

DIGITAL SAVINGS GROUP (DSG) TOOLKIT

DIGITAL USER DIALOGUES

GUIDING SAVINGS GROUP MEMBERS THROUGH DIGITAL TRANSFORMATION







WOMEN FOR WOMEN INTERNATIONAL

DSG TOOLKIT: DIGITAL USER DIALOGUES



Authors

Lauren Hendricks, consultant Dennis Mello, Global Communities Paulina (Paula) Rudnicka, Global Communities

Acknowledgments

The authors are grateful for the valuable contributions of multiple people. Iris Navarro (Women for Women International), Mellisa Mazingi (Women for Women International), Theogene Ruhumuriza (Women for Women Rwanda), Philipos Ageze (Global Communities), Hillary Dashina (Global Communities). Special thanks to colleagues from Tanzania (Global Communities), Ethiopia (Global Communities) and Rwanda (Women for Women) for their contributions to the formative gender analyses and peer-review workshops.

Additional thanks to those who provided inputs during the peer-review roundtable discussions: Tamrat Abera (Mercy Corps), marc bavois (CRS), Koen De Beer (Cyclos), Bindi Jhaveri (Grameen Foundation), Tigist Mengitsu (Jamii-One), Yukiko Yamada Morovic (World Vision), Ethel Mulenga (World Vision), David Panetta (LGP), Courtney Purvis (World Relief), Charlotte Ronje (Jamii-One), Karen Vandergaag (CARE), and Wes Wasson (DreamStart Labs).

The Digital Savings Group (DSG) Toolkit was developed by Global Communities in partnership with Women for Women International. Work began under the SEEP Network's Women Saving for Resilience (WS4R) Innovation Fund, funded by the Bill & Melinda Gates Foundation, and was completed through the generous support of other donors.

The DSG Toolkit was created for informational, non-commercial purposes and published on the DSG Hub by Global Communities. The DSG Toolkit can be distributed for non-commercial purposes without the authors' permission. Please credit Global Communities and Women for Women International while distributing the toolkit.

Organizational Websites

www.globalcommunities.org www.womenforwomen.org www.dsghub.org

INTRODUCTION

3

Recent years have seen an increased interest in, demand for, and introduction of digital tools for savings groups around the globe. There now exists a wide range of digital solutions which allow savings groups to do many things, including digitizing their record keeping, replacing physical cash with digital wallets and mobile money, and more.

The digitization of savings groups has the potential to accelerate the many benefits of traditional savings groups by expanding digital identities and bridging the gap to formal financial services, particularly for women. It may also help facilitate participation in the formal economy. We have to remember, however, that digitization happens in the context of a persistent gender digital divide, where women's access to and use of mobile and digital technologies are constrained by rigid gender norms, unequal power dynamics, and resource limitations. Our **research** shows that if not done right, digitization can have negative consequences for women's ability to participate in, lead, and benefit from savings groups. Without adequate training and support, women may experience marginalization and exclusion, especially in mixed-gender groups, where men are often more tech-savvy and therefore more likely to play leadership and digital recordkeeping roles. Women may also face increased risks of data privacy violations and gender-based violence, including technology-facilitated violence.

While the number of technology solutions for savings groups continues to grow, there exists little by way of guidance and tools to support implementers, trainers and groups as they progress through the various stages of digitization. To address this, Global Communities and Women for Women International created the **Digital Savings Group (DSG) Toolkit**. The toolkit consists of seven practical tools to support safe, effective, and gender-responsive digitization of savings groups. These tools include practical guidance for implementers and trainers across multiple aspects of digitization. There is a tool to help implementers gauge their preparedness to launch or expand a DSG project (Digital Preparedness Checklist); a Project Staffing tool to explore changes in the positions and skills needed to support a DSG project; a Monitoring and Evaluation tool to identify key evaluation domains and indicators; tips on Promoting Women's Digital Capabilities; a tool on Addressing Risks of Gender-based Violence; a series of Digital User Dialogues for use directly with savings group members; and a Data Privacy and Security tool with key questions implementers should ask technology providers when considering a digital solution.

Each tool was designed so it can be used by those implementers just beginning to think about their first digital savings group project or by those who are mid-project or preparing to expand. They can be used individually or as a complete set, depending upon the needs of the implementer.



The DSG Toolkit consists of seven practical tools to support safe, effective, and gender-responsive digitization of savings groups. These tools can be used in any order, individually, or in combination, depending upon the specific needs of each organization.

The DSG Toolkit was developed by Global Communities in partnership with Women for Women International. Work began under the SEEP Network's Women Saving for Resilience (WS4R) Innovation Fund, funded by the Bill & Melinda Gates Foundation, and was completed through the generous support of other donors.



DIGITAL USER DIALOGUES GUIDING SAVINGS GROUP MEMBERS THROUGH DIGITAL TRANSFORMATION

Purpose	Mobile phones are much more than just a tool for making calls. Depending on the type — basic phone, feature phone or smartphone — they allow people to connect over social media, send money, download applications (apps) and use the internet. These digital tools offer a wide range of benefits to the user, but it takes specific skills and knowledge to use a mobile phone effectively and safely.
	The resources and dialogue suggestions provided in this tool kit were created to help facilitators demonstrate the value and the functionality of mobile phones and mobile internet to savings group members, while educating users on basic concepts related to online safety, data protection and privacy.
Audience	Staff of implementing organizations, field agents, community- based trainers, community digital champions and DSG members
Time needed to implement this tool	 Completion of individual dialogues with a savings group – 20 to 45 minutes'
Format	This tool is built as a series of digital user dialogues intended to build knowledge and skills for savings group members around how to safely use mobile phones, how to protect their data and how to identify and reduce the risk of technology facilitated gender-based violence (GBV).
How to use this tool	The tool is designed as a journey that takes participants from basic communication skills through more complex skills such as using apps and the internet. Although this framework guides the overall flow of this toolkit, it has been designed so that each dialogue can be delivered on its own. This allows the facilitator to choose which sessions to use depending on what is relevant to their audience.
	It is intended to be used by staff of implementing organizations to train field agents and community-based trainers who can use it to facilitate discussions with DSG members around online safety, data protection and privacy.
	Facilitators should review the dialogue materials in this tool and adapt them to deliver context-specific, gender- responsive and inclusive sessions to their audiences. Facilitators should review provided examples and questions to ensure they are appropriate for participants. They should
	continued on next page

5

How to use the tool - continued	also assess which apps and programs are most commonly used in their area and adapt dialogues accordingly.	
	Field agents and community-based trainers should be well- prepared to deliver this content to the DSGs they support. They should be confident in performing all the tasks, such as blocking a number, that they can demonstrate to the groups.	
	This tool includes both dialogues and handouts, which can be shown and/or left behind with DSGs and community digital champions, so that lessons can be reinforced when a trainer is not available or when members encounter a problem.	
	Discussing GBV risks through user dialogues User dialogues can be an effective way for DSG facilitators and members to discuss GBV risks and mitigation tactics for women using digital technology. These discussions may take place over several meetings, as groups get more familiar with mobile technology and the topics become more relevant. This tool builds from the user journey map covered in the Addressing Risks of Gender-based Violence tool.	
	User dialogues are not meant to discourage groups from digitizing, but members should be aware of risks. Ensure facilitators (field staff and volunteers) are comfortable and prepared to guide sensitive conversations.	
	GBV is a highly sensitive topic and can trigger traumatic memories, particularly among survivors. Accordingly, the tool includes safeguarding tips to reduce the risk of re- traumatization among participants. Prior to user dialogues, instruct facilitators to never solicit personal stories of abuse and to inform participants that they may remain silent or leave the discussion at any time without any repercussions. In addition, map out local GBV service providers and provide the list to the facilitators so that they can make appropriate referrals as needed. You may also wish to enlist a local GBV specialist to co-facilitate some dialogues. You may choose to implement each dialogue or only use those that are most relevant to your context.	
	 When feasible, facilitators should share information needed to report GBV along with a list of GBV resources in the area with participants. Be mindful of how you share this information given varied levels of numeracy and literacy and remind participants to keep this information private if they fear potential backlash by perpetrators of GBV. Phone numbers to report harassment and abuse if this is an action that survivors wish to take List of GBV resources and services in the area 	
	The text box below summarizes key safeguarding tips for facilitators.	
Materials needed	Handouts and posters in annex	
Acknowledgements	This tool and the handouts in the Annex are primarily adapted from GSMA's "Connected Society: Mobile Internet Skills Training Toolkit " with input from other sources.	



Facilitator's Safeguarding Tips

Remember

Some of the topics you may discuss in this section are very sensitive. If you are not comfortable talking about them, the participants will not be comfortable either. Before the session, talk to your colleagues about these issues and get their advice. Your priority is to keep your participants safe, but do not avoid these tough conversations altogether, even if they make you a little uncomfortable.

Discussions around GBV may bring up actual lived experiences of genderbased violence, which may trigger traumatic memories, particularly among survivors.

Never:

- Solicit personal stories of abuse
- Push a participant to share more than they are comfortable
- Tell a story of a woman who has not given you permission to do so
- Use GBV survivors' names or other information that can identify them in the community

Always:

- Inform participants that they may choose to stay silent or leave the discussion at any time without any repercussions
- Express sympathy and concern for the storyteller
- Share resources, such as information about nearby GBV service providers, where the storyteller can get additional help.

7



Tool Modules:

Mobile Account Opening | Basic Phone Use | Mobile Money | Social Media | Apps | Mobile Internet | Data Protection and Privacy | Data Costs



Opening a Mobile Account

Opening a mobile account is often the first step on a digital journey.

Explain:

"Getting a new phone can be exciting, but the process can come with some risks and challenges. For example, some women may face disapproval from or even conflict with their spouses or family members while others may experience disrespectful treatment and harassment from mobile network operator (MNO) agents. It is important to take these risks seriously in order to stay safe.

There are many things you can do to stay safe while buying and setting up your new phone. Remember that you have the right to be treated with care and respect by anyone, including your spouse, family, friends, community members and vendors."

Bring the benefits to life

Tell your own story of how you (the facilitator) opened your first mobile account. Mention the positive benefits of having your own phone and account and how you stayed safe when getting your first phone. Discuss the conversations you had with your friends and family.

Bring the risks to life

Ask participants to share stories they have heard about, or problems others experienced when purchasing a phone. If no one shares, tell a story you know. This might help get the conversation moving. Some risks that might come up include:

- Partner or other family members do not support women getting a phone and this causes conflicts or even GBV at home.
- MNO agent takes a woman's number and uses it to send her harassing calls and messages.
- Agent makes inappropriate remarks or requires excessive fees or favors in exchange for a SIM card.

Some advice to include

- Explain what paperwork is needed to buy a mobile phone and register a number; explain what to do if clients are missing any documents.
- Discuss the risks and benefits of sharing a mobile phone with others or getting a secondhand phone. For example, older phones may not get security updates and could be infected with harmful viruses that can damage user data.
- Explain that it is important to restore previously used phones to their factory settings before first use.

Tool Modules:

Mobile Account Opening | Basic Phone Use | Mobile Money | Social Media | Apps | Mobile Internet | Data Protection and Privacy | Data Costs

q	0	
	$\equiv \equiv$	

Some advice to include - continued

- Emphasize the importance of setting up a personal identification number (PIN) or a passcode on a mobile device so that others cannot access the phone and personal information stored on it without a user's permission.
- Talk about the need to check and adjust privacy settings in the phone operating system before using it.

Share

When feasible and as needed, share the following information with the participants. Be mindful of how you share this information given their varied levels of numeracy and literacy. Remind participants to keep this information private if they fear potential backlash.

- List of recommended MNO agents in the area.
- Phone numbers to report harassment and abuse if this is an action that survivors wish to take.
- List of GBV resources and services in the area.
- List of numbers to local MNOs where users can report harassing callers.

MAKE SAFETY RELEVANT

Discuss with participants how staying safe when buying the phone and opening an account is important.

Ask:

"Have you talked to your family about getting a phone?"

Help the group discuss any resistance they have faced from family members or spouses. How have others managed this?

"Are there things that worry you when you go to buy a new phone?"

Help participants understand how they can be safe in these areas.



Tool Modules:

Mobile Account Opening | *Basic Phone Use* | Mobile Money | Social Media | Apps | Mobile Internet | Data Protection and Privacy | Data Costs



Basic Phone Use

Most people use their mobile phones to make calls and send and receive text messages.

Explain:

"A mobile phone is a way to communicate with your friends, family and business associates. It can be a valuable tool to help you build your business and stay close to your loved ones. Many mobile phones will also allow you to access information and services on the internet.

Your phone also comes with risks. Calls and texts can cost you money, depending on your plan. And you could receive suspicious and inappropriate calls or messages from people who want to bother you or steal from you. Remember that you are the boss of your phone. You can turn it on or off and choose whether to answer a call or text. You can also block numbers and choose who you share your number with."

Bring the benefits to life

Tell your own story of how you have benefitted from using a phone, for example a time you were able to call a family member or used text messaging to conduct business.

Bring the risks to life

Ask participants if they know anyone who has experienced problems with a phone, for example received suspicious or inappropriate calls and texts or had an argument about the cost. If no one shares, try to share a story you have heard. This might help get the conversation moving. Some risks that might come up include:

- · Conflict with a partner over the cost of airtime or time spent on the phone
- · Partner becomes suspicious of who they are calling and texting
- Partner monitors or demands to see the user's text messages and call history
- Receiving unwanted, harassing texts or phone calls
- Spam and/or scam calls or messages

Some advice to include

- Discuss the risks and benefits of sharing a mobile phone with others
- Talk with the participants about how to practice safe digital behaviors on their mobile phones, for example by:
 - adjusting privacy settings on the phone
 - choosing strong passwords and PINs and keeping them secret

Tool Modules:

Mobile Account Opening | *Basic Phone Use* | Mobile Money | Social Media | Apps | Mobile Internet | Data Protection and Privacy | Data Costs



Some advice to include - continued

- reporting and blocking unwanted numbers, especially when someone is harassing them
- erasing text messages and call histories; or
- installing caller identification and spam blocking applications, such as Truecaller.
- Ask participants about what they do to stay safe.
- Discuss how to report a harassing caller.

PHISHING SCAMS

'Phishing' is a name given to the practice of trying to trick mobile phone and internet users into sharing personal or confidential information. Phishing scams are unfortunately very common, and you should be suspicious of calls, SMS messages or e-mails requesting personal information from people you don't know. Phishing scams can include:

- Attempts to get your bank or mobile money account information: "We need to send you money, and we just need your account number to verify"
- "You won a contest. Send us your account information to claim your winnings."
- Messages that look like they come from an actual business: "This is Airtel, we need your PIN or passcode." Remember, legitimate companies will never ask you to share your password, account number or PIN through a call, SMS or email. If you are unsure if a request for information is trustworthy, call the company from the number on their top-up card or website.

Demonstrate

- Demonstrate how to block a phone number and delete a text message. If
 possible, use a second phone to send participants a text, and then demonstrate
 how to block the number and delete the text. Do not use your own number, as
 you may want the participants to be able to contact you in the future.
- Demonstrate how to check phone credit and data balances.
- Demonstrate how to check for a network connection, connection level and battery level.

Tool Modules:

Mobile Account Opening | *Basic Phone Use* | Mobile Money | Social Media | Apps | Mobile Internet | Data Protection and Privacy | Data Costs



MAKE SAFETY RELEVANT

Discuss with participants how staying safe when using the phone is important.

Ask:

"Have you talked to your partner about how you will pay for airtime or how much airtime you will use in a week?"

Help the group discuss any resistance they have from partners on airtime costs. How have others managed this?

"Have you or anyone you know been harassed over the phone?"

"Have you ever received scam messages: an offer of free money, a notice of a lottery winning or a request for your PIN or account info? If so, what did you?"

Help the group understand how they can be safe in digital areas

Explain:

- Your phone allows you to call and send messages to friends, family, and people you do business with. You can even send messages to people on the other side of the world that you haven't met before. However, this means that sometimes people may send you messages that you don't want to receive."
- "Keep your information private, block unwanted contacts and teach your children to do the same if they use your phone."
- "On your phone or on the internet you are able to stop any unwanted messages you receive."

Ask the participants how they send messages to others on mobile phones.

Demonstrate how to block numbers and unwanted messages on their phones and applications such as WhatsApp, Gmail and Facebook.

In the Annex you can find a series of posters called "<u>How to Block</u>." Share these with the participants.



Tool Modules:

Mobile Account Opening | Basic Phone Use | *Mobile Money* | Social Media | Apps | Mobile Internet | Data Protection and Privacy | Data Costs



Mobile Money

Mobile money allows you to send and receive money using your mobile phone.

Explain:

"Mobile money is one of the most used features of a phone. With a mobile money account, you can send and receive money to/from any other person, even if they do not have a phone. This includes your family members, friends, vendors and business associates.

Mobile money has great benefits, but it comes with risks and challenges. The money you send over the phone is real money. If you accidentally send it to the wrong number, it can be hard to get it back. In addition, some women may face disapproval from their partner or family members over their digital transactions while others may be mistreated or even harassed by mobile money agents. It is important to treat these risks seriously to stay safe. Remember that you have the right to be treated with care and respect by anyone, including your spouse, family, friends, community members and vendors."

Bring the benefits to life

Tell your own story of how you have benefitted from using mobile money, for example a time you were able to send or receive funds to meet an urgent need.

Bring the risks to life

Ask participants if they know of anyone who has experienced problems with mobile money. If no one shares, share a story you have heard. This might help get the conversation moving. Some risks that might come up include:

- Partner monitors the user's transactions on the phone and resents her for making financial decisions
- Risk of experiencing harassment from the mobile money agent, or while traveling to the agent
- Members of the community feel threatened or perceive a woman's use of mobile money as challenging masculine roles
- Risk phone theft or cash after cash-out

Some advice to include

- Explain what needs to be done to open a mobile money account or tell participants where they can find the information.
- Discuss how important it is to do your own transactions and advise participants not to hand their phones to agents or someone else to do it for them. If they need advice or a reminder on how to make a transaction, they should ask a

Tool Modules:

Mobile Account Opening | Basic Phone Use | *Mobile Money* | Social Media | Apps | Mobile Internet | Data Protection and Privacy | Data Costs



Some advice to include - continued

trusted friend or family or community member. Also discuss how important it is to finalize transactions before passing on a shared phone.

- Talk with participants about how to practice safe digital behaviors on their mobile phones to protect their mobile money and other private information, for example by:
 - choosing a strong password or PIN and keeping them secret; never giving them to mobile money agents or even friends and family.
 - never writing down PIN numbers, especially on your phone cover, visible location or in a place where others can find it.

Ask participants what they do to stay safe.

- Discuss how to have safe, open, productive conversations about money and financial decision-making with partners and other family members.
- Discuss how to report an agent who engages in inappropriate behavior or is overcharging for transactions.
- Discuss how to report a mistake in a transaction and leave a list of customer service numbers for the different providers.

Demonstrate

Demonstrate how participants can send money to a friend.

Ask participants if anyone has a need to send money using their account and if they would like to demonstrate how sending money works. If the answer is yes, talk them through it so that the whole group can hear, but make sure that no private information is revealed during the process. Be sure to go all the way to the SMS text confirmation so they know the transaction went through.

If no one wants to be an example, demonstrate how it can be done on your phone.

Share

When feasible and needed, share the following information with the participants. Be mindful of how you share this information given their varied levels of numeracy and literacy.

- List of recommended mobile money agents in the area.
- Handouts "Staying Safe Using Mobile Money."

Share any additional advice or recommendations with the participants that you believe might be useful to them.

MOBILE MONEY: Remember that your PIN is your own personal number. It is important that you keep it private as it is how you access your account. Be careful about sharing this number with anyone, even mobile money agents or customer care staff, whether in person, via SMS or the mobile internet.



Tool Modules:

Mobile Account Opening | Basic Phone Use | Mobile Money | *Social Media* | Apps | Mobile Internet | Data Protection and Privacy | Data Costs



Social Media

Social media allows you to connect easily with friends and family.

Explain:

"Social media includes apps like Facebook, Instagram, YouTube, TikTok and Twitter. These platforms offer great opportunities to communicate with friends and family, learn new things (often for free), and even do business online. Some of them, like WhatsApp, can be cheaper than using SMS messaging.

Social media has some risks including not always knowing who is seeing your information. Strangers can contact you and ask you to be their online "friend," which can give them access to images and information you have shared on social media. Dishonest people can use social media to scam people out of money. In addition, some people post hateful comments and use social media to harass, bully, blackmail or threaten others. This behavior is called online violence and is often directed towards women and girls. It is important to treat these risks seriously to stay safe on social media. Remember you have the right to be treated with care and respect by anyone, including strangers online."

- You can take steps to manage who sees your 'posts' on social media. If you only want your close friends or family to see what you post, you can limit other people from seeing what you put out there through privacy settings.
- Remember that the internet is a public place, and you cannot always control what happens to your content once you have shared it. You should only post things that you want other people to see now and in the future. Some people say, 'What goes on the Internet, stays on the Internet,' because once you share something online, it is very hard to remove it permanently.
- Remind your children that if they wouldn't want their head teacher or grandmother to see something, they should not risk posting it.

Bring the benefits to life

Tell your own story of how you have benefitted from using social media. Use an example of when you connected with a group of friends or family at one time.

Bring the risks to life

Ask participants to share if they know of anyone who has experienced problems on social media. If no one volunteers, share a story you have heard. This might help get the conversation moving. Some risks that might come up include:

- Partner is jealous of who the user is messaging or interacting with on social media
- Online harassment or bullying on a social media platform
- Being contacted by strangers
- Online scams

15

Tool Modules:

Mobile Account Opening | Basic Phone Use | Mobile Money | *Social Media* | Apps | Mobile Internet | Data Protection and Privacy | Data Costs

♪
_

Some advice to include

Social media platforms, like Facebook, have become powerful tools. Although they can be a useful way of keeping in touch with people, they also have dangers. Here are some tips to stay safe:

- Don't overshare. Sharing too much personal information across social media sites can be dangerous. Things such as your address, birth date, schedule and other facts about your life could be used to steal from you or even harass you. You should always ask if you'd be comfortable with strangers knowing the things you share.
- Update your privacy settings. Most social media sites allow you to have some degree of control over who sees information on your social media profiles. However, they often default to sharing quite a bit of personal information. You should regularly check to see how your information is being presented, and who can see it.
- Block suspicious accounts or abusive users. If you get a friend request from someone you don't know, don't accept it. Think critically about the requests from someone you know, if you spot anything suspicious, you can block the account, meaning it can no longer interact with you. Similarly, you can block any user who harasses you or engages in other abusive or inappropriate behaviors. You can also report users to the social media platform on which the abuse took place, so the company can take appropriate action against them (for example, remove the abusive post or even deactivate their social media account). See relevant handouts in <u>Annex</u>.

Ask participants what they do to stay safe.

Demonstrate

Demonstrate how participants can delete a contact on WhatsApp.

Using a second phone or number, send a contact request to a participant, and have them accept it. Exchange a message or two. Then talk them through deleting you as a contact — do not do it for them. Explain that all social media apps allow them to block or unfriend contacts and report abusive users. Make it clear they do not ever have to endure harassment on social media.

Also show them how to "delete and report - do not have them delete and report the contact - but show them it is an option they can use if they are being harassed.

Tool Modules:

Mobile Account Opening | Basic Phone Use | Mobile Money | *Social Media* | Apps | Mobile Internet | Data Protection and Privacy | Data Costs



MAKE SAFETY RELEVANT

Discuss with participants why staying safe when using social media is important.

Ask:

"How might your partner react to you talking to friends or strangers over social media?"

Help the participants discuss how they will manage their partner's expectations.

"Has anyone you know been harassed over social media? Have you ever witnessed any hateful or inappropriate behavior on social media?"

Discuss what happened and how participants handled the situation. Refer to the "Facilitator's Safeguarding Tips" in the introduction to this tool before starting this conversation.

Help the participants understand how they can be safe on social media.

17



Tool Modules:

Mobile Account Opening | Basic Phone Use | Mobile Money | Social Media | *Apps* | Mobile Internet | Data Protection and Privacy | Data Costs

18

Apps

An app (application) is a program that can be downloaded onto your phone.

Explain:

"There are thousands of apps available that can do anything from providing online education and entertainment to allowing you to transfer money and managing savings group records.

Apps have some risks and not all apps are safe to download, as some can steal information and data from your phones. Others have hidden charges that can end up costing lots of money. This might be stressful for you and your family, causing conflicts and disagreements in your home. In addition, many apps collect personal information about you that can be shared or sold to other companies. Some apps can also expose you to unwanted explicit images, in-app harassment or even track your whereabouts in real life. It is important to treat these risks seriously and only download apps from trusted app stores."

Bring the benefits to life

Tell your own story of how you have benefitted from using an app.

Bring the risks to life

Ask participants if they know of anyone who has experienced problems with apps. If no one shares, share a story you have heard, this might help get the conversation moving. Some risks that might come up include:

- In-app harassment and hidden charges
- Jealousy from friends or family that you are getting too 'advanced' using the phone
- Conflicts at home

Some advice to include

- Discuss how to download apps safely (from trusted app stores such as Google Play Store and the Apple App Store), delete apps from the phone and close in-app accounts with private information.
- Talk with the participants about how to practice safe digital behaviors on their mobile phones, for example by choosing strong passwords on apps and keeping them secret.
- Some apps have hidden charges; inform the participants that they can turn off the 'in-app' purchases in any app to prevent accidently incurring costs.
- All mobile apps collect information about us when we use them. This includes information that we enter (name, date of birth, gender, etc.) and information that we do not enter, including our locations and data on how we apps are used.

Tool Modules:

Mobile Account Opening | Basic Phone Use | Mobile Money | Social Media | *Apps* | Mobile Internet | Data Protection and Privacy | Data Costs



Some advice to include - continued

 Some of this information is required for the app to work correctly. For example, a savings group recordkeeping app needs to gather members' names, savings information and loan information. Additional information may be collected and used to target advertisements and additional products or features to app users.

Ask participants about what they do to stay safe.

Demonstrate

Inform participants about the difference between removing an app from the phone's home screen, deleting an app from the phone and deleting an account associated with an app.

Before the session, download a series of apps onto a demo phone. Pass the phone around the group and have each member delete one of the apps.

Explain to participants what an app is asking when it requests to share data or suggests paying for extra features or content, demonstrate what this may look like. Explain that participants don't have to say yes in order to use the app, provide an explanation of what information the app is trying to access and why.

MAKE SAFETY RELEVANT

Discuss with participants why staying safe when downloading and using apps is important.

Ask:

"Has anyone in the group used an app? What was your experience?" "What are some of your favorite apps?" "What risks are you worried about when using apps?"

Discuss concerns and how participants could handle them.



Tool Modules:

Mobile Account Opening | Basic Phone Use | Mobile Money | Social Media | Apps | *Mobile Internet* | Data Protection and Privacy | Data Costs



Mobile Internet

Mobile internet provides access to knowledge, information and entertainment from around the world on your mobile phone.

Explain:

Mobile internet allows you to access information and knowledge from around the world. It provides entertainment, facilitates access to services and credit, and even allows people to do business online, connecting them to a global marketplace.

The internet is an extremely useful tool that can be used to connect to information, services and opportunities, but it comes with risks. It is a public space, and you should treat it like you are in a public marketplace. Keep your personal and financial information secure on the internet. And remember, you do not really know the people you meet on the internet; they might not be who they say they are. While many people have formed real friendships through the internet, dishonest people can use the internet to trick or scam people out of money. Others use the internet to harass, bully, blackmail or threaten others and there are at times hateful comments, disturbing or explicit content and misinformation online. This behavior is called online violence and is often directed towards women and girls. It is important to treat these risks seriously to stay safe. Remember that you have the right to be treated with care and respect by anyone, including strangers online. Finally, be mindful that anyone who has access to your phone can see which websites you have visited, so if you are uncomfortable sharing this information, delete your browsing histories. Enjoy the internet but continue to be cautious.

Bring the benefits to life

Tell your own story of how you have benefitted from using the internet. Share the wide variety of things you have used the internet for.

Ask the participants to share how they have used and benefitted from the internet.

- "What do you (or would you) use the internet for?"
- "What do you think are some benefits of using the internet?"
- "What is the difference between the internet, Facebook and mobile phone applications?"

Bring the risks to life

Ask participants to share if they know of anyone who has experienced problems on the internet. If no one shares, share a story you have heard. This might help get the conversation moving. Some risks that might come up include:

- Online harassment, luring, exploitation and other forms of online violence
- Unwanted explicit or violent content (text, images and videos).
- Online scams, fraud, identity theft

Tool Modules:

Mobile Account Opening | Basic Phone Use | Mobile Money | Social Media | Apps | *Mobile Internet* | Data Protection and Privacy | Data Costs



Some advice to include

Talk with the participants about how to practice good digital citizenship and how to use the internet in a safe and productive way.

- Discuss how to use the back or home button if you stumble across something on the internet that you do not want to see.
- Discuss the fact that the internet keeps a record of visited websites, called browser history. You can erase this information so that no one else can see it.
- Most websites also use 'cookies' or small packets of information to remember how you used the website. You can turn off this tracking and you can also delete your 'cookies' if you use a shared phone.
- Discuss that not everything you see on the internet is true. Talk about trustworthy websites participants can visit to find reliable information.
- Discuss how to report abusive or inappropriate content on sites like Facebook or YouTube.
- Explain how to understand if a website is secure or trustworthy (e.g., the 'padlock' icon). If you look at the address line on most websites on the left-hand side, you'll see a padlock. It means that the website meets internet safety standards, most websites have it. Never enter your private information into a website that does not have the padlock icon.
- Mention that there are many ways we share personal information (or personal data) whenever we access the internet. This is explained in more detail in the dialogue on <u>Data Protection and Security</u>.

Demonstrate

Pull up a website and show the participants the small padlock symbol that indicates a secure website. Then pull up a website that doesn't have the padlock.

Ask participants what they do to stay safe online.

Demonstrate how to turn on SafeSearch in Google Chrome. If you use this feature, Google Chrome will only show you websites that are suitable for the whole family. You may also demonstrate how to browse in private using Google Chrome's incognito mode.

Give or show participants the poster explaining the 5 key tips for spotting false information online. <u>See Poster</u>

- 1. Not everything on the internet is what it says it is. Be careful!
- 2. People can make fake versions of a website or an app to make it look like a reputable company (e.g., your phone company) or organization (e.g., your government). If you are unsure if a website is real, ask someone you trust.
- 3. People sometimes put false information on the internet or share it through

Tool Modules:

Mobile Account Opening | Basic Phone Use | Mobile Money | Social Media | Apps | *Mobile Internet* | Data Protection and Privacy | Data Costs



The 5 key tips for spotting false information online - continued

WhatsApp or Facebook. Don't share something with other people without thinking critically first.

- 4. Factcheck news or other content you find on the internet by visiting additional trustworthy sites.
- 5. If you think something you see is dangerous, abusive or inappropriate, you can 'report' it to the company (e.g., WhatsApp).

MAKE SAFETY RELEVANT

Discuss with participants why staying safe when using the internet is important.

Ask:

"What are you worried about when you access the internet?"

Discuss these worries ask how participants would handle them.



Tool Modules:

Mobile Account Opening | Basic Phone Use | Mobile Money | Social Media | Apps | Mobile Internet | *Data Protection and Privacy* | Data Costs



Data Protection and Privacy

It is very important to keep your personal data private and safe

Explain:

When you use apps, social media or the internet we share different types of personal information – often called personal data, or simply data. We leave digital footprints when we access the internet, post on social media or use an app. When we do these things, companies collect data or personal information from us. Given its importance, it's essential to know how to protect your data.

Main points:

- Nearly every time you use your phone or the internet, you are sharing information. This includes when you enter information in forms and when you are looking at websites, videos or listening to music.
- When you share personal data online, over social media or in apps it can be collected and used by companies. Some of this can be beneficial, but there are times data can be used to harm you.
- Because the data you share online is public, you must be careful what you share. Once you share it, it can't be taken back.
- There are ways to protect your data online, but you must take steps to do that, it is not automatic.
- If your data is stolen, there are steps you can and must take to protect yourself.

DEFINING DATA, DATA PROTECTION AND DATA PRIVACY

In this tool, **data protection (security)** is understood as systems and processes designed to secure the privacy, availability, and integrity of data collected through mobile phones. This includes the prevention of unauthorized access or misuse of the data that mobile phone users have agreed to share. **Data privacy** is defined as the right of mobile phone users to have control over how their personal data, including personally identifiable and financial information, is collected, stored, and used.

The word 'data' can mean different things depending on how it is used.

One definition describes your personal information that is collected by your phone company or through social media and the internet. This includes both:

 personal information that you share through your phone when signing up for an app, opening a mobile money account or using a DSG record keeping app.

Tool Modules:

Mobile Account Opening | Basic Phone Use | Mobile Money | Social Media | Apps | Mobile Internet | *Data Protection and Privacy* | Data Costs



DEFINING DATA, DATA PROTECTION AND DATA PRIVACY

 personal information that mobile phone companies, websites and apps collect about you when you access social media or the internet such as location data, browsing history and how you use the website or app.

This User Dialogue discusses what you can do to protect your personal data.

Another way the word data is used is to refer to the credit you need to use the internet – these are often called 'Internet Bundles' or 'Data Bundles' and can be purchased like airtime or talktime. This type of data and costs are explained more in the next User Dialogue.

What is personal data?

Personal data is any information about you as an individual. That includes pieces of information which can lead to identifying you as a person. If you share anything about yourself online or through apps, companies or others can collect this information. For example, your personal data includes:

- Your name, birthday or gender
- Phone or identification numbers, such as your passport number or national identification number or national insurance number
- Your physical home address or your smartphone's location history (tracked by many apps)
- Any online identifier, such as your email address or your phone's IP address (a specific online identifier)
- Financial information including around your personal savings, loans and repayment history (examples of specific data collected through DSG apps are given below).

There are also other types of sensitive data that count as personal data:

- Your racial or ethnic origin
- · Your political opinions, religious or philosophical beliefs
- Details about your personal and professional life, including family, friends, colleagues or business associates
- · Biometric data that can identify you, such as fingerprint or facial recognition data
- Information relating to your physical or mental health.

Ask:

"What types of information do you think of as personal information?" "Do you feel comfortable sharing this information with companies? How about with strangers online?"

Tool Modules:

Mobile Account Opening | Basic Phone Use | Mobile Money | Social Media | Apps | Mobile Internet | Data Protection and Privacy | Data Costs



There are many steps you can take to keep your personal data safe. Let's look at how our data is used online and why protecting it is important.

How can your personal information be used?

Explain

Companies use personal information and data to better understand customers and target them with different products and services. Every time you use your phone you create data, this can have benefits and risks for you as a user, so it's important to know what those are. Some of the ways companies can use your personal data include:

Advertising

Different websites and apps can track when you search for products or make online purchases. They use that information to advertise similar products to you. Many apps are free to download and use, but companies will often collect user data and sell it to advertising companies. They may not know any of your personal details, but they will still be able to target you with advertisements.

A useful example is music streaming services (name a local service Mdundo, Boomplay, Audiomack or Spotify). As you listen to songs, Spotify identifies similar songs to develop a profile for you. From here, it finds and recommends songs that fit your profile but that you have not listened to. You may like this because it introduces you to new music or you might be annoyed that Spotify knows so much about you.

For DSG members there are different levels of personal information or data that may be collected when a group uses a DSG app. Information collected through a DSG app could include:

- Group name
- Member names
- Meeting location and times
- Financial transaction information (savings, loans)
- Savings and loan balances of group and individual members
- Loan repayment history information
- Share prices and share out values
- Group profit
- Member turnover

Tool Modules:

Mobile Account Opening | Basic Phone Use | Mobile Money | Social Media | Apps | Mobile Internet | Data Protection and Privacy | Data Costs



DSG data can be shared with others, but only if you agree that it is okay to be shared. This is known as giving your consent. There are both benefits and risks to sharing your data with others as explained in the following table.

WHO	BENEFIT	RISK
Implementing non-governmental organizations (NGO)	NGO can offer specific training and support needed by group based on data collected from group members. This data is typically shared as group level data (i.e., total group savings, loans), not at the individual level.	NGO might not have strong data security protocols and your data could be stolen. NGO might be required to share data with the government or donors.
Bank or microfinance institution (MFI)	Banks and MFIs can use the information to identify who could be a good customer for formal credit or other financial products.	Banks may encourage people or groups to take loans that they cannot afford to repay.
Government	Government could use data to know where more banking services may be needed.	Some members may not want their information shared with the government.

Credit Scoring

Some companies will look at the way you use your phone to understand if they should offer you a loan. They might look at data on how often you top-up your data, how often you use mobile money and how you perform other transactions.

Credit Reporting

There are many services now where you can access small loans from your phone (facilitator should mention names of local products, like M–Pawa in Kenya). If you are late making payments on these loans, this data gets recorded, and may be reported to a credit rating agency. As a result, you may have trouble getting a loan in the future.

Why protecting your data is important?

Fraud. Cybercrime is on the rise, so keeping your data secure helps prevent people from accessing your accounts. Whether it's your bank details, login information or other account details, if someone has that information, they can use it to steal from you.

Tool Modules:

Mobile Account Opening | Basic Phone Use | Mobile Money | Social Media | Apps | Mobile Internet | Data Protection and Privacy | Data Costs



Control. Ultimately, protecting your data means you retain control over who uses it and how it is used. Once it's stolen, it can often be very hard to get back full control.

Ask: "Have you heard about people who have had their data stolen?" "What do you worry about people doing with your data?"

Your rights and freedoms. You have the right to own your information and data. You also have the right to decide which personal data you share. Some websites and apps will require that you only share a few details to use their services while others require that you share more details. It is always up to you to decide if you are comfortable with sharing your information. You always have the choice to decide not to use an app, or to only share the minimum level of information required. Keeping your personal data safe means that you are protected. It avoids situations where an organization or individual uses your information against you.

How to protect your data

Now that you understand why data protection is so important, let's talk about how you can protect your data. The important thing here is to understand some ways in which your information might not be safe, from here, you can take the necessary steps to secure it.

On your phone

Pay attention to passwords and PIN codes

Passwords are your first line of defense. It can be tempting to use the same password on all apps or websites, but for important accounts, try to use different passwords. That way if someone finds one of your passwords, they cannot access all of your accounts. To make your passwords strong, you should use a combination of upperand lower-case letters, numbers and symbols. You should keep your passwords private and avoid writing them down in places where others can find them.

Be careful of what data you share

Many websites and online services will ask you to share personal information and private data when you sign up. It is worth paying attention to what is required and what is requested. You may not need to hand over anything more than your name and email address. Similarly, you should try to find out what the website will do with your data and who they share it with. Many websites outline this in their privacy policies posted at the bottom of each page.

Be mindful of public Wi-Fi

When you are on public Wi-Fi, there is a higher risk that the data you send could be intercepted by other parties. Be careful doing things like banking and sending sensitive information while connected to public Wi-Fi.

Tool Modules:

Mobile Account Opening | Basic Phone Use | Mobile Money | Social Media | Apps | Mobile Internet | Data Protection and Privacy | Data Costs



Only use secure websites

When you visit a website, you will often see a small padlock symbol at the top of the browser navigation bar. This means the information you send or get through the website is more secure and is less likely to be stolen. You should still be careful, even when this symbol is present. You should not share personal data on sites that do not have the padlock symbol.

Don't click on suspicious email or SMS links

A popular way of trying to access your personal data is to use what's known as phishing scams. These are often sent via SMS or email and try to trick you into handing over your data. It could appear to be from someone you know, and usually requires you to click on a link or download an attachment. You should not do either until you're entirely sure it's legitimate.

Use anti-virus and anti-malware software

Cybercriminals - often called 'hackers' - use malicious programs called malware which can infect and damage your device like a virus and steal your data. Install good, reputable anti-virus and anti-malware programs to keep your device safe from these threats. Do not follow suspicious website links and do not open suspicious emails or texts. This is how malware can get downloaded into your device, without your knowledge.

Erase data from used phones

Clear your data from your old phones before you sell it or throw it away, do the same if you purchase a used phone. The easiest way to clear data is to restore the device to factory settings.

Update your software

Operating systems are frequently updated to make sure they're not vulnerable to malicious attacks and hacks. Many devices automatically download and install the latest updates, but it's possible to turn them off. If you haven't updated your phone in a while, make sure you have the latest operating system updates installed. You can often find software updates in your phone's settings.

Pay attention to app sharing

When you install an app on your phone, you'll often get a notification asking for your permission to share certain information, including your location. It's essential that you keep track of which apps are sharing what data, as some will take more than you might expect.

Tool Modules:

Mobile Account Opening | Basic Phone Use | Mobile Money | Social Media | Apps | Mobile Internet | Data Protection and Privacy | Data Costs



Backup your data

If you're concerned about losing things stored on your phone, like messages or photos, you should consider backing up your data. Whether it's by using a cloud storage service, or other methods, it can ensure that you don't lose valuable information.

Demonstrate

Demonstrate to participants how to change phone passwords and ask each one to practice by changing their password, and then changing it back again. Passwords are very sensitive, so support each participant when they change it for the first time. But do not watch the final time they change their password. It is important to practice what we teach on password security.

DISCUSS: What to do if your data is compromised

Even when you know how to protect your personal information, there can be instances when someone accesses it without your permission. Here are some things you can do:

- Change your passwords. If you know someone has gotten access to your phone, or has seen your data, the first thing you should do is change your passwords. Think about not just your phone's password, but also app, social media and other internet passwords.
- Keep an eye out for fraud. If someone has accessed your phone accounts, keep an eye on your mobile money and bank accounts to ensure no one is accessing them. If necessary, go to the bank or a mobile money agent to update them and change your passwords.
- Report it. If you think your personal information has been compromised, report it. If it was stolen through a social media site, you can report it there. You should also let your bank and other institutions know to set up extra security on your account.



Tool Modules:

Mobile Account Opening | Basic Phone Use | Mobile Money | Social Media | Apps | Mobile Internet | Data Protection and Privacy | *Data Costs*



Data Costs - Data and Internet Bundles

What is it?

Whenever you use the internet on your phone, you are using data, this means you need to buy data or internet bundles from your mobile network. Some activities on the internet use more data such as music or video streaming and downloading.

You can buy data for the internet; it is like buying phone credit for calls and messages. Internet data can be purchased from your local mobile network agent or phone credit seller who will top it up for you.

Sometimes internet data can also be bought in 'data vouchers' or 'data cards' or with mobile money that you can use to top up your mobile internet.

What uses Data?

Show the cost poster. See Poster in Annex

"Different activities use different amounts of data. Viewing text messages uses the least amount of data, then looking at images, playing and downloading music, stickers and ringtones while downloading and playing videos uses the most data. Videos tend to use more data than other internet activities, so be mindful of this while watching videos online."

Explain that "software updates also use data and will cost money."

How do you Check Your Data Costs?

"It is useful to check your data to understand how much you have used, and different activities impact data cost."

You can check how much data you have, just like when you check how many minutes or texts you have by typing in a code on your phone from and receiving a response from your mobile network."

Demonstrate

Demonstrate to the participants how to check data. This will differ depending on which country you are in and which network you use, ask a mobile agent if you need help.







Easy tips for internet safety



'Block' or ignore people you don't know, or who are bothering you



Keep your personal information private



Tell someone you know and trust if you feel uncomfortable about anything you see or experience



Be polite and respectful to people



WhatsApp How To 'Block' How to use











How to 'block' on Gmail









How to 'block' on Facebook





Reporting a page on Facebook













What is mobile money



It's like having a wallet on your phone.



Cash can be deposited and withdrawn from your mobile money account with your agent.



You can send money to other people, pay bills, pay for goods.



Your PIN number is the way you can use your account.

Registering for mobile money account



You need a SIM card from your mobile operator. Your money agent will register you for mobile money.



To register for mobile money, you need proof of identity.



Go to your agent every time you need to deposit or withdraw money from your account.



Once these steps have been completed you can start using your mobile money account!

What you can do with mobile money



Staying safe using mobile





Message





Phone



Agents

5 key things to know about mobile money





5 key things to know about mobile money

Account registration

who will help you create an account. To do this you will need a SIM card To use mobile money you will need to register at a mobile money agent and some ID documents (like a passport, driving license or voters card)

Mobile money account

mobile money you can send and receive money from people, and make A mobile money account is like having a wallet on your phone. With payments just using your phone - all without having a bank account

Mobile money agent

A mobile money agent is who you go to when you need to deposit or withdraw money from your account. They can help you if you have a problem with your account

Mobile number

A mobile phone number – the one you use to call and SMS people -are someone using mobile money you use their mobile number. This is the important for mobile money. When you want to send money to same if they want to send money to you.

PIN number

money account. You will need to type this into your phone when using This is your personal number which helps you protect your mobile mobile money. Keep it safe and don't share it with anyone!



Device Security





1

Next

100 C 100 C

Bet some lock for some lock

I

Accessing 'search history' in Chrome



False information



Report it



Data Costs

