

# MOBILE INFORMATION LITERACY CURRICULUM

## *Module 4 Guide: Working Online and Using Information via Mobile Devices*

Sheryl Day

April 2015



## HENRY M. JACKSON SCHOOL OF INTERNATIONAL STUDIES (JSIS)

The Henry M. Jackson School of International Studies (JSIS) combines the social sciences, humanities, and professional fields to enhance our understanding of our increasingly interconnected globe. The school is named for late Senator Henry M. Jackson, in recognition of his interest and support for the school and for the field of international affairs. The Jackson School's commitment to regional, cross-cultural, and comparative studies extends well beyond the boundaries of its many formal academic programs. The school has eight Title VI National Resource Centers (NRCs)—Canadian Studies; East Asia Center; Center for West European Studies; International Studies; Middle East Studies; Ellison Center for Russian, East European & Central Asian Studies; South Asian Studies; and Southeast Asian Studies—Devoted to outreach and public education activities. Each NRC receives Foreign Language and Area Studies (FLAS) fellowships, awarded to graduate students throughout the University. The Jackson School is the number one recipient of NRC and FLAS awards in the country.

## TECHNOLOGY & SOCIAL CHANGE GROUP

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 over 50 countries, TASCHA brings together a multidisciplinary network of researchers, practitioners, and policy experts to advance knowledge, create public resources, and improve policy and program design. Our purpose? To spark innovation and opportunities for those who need it most.



## ABOUT THE AUTHOR

**Sheryl Day** is a Ph.D. candidate at the University of Washington Information School.

## ACKNOWLEDGEMENTS

The development of this curriculum would not have been possible without significant input from Daniel Arnaudo and Dr. Jessica Beyer (both of University of Washington). Chris Coward and Mike Crandall (also from University of Washington) provided invaluable guidance on defining and situating the curriculum into the wider international efforts to extend information literacy to digital and mobile platforms. Pilot implementation of the curriculum and essential evaluative feedback on its application could not have been possible without Thant Thaw Kaung of Myanmar Book Aid Preservation Foundation and Zaw Zaw Htet Aung of Yone Kyi Yar Knowledge Propagation Society. Thanks also go to the *Information Strategies for Societies in Transition* project program directors Sara Curran and Mary Callahan and team members Chris Rothschild and Melody Clark (all of the University of Washington); and Catherine Beyer and Samantha Becker, also from the University of Washington.

This is a product of the *Information Strategies for Societies in Transition* program. This program is supported by United States Agency for International Development (USAID), Microsoft, the Bill & Melinda Gates Foundation, and the Tableau Foundation. The program is housed in the University of Washington's Henry M. Jackson School of International Studies and is run in collaboration with the Technology & Social Change Group (TASCHA) in the University of Washington's Information School, and two partner organizations in Myanmar: the Myanmar Book Aid Preservation Foundation (MBAPF) and Enlightened Research Myanmar (EMR).

## KEYWORDS

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

## RECOMMENDED CITATION

Day, S. (2015). *Mobile Information Literacy Curriculum Module 4 Guide: Working Online and Using Information via Mobile Devices*. Seattle: Henry M. Jackson School of International Studies & the Technology & Social Change Group, University of Washington Information School.

## COPYRIGHT, LICENSE, DISCLAIMER

Copyright 2015, University of Washington. This content is distributed under a [Creative Commons Attribution-ShareAlike 3.0 license](https://creativecommons.org/licenses/by-sa/3.0/).

The views, opinions, and findings expressed by the author of this document do not necessarily state or reflect those of the University of Washington, or the project partners.



## Table of Contents

<b>ABOUT THE CURRICULUM</b> .....	4
<b>CURRICULUM DEVELOPMENT</b> .....	5
<b>HOW OTHERS CAN IMPLEMENT THE CURRICULUM</b> .....	5
<b>PREPARING FOR CONDUCTING TRAININGS</b> .....	6
<b>ABOUT THIS MODULE</b> .....	7
<b>MODULE 4: WORKING ONLINE AND USING INFORMATION VIA MOBILE DEVICES</b> .....	8
OUTLINE .....	8
ASSUMPTIONS .....	8
PREPARE AHEAD .....	8
BACKGROUND INFORMATION .....	8
OVERVIEW .....	8
PRIVACY AND SECURITY .....	8
NETIQUETTE .....	10
CREDIT, CREDIBILITY, AND COPYRIGHT .....	11
THE CLOUD .....	12
ACTIVITIES .....	13
ACTIVITY 4.1: BASIC PROTECTION MEASURES .....	13
ACTIVITY 4.2: USING FACEBOOK GROUPS .....	14
ACTIVITY 4.3: USING ONLINE CONTENT .....	14
ACTIVITY 4.4: INTRO TO GOOGLE DOCS .....	15
WRAP UP .....	16

The Mobile Information Literacy curriculum is a growing collection of training materials designed to build information literacies for the millions of people worldwide coming online every month via a mobile phone.

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 better curricula address not only skills, but also concepts and attitudes. 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? As part of the [Information Strategies for Societies in Transition](#) project, we developed a six-module curriculum for mobile-first users. The project is situated in Myanmar, a country undergoing massive political, economic, and social changes, and where mobile penetration is expected to reach 80% by the end of 2015 from just 4% in 2014. Combined with the country's history of media censorship, Myanmar presents unique challenges for addressing the needs of people who need the ability 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.

## About the Curriculum

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.

The curriculum focuses on critical thinking in a digital environment of smart phones, mobile phones, and tablets, filling a critical gap in digital information literacy curricula. Existing curricular models assume people learn on a personal computer (PC). While this has been the case historically, the next billion people coming online will most likely learn on a mobile device. This has huge implications for how people get online, how they access and experience the internet, how much they produce in addition to consume information, and even how they conceptualize the internet itself. For instance, research shows that in Myanmar (and many other countries) more people use Facebook than the internet. Mobile-specific practices, such as zero-rating, mean people are coming online much more frequently through a handful of "walled garden" applications without an understanding of and similar access to the broader internet. Also, some mobile applications and websites don't offer the full functionality of their PC counterparts. The curriculum aims to address these differences and empower mobile internet users to be equal participants in the online world.

The curriculum includes the following six modules:

- Module 1: Introduction to Mobile Information and Communication Technologies (ICTs)
- Module 2: A Mobile Lens on the Internet
- Module 3: Basic Web Searching via Mobile Devices
- Module 4: Working Online and Using Information via Mobile Devices
- Module 5: Putting It All Together
- Module 6: Module 5 Project Presentations

## Curriculum Development

Our initial efforts sought to combine several frameworks in creating a comprehensive mobile information literacy curriculum: [EU DIGCOMP](#), [SCONUL](#), and [Empowering 8](#). At the time of our review there were none that explicitly addressed all of the skills, concepts and attitudes for mobile-centric users. The EU DIGCOMP framework explicitly acknowledges that no curriculum for the mobile environment has been developed. Nevertheless, once we identified our target group as beginner-level participants with no knowledge of the internet, World Wide Web, and mobile technology use, the EU DIGCOMP proved to be the most appropriate framework for designing a basic beginner-level curriculum. SCONUL and Empowering 8 were more appropriate for those with at least a minimum baseline digital information literacy.

## How Others Can Implement the Curriculum

The curriculum and training guide were designed to be flexible and customizable, depending on the baseline skills of those being trained, and translated into other languages. In countries and contexts like Myanmar, where for many using a mobile phone marks their first experience with the internet and digital technology, these training materials can be used by various organizations, such as libraries and NGOs, to both train their staff and to build knowledge, skills, and mobile information literacy competencies within the populations they serve. In Myanmar the materials have been translated into Burmese, and master training sessions have been conducted to train library staff to further train their colleagues, as well as library patrons. Our partners in Myanmar have also conducted training sessions at the Ministry of Information.

The curriculum materials are offered here with a [Creative Commons Attribution-ShareAlike 3.0 license](#), so others are free to use, adapt, and share the materials with attribution. We are also available to help organizations create customized materials based on their particular country or regional contexts and literacy training needs.

If you have questions on the curriculum or would like more information on how we can help, please email us at [tascha@uw.edu](mailto:tascha@uw.edu). We also encourage individuals and organizations that use and adapt this curriculum and training to provide us with any feedback, ideas, and adapted materials. There are many ways you can do this: email [tascha@uw.edu](mailto:tascha@uw.edu), leave a comment and upload materials on the main Mobile Information Literacy curriculum webpage <http://tascha.uw.edu/mobile-information-literacy-curriculum>, and/or participate on our Facebook page <https://www.facebook.com/MobileInformationLiteracy>.

## Preparing for Conducting Trainings

By default, digital information literacy implies access to information on the internet. Technology often fails or can be difficult for many to use under time and pressure constraints. A good practice is to test run the presentation on the equipment in the facility well ahead of the actual training. This ensures that the presentation will go as intended and so trainers can determine and anticipate alternative options. Before conducting any presentation, trainers should be sure that:

- The training facility is equipped with the necessary materials and technology
- All equipment has been tested and is operational
- They are familiar with how to operate the equipment
- They have a backup plan for continuing the training should issues arise

## About this Module

### **Working Online and Using Information via Mobile Devices**

In this module, we will cover privacy and security measures, online etiquette, referencing online sources, and working in collaborative online environments.

#### **Prerequisites:**

- Module 1: Introduction to Mobile Information & Communication Technologies (ICTs)
- Module 2: A Mobile Lens on the Internet
- Module 3: Basic Web Searching via Mobile Devices

#### **Topics covered:**

- Privacy and security measures
- Online etiquette
- Referencing online sources
- Working in collaborative online environments

#### **Questions you will be able to answer at the end of this module:**

- How do I protect my privacy online?
- What are some rules and guidelines for online behavior?
- How do I use and reference online sources?
- How do I work online with others?

#### **How long does this module take?**

3 hours (180 minutes)

# Module 4: Working Online and Using Information via Mobile Devices

Estimated total time: 3 hours

## Outline

- |   |            |
|---|------------|
| 1. Overview                               | <1 min     |
| 2. Privacy and Security                   | 5 mins     |
| 3. Netiquette                             | 5 mins     |
| 4. Credit, Credibility, and Copyright     | 4 mins     |
| 5. The Cloud                              | 1 min      |
| 6. Activities                             | 150 mins   |
| – Activity 4.1: Basic Protection Measures |            |
| – Activity 4.2: Using Online Content      |            |
| – Activity 4.3: Facebook Groups           |            |
| 7. Break                                  | 15 mins    |
| 8. Activity 4.4: Intro to Google Docs     | 50-75 mins |

## Assumptions

- All participants have mobile devices such as smartphones or tablets.
- Wi-Fi is available at the facility for participants to access.
- Participants have completed Module 3: Basic Web Searching via Mobile Devices.

## Prepare ahead

Review the activities and ensure that you set up any necessary demo requirements on your device ahead of the module.

## Background information

Understanding how to work with online information and collaborating with others online are essential to developing digital information literacy. In the online space, it is important to build awareness and take precautions against security vulnerabilities just as one would in a physical space.

## Overview

(<1 min)

Briefly introduce the title of this module, and what will be covered:

- *This is Module 4: Working Online and Using Information via Mobile Devices. In this module, we will cover privacy and security measures, online etiquette, referencing online sources, and working in collaborative online environments.*
- *As a reminder, the best way to learn digital information literacy is by learning new concepts and then applying what you've learned. This workshop is designed to be highly interactive to help you learn new concepts and retain what you've learned. Feel free to interrupt if something is unclear.*

## Privacy and Security

(5 mins)

[Slide: Privacy, Why Bother?]

- *Similar to the physical environment, where we must take certain precautions to ensure privacy and security for ourselves and others, the online environment has its own particular set of precautions that are important to be aware of. Why would we want to protect our privacy? [Take a few answers, and provide local examples.]*

[Slide: Privacy and Security]

- *As we learned earlier, we can adjust the settings in apps that we download and use on our mobile devices to limit the data that can be accessed and shared about us. Do you remember what some of those settings were? [Take a few answers, should include: location, access to contacts, camera, microphone, etc.]*

If you receive little or no answers covering browsers, emphasize the following security measures to safeguarding information when using browsers:

- Do not track – prevents third parties from monitoring the websites that you visit.
- Private browsing – prevents browsers from saving websites that you visit in the browser search history. Private browsing does not mean your browsing is invisible to others. It just that a record is not made in your browsing history.
- Clearing browser history and cookies – allows users to clear previously saved browsing history and the cookies that identify browser users.

[Slide: Facebook Privacy Policy]

- *What are some security measures we can take to protect privacy when using social media like Facebook?*

[Take a few answers and discuss.] Because Facebook is so prevalent in Myanmar and is often the first, if not only, exposure to the Internet for many, focusing on privacy and security within Facebook is essential to understanding these concepts.

[Slide: Who is Responsible for Privacy and Security?]

- *Who is responsible for ensuring your privacy and the security of your information? [Take a few answers.]*
- *Since its inception, Facebook has changed and updated its privacy policies and security measures. Companies that provide services or products must provide mechanisms to protect privacy and security, but individuals must stay aware of these mechanisms and actively practice privacy and security.*

Emphasize that with rapid changes in ICTs, that how security works and privacy are protected will continuously change, but the need to protect privacy and have security measures is constant and is the main concept to remember. Encourage participants to stay vigilant about always ensuring that they take necessary precautions to protect their privacy and stay aware of available security measures. Discuss the option to blind carbon copy (bcc) email addresses as opposed to sending mass emails with all email addresses visible. There are advantages and disadvantages to using bcc. Hiding addresses protects recipients from email scams and viruses that target email recipients, but hiding addresses may also have negative social impacts to recipients who may be concerned that the message is part of an email scam.

- *Even with the most sophisticated technological security measures, oftentimes the most vulnerable security weakness that can be exploited is people themselves. Social engineering is a technique used to gain trust from unsuspecting victims in order to persuade them to share valuable information such as passwords, personal information, and more.*

- [Provide a local example of a social engineering scam]
- *What indicators can help you identify a social engineering scam?*  
[Briefly discuss] Remind participants of email vulnerabilities, particularly where hypertext are used to mask hyperlinks. Emphasize the personal responsibility that individuals have in ensuring their online security.
- *Using unverified 3<sup>rd</sup> party apps is a vulnerability, but so is using alternative app providers outside of Google Play on your Android devices or the App Store for iPhone devices for downloading apps. While there may be some advantages to using other app providers, the important thing to know is that we should always be aware of the vulnerabilities in using information resources. Downloading and installing unverified apps can lead to malware and viruses on your devices that can cause problems in your device and compromise your information and security.*

## Netiquette

(4 mins)

[Slide: Netiquette]

- [Use local examples in place of these.] *In most libraries, for example, patrons are expected to be quiet and respectful of the fact that other patrons are sharing the reading space; talking is to be kept to a minimum, and whispering or speaking quietly is expected. On the other hand, at rock concerts, reduced personal distance, physical touching, and sometimes even shoving are the norm; shouting is an expected and necessary means of communication. In a scholarly setting, participants are expected to provide logical arguments with evidence for their statements and speak without extreme emotion; whereas, at a rally or protest, emotion is necessary to persuade others of their cause.*
- *Netiquette, short for "Internet Etiquette," involves the norms and behaviors, codes of conduct, and general etiquette of interacting online. Similar to physical spaces, there are a variety of online spaces, each with their particular norms and codes of conduct.*
- *There are many differences compared to physical space that impacts communication in the online space. For one thing, users generally can't see each other, and, often, don't know each other. This anonymity can be positive or negative. Anonymity can empower people to speak in ways and about things that they otherwise would not in a physical setting amongst people who can see them or that they know.*
- *Another difference: expressing oneself without the benefit of being able to use physical gestures, cues, and emotion. What are some methods you use to express yourself online? [Emoticons, Internet slang / netspeak, capitalization and punctuation, etc.]*
- *Another set of major differences between online and physical spaces is the permanence of information and the ability to disseminate information widely and rapidly to unprecedented numbers of people across the globe in an instant. As a result, Cyberbullying, or bullying online, and hate speech can be particularly damaging.*
- *What are some consequences of violating netiquette expectations?*  
Examples:
  - Conversation degenerating and moving off topic
  - Other participants choosing to exit the online space
  - Receiving criticism and social pressure from other participants
  - Being banned from further participation in an online space

- Legal repercussions (i.e. defamation law, libel, slander, etc.)
- Physical violence
- *How can you ensure that you are engaging in proper netiquette?*  
[Take some examples and discuss briefly.]

## Credit, Credibility, and Copyright

(4 mins)

[Slide: Credit, Credibility, and Copyright]

### Paying Credit Where Credit is Due:

- *Related to netiquette and part of online responsibility is properly crediting online sources of information. In addition to acknowledging another's work by paying credit where credit is due, crediting online sources has the added benefit of boosting the credibility of the referrer by providing evidence of their statements and claims. Having resources credited is also mutually beneficial to the information provider in bolstering their credibility.*

[Provide a relevant local example of how this mutual benefit functions. For example, when a news website refers to your website as a source of credible information, the news website demonstrates its credibility by providing evidence of the news story; in addition, your website reputation as a credible resource is bolstered by the fact that a news website found it to be a credible source.]

Note the distinctions between plagiarism and copyright:

- Plagiarism = presenting copied information as one's original work. Example: copying someone's blog post or other writing and posting or writing as your own.
- Copyright infringement = using a copy of a work without the author's permission. Example: making multiple copies of a book, music, or journal article and distributing them to your friends.
- *There are a variety of ways to credit sources of information. What are some ways to credit information sources that you are familiar with?*  
Relevant examples that you provide will depend on the experience and interests of your participants. For example, students and professionals may want to learn formal, academic methods for citing references.

### Credibility:

The proliferation of online information and ICTs can make it difficult to determine legitimate, credible information and sources. Email phishing scams can often be identified by their unbelievable, "too good to be true" offers, "get rich quick" propositions. Many of these early phishing scams were characterized by poor grammar, punctuation, and spelling; however, phishing scams are increasingly more sophisticated. Particularly over email and phone, phishing scams may identify targets by name, mention legitimate company names or use legitimate logos and company identifiers, and may even have some relevant information related to targets.

- *Finally, as we discussed earlier, the credibility of the source itself must also be determined. How might you determine whether or not a source is credible?*

Encourage participants to think and discuss briefly, filling in as necessary with:

- Author and credentials. Has he/she written other articles considered to be credible? Are the author and his/her credentials considered respectable and authoritative on the subject matter?

- Type of organization. Is the organization considered to be reputable and a credible source for information? What type of information do they provide?
- Content. Does the information appear to be accurate?
- Writing style. Is the information written in a manner that is appropriate as a credible information source?
- References. Do other reputable sources reference this work? Does this work reference reputable sources?
- Date. Is the information current?
- Retrieval. How did you find this resource? Was it found through a reputable channel, for example through a knowledge database or peer-reviewed resource?
- Appearance, spelling, and grammar. Is the format and presentation of the resource appropriate?
- Particularly for email or phone phishing scams, are the messages asking for money, personal, or otherwise valuable information? Most legitimate organizations will not do so over email and phone since this is not a secure form of communication. Do images and logos appear blurry (indicating that they are copies, not originals)?

Phishing scams and non-credible resources are increasingly more sophisticated. Encourage participants to stay vigilant in protecting themselves online.

➤ *Why does credibility matter?*

There are a number of reasons in various situations: rumor, misinformation, disinformation, etc.

Copyright:

While copyright laws may differ, be nonexistent, or are not enforced in some places, it is important to understand the concept of copyright. Copyright laws are meant to protect the rights of authors related to their works of creation. Using copyrighted material without permission is a legal violation, and violators can be subject to prosecution. Trainers should express this in a manner that is appropriate for their participants in the given situation.

➤ *What are some things you can think of that can be violations of copyright?*

Sharing music, pirating software, using online images, sharing digital copies of books, articles, etc.

➤ *How do we comply with copyright?*

This varies, and copyright is a complex, complicated topic that can be tricky to navigate. Generally, acquiring permission from the author to use the work and/or including copyright acknowledgements when using copyrighted information are the minimum requirements. Participants should be made aware that although it is easy to get and use online images, that most are protected by copyright. Participants, however, can and should be encouraged to search for images that are in the public domain and, therefore, not subject to copyright.

## The Cloud

(1 min)

[Slide: The Cloud]

While the Internet has often been represented with the image of a cloud, the contemporary definition of “the cloud” represents more functionality than just the network of networks. Whereas users relied on their devices to manipulate and store information, cloud service providers enable users to manage, store,

and manipulate data over the Internet. The National Institute of Standards and Technology describes cloud computing as a model that provides on demand, ubiquitous access to a shared pool of Internet resources. In essence, the Internet is an unstructured network of networks where users can search and access information, while the cloud represents a structured, yet flexible, network of rapidly configurable resources on the Internet. The cloud is characterized by three service models: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). Depending on the level of participants, trainers will need to adjust how they describe the cloud. It may simply suffice to describe the cloud as:

- *The online space where information can be created, stored, managed, and manipulated.*
- *How many of you have worked in the cloud?*  
Participants work in the cloud by default when using their apps without realizing it.
- *The remainder of our activities will be in the cloud. You will use your devices locally, but the information you manipulate will exist on the cloud.*

## Activities

(120 mins)

### Activity 4.1: Basic Protection Measures

(10-30 mins)

[Slide: Activity 4.1]

Understanding basic protection measures will be helpful for trainers to coach their future participants on how to secure their personal and organization devices, apps, and accounts.

1. Have participants identify security settings and modify as necessary:
  - Device (e.g. password, lock, location settings, remote lock / find / erase, etc.)
  - Frequently used apps, especially social media and messaging apps
  - Browser apps (e.g. Do not track, clear data / history / cookies, etc.)
2. Practice opening private tabs in browsers
3. Open several browser tabs and do random searches
4. Close down the browser, then reopen and view search history
5. Clear history and cookies, then reopen, and view search history to ensure it is blank
6. Secure accounts (e.g. social media, email, etc.)

Discussion (5-15 mins):

- *What security options did you find?*
- *Which did you think were important to set? Why?*
- *How might these security options be important for your organization or personally?*

Demo (1 min):

Display and share an example of real and fake links that you've created in Facebook. Emphasize that participants should always hover over hypertext in order to view the actual hyperlinks to ensure they aren't being deceived.

- *Remember that security features are only part of the security equation, and that it's up to you to remain vigilant about your online security. Where do these links take you? How do you know?*

Demo (1 min):

Use an example of sending messages to multiple individuals in an email with the carbon copy (cc) and blind carbon copy (bcc) options. Demonstrate the same message in a listserv.

- *Do you see advantages to using listservs over group emails? How might you use this in your organizations?*

Depending on how administrators set listservs settings, a major advantage of listservs is the passive means of adding more members. For example, a library or government organization may allow the public to add themselves to listservs to receive email messages. This reduces the load and potential for mistakes in including or excluding email contacts in repeated emails to changing groups. In addition, sending one message to a listserv eliminates the restriction that many email clients and email hosts impose on limiting the number of recipients in an email message to prevent spam.

## Activity 4.2: Using Facebook Groups

(30 mins)

[Slide: Activity 4.2]

Facebook groups are a useful space for communicating with others online but in a distinct space within Facebook. We will use Facebook groups as a way to understand digital information literacy. Trainers should create a larger Facebook group for the participants that they can use for examples, participant questions, and discussion.

Group Work (5-15 mins):

1. Have groups create a Facebook group for themselves
2. Instruct groups to modify the settings to limit membership
3. Have groups add you to their Facebook group
4. Encourage group members to interact and explore in their Facebook group space
  - Posts vs. messages
  - Attaching photos and videos
    - Single photos / multiple photos
  - Tagging photos
  - Creating and managing albums
    - Name / rename albums
    - Delete albums
  - Editing posts
  - Changing the visibility in posts
  - Deleting posts

Discussion (5-15mins):

- *What are some other security options you found for protecting information in settings?*
- *What advantages and disadvantages can you think of related to these settings?*

## Activity 4.3: Using Online Content

(30 mins)

[Slide: Activity 4.3]

Downloading and Saving Files:

Have participants:

1. Find an article in Wikipedia
2. Download and save the article as a PDF
3. Navigate to the saved file

#### Attaching and Sharing Files:

Have participants:

1. Send the PDF as a link in email and to the listserv
2. Upload the PDF to Dropbox
3. Upload the PDF file to their Facebook group page

#### Saving and Sharing Website Links:

Using the same Wikipedia article, have participants:

1. Bookmark the link
2. Share the link to Facebook
3. Share the link in email
  - Advanced: change the hypertext of the link

#### Saving and Sharing Images:

Have participants:

1. Find an image in Google search
2. Send the image in email as an attachment
3. Include the link and credentials to acknowledge the source of the image

## Break

(15 mins)

## Activity 4.4: Intro to Google Docs

(50-75 mins)

[Slide: Activity 4.4]

Demo (10-15 mins): Getting Started with Google Docs

- Navigating to Google Docs
- Creating a new Google Docs document
- Typing text in the document
- Creating a table in the document
- Inserting an image in the document

Note: Ensure that trainers test this functionality ahead of time to get acquainted with the process. Inserting an image is not possible using the Google Docs app on mobile phones and tablets. Trainers will need to use the desktop version in a tablet to do this. A workaround is to save the document as a Word doc and download on your device, then add the image, and reupload the doc to replace the preexisting Google Doc. If you have a sufficiently capable group of participants, instruct them that this is not a straightforward procedure and challenge them to find information on the Internet to figure this out.

- Sharing the document:
  - With others from Google Docs
  - In Email, Facebook, Dropbox (if applicable), listserv, etc. as a link
  - In Email, Facebook, Dropbox (if applicable), listserv, etc. as an attachment

#### Group Work (40-60 mins):

1. Have groups create a single Google Doc to work together on
2. Have groups share the document with each other and with you
3. Instruct the groups to explore together and figure out how to:
  - Insert a table
  - Enter content into the table

It might be helpful to provide elements for the table, for example: a table containing the names of groups members, contact information, and organizations.

  - Insert an image

You may wish to challenge participants by having them insert images from various sources such as from their camera, attachment from an email, from a website, etc.

## Wrap Up

[Slide: Review]

- *This concludes module 4. You now understand basic privacy and security measures, online etiquette, referencing online sources, and working in collaborative online environments.*
- Take any questions or comments if any.

[Slide: Congratulations]

