make this possible: Melody Clark, Maria Garrido, and Chris Rothschild.

COPYRIGHT, LICENCING, DISCLAIMER

Copyright 2018, University of Washington. This content is distributed under a Creative Commons Attribution Share-Alike license. The views, opinions, and findings expressed by the authors of this document do not necessarily state or reflect those of TASCHA, the University of Washington, or the research sponsors.

TECHNOLOGY & SOCIAL CHANGE GROUP (TASCHA)

The Technology & Social Change Group (TASCHA) at the University of Washington Information School explores the design, use, and effects of information and communication technologies in communities facing social and economic challenges. With experience in 50 countries, TASCHA brings together a multidisciplinary network of social scientists, engineers, and development practitioners to conduct research, advance knowledge, create public resources, and improve policy and program design. Our purpose? To spark innovation and opportunities for those who need it most.

CONTACT

Technology & Social Change Group  
University of Washington Information School  
Box 354985  
Seattle, WA 98195

Telephone: +1.206.616.9101  
Email: tascha@uw.edu  
Web: *tascha.uw.edu*

Table of Contents

[Module 2 Overview 4](#_Toc521414399)

[Objectives 4](#_Toc521414400)

[Materials 4](#_Toc521414401)

[Module Guide 4](#_Toc521414402)

[Introductions 4](#_Toc521414403)

[Learning Objectives 5](#_Toc521414404)

[Icebreaker 5](#_Toc521414405)

[Applying prior knowledge 6](#_Toc521414406)

[Creating accounts 6](#_Toc521414407)

[Activity 2.1: Password Guessing Game 7](#_Toc521414408)

[10 minute break 10](#_Toc521414409)

[Searching for information on smartphones 10](#_Toc521414410)

[Investigating what we find online 11](#_Toc521414411)

[Activity 2.2 Online Scams 12](#_Toc521414412)

[Activity 2.1 Images 16](#_Toc521414413)

[Fake news infographic 17](#_Toc521414414)

[Activity 2.2 Online Scams printout 18](#_Toc521414415)

# Module 2: Mobile Security and Information Searching

## Module 2 Overview

Estimated total time: 3 hours

### Objectives

* Learn how to set up email account
* Learn how to set up accounts on applications
* Learn how to create secure passwords
* Learn privacy & security best practices (locking phones, etc.)
* Learn about phishing via email, text, links, etc.
* Learn how to compose emails, attach files, etc.

### Materials

* Projector
* Blackboard/whiteboard (ideally)
* Paper
* Pencils
* Markers/Colored pencils/Crayons
* String
* Tape
* Printout of Images
* Activity packet 2.1
* Activity packet 2.2
* A bag, bucket, cup, or hat

## Module Guide

### Introductions

(5 minutes)

Begin by welcoming the class and introducing yourself. If it’s your first time teaching the participants, provide time to discuss your background, any experience you have with the information and communications technology, and any other relevant information you wish to share.

Outline the structure of the day and provide time to address any other administrative issues that need to be brought up before class begins.

Pause to ask if anyone has questions so far.

### Learning Objectives

(10 minutes)

Introduce to the class that today will focus on working on the web, creating accounts, using content, and staying safe. Often, when you download an app or go to a certain website, you have to create an account. What’s an account?

Who can define what a username is? Who can define what a password is? Why do you think it is important to protect yourself online? Is the internet a dangerous place?

Then, take some time to review concepts from the previous lesson. For example, what is the difference between an app and a browser?

Pause to answer any questions.

### Icebreaker

(10 minutes)

Now that participants understand the purpose of this module, take some time for the participants to review some concepts and get ready to learn some more. Ask participants to pair up with someone they do not know very well. Give the participants a few minutes to introduce themselves to one another.

Then, have each pair take turns explaining one thing that they’ve done with their smartphone since the last module without speaking, drawing, or writing (singing is allowed). While one person is acting, the other tries to guess what they mean. (If the Module 2 happens the same day as Module 1, the prompt can be “one thing that they learned they could do with their smartphone in the last module.”)

To start, act out your own example of what you have done on your smartphone since the last class. If necessary, feel free to draw phone functionalities on the board before beginning the activity so participants can reference specific apps or phone functionality, like Wi-Fi or WhatsApp.

Examples that the participants could use include:

“I used Facebook to share a picture”

“I used Whatsapp to speak with my daughter at school”

At the end of the activity, ask two people to share their pantomime with the whole groups so that everyone can try to guess what they did.

(Mozilla, Digital Skills Observatory | [*All About Accounts*](https://mozilla.github.io/curriculum-final/kenya-dso-interventions/intervention-two.html#step-2))

### Applying prior knowledge

(15 minutes)

This activity serves two purposes:

* Introduce some of things a smartphone can do to participants
* Better understand the skill level/experience of participants

In this activity, the classroom will stand and will separate themselves out into different areas of the room based off of a smartphone feature function. Four corners of the room will designate how familiar/unfamiliar a participant is with using a smartphone for a certain activity. The first corner will represent being completely unfamiliar, the second corner will represent having heard of the function before but never using it, the third corner represents using the function once or twice, and the fourth function represents using the function frequently. After each prompt, also ask if the task can be performed on a feature phone. Suggested prompts include:

* I used a smartphone for WhatsApp.
* I used a smartphone for banking.
* I used a smartphone for making ugali.
* I used a smartphone to withdraw money from my account.
* I used a smartphone to record a movie.
* I used a smartphone to make a website.
* I used a smartphone to locate people who have called me.
* I used a smartphone to pay my bills.
* I used a smartphone to apply for jobs.
* I used a smartphone to access government services.
* I used a smartphone to search for information.

After the participants organize themselves after each prompt, take some time to discuss with the participants. If a student has heard of a function but never used it, why? If someone uses the function all the time, why do they do so? Has it simplified their lives?

(*Mozilla Digital Skills Observatory,* [*The Smartphone EcoSystem*](https://mozilla.github.io/curriculum-final/kenya-dso-interventions/intervention-one.html#step-3)*)*

### Creating accounts

(30 minutes)

(Show the class your phone or project an image on the screen of the Gmail app login)

Tell the class that you just downloaded the app Gmail on your phone. You’ve opened the app and the screen says “Sign In.” Ask the class, “What does this mean?”

Explain that some apps require you to make an account to use them. An account is like entering an agreement with a company. The company will ask for information and or money in exchange for you using the app.

When you decide to make an account on a website or an app, what information do you usually need to give?

* Name
* Email Address
* (sometimes) location, occupation
* (sometimes) gender, birthday

What are some of the potential downsides to creating accounts on a website?

* Giving your information to someone you don’t know.
* Some services sell your information to other companies.
* If the site or app gets hacked, your information could be exposed (why it’s important to have different passwords which we will talk about later).

Before creating an account with an app, ask:

* "What benefit do you get from having this account?"
* "What benefit does the company get?"
* “Can I use the app without creating an account?”
* "Why does the app want certain information?”

Say, let’s answer these questions about Gmail:

Ask, “What benefit do you get from having this account?”

The ability to send and receive emails with a Gmail account. (You’ll find that it’s important to have an email address to use other apps and communicate with others online.)

Ask, “What benefit does the company get?”

Information about you, show you advertisements, easier to use other services

Ask, “Can I use the app without creating an account?”

No, in fact, for email, you want to have a unique, secure account. You don’t want others to impersonate you!

Ask, "Why does the app want certain information?”

It should be apparent and/or the app should tell you why it needs information. Google tells you why it wants certain information. (That doesn’t mean it won’t use the information for other purposes! Unless it explicitly says so).

Ask, “Should I create an account?”

Reiterate that different apps will require different accounts. You’ll want to ask the questions every time you need to create an account.

### Activity 2.1: Password Guessing Game

(30 minutes)

*Adapted from Mozilla, Digital Skills Observatory |* [*All About Accounts*](https://mozilla.github.io/curriculum-final/kenya-dso-interventions/intervention-two.html#step-4)

**Objectives**:

* Learn how to create secure passwords
* Learn about privacy settings on applications
* Understand the importance of secure passwords
* Understand the possible danger of having your password stolen
* Think critically about creative and memorable ways to strengthen password security

**Materials Needed:**

* 5 pieces of paper or cards per person (the name or logo from a different app or service should be on each card)
* Markers or pens
* A bag, bowl, bucket, cup, or hat for mixing up the papers

**Introduction**: (Use the following information to introduce and explain the activity to the class)

Explain to the participants that there are many great things you can use the internet for, but it is important to remember the internet is open to everyone in the world. Therefore, just like in the real world, the internet should be treated like a large, public park. Safety is important on the internet, just like it is important in any large public area. This activity is meant to have participants understand why a single password makes their accounts unsafe.

Give each participant five small pieces of paper. Each paper should have the name or logo of a popular app or service.

Invite participants to make up a password for each app or service and to write it on the back of the card. Be sure to help anyone who needs it. Make sure you tell participants to make up passwords, not to use their real ones.

Collect the cards and jumble them in some kind of container.

Ask the participants to take turns picking a random card, reading the password to the group, and leading a discussion to figure out who wrote that password.

Play until several passwords have been correctly guessed. Then move on to facilitate a discussion about password security as described below.

As you play, it should become clear that passwords made up of personal information (like names or dates) and repeated passwords make it easy to guess to whom those passwords belong. Explain that the reverse is also true - impostors can easily break passwords made up short passwords made up of sequential numbers (like 1234) and they can guess passwords that are made of simple words, as well (like “mydata”). Impostors can use what they know about you to guess passwords based on important dates in your life (such as birthdays or anniversaries) or the names of people (including celebrities and sports teams) or places you know.

Ask participants to suggest other ways to create stronger passwords that aren’t so easily guessable by impostors who want to steal their accounts, data, and money. If they are unsure, suggest creating individual passwords for each app or service they use with:

* keep passwords simple, long, and memorable
* phrases, lowercase letters and typical English (or your local language) words work well.

In the past, experts suggested special characters and a mix of lower and uppercase letters. However, what’s most secure is to create a long, memorable password.

<http://www.npr.org/sections/alltechconsidered/2017/08/14/543434808/forget-tough-passwords-new-guidelines-make-it-simple>

For example, a good password would be “mygrandmaboughtmemyfavoriteshirt”

Another way to create a good password is take a sentence like “I buy 2 mangos at the market every week” and use the first letter of each word to create a password.



Sometimes sites have specific rules about passwords. For example, the password must have upper and lowercase letters or must use a number or “special character.”

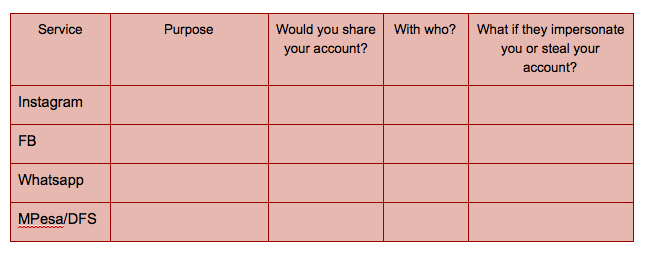
Ask participants to reflect and explain why having the same password on multiple apps or services make it easier for impostors to break into their accounts.

Here are other ways to think about these problems:

Imagine you are coaching a soccer team. You always use the same formation of players with six strikers and five midfielders. You have no defense and no goalie. Every team knows how to beat you, but you do not change your formation. This is like having a weak password any impostor can guess or figure out using hacking technology to “win” control of your accounts.

Imagine that you are the creator of the game called Temple Run. You made ten levels in the game. However, a player can do the same thing in each level to win the game. All they have to do is run in a straight line. That is like setting up ten accounts with just one password you reuse. An impostor can “beat” you at your password “game” by stealing the same password and using it again and again for all ten accounts (your different “levels”).

Next, ask participants to consider the risks of impostors taking over their accounts on popular apps and services. Use an organizer like this one to frame the conversation:



You can also ask something like, “What if someone impersonates you on an account? Would that ever be okay?”

### 10 minute break

### Searching for information on smartphones

(20 minutes)

Ask the class, “using only my phone, how would I find the population of Nairobi?”

Remember from Module 1 that websites are simply a way to visualize information that is on the Internet. There are many different types of websites, such as social media websites like Facebook, news websites such as [use local example], web logs or “blogs” for short, reference websites such as merriam-webster.com, collaborative knowledge-based websites such as Wikipedia, and more.

One particular type of website is especially useful for simply searching the Internet for information: search engine websites.

Search engines are code, or algorithms, that take your requests for information and comb through databases of information and websites that have been indexed to give you a list of websites and information resources that might be relevant. Can you name any search engines you might have used?

Take answers from several participants and then list some common search engines.

One of the most popular search engines is Google. Tell the participants that you can get information on places, jobs, cooking recipes, songs, news, and information for school. Ask someone how they’ve used Google Search. Be sure to ask for specific examples.

Ask trainees to open the Google App on their phone and search for something. Have them use the different tabs (such as images) to see different search results.

(*TASCHA, Mobile Information Literacy Curriculum,* [*Module 3*](http://tascha.uw.edu/mobile-information-literacy-module-3/)*)*

### Investigating what we find online

(30 minutes)

What are some popular internet stories that you wonder about? These could be something shared on WhatsApp or something you read in the newspaper.

Make a list of the stores on a sheet of paper.

Ask the class, how can you figure out if a story is true? List their responses. Then show the IFLA Fake News Infographic



Then have them break into teams of 2-3 people to investigate those stories. You can assign particular stories to particular groups if you want or let every group investigate all the stories or just the stories that interest them.

After 10-15 minutes of investigation, bring the whole group back together. Ask each team to share one investigation with the whole group and to explain why they think the story they investigated is trustworthy or not. What was the reasoning that you used to investigate?

Use the last 5 minutes of this activity to run a short, reflective conversation using questions like:

* What do trustworthy stories often have in common with one another?
* What do untrustworthy stories often have in common with one another?
* What are some of the ways authors of untrustworthy stories use to trick people?
* Are all pictures and videos trustworthy?
* What advice do they have for new internet users about staying away from untrustworthy stories and sites?

*(Adapted from Mozilla, Digital Skills Observatory |* [*What is possible online?*](https://mozilla.github.io/curriculum-final/kenya-dso-interventions/intervention-four.html#step-2)**)**

### Activity 2.2 Online Scams

(30 minutes)

Spam and Phishing definitions adapted from DigitalLearn.org [Online Scams](https://www.digitallearn.org/courses/online-scams)

**Objectives:**

* Introduce the concept of spam and phishing
* Learn to differentiate legitimate, spam, and phishing emails, calls, and texts

**Materials Needed:**

* Printouts of legitimate, spam, and phishing calls, emails, and texts, labels that say “legitimate,” “spam,” and “phishing” placed in five packets
* Paper
* Pencils, pens, markers, or crayons

**Introduction: (Use the following information to introduce and explain the activity to the class)**

First, review what are scams. Ask the group:

* What is a scam?
* What are examples of offline scams? (trick out of money etc)

Online scams can come in many shapes and forms. You may encounter them on a website, in an email message, including a type of scam called phishing, or in a pop up window.

Mobile Spam:

* Junk email sent to many people at once
* Includes fake links for you to click
* Asks you to call a fake phone number
* Asks you to transfer money

Of course, you can get spam calls as well. [According to a 2017 report, 91% of spam calls in Kenya were scams.](https://blog.truecaller.com/2017/07/13/truecaller-insights-special-report-the-top-20-countries-affected-by-spam-calls/) The other spam calls were from financial institutions offering banking products or credit card offers.

Mobile Phishing

* Claims to be from an organization that you’ve heard to win your trust
* If includes a link - leads you to a fake website
* Asks for your personal information

**Activity:**

Get in groups of 2 - 3. I’ll give you a packet of examples of legitimate, spam, and phishing emails, calls, and texts and sort them based on type.

When 10 minutes remain, go through each example:

**Spam**

Taji received a text message; “C0NAL3RT Confirmed. You have received Ksh 3,065 from Mwalimu Jini 07\*\*\*\*\*\*\*\*, new M-PESA balance is Ksh 6,965…” He was not expecting money from anyone.

He phone rang. The person who had erroneously sent him the money was calling to claim it back.

Ask - what could Taji do to confirm if it was real or fake?

* Dial \*234# to check her M-PESA mini-statement. No money was transfered.
* After, report number to 333 and police.

from [Dealing with Fraudsters, SafariCom](https://www.safaricom.co.ke/blog/dealing-with-fraudsters/)

From: Bruce.Roberts@outlook.com

Subject: Win $$$

Win $750,000 in Cola Cola Compnay yearly promo.To qualify,Email thecorrect answer to the question given below to Mr. Frank Joe via email ([mrfrankdesk@outlook.com](mailto:mrfrankdesk@outlook.com)) Question: Who won the 2010 FIFA World Cup in South Africa? (A)Usa (B)Spain(C)Australia(D)China

Ask - how would you know it’s a scam?

* Typos
* Easy answer for a lot of money
* promo for Coca Cola but outlook.com email

You receive a call from a number with the prefix +375. They ring once and hang up. You don’t recognize the number and weren’t expecting the call. Should you call back?

No - only call back numbers that are familiar to you - especially if international calls. you can try searching the web for the prefix or the number to see who it is.

“Those who do [call back] find themselves listening to advertisements for all sorts of dodgy services. Some firms try to hook callers into subscribing, say, to high-priced chat-lines or Internet services. Others dupe callers into providing credit-card numbers. Using caller-identification in reverse helps to harass more users. Some victims decide it is easier to pay than face fresh hassles. Even if only a small fraction are snared, it is still a lucrative ploy: their own charges are small since they never give their quarry a chance to answer.”

From <https://www.snopes.com/fraud/telephone/onering.asp>

**Phishing**

From: a co-worker

Subject: Hello

Just wanted to make sure you receive the message I tried to deliver you earlier, but it doesn’t seem to have got through. Please view the document I uploaded using Google docs check it out here. CLICK HERE and log in with your email and let me know your opinion on this.

Thanks

From: IT@s.company.com

Subject: IT Helpdesk Alert

Hello,

Please click here for meeting details.

Thank you.

IT Dept

### 

**Legitimate**

From: coworker (via Google Docs)

Subject: Mobile Information Literacy Curriculum outline

Mary Martha has invited you to **edit** the following document:



[resource mobilization plan](http://docs.google.com/a/uw.edu/document/d/1EB-F2JpMEpnTz1Wh3mQfmf_4_a4cAhqgPOxTAr6Lx6E/edit?usp=sharing_eil&ts=59e8d3c7)

[**Open in Docs**](http://docs.google.com/a/uw.edu/document/d/1EB-F2JpMEpnTz1Wh3mQfmf_4_a4cAhqgPOxTAr6Lx6E/edit?usp=sharing_eip&ts=59e8d3c7)

|  |  |
| --- | --- |
| Google Docs: Create and edit documents online.  Google Inc. 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA  You have received this email because someone shared a document with you from Google Docs. | Logo for Google Docs |

## Activity 2.1 Images





## Fake news infographic

Source and translations: <https://www.ifla.org/publications/node/11174>

## Activity 2.2 Online Scams printout

Taji received a text message; “C0NAL3RT Confirmed. You have received Ksh 3,065 from Mwalimu Jini 07\*\*\*\*\*\*\*\*, new M-PESA balance is Ksh 6,965…” He was not expecting money from anyone.

He phone rang. The person who had erroneously sent him the money was calling to claim it back.

From: Bruce.Roberts@outlook.com

Subject: Win $$$

Win $750,000 in Cola Cola Compnay yearly promo.To qualify,Email thecorrect answer to the question given below to Mr. Frank Joe via email ([mrfrankdesk@outlook.com](mailto:mrfrankdesk@outlook.com)) Question: Who won the 2010 FIFA World Cup in South Africa? (A)Usa (B)Spain(C)Australia(D)China

You receive a call from a number with the prefix +375. They ring once and hang up. You don’t recognize the number and weren’t expecting the call. Should you call back?

From: a co-worker

Subject: Hello

Just wanted to make sure you receive the message I tried to deliver you earlier, but it doesn’t seem to have got through. Please view the document I uploaded using Google docs check it out here. CLICK HERE and log in with your email and let me know your opinion on this.

Thanks

From: IT@s.company.com

Subject: IT Helpdesk Alert

Hello,

Please click here for meeting details.

Thank you.

IT Dept

From: coworker (via Google Docs)

Subject: Mobile Information Literacy Curriculum outline

Mary Martha has invited you to **edit** the following document:



[resource mobilization plan](http://docs.google.com/a/uw.edu/document/d/1EB-F2JpMEpnTz1Wh3mQfmf_4_a4cAhqgPOxTAr6Lx6E/edit?usp=sharing_eil&ts=59e8d3c7)

[**Open in Docs**](http://docs.google.com/a/uw.edu/document/d/1EB-F2JpMEpnTz1Wh3mQfmf_4_a4cAhqgPOxTAr6Lx6E/edit?usp=sharing_eip&ts=59e8d3c7)

|  |  |
| --- | --- |
| Google Docs: Create and edit documents online.  Google Inc. 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA  You have received this email because someone shared a document with you from Google Docs. | Logo for Google Docs |