DIGITAL SAVINGS GROUP (DSG) TOOLKIT

Tools to support safe and gender-responsive digitization of savings groups

Global Communities

WOMEN FOR WOMEN INTERNATIONAL

DIGITAL SAVINGS GROUP (DSG) TOOLKIT

Tools to support safe and gender-responsive digitization of savings groups

Global Communities
Partners for Good

WOMEN FOR WOMEN INTERNATIONAL

Authors

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

Acknowledgments

The authors are grateful for the valuable contributions of Loise Maina, Iris Navarro, Mellisa Mazingi and Faith MacPherson (Women for Women International), Theogene Ruhumuriza, Ezekiel Rukema, and Didier Uyizeye (Women for Women Rwanda), Philipos Ageze and Hillary Dashina (Global Communities). Special thanks to colleagues from Tanzania (Global Communities), Ethiopia (Global Communities) and Rwanda (Women for Women Rwanda) 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.

Organizational Websites

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

TABLE OF CONTENTS

INTRODUCTION

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.

DIGITAL SAVINGS GROUP (DSG) TOOKLIT - *Toolkit "Map"*

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.

DSG TOOLKIT:

DIGITAL PREPAREDNESS CHECKLIST

DIGITAL PREPAREDNESS CHECKLIST

Facilitator's Guide

Preparation

The Program Designer, Manager and the Facilitator should review the tool and adapt it to their program. Not all components will apply, and they can be deleted while others may need to be contextualized. The Facilitator should then convene key staff members for a two-hour workshop to complete the checklist.

Objectives

- Prepare for or improve efforts to digitize savings groups in an effective and gender-responsive manner through a review of key considerations for implementers, savings groups, their communities and other stakeholders
- Assess organizational preparedness to launch or scale digitization of savings groups
- Examine approaches and resources needed to advance gender equality in the context of digital savings groups (DSG) projects, reduce gendered risks and barriers to digitization and address intended and unintended gendered consequences of digitization
- Identify resources needed for effective digitization of savings groups

Participants

Program managers, designers and implementation staff; monitoring and evaluation (M&E) team, gender specialist

Materials

1. Copies of the checklist for each participant
2. Flip chart which replicates the checklist for recording answers and notes in plenary session

Facilitator's Notes

- Some participants may feel that this tool is a direct assessment of their skills and knowledge. It is important to emphasize in the introduction that the purpose of the tool is to prepare for the project and ensure its success. It is not an individual assessment, and it will not impact the staff members' performance evaluation or ability to remain in their position. Encourage participants to share honest opinions about professional development opportunities they think they might need to perform digitization-oriented tasks effectively and in a gender-responsive manner.
- In plenary, limit discussion of areas where there is agreement, whether the answer is yes or no. Reserve discussion time for areas where groups had different answers, or where questions remained unanswered. Help the group explore the issue in plenary, but do not feel the need to reach consensus.
- If there is no time to discuss all areas of deficiency or disagreement, select those that you believe are the most important for plenary discussion. Follow up with participants after the workshop to solicit further input on the areas which were not covered.

Staff Workshop (2 hours): Session Flow and Description

Workshop Agenda

1 *Introduction – 15 minutes*

If the group is unfamiliar with each other, have participants share their name, position and a brief description of one instance when they were alerted to the importance of gender awareness in their work.

Share session objectives with participants.

Elicit participants' expectations for this staff workshop.

Discussion Questions:

- Why are these approaches, skills and resources critical to the success of a savings group digitization program?
- What are the risks of implementing a program without these skills and resources?
- How does using a gender lens influence project approaches and the types of skills and resources needed for savings group digitization?

2 *Small Group Discussion – 45 minutes*

Activity: Complete the Digital Preparedness Checklist

Assignment: Divide participants into two to three small groups and give them ten minutes to read the checklist, then discuss and answer each question on the checklist. Note any areas where participants are unsure and what information they would need to feel confident to give a yes answer. Discuss potential solutions — resources and adaptation strategies — for addressing checklist items where the group answered no.

3 *Plenary Group Debriefing – 60 minutes*

Activity: Digital Preparedness Checklist Discussion

Assignment: Drawing from the small group discussion, quickly identify the areas where all groups answered yes, there is no need to discuss these in plenary. Then spend a few minutes discussing each of the areas where all teams answered no. Take notes on recommendations for how to address these areas.

Finally, dedicate five to ten minutes to discuss each area where there was disagreement. Allow each small group to explain their rationale for their answer, if the group comes to an agreement after the discussion, note it. But you do not need the group to reach a consensus; simply take notes of the main arguments.

Post-Workshop Action Planning

Program designers and managers should review the results of the workshop and develop an action plan to address deficiency areas.

Digital Preparedness Checklist

Purpose	This checklist is designed to help implementing organizations gauge their own preparedness to digitize savings groups and to do so in a gender-responsive manner. The checklist will help implementers understand what they need to do to take on the technology, identify required training and support and address gender considerations in digitization projects. These include strategies to advance gender equality in the context of digital savings groups projects, reduce gendered risks and barriers to digitization and address intended and unintended gender consequences of digitization.
Audience	This tool is intended for staff of organizations implementing digital savings group (DSG) projects, specifically program designers and managers; monitoring and evaluation (M&E) team; and gender specialist.
Time needed to implement the tool	• Review of the tool by program designers and managers – 30 minutes plus time needed to adapt and contextualize the tool • Staff workshop - 2 hours • Post-workshop action planning – time to be determined by project designers and managers
How to use this tool	This tool can be used in different ways depending on where an implementing organization is with its digitization efforts. It can be used to aid planning and design of a digitization program, or it can be used after digital tools have already been introduced to reflect on the effectiveness of digitization efforts. In project planning and design, use the checklist to identify key preparedness, training and sensitization activities required in the program. In preparation for (or during) implementation, review the checklist below and mark 'yes', 'no', or 'unsure' for each statement. Make notes anywhere you answer 'no' or 'unsure' to explain your answer. Where needed, identify and list existing resources, which can help you address any deficiencies and adapt project strategies accordingly. Ideally, the checklist should be used at the project design phase and revisited during implementation through pause-and-reflect sessions. Use the Facilitator's Guide to guide this process through individual, group and plenary review sessions with your staff members.

DIGITAL PREPAREDNESS CHECKLIST

		Rating	Notes
Implementing Organization – Digital Preparedness			
1	Staff across all key positions have the needed digital skills and capabilities. If not, we have a plan to train our team.	Yes No Unsure	
2	Staff have mobile devices; internet access and data plans they need to support the project. If not, we have a budget to provide them.	Yes No Unsure	
3	Staff are trained on the digital tools selected for the project and know how to use them in practice. If not, we have a plan to train our team.	Yes No Unsure	
4	We have a plan for training savings group members on how to use the digital tools selected for the project.	Yes No Unsure	
5	We have defined objectives, measures of success, monitoring and evaluation metrics to be able to measure changes brought about by the introduction of DSG technology.	Yes No Unsure	
6	We have the software necessary to safely store and manage program and client data. This means that only authorized staff have access to personal, individual data. It also means that data cannot be hacked or accessed by unauthorized personnel.	Yes No Unsure	
7	We have a plan to migrate groups' paper records to the digital platform, including a plan to audit all paper records prior to moving to digital.	Yes No Unsure	
8	We have data privacy and protection protocols in place.	Yes No Unsure	
Implementing Organization – Gender Considerations			
9	We have conducted a gender-sensitive needs assessment and selected a digital solution that best meets the needs and interests of savings group members, including women.	Yes No Unsure	
10	We have employed gender-responsive and inclusive recruitment, retention and advancement strategies to select and manage key staff and stakeholders involved in the DSG project (e.g., Gender Specialist, Program Manager, Field Agent, Community Facilitator and Community Digital Champion).	Yes No Unsure	

DIGITAL PREPAREDNESS CHECKLIST

		Rating	Notes
Implementing Organization – Gender Considerations			
11	Our team understands the basic principles of gender equality, Do No Harm, and Safeguarding and is prepared to apply them in the DSG project. If not, we have a plan to train our team on these concepts.	Yes No Unsure	
12	Project-level participatory gender analysis has been completed.	Yes No Unsure	
13	Gender strategy and safeguarding action plan addressing gender barriers and risks to digitization, including gender-based violence (GBV), have been developed, validated with local stakeholders and operationalized.	Yes No Unsure	
14	We have a plan for using gender data to adapt digitization strategies as needed and evaluate gender impacts of the DSG project.	Yes No Unsure	
15	We have a plan to engage men in the community to challenge harmful gender norms contributing to the gender digital divide and support the value proposition of women's use of digital tools.	Yes No Unsure	
16	We have a plan for community awareness raising and engagement around gender norms and other barriers that limit women's use of digital tools.	Yes No Unsure	
Savings Groups			
17	Group members understand the purpose of and support digitization (regardless of gender in mixed groups).	Yes No Unsure	
18	Digital Capability Assessment has been conducted to gauge group members' digital preparedness.	Yes No Unsure	
19	We have a plan to provide digital capability training to group members, especially women who may have lesser access to and experience with digital technology.	Yes No Unsure	
20	Necessary group members (e.g., recordkeepers) have access to mobile devices, the internet and data plans. If not, we have a budget and/or plan to ensure they have access.	Yes No Unsure	
21	Group meets in an area with enough connectivity to support the use of digital tools.	Yes No Unsure	

DIGITAL PREPAREDNESS CHECKLIST

		Rating	Notes
Savings Groups			
22	Women are encouraged and supported to take on leadership and recordkeeping positions, especially in mixed-gender DSGs.	Yes No Unsure	
23	Group members are aware of the costs, benefits and risks of digitization, including GBV and data privacy violations.	Yes No Unsure	
Community			
24	Community members have been engaged around gender norms and other barriers that limit women's use of digital tools.	Yes No Unsure	
25	Men in the community have been sensitized to the purpose of the digitization of savings groups and its potential impact on gender relations.	Yes No Unsure	
26	Community and government leaders have been informed and engaged to support savings group digitization.	Yes No Unsure	
Other Stakeholders			
27	Digital record keeping application enables savings groups to meet government reporting requirements.	Yes No Unsure	
28	Local women-focused organizations and GBV service providers have been identified to support the project as needed and to	Yes No Unsure	

DSG TOOLKIT:

PROJECT STAFFING

PROJECT STAFFING

Facilitator's Guide

Preparation

All participants should review their current job descriptions (JDs) and the sample JDs presented in the tool. Program Managers and Human Resources (HR) specialists should also review the "Key Considerations for Staffing Digital Savings Group (DSG) Programs" section of the tool. The Facilitator should review the entire tool and convene staff members with similar titles and functions for one-to-two-hour small group sessions.

Tips: Consider having a staff member from HR serve in the facilitator role for this process. Inviting a gender specialist and/or a Diversity, Equity and Inclusion (DEI) officer to group sessions is recommended. If there is only one staff member with a specific function (e.g., project-level Gender Specialist), consider pairing them up with an HR representative or a staff member with a similar title within the organization.

Objectives

- Revise JDs for all existing team members to allow them to successfully implement savings group digitization project (when existing savings group (SG) staff are adding supporting DSG's to their roles)
- Revise and update standard savings group staff JDs to incorporate key responsibilities and qualifications required for a DSG project (when creating JDs for new DSG projects where staff have not yet been hired)
- Review key considerations for staffing DSG programs which cover inclusive hiring, retention and advancement strategies create a training and professional development plan for new and existing staff to meet any missing qualifications
- Reassure existing staff of their role in a digitization program; encourage them to be open to change and willing to learn new skills

Participants

Program designers and managers; village or community agent or trainer, gender specialist, DEI officer, HR representatives

Materials

1. Copies of current JDs
2. Copies of the JD tool with sample responsibilities and qualifications
3. Copies of organizational JD templates for new positions
4. Copies of organizational JD templates for new positions

Small Group Sessions (1–2 hours): Flow and Description

This exercise does not need to happen in a single session. The facilitator should create groups of staff with similar JDs and groups should schedule a time to meet and complete the exercise.

1 *Introduction*

Share exercise objectives with participants, this can be done over an e-mail that also explains the exercise.

2 *Group Sessions – 1 to 2 hours*

Activity: Review JDs

Assignment: Team members who share similar job titles and functions should meet as a group to review their existing JDs and the sample additions provided in the tool. They should make specific recommendations on changes to the original JDs based on their understanding of the requirements for the savings group digitization program.

Discussion Questions:

- Which responsibilities and qualifications need to be added to the JDs to successfully implement the savings group digitization project? Are there any responsibilities and qualifications that are no longer needed?
- What training or support will current and incoming staff need to meet the revised responsibilities and qualifications?

3 *Manager Review*

Activity: Managers review and revise JDs

Assignment: Once the teams have finished the JD reviews, program managers should meet as a group to review and revise the suggested changes. Each manager should present their team's recommendations and work with other managers to make revisions as needed.

The management team should then discuss any training or support existing and incoming staff members will need to meet the responsibilities and qualifications of the revised JDs. Managers should also identify any new hires that are needed on their team. Additionally, managers should assess if and how the revised JDs require compensation or benefit adjustments.

Managers should work with HR on adjustments to JDs and related compensation and benefits.

Facilitator's Notes

- Changes to JDs can be a stressful time for many staff members. Make an extra effort to reassure staff of the support they will receive to meet these new requirements (if this is the case).
- Inform the participants that the management will address salary issues once the new JDs or revisions to existing JDs are completed. Do not make any promises and do not set any undue expectations.
- Groups may tend to focus on technical and digital skills. Encourage them to also discuss gender issues and skills that will help them support women through the digitization process.

Project Staffing

Purpose	This tool includes sample job descriptions (JDs) for key digitization project staff, including program managers, community-based trainers (facilitators), field agents (supervisors), community digital champions, gender and inclusion specialists and Information Technology (IT) specialists. The JDs focus on knowledge, skills and abilities related to mobile and digital technology as well as gender integration. The tool includes both "Roles and Responsibilities" and "Qualifications," which can be added to existing JDs (for either current staff or staff to be hired) to ensure they have adequate skills to support the gender-responsive digitization of savings groups. *These roles and skills are additions to standard savings groups roles and qualifications.* It may not always be possible to hire staff with all the necessary skills since this is an evolving field. Managers should plan to train new staff and existing team members to meet necessary skills. Ability and willingness to learn should be key attributes in the recruitment process.
Audience	This tool is intended for staff of organizations implementing digital savings group (DSG) projects, specifically program designers and managers, country managers and gender specialists
Time needed to implement the tool	• Review of the tool and existing JDs – one to two hours • Small group sessions – one to two hours • Finalization of JDs, compensation adjustments, and revisions to the recruitment, retention and advancement processes – time to be determined by program managers and Human Resources specialists
Outline	• Key Considerations for Staffing DSG Programs • Sample roles and responsibilities • Sample qualifications
How to use this tool	Review all sections of the tool and compare them to the existing JDs and HR practices in your organization, edit JDs as necessary. Be aware that many organizations have different position titles and many combine or divide positions in different ways. Use the Facilitator's Guide to guide this process through individual and group review sessions. <u>Positions included in the tool</u> Community Digital Champion Community-based Trainer (Facilitator) Supervisor/Field Agent Program Manager Gender and Inclusion Specialist IT Specialist

PROJECT STAFFING

Key Considerations for Staffing DSG Programs

Digital transformation can be a highly technical process, with program designers and managers focused on selecting and adopting the right technology. But it will also be a huge transformation for your team, staff and volunteers, you will want to make sure that they have both the right attitude and skill set for the transformation.

What to do with existing staff

When looking to digitize savings groups, it is important to remember the need to provide professional development and support to existing staff. Not only will their role in supporting savings groups change, but they will likely need to learn new digital skills to provide support to the groups and ensure that the program is implemented successfully.

When done properly, this results in engaged, confident employees who are able and willing to support digital transformation. When done poorly, however, it can result in unengaged, unwilling workers who stick to the familiar, inefficient ways of working. If staff who work directly with savings groups (e.g., Field Agents, Village Agents, Community Trainers or Facilitators) are resistant to digital transformation, they will communicate this to the savings groups, and this can create resistance to embracing new technology.

We recommend putting in place a change management process focused on staff. How will employees react to news of the change? Will training be required? What resources should be made available to staff to assist them? How will you communicate with staff during the process?

Depending on the skills and history your team has, you may need a plan to train them to meet new job requirements. You may also need to revise JDs and consider increasing staff salaries or benefits, especially if they are required to take on additional responsibilities.

Where and how to recruit women

Most communities in which we work face a significant digital gender gap. This means that as you start a project focused on DSGs, you will likely face a challenge in hiring women with the necessary digital skills as staff or volunteers.

'Hire to Train and Train to Hire' is an old saying but one that is particularly relevant in this context. When looking to hire new staff for savings group digitization projects, focus on women who are willing and eager to learn new skills, and who bring other capabilities that will make them successful mentors and trainers for the groups. Develop a plan and invest in training them, not just in the selected digital technology, but on basic digital skills.

Work with your HR team to devise recruitment strategies aligned with the principles of diversity, equity, inclusion and belonging. Recruit in spaces that already have women using digital tools, such as mobile network operators, colleges and vocational schools offering information technology (IT) education, and proactively publicize job opportunities among female mobile money agents or phone sellers. Also look across your own organization; you may have women on your IT team that are interested in a move to a more programmatic role, and these women could become digital champions for other staff members on your team.

How to retain staff

Consider if you have budgets and systems in place to provide your team members with adequate and equitable compensation, benefits and advancement opportunities that correspond with their new roles, responsibilities and qualifications. Also consider if you have systems in place to offer reasonable workplace accommodations to women, people with disabilities and other employees with diverse needs (e.g., mothers of young children).

PROJECT STAFFING

Job Descriptions

Community Digital Champion (Volunteer)

Roles and Responsibilities

- Raise awareness among savings groups and community members about the benefits and risks of digitization, including gender risks, barriers and how to mitigate them
- Demonstrate how to use mobile technology and digital tools to savings group members
- Promote a learning-by-doing approach, supporting group members, especially women, to learn digital skills and tools at their own pace
- Advise savings group members of the technology-enabled risks and ways to mitigate them
- Support members in the use of digital technology outside of group meetings if needed and feasible

Qualifications

- A confident and active user of mobile technology and digital tools, including texting, mobile money and social media
- A supportive mentor, comfortable working with women who have little to no prior exposure to digital technology
- A positive attitude towards women's access to technology
- Willingness to learn and communicate basic concepts about gender equality and inclusion in the context of digitization projects
- Knowledge of or willingness to learn basic concepts about data privacy and security

Community Based Trainer (Facilitator)

Roles and Responsibilities

- Train and mentor savings group members in the use of mobile technology and digital tools
- Educate savings group members about the benefits and risks of digitization projects; facilitate group discussions on gender risks and barriers and how to mitigate them
- Monitor savings groups for challenges with using digital tools; support groups to resolve the challenges or raise them to a supervisor if they cannot be easily solved
- Monitor and resolve any conflicts in the groups related to the use of new digital tools
- Support female group leaders on the use of digital tools for group management; encourage women to take on leadership positions in mixed-gender digital savings groups
- Support a learning-by-doing approach within the groups, encouraging members, especially women, to practice their digital skills.

Qualifications

- A basic understanding of and interest in technology as a tool for managing savings groups
- A regular and confident user of technology, especially digital tools and applications
- A supportive mentor, comfortable working with women who have little to no prior exposure to digital technology
- A positive attitude towards women's access to technology
- Willingness to learn and communicate basic concepts about gender equality and inclusion in the context of digitization projects

Job Descriptions

Supervisor/Field Agent

Roles and Responsibilities

- Train savings group members in the use of mobile technology and the chosen digital tool
- Bring together communities, local leaders and other stakeholders to understand and support savings groups and their members in the use of mobile technology and digital tools
- Facilitate community awareness sessions and gender dialogs with group members and their partners to increase understanding of the benefits and risks of women's use of technology for group operations and personal matters
- Train group leaders and recordkeepers in the use of digital tools for group management, ensuring that women leaders are fully engaged and not marginalized during the digitization process
- Translate and adapt digital training materials
- Collect gender-sensitive data and provide feedback to the Program Manager, Gender and Inclusion Specialist and the technology provider on the ways that group members use the digital tools, any challenges they face, and ways that the tools and processes can be improved to enhance user experience, participants' safety and data privacy and security

Qualifications

- At least an intermediate understanding of and interest in digital technology as a tool for managing savings groups and their records
- A regular and confident user of technology, especially digital tools and applications such as Mpesa (or the local mobile money platforms), Shazam, Bolt, Spotify, Zumia or other popular apps in the local market
- A basic understanding of how cloud-based technology works and the ability to communicate this to audiences with less exposure to technology.
- Experience using Google and the Google platform
- A positive attitude towards women's access to technology
- Willingness to learn and communicate basic concepts about gender equality and inclusion in the context of digitization projects
- Experience facilitating gender dialogs and/or community awareness sessions on sensitive subjects
- A self-starter with creative problem-solving skills in low-resourced settings
- Experience working with technical support staff; ability to anticipate what information they may need to help fix a technical problem.

Program Manager

Roles and Responsibilities

- Lead the design and implementation of program strategies to incorporate digital tools into savings groups programs in a safe, inclusive and gender-responsive manner
- Support the process of defining and understanding the needs of savings groups, and how those can be met with digital tools
- Support the process of identifying risks and challenges, including gender barriers, faced by savings groups and their members in the digitization process; oversee the development and implementation of strategies to mitigate these risks and challenges
- Ensure that the monitoring and evaluation team incorporates and analyzes gender-sensitive indicators to monitor and assess the outcomes of digitization on women, men and group power dynamics; incorporate results into program design/adaptation
- Manage partnership with the selected technology provider and ensure that the company is responsive to the diverse needs and interests of savings group members, including women

continued on next page

Job Descriptions

Program Manager - Continued

Qualifications

- Knowledge of new and emerging technologies and their application to solving development challenges (e.g., operating mobile apps, e-learning or SMS technology)
- Experience designing or managing digitization interventions a strong asset
- Solid understanding of and deep commitment to the concepts of gender equality, gender integration and gender-transformative programming; demonstrated ability to apply these concepts in the context of financial inclusion, economic development and /or digitization projects

Gender and Inclusion Expert

Roles and Responsibilities

- In close collaboration with program staff and community facilitators, lead participatory gender analysis and gender strategy development to ensure gender-intentional digitization efforts
- Train staff on gender integration and social inclusion; sensitize staff to the risk of gender-ignorant digitization
- Review program documentation with a gender and social inclusion lens
- Support gender-responsive and inclusive staff recruitment, development and retention strategies
- Identify or create tools and training materials for program teams to incorporate into digitization programs to address gender barriers and risks
- Lead and/or oversee gender dialogs, male engagement interventions and community awareness sessions on gender equality
- Support staff in identifying and understanding gender-based violence (GBV) risks faced by savings groups members in the digitization process and develop strategies to mitigate them
- Support tracking of the challenges and risks associated with women's' access to and use of mobile technology and digital tools; develop and oversee program-wide mitigation strategies
- Support the monitoring and evaluation team to disaggregate all people-level indicators by sex and incorporate gender-sensitive indicators to assess the outcomes of digitization on women, men and group power dynamics; incorporate results into program design/adaptation
- Provide on-demand technical assistance and advice to support gender-intentional savings group digitization activities.

Qualifications

- Strong commitment to feminist values, human rights and advancing women's leadership
- Deep knowledge of gender equality principles and best practices on gender integration at the nexus of financial and digital inclusion; ability to apply this knowledge in the context of digital savings group projects
- Knowledge of social inclusion principles
- Understanding of male engagement and gender-transformative approaches in economic advancement programs and interventions
- Demonstrated ability to lead project-level gender analyses and strategy development
- Experience developing and delivering capacity strengthening training on gender integration and social inclusion, preferably in programs using digital technology
- Experience facilitating gender dialogues and/or community awareness sessions on gender equality and social inclusion a strong asset
- Experience developing and/or implementing GBV prevention and risk mitigation strategies preferred; understanding of GBV, including technology-facilitated violence is required
- Foundational understanding of how savings groups function and are managed

Information Technology (IT) Specialist

Roles and Responsibilities

- Train program staff and groups on the use and troubleshooting of the digital savings group tool or platform
- Support data migration of groups' paper-based records to the platform
- Work with program management to develop a customer support (software troubleshooting) mechanism to escalate IT challenges in groups to higher levels and ensure timely resolution
- Provide back-end software troubleshooting for software bugs (only applicable if you are using your own platform)
- Provide technical support to program staff and partners in how to develop reports or analyze data from the digital savings group dashboard

Qualifications

- Analytical, statistical and programming skills to collect, analyze and interpret large data sets
- Training skills to train program staff in troubleshooting

PROJECT STAFFING

Example Interview Questions

It is important to think through practical interview and assessment questions to evaluate actual knowledge and skills. A few examples of these types of questions are included below:

Questions for Program Supervisors and Savings Group Trainers:

- Tell me about some apps you use and why you use them.

  Exposure to YouTube and Facebook is not enough to be successful; we need people who use apps as tools to improve various activities or processes in their lives (common local examples could include Mpesa, LiveFootball, Runtracker, VoucherMaster, Shazam or Bolt)

- What do you see as some potential challenges in utilizing a savings group app in your community? How would you address them?

  It's important that staff and volunteers understand both the technology and the context enough to identify probable challenges such as poor network and electricity in rainy season, low levels of digital literacy at the community level, group disagreements around data use, etc. We want people who can come up with creative solutions to problems.

- Tell me what you know about cloud-based technology and how cloud-based savings group records might be beneficial to a group
- How would you explain cloud-based technology to someone who has never used a computer or seen a smart phone?

Example practical exercise:

While this will vary slightly for staff and volunteers, a practical exercise should involve giving candidates a phone or a tablet and an internet connection and asking them to figure out how to do something they have likely never done before. They need to demonstrate that they know how to look for and find an answer on their own. For example:

- (Staff) - Create a Google account and access/edit a shared document
- (Staff and volunteers) - Find and download an app in the Google PlayStore and complete a task in that app
- (Staff and/or volunteers) - Change the device's time, date or language

DSG TOOLKIT:

MONITORING AND EVALUATION OF DSG PROJECTS

MONITORING AND EVALUATION OF DSG PROJECTS

Facilitator's Guide

Preparation

Developing a thoughtful and gender-responsive monitoring and evaluation framework for digital savings group (DSG) projects requires a team effort led by an experienced monitoring and evaluation (M&E) team and gender specialists. The process proposed below will support the project team in using a gender lens to either design an M&E framework for a new digitization project or revise an existing M&E plan for ongoing projects.

The Facilitator and all participants should review the tool and key program documents — an M&E plan if already in existence — to understand if and how the program integrates gender and monitors progress. The Facilitator may also choose to share the Bill & Melinda Gates Foundation's (BMFG) "Conceptual Model of Women's and Girls' Empowerment," or any other relevant framework with participants. The Facilitator should then convene staff members for a staff workshop.

For the ranking exercise below, the project and M&E leads should have a sense of how many gender-sensitive indicators can be realistically tracked in the DSG project. Each participant should only be given that number of dot stickers for the ranking exercise.

Tip: This process, including the staff workshop, should be led by an experienced M&E specialist in collaboration with a gender specialist.

Objectives

- Gain familiarity with the domains of women's empowerment and gender-sensitive indicators relevant to DSG projects
- Review and assess the relevance of sample indicators to the DSG project
  - Choose from the list of suggested indicators
  - Suggest new indicators
- Assess when and how information will be collected, analyzed and used

Participants

Program managers and designers, M&E team and gender specialist

Materials

1. Copies of the BMGF Conceptual Model of Women's and Girls' Empowerment for each small group
2. Flip chart which replicates the BMGF Conceptual Model
3. One flip chart for each of the three domains of women's empowerment, divided into sections for the subdomains
4. Sticky notes for participants
5. Dot stickers for participants (if they are unavailable, give participants colored markers and tell them how many indicators they can mark on the chart)

Facilitator's Notes

- Participants are likely to select indicators for each of the subdomains. Encourage them to only select indicators for the most relevant subdomains.
- Keep the participants focused on women's empowerment indicators, it will be easy for them to slip into general project indicators.

Staff Workshop (105 min.): Session Flow and Description

1 *Introduction – 15 minutes*

If the group is unfamiliar with each other, have participants share their name, position and a brief description of a time M&E (gender) data taught them a lesson about the impacts of a project.

Share session objectives with participants and answer any questions.

2 *Plenary Discussion – 60 minutes*

Activity: Review the sample monitoring framework

Assignment: Give a short 10 to 15-minute overview of the sample monitoring framework and engage participants in a discussion around it.

Plenary Discussion Questions:

- How will using a gender lens influence the indicators we will monitor during the project?
- Do we currently disaggregate our data by gender? Is our M&E system set up to disaggregate data by gender?
- What are the benefits of implementing a gender-responsive M&E plan? Are there any concerns?
- Which domains and subdomains are the priority for this project?
- Which subdomains are not relevant or cannot be considered as direct outcomes of the project?
- What are the gender outcomes the project is seeking to achieve in each of the three different domains?

continued on next page

Session Flow and Description

3 *Brainstorming and Ranking – 90 minutes*

Activity: Develop indicators for each domain and relevant subdomain that project will monitor.

Assignment: Give the group 30 minutes for the 'Agency' domain. Ask participants to choose or develop new indicators for each of the relevant subdomains. Have participants write one indicator per sticky note and attach the sticky notes onto the flip chart. Repeat this exercise for the 'Resources' and 'Institutional Structures' domains.

While the group is working on subsequent domains, the facilitator should review each domain and group similar indicators. Once all three domains are finished, the facilitator should summarize the responses for each domain (or ask a different participant to report out on each domain).

Once the domains are summarized, each participant should be given dot stickers or colored markers. The facilitator should explain that the project is aiming for a specific number of indicators, and therefore each participant has been given that number of stickers. Participants should then use their stickers or markers to vote for indicators.

After the voting the facilitator should report out the results and then facilitate a group discussion. The facilitator should highlight which indicators received the most votes. Try to address the following questions:

- How do you feel about the leading indicators? Are any subdomains or critical indicators missing? Is that a problem?
- How will the team collect data on the selected indicators? Does the team have the resources and systems to collect this data?
- How will the team analyze and apply this data?

Next Steps

The program and M&E leads should review the results of the workshop and develop a final list of indicators.

Once the indicators are selected the M&E team will need to develop questionnaires and a data collection plan for each of the indicators.

Monitoring and Evalution of DSG Projects

Purpose	This tool is designed to improve digital savings group (DSG) implementers' understanding of the impacts of digitization on groups and their members using gender-sensitive indicators and monitoring approaches. The tool includes sample indicators and a monitoring and evaluation (M&E) framework.
Audience	This tool is intended for staff of organizations implementing digital savings group (DSG) projects, specifically the M&E team, program designers and managers and gender specialists. The tool implementation process should be led by an experienced M&E professional in collaboration with a gender specialist.
Time needed to implement the tool	• Review of the tool, existing M&E plan (if available), and supporting materials - two hours • Staff workshop – three hours • Next steps – time to be determined by the M&E lead
How to use the tool	Review the tool with an understanding that it is not intended to be a stand-alone M&E framework. Rather, it should be adapted and incorporated into the project's broader M&E plan. The indicators presented in this tool offer the opportunity to monitor a wide range of impacts of digitizing savings groups. As women make up most savings group members worldwide, the indicators are organized into groups around the components of the Bill & Melinda Gates Foundation's "Conceptual Model of Women's and Girls' Empowerment." Project teams may choose to organize their indicators differently. The list of indicators is not exhaustive and does not need to be used in its entirety. DSG implementers can and should select those indicators that are most relevant for their projects. The indicators are intended to track project outcomes in order to improve gender-responsive and data-driven decision making, adaptation and learning. Use the Facilitator's Guide to guide the process of selecting indicators through individual review and group exercises. Following the selection of indicators and adapting them to a specific context, the M&E team should develop tools to collect the relevant data (e.g., survey questionnaires or focus group discussion guides) and work with the program team to analyze the data and adapt digitization strategies as need. These will need to be determined on a project-specific basis. This tool is most suitable for project design and monitoring efforts, but can also be used for baseline, midline and endline evaluations.

SAMPLE INDICATORS AND MONITORING FRAMEWORK

Introduction

The sample indicators below are intended to help implementers collect critical data to understand the full impacts of introducing digital tools to savings groups. The M&E framework calls for both gender-disaggregated data (GDD) and gender-sensitive indicators. GDD provides visibility into how programming impacts women and men, which is particularly important in projects supporting mixed-gender DSGs, while gender-sensitive indicators allow implementers to isolate outcomes that specifically impact gender equality and/or women's empowerment.

Strong gender data provides transparency within programming and allows implementers to ensure that their programs meet specific needs and interests of women, contributing to more equitable and sustainable outcomes. This is especially important given the limited guidance in the sector around measuring how digitization affects women's ability to participate in, lead and benefit from savings groups on an equal basis with men, particularly in the context of widespread gender digital divide.

Note the indicators presented in this tool are, in addition to the standard indicators used with respect to savings groups, to demonstrate impact due to digitization.

M&E Framework

Although there are many frameworks for women's empowerment, this tool organizes indicators according to the Bill & Melinda Gates Foundation's "Conceptual Model of Women's and Girls' Empowerment" illustrated below.

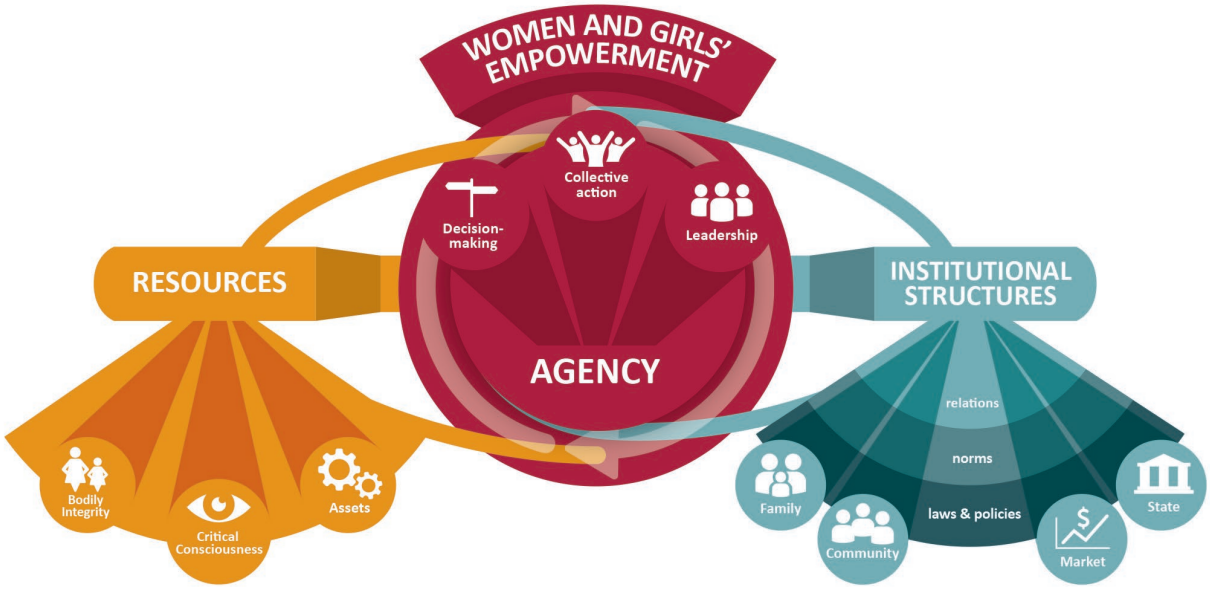


Figure: Image reproduced from Bill & Melinda Gates Foundation's Conceptual Model of Women's and Girls' Empowerment

MONITORING AND EVALUATION OF DSG PROJECTS

Women's Empowerment Domains	Indicators
Note: Where appropriate (e.g., in mixed-gender savings groups) all people-level indicators should be disaggregated by gender.	
Agency	Agency-level indicators are intended to measure how digitization has affected women's ability to meaningfully participate in the savings group, make and influence decisions at the group and household levels and hold leadership positions within and outside of the group. More specifically, these indicators should measure changes (improvements or backsliding) in the following areas: • **Individual agency** ("power to," e.g., changes in the capacity to make meaningful choices and decisions about participation in the group) • **Collective agency** ("power with," e.g., changes in the ability to effectively collaborate with others within the group)
Meaningful participation in group activities	• Participation in the group (e.g., meeting attendance and retention post-digitization) • Social cohesion within the group (communication, collaboration, support and solidarity) • Trust in group financial records • Group conflict levels • Individual knowledge of group financial information (e.g., group balance) • Efficiency of group meetings • Savings and loan behaviors
Decision-making ability (influence over decisions and autonomy to make independent decisions)	• Decision-making ability at the household level (productive and reproductive) • Decision-making ability at the group level
Leadership	• Leadership within the group • Leadership outside the group
Resources	Resource-level indicators are intended to measure how digitization has affected (improved or decreased) women's access to, ownership, ability to control and ability to use resources at the household and group levels. Resources are understood broadly as "assets" (individual and group), "critical consciousness," and "bodily integrity." They are sometimes framed as preconditions to empowerment.
Assets (human, material and social resources; time; knowledge and skills)	• Individual mobile phone ownership and/or use • Access to and/or use of the internet • Digital capabilities, i.e., knowledge, attitudes (confidence, trust) and skills needed to use technology safely and effectively • Amount of time spent on a) using digital tools; b) participating in group activities; c) household and caregiving responsibilities; d) income-generating activities • Access to and control over household material resources (income, savings and loans) • Changes in household material resources (income, savings and loans) • Division of labor at the household and group levels • Use of digital communication • Social capital (e.g., quality of intimate partner relationships, peer support)

MONITORING AND EVALUATION OF DSG PROJECTS

Women's Empowerment Domains	Indicators
Resources - Continued	
Critical consciousness (self-awareness of how inequalities and power operate in our lives; "power within")	• Changes in perceptions, trust and self-esteem following adoption of technology • Self-efficacy in using digital devices and tools at the household and group levels • Confidence in using digital devices and tools • Control of resources (i.e., Do women have increased autonomy to make decisions on how to use their own resources)
Bodily integrity (women's control over their physical and mental well-being as well as safety, security and freedom from violence)	• Intimate partner violence (knowledge, attitudes and experience) • Gender-based violence at the community level (knowledge, attitudes and experience) • Technology-facilitated violence (knowledge, attitudes and experience) • Data privacy and security (knowledge, experience) • Cybercrimes (knowledge, experience) • Feeling that the individual has the knowledge and resources to protect themselves from digital risks
Institutional Structures	Institutional-level indicators are intended to measure how digitization has affected (improved or weakened) women's relationships with institutional structures in which they live and work. Selected indicators can also be used to measure if project-level digitization efforts have had direct or indirect influence over higher-level institutional arrangements, e.g., by contributing to policy change or the development of DSG industry standards.
Family (spouse, household members and extended family)	• Gender attitudes and perceptions toward women's mobile phone and internet use • Gender attitudes and perceptions toward women's economic and DSG participation • Intrahousehold relations
Community (neighborhood, village, town, social groups and organizations)	• Gender attitudes and perceptions toward women's mobile phone and internet use • Gender attitudes and perceptions toward women's economic and DSG participation • Digital access to community information • Digital access to and use of community-based services (e.g., GBV hotlines or online healthcare and vocational training services)
Market (businesses, labor market)	• Digital access to market information • Digital access to business support services • Access to and use of formal financial services (including digital financial services) • Connections to markets through digital channels • Participation in online selling or buying (e-commerce) • Project contributions to DSG industry standards

MONITORING AND EVALUATION OF DSG PROJECTS

Women's Empowerment Domains	Indicators
Institutional Structures - Continued	
State (governments and the public sector at multiple levels)	• Digital access to government information • Access to and use of e-government services • Digital civic participation • Group registration with required government entities • Project contributions to laws and policies regarding women's control of assets and resources

DSG TOOLKIT:

PROMOTING WOMEN'S DIGITAL CAPABILITIES

PROMOTING WOMEN'S DIGITAL CAPABILITIES

Purpose	Limited digital capability—understood as knowledge, attitudes and skills necessary to use digital tools effectively, confidently and safely —is a key barrier to women's adoption of technology, including digital solutions for savings groups. This tool provides practical tips and suggestions for promoting digital capability among women as part of any digitization project.
Audience	This tool is intended for savings group-facing staff and volunteers of organizations implementing digital savings groups (DSGs), specifically community digital champions, community-based trainers (facilitators) and supervisors/field agents. It should also be reviewed by program managers and gender specialists, who should work with implementing staff on strategies and resources needed to implement the tool in practice, i.e., train, coach and mentor DSG members, especially women, to enhance their digital capabilities and otherwise support them through the digitization process. These tips are NOT meant to be shared with savings group members – see Digital User Dialogues for tips to share with group members.
Time needed to implement the tool	Quick review – 20 to 30 minutes **Thorough review and discussions:** • Review with team members to devise strategies and identify resources for implementing it – two hours • Training, coaching and mentoring savings group members on digital capabilities – time to be determined by program managers and field staff based on the needs, interests and available resources
How to use this tool	Read and familiarize yourself with these useful tips. Discuss them with your team members and think about how you might change or adapt your digitization project strategies to incorporate these tips. Make sure that you have sufficient budget to cover any training and coaching needs. In addition, identify and list any local or organizational resources that may help you apply these tips in a cost-effective manner. Select the tips that apply to your program and your context. Not all tips may apply, or there may be too many tips to effectively incorporate. These are intended to be helpful pieces of advice. Pick the ones that are most relevant for your program and use them.
Acknowledgements	"Empowering Women on a Journey Towards Digital Financial Capability", Women's World Banking, Marina Dimova, Jaclyn Berfond, Sonja Kelly and Whitney Mapes

PROMOTING WOMEN'S DIGITAL CAPABILITIES

Recommendations	Resources
Who	
Know your client, assess existing capabilities Ensure you know existing digital capabilities and needs of savings group members, including women, so that you are pitching relevant training. Consider disability and the levels of literacy and numeracy among group members, with due attention to any gender differences. This will help you devise training approaches (e.g., use of audiovisual materials) which are best suited for your audience.	While there are no off-the-shelf digital assessment tools appropriate for savings groups, it is advised to look at 5 key areas: **Communication** – this includes making calls, texting, participating in group chats, emailing, posting on social media and using WhatsApp or similar communication platforms **Accessing Information and Content** – this includes using search engines and learning platforms; using photo, video and music sharing platforms; and downloading and using digital applications **Transacting** – including mobile money and online purchasing **Problem Solving** – this includes accessing and using mobile technology to solve problems, for example identify an agricultural pest or understand a government policy **Being Safe and Legal** – this includes basic understanding of legal and safety standards for using digital tools, including such concepts as data privacy and security and technology-facilitated violence (e.g., online harassment) If you want to develop an assessment, this reference might be helpful: ITU Digital Skills Assessment Guidebook
Personalize the content – use real women as examples Use characters, environments and languages that are common to the trainees. Use examples and use cases that resonate in their lives. It can be also helpful to use personas to talk about the different experiences that women have with digital tools. These can be particularly helpful in contexts where women are reluctant to share their own stories. You will want to adapt the personas to make them relevant to your trainees.	You may find the following resources helpful: • GSMA MIIST Persona Posters a GSMA MIIST Personas for Mobile Internet Skills • Strategic Impact Advisors User Personas
What	
Teach relevant skills Digital skills content is better received when it includes details and messages tailored to the specific needs of the women on the receiving end. These details draw the participants' attention and ensure the training is relevant to and resonates with them.	You may wish to review the following resources and adapt one of them for the purposes of your project: • Hey Sister: Show Me the Mobile Money • GSMA Mobile Internet Skills Training Toolkit • DigiWomen: A digital tool development to train women from rural areas on literacies • HerVenture: App for women entrepreneurs

page 1 of 4

PROMOTING WOMEN'S DIGITAL CAPABILITIES

Recommendations	Resources
What - Continued	
Promote trust and confidence in technology Technology can be new and frightening to savings group members. Research shows that women often lack confidence in using digital technology and fear that they might do something wrong, which discourages them from using digital tools. Let your participants handle mobile phones and practice the skills repeatedly, so they gain comfort and confidence with the technology. Identify community digital champions who can support them.	Community Digital Champion Job Description included in Project Staffing tool of this toolkit
Address risks, myths and misconceptions The online environment brings risks, including violence, fraud, data privacy violations, unwanted exposure to explicit content and more. Many of these risks are gendered. For these reasons, enabling women to use digital technologies also entails supporting them to understand how to use them in a safe and secure way. It is particularly important to teach users how to protect their data and privacy and how to protect themselves from cybercrimes and technology-facilitated violence. The community in which you are implementing a digital savings group (DSG) project may have various misconceptions about the use of digital technology. For example, some people may think that mobile phones promote unfaithfulness or distract women from household responsibilities. It is important to create a safe space for participants to discuss and debunk or otherwise address these myths and misconceptions.	Ask your trainees about their concerns around the use of technology and teach them how to use online resources to fact check the extent to which these concerns are valid. Talk about trusted and unreliable sources of information. Use the tools included in this toolkit (Addressing Risks of Gender-based Violence and Digital User Dialogues) to explore the risks with the participants. Remember that it is always better to show a trainee how to answer their own questions than to simply answer them yourself. There is also a lesson on this subject in **Hey Sister: Show Me the Mobile Money**
When	
Adjust timing to women's schedules, including their income-generating, household and caregiving responsibilities Training initiatives need to reach women at the times when they would be most receptive to learning, and most able to complete a recommended call-to-action. It is important to look for milestones at which it would be easier for women to adopt the desired behaviors and face the fewest barriers to doing so. This often means planning initiatives to reach trainees directly before, during or immediately after the behavior we aim to drive would occur.	

PROMOTING WOMEN'S DIGITAL CAPABILITIES

Recommendations	Resources
When - Continued	
Keep it simple and timely – keep each skill to 10-15 minutes, teach one skill at a time Structure the content into simple, digestible messages that are easy for women to understand, rather than complex and abstract digital concepts. Break complex content down into clear 'rules of thumb' that can directly address the specific pain points women face in using mobile phones and digital tools. For example, these 'rules of thumb' could explain steps to adjust privacy settings on a mobile device, open a mobile money account or use a digital application to track savings goals. Using simple rules makes it easier for women to retain information, internalize new concepts and see the immediate ways in which they can put the new knowledge, attitudes and skills into practice.	The Digital User Dialogues tool is divided into short modules that can be taught at the end of a savings group meeting.
Where	
Train in a safe space Identify a safe and supportive space for women to learn digital skills, where they can openly ask questions and discuss concerns. Provide ample opportunities for participants to practice digital skills on their own or in one-on-one coaching sessions. This is particularly important as some women will not want to be observed using digital technology.	
Leverage women's social circles as a learning channel Everyone learns at different speeds. Consider utilizing community digital champions and early adopters as mentors to support other women in the group as they practice and learn new skills. Women will also feel more confident if they are not the only ones in the community using a new technology. If the whole group is using a new digital tool, it will be seen as more common in the community. Match trainees in groups with others who have similar knowledge and skill levels so that they feel confident and interested. You can use the personas referenced above and ask participants to join the group of the persona they identify with. Feel free to move trainees into different groups after the training has started if it becomes apparent that trainees are not at a similar skill level to others in their groups.	

PROMOTING WOMEN'S DIGITAL CAPABILITIES

Recommendations	Resources
How	
Understand digital financial capability and best practices for training	You may wish to review this resource: Better Practice Guidance on Women's Digital Financial Capability, Center for Financial Inclusion
Simplify, use local language, and make the training inclusive for participants with disabilities and low levels of literacy and numeracy Use terms, language and examples that are simple and familiar to women participating in the training. Use audiovisual materials and consider partnering with local organizations which specialize in promoting literacy and disability inclusion.	
Facilitate learning-by-doing; support women to practice on their own or with a mentor Digital projects should provide women with opportunities not only to learn, but also to do. The adoption of new skills and behaviors does not happen through information or observation alone; it requires personal experience, practice, repetition and habit formation. Consider lending the group phone to members who otherwise do not have access to digital tools.	See the Digital User Dialogues tool for hands on exercises you can use with your trainees.
Find Helpful CICO Agents Visiting a Cash-In-Cash-Out (CICO) agent may be the first time that a woman must use her new skills in front of someone else, especially a stranger. CICO agents are a risk point for women. Identify a few helpful agents in the community who will agree to support learning for the participants and agree to best practices such as never asking for their PIN code.	If appropriate, create and share a list of names and numbers of vetted CICO agents. If possible, make sure there is an equal number or more of female agents on the list as women might be more comfortable interacting with other women.

Additional Resources

GSMA, Developing Mobile Digital Skills in Low and Middle Income countries

Google Digital Skills in Africa - These tools are meant for a slightly more sophisticated user, and focus on business skills and marketing

DSG TOOLKIT:

ADDRESSING RISKS OF GENDER-BASED VIOLENCE

ADDRESSING RISKS OF GENDER-BASED VIOLENCE

Purpose	As mobile and digital technologies become more available, they bring the increased risk of technology-facilitated gender-based violence (GBV). An unintended consequence of digitization and technology is an increased risk of technology facilitated GBV. Technology does not need to be used directly to harm someone, because in many contexts women's mobile phones and internet usage challenges traditional gender norms. There are specific risks for GBV associated with the digitization of savings groups, research indicates that domestic conflict and violence may occur when a partner gains insight into user's private savings information through text messages received on shared devices. This tool was created to inform implementing organizations on the risks of GBV as a result of a woman's digital journey and strategies to help mitigate specific risks. Strategies could include community education, gender dialogues and GBV service mapping; promoting informed digital citizenship and safe digital behaviors; raising awareness on how to manage a digital footprint in a safe, responsible way that does not exacerbate existing risks; and sharing tips on what can be done when violence occurs.
Audience	This tool is intended for staff and volunteers of organizations implementing digital savings groups (DSGs), specifically program designers, managers and gender specialists. Implementing organizations, in particular training staff and volunteers, are encouraged to use a companion tool, Digital User Dialogues, to raise awareness about GBV and other safety risks among DSG members.
Time needed to implement the tool	• Review of the tool, selection of relevant risks and mitigation strategies, contextualization and initial planning should take three hours • Validation of risks and strategies with field staff, partners, group and community members – time to be determined by project managers based on needs and available resources to conduct a more thorough risk assessment and/or gender analysis • GBV service provider mapping – time to be determined by project managers based on needs
How to use this tool	The tool consists of two sections: "Key Definitions" and a "User Journey Map" designed for use at project management level to identify GBV risks and develop strategies to address them.

How to use this tool (continued)	Review the tool to familiarize yourself with potential GBV risks that women participating in digital savings groups (DSGs) may face while accessing and using digital technology. Determine which risks might occur in the context of your specific DSG project and select strategies that you can employ to prevent and mitigate identified risks. If feasible, conduct a community-based risk assessment to identify further risks and mitigation strategies appropriate to the context of your project. This assessment may occur in conjunction with the project-level gender analysis and gender action planning. Otherwise, do your best to validate (keep, add or remove) and contextualize selected risks and strategies with field staff, partners and group members. User dialogues can be an effective way for DSG facilitators and members to unpack harmful gender norms and practices that may increase GBV risks for women using digital technology. If feasible and appropriate, review, adapt and use the companion tool, "Digital User Dialogues," to facilitate conversations with savings group members about GBV and other risks across each stage of their digital journeys. These discussions may take place over several meetings, as groups get more familiar with mobile technology and dialogue topics become more relevant. User dialogues are not meant to discourage groups from digitizing, but instead to make them aware of risks and provide ideas on how they can stay safe. Please ensure facilitators (field staff and volunteers) are comfortable and well-prepared to guide conversations on safety. Some topics will be sensitive. If facilitators are not skilled at or comfortable talking about them, the participants will not be comfortable either. Before sessions, facilitators should practice presenting material on risk and safety with colleagues. Remember, the priority is to keep participants safe, but not to avoid tough conversations altogether, even if they make facilitators a little uncomfortable. 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 commencing user dialogues, instruct facilitators to never solicit personal stories of abuse and to inform participants that they may choose to stay silent or leave the discussion at any time without any repercussions. In addition, map out local GBV service providers and provide the list to facilitators so that they can make appropriate referrals as needed. You may also wish to enlist a local GBV specialist to co-facilitate some of the conversations. You may choose to implement each dialogue or only use those that are most relevant to your needs. When feasible, facilitators should share the following information with the participants. Be mindful of how you share this information given their levels of numeracy and literacy. Remind participants to keep this information private if they fear potential backlash by perpetrators of GBV: 1. Phone numbers to report harassment and abuse if this is an action that survivors wish to take 2. List of GBV resources and services in the area

Key Definitions [1]

Gender-based violence (GBV) refers to harmful acts directed at a person, or a group of people based on their sex or gender. It includes physical, sexual, verbal, emotional, psychological and spiritual abuse; threats, coercion and arbitrary deprivation of liberty; and economic or educational deprivation, whether occurring in public or private life. GBV takes on many forms, for example intimate partner violence, rape, early and forced marriage, female genital mutilation/cutting, sexual harassment or cyberbullying.

Technology-facilitated GBV is action by one or more people that harms others based on their sex or gender or by enforcing harmful gender norms. This action is carried out using the internet and/or mobile technology and includes such acts as stalking, bullying, sexual harassment, doxing, revenge pornography or other forms of image-based abuse, trolling, defamation, hate speech and exploitation.

Online GBV is a subset of technology-facilitated GBV and entails the use of the Internet to engage in activities that result in harm or suffering to a person or a group of people online or offline because of their sex or gender. GBV online can occur both in private or public online spaces, including social media, email, instant messaging, group chats, as well as knowledge-sharing, dating, gaming and other online platforms.

User Journey Map: Identifying GBV Risks and Mitigation Strategies

Please note that while men, boys and people with diverse gender identities experience GBV, this tool has been developed with women and girls in mind. Accordingly, the term "user" refers to women using digital technologies and tools while the term "partner" refers to the user's male intimate partner (often a spouse).

Purchasing a Mobile Phone and Opening an Account	Basic Mobile Phone Use (Calling and Texting)	Using Digital Financial Services (Online Banking, Mobile Money) and DSG Applications	Using Social Media and Mobile Applications	Using Mobile Internet
What is the prospective or current user doing?				
User seeks permission and money from her partner to purchase a phone or a SIM card User travels to a physical mobile network operator (MNO) location to purchase a phone, data and/or open an account User interacts with a male MNO agent User visits a government office to obtain an identification card needed to register her account	User makes or receives calls and texts to/from family, friends and strangers User seeks permission and money from her partner to purchase data and/or airtime.	User travels to reach a bank, mobile money or cash in - cash out (CICO) agent User receives calls or text messages on a personal or shared mobile phone with balances, saving and loan information, repayment reminders, or requests to verify transactions	User checks or posts on Facebook, Twitter or other social media platforms User downloads and inputs personal information into mobile applications (apps) User makes in-app purchases and subscriptions User downloads an app that may trigger a negative reaction from her partner User unwittingly shares personal, inappropriate or embarrassing information with the general public on social media	User conducts online searches and visits websites User unwittingly follows insecure links and visits untrustworthy websites

page 1 of 3

User Journey Map: Identifying GBV Risks and Mitigation Strategies

Purchasing a Mobile Phone and Opening an Account	Basic Mobile Phone Use (Calling and Texting)	Using Digital Financial Services (Online Banking, Mobile Money) and DSG Applications	Using Social Media and Mobile Applications	Using Mobile Internet
What are the GBV risks?				
Partner denies permission, suspects infidelity or is otherwise suspicious about why the user wants to purchase and use a mobile phone MNO agent makes harassing remarks, requires (sexual) favors or otherwise takes advantage of the user	Partner who is suspicious of user's calling and texting activities Partner monitors or demands to see user's text messages and call history Partner uses the mobile phone in a way that exacerbates existing offline intimate partner violence (e.g., abusive texts or surveillance) User receives harassing texts or phone calls from a family member, acquaintance or stranger Couple has conflict over the cost of airtime or the time that is spent on the phone and internet	Partner monitors or demands to see user's text messages, call history and financial information Couple experiences conflict over financial transitions or the mere use of financial services Financial agent makes harassing remarks, requires (sexual) favors or otherwise takes advantage of the user User experiences GBV during travel, especially if walking or using public transportation	Partner is jealous of user's social media interactions and tracks her online presence Couple has conflict over social media and app usage User witnesses or is personally affected by one or more forms of online GBV perpetrated by her family member, acquaintance or stranger(s) Partner monitors user's app use and in-app purchases or subscriptions User experiences in-app harassment or hidden charges Community members are suspicious of outside information and see the user as undermining the social fabric of the community; they are hostile toward the user	Partner monitors user's internet use and browsing histories User experiences online GBV, hacking, or scams causing further stress or conflict in the household

Common Issues

- Community members without mobile phones feel alienated and jealous; they perceive that the user must have obtained funds for the phone from "illicit" or "inappropriate" sources and are hostile toward the user
- Men in the household or community feel agitated and threatened because women's use of digital financial services challenges traditional gender norms and is perceived as undermining men's power, abilities and financial status; they are hostile toward the user

What can implementing organizations do to prevent and mitigate GBV risks?

Facilitate dialogues at the household or group levels and/or implement community awareness sessions to challenge harmful gender norms and practices that limit women's access to and use of digital technologies

Create and distribute a list of institutions and numbers to report GBV per the survivor's choice

Map out, create and share a list of local GBV service providers

Create and distribute a list of trusted bank, mobile money or CICO agents

Teach savings group members how to perform digital transactions on their own and finalize transactions before passing on a shared phone

User Journey Map: Identifying GBV Risks and Mitigation Strategies

Purchasing a Mobile Phone and Opening an Account	Basic Mobile Phone Use (Calling and Texting)	Using Digital Financial Services (Online Banking, Mobile Money) and DSG Applications	Using Social Media and Mobile Applications	Using Mobile Internet
What can users do to stay safe while using digital technology?				
Choose a recommended MNO agent and—if possible—travel with a trusted family member or friend	Think critically before giving your phone number to others Change your phone number if harassing texts or calls persist	Choose a recommended financial agent and—if possible—travel with a trusted family member or friend Whenever possible, perform digital transactions on your own in a safe space	Be thoughtful about who is on your social media "friend" lists Download only trustworthy or well-known apps; do not follow suspicious links in pop-ups, advertisements or emails	Only visit trustworthy websites Do not follow suspicious links in pop-ups, advertisements or emails

Common Issues

- If you experience harassment or abuse, or if you feel you are in danger, seek help from a trusted individual or specialized service provider
- Familiarize yourself with how to report abuse if you choose to do so
- Think critically when sharing your phone or phone number with others; be mindful they may access your private information if the phone or apps are not password-protected
- Keep emergency numbers in your phone
- Practice safe digital behaviors on your mobile phone

Safe Digital Behaviors

Teach savings group members about how to practice safe digital behaviors on their mobile phones, for example how to choose strong passwords or PINs and how to keep them secret; erase text messages and call histories, select privacy settings on social media platforms; share private information and images responsibly; know how to discern fact from fiction; know how to identify online abuse or scam; block, mute or unfriend abusive users; and refuse to engage in and report poor or harmful behavior. Refer to the companion tool, Digital User Dialogues, to facilitate conversations about these topics at the group level.

[1] These definitions have been adapted from the following sources: U.S Department of State and United States Agency for International Development (USAID), United States Strategy to Prevent and Respond to and Gender-Based Violence Globally (2016); American Bar Association Rule of Law Initiative (ABA ROLI) and RIWI Corp., Global Perceptions of Gender-Based Violence Online: Survey Findings and Call To Action (2019); International Center for Research on Women (ICRW), Technology Facilitated Gender-based Violence: What Is It, and How Do We Measure It? (2018).

DSG TOOLKIT:

DIGITAL USER DIALOGUES

GUIDING SAVINGS GROUP MEMBERS THROUGH DIGITAL TRANSFORMATION

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

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. 1. Phone numbers to report harassment and abuse if this is an action that survivors wish to take 2. 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 gender-based 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.

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.

continued on next page

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.

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

continued on next page

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.

continued on next page

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 "How to Block." Share these with the participants.

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

continued on next page

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.

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

continued on next page

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 Annex.

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.

continued on next page

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.

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.

continued on next page

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.

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

continued on next page

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 Data Protection and Security.

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. *See Poster*

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

continued on next page

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.

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.

continued on next page

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?"

continued on next page

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

continued on next page

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.

continued on next page

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 upper- and 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.

continued on next page

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.

continued on next page

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.

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.

DSG TOOLKIT:

DATA PRIVACY AND SECURITY

KEY QUESTIONS TO ASK TECHNOLOGY PROVIDERS

DATA PRIVACY AND SECURITY

KEY QUESTIONS TO ASK TECHNOLOGY PROVIDERS

Purpose	Digital transformation offers invaluable benefits to savings group members and implementers, but it comes with new challenges related to consumer protection. This includes risks of data privacy violations and data security breaches, which can damage members' personal and financial well-being, while also creating serious legal, financial and reputational implications for entities supporting SGs including implementing organizations and their vendors. By design, digital solutions for savings groups collect a wide range of data from DSG members, including their financial records and personally identifiable information (PII), such as names, photographs, phone or national identity numbers. Digital solution providers (e.g., fintech companies) are de-facto custodians of group and member data, which can be prone to hacking, manipulation and cyber-attacks if appropriate protocols for data collection, storage, processing, use, transfer, alternation, disclosure or deletion are not in place. Implementing organizations must understand these risks and data protection measures must be integrated into a digital solution's architecture before introducing it to savings groups. This tool is designed to help DSG implementers ask technology providers the right questions about their data security policies and protocols, with the goal of protecting the data privacy rights of DSG members.
Audience	This tool is intended for staff of organizations implementing DSG projects, specifically program designers, program managers, information technology (IT) managers, data protection specialists and general counsels.
Time needed to implement the tool	• Review of the tool – 30 minutes • Conversations and the collection of information from digital solution providers – time to be determined by project managers • Additional research about local and global data privacy and security standards – time to be determined by project managers, data protection specialists and general counsel
How to use this tool	The tool defines data privacy and security in the context of DSGs and includes a list of questions to ask digital solution providers while evaluating their vendor proposals.

continued on next page

How to use the tool - continued	Implementers can include these questions in their requests for proposals and use them to guide their conversations and contract negotiations with vendors. In either case, implementers should ask vendors to answer these questions in writing. Some issues are complex, and it is important to ask for clarification until satisfactory answers are obtained. Ideally, questions listed in the tool should be addressed in the process of selecting a digital solution for savings groups, before starting implementation. The tool will also be useful for organizations that are already using a digital solution to support savings groups, especially if there are concerns about data privacy and security or if the technology provider plans to introduce new software features which may increase data privacy and security risks. Implementers are also encouraged to use the companion tool, "Digital User Dialogues," to facilitate conversations with DSG members about how their data will be used, secured and what steps they can take as a group or on their own to further protect their data. Implementers and their vendors should review data privacy laws applicable to national markets where DSG solutions are being deployed. They should also consider applying best practices and globally recognized data privacy standards, even if they are not legally bound by them. This includes, for example, the General Data Protection Regulation (GDPR) of the European Union.
References	Digital Savings Groups Learning Brief (2020) Quickly Identifying Potential Data Risks (2022)

Definitions

While data privacy and data security are sometimes used interchangeably, they are different. Data privacy refers to the rights of individuals with respect to their personal information, and the proper usage, collection, retention, deletion and storage of data. Whereas data security refers to policies, methods and means to secure personal data.

Data Privacy

The protection of personal data from those who should not have access to it and the ability of individuals to determine who can access their personal information.
(Sources: CloudFlare, Data Privacy Manager)

Data Security

Controls, standard policies and procedures to protect data from a range of issues, including unauthorized access, accidental loss or destruction.
(Sources: Digital Guardian, Data Privacy Manager)

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 prevention of unauthorized access or misuse of 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.

Data Privacy and Security Questions to Ask Digital Solution Providers

1. *Do you have a Privacy Policy? Is it publicly available? Can you please share it with us?*
2. *Do you have a Data Protection Officer?*
3. *What the data security protocol for your product?*

   Data security protocols are the software and behavioral rules that guide how employees handle and access data collected through websites or mobile applications, such as those used to manage DSGs. These protocols should include strong encryption when transmitting data and storing it on both the mobile phone and server. Vendors should have clear guidelines that demonstrate the organization's approach to data security. This will include things like SSL certificates (digital certificates that authenticate a website or a mobile application's identity and enables an encrypted connection), virtual private networks (VPNs), multi-factor authentication and more.

   Security controls should be publicly available. If a vendor must draft them specifically in response to your request or has trouble explaining them, they may not have adequate controls in place.

4. ***Have you conducted data mapping for your product? If yes, can you please share it with us? If not, please answer the following questions.***

   Conducting data mapping is a crucial first step in ensuring compliance with data privacy laws, standards and best practices. It is imperative to know what data will be collected from DSG members through the digital solution, how this data will be stored and transferred, whether an internal or external party will have access to it and what safeguards are in place to protect this data (e.g., IT controls or contractual protections). Please note that a vendor may ask for a non-disclosure or confidentiality agreement prior to disclosure, which is typical.

   a) What data does your product collect from savings group members? Please include both sensitive and non-sensitive data points, including all personally identifiable information (PII) and location data if applicable.

   b) How will you protect the rights of DSG members as data subjects?
      - Right to information
      - Right of access
      - Right of rectification
      - Right to erasure
      - Right to restrict/object to processing
      - Right of data portability
      - Right to object
      - Right to be notified of data breaches
      - Right to avoid automated decision-making

   c) Where will DSG group and DSG members data be stored?

   Vendors can store data in a variety of places, like on premises, in the cloud or both. Make sure you understand where the DSG data is being stored and how it is backed up.

   Companies with remote employees should be optimized for mobile and virtual platforms, as well as able to provide a consistent and secure environment for them to access data.

   d) How will you process and use DSG member data?

   e) Who will have the capacity to alter, archive or destroy DSG member data?

5. *Have you achieved any recognized data protection standards?*

   There are a variety of data protection standards governing how organizations approach data security: ISO 27001, SSAE16, and Safe Harbor, among others, these provide companies with a clear blueprint dictating how to safeguard data. ISO 27701 is the new international standard in data privacy and is particularly noteworthy. It was designed with the General Data Protection Regulation's (GDPR) principles of privacy by design and by default in mind, so it is fully compliant with modern data protection standards and expectations.

   Your vendor may be too small to be certified by any of these standards, but it is worth asking. Even if they are not certified, it is good to understand if they adhere to certain standards.

6. *How do you assess your employees' knowledge about data security?*

   Some of the most damaging data breaches result from human error. In an ideal world, your vendor will conduct regular data protection training, or it might be part of new employee onboarding.

7. *Do you separate customer data from the main infrastructure?*

   If your vendor's main infrastructure is hacked, you want to know that the DSG members' data is safe — ideally in a cloud-based environment.

   If they are kept separately, it is also worth enquiring about internal access controls. It is important that only necessary users can access client information. Cloud computing can be highly secure if the right access controls are in place and customer data is kept separate from the main infrastructure.

8. *Do you work with other third parties to deliver your solution? Do they have access to DSG member data? If yes, what are their data security protocols?*

   Many vendors rely on third parties for part of their solution, and those vendors might not have tight data security protocols. Using a third-party is not in and of itself concerning; it is quite common for Software as a Service (SaaS) companies. You need to enquire about third-party data protection policies and standards.

9. *What is your disaster recovery plan for your product?*

   No matter how tight their security, there is always the chance that the vendor will suffer a data breach. In that event, they need to have a solid recovery plan in place. Not only will it help protect the DSG member data, but it means they can get back up and running as soon as possible.

10. *Do you perform routine disaster recovery tests for your product?*

    A plan is only as good as its execution. Routine tests prove that security is a top priority, and they make sure that everyone knows what is expected of them in a crisis. Disaster recovery tests ensure the recovery plan is completed as smoothly and painlessly as possible.

11. *Are you GDPR compliant?*

    Depending on your donor requirements, you may need your vendor to be GDPR compliant. GDPR applies to all companies that conduct business or engage with customers in the European Union.

12. *What are my data privacy compliance needs from a legal and ethical standpoint?*

    This is something you should understand before you talk to your vendor. But the vendor should also be able to advise you on these issues in your jurisdiction, and they should understand and ensure that you follow legal standards.

    Increasingly countries have data sovereignty laws that guide how data gathered from citizens can be stored and used. You should seek legal counsel, even if you outsource your data storage and management to a service provider, you likely have legal liability. Be sure to thoroughly check your vendor's track record and credentials to ensure they can handle your unique data compliance and security needs.

13. *What is your software update policy?*

    Old software can put systems and networks at risk for cyberattacks. That is why it is a good idea to ask the vendor if they automatically update their software solutions.

14. *Do you have filters or similar features that will protect DSG members from cyberthreats?*

    Does the solution have built-in protection that stops things like malware and phishing messages from reaching people who use the tool?

15. *Who will have access to DSG member data? Please include all internal and external parties.*

    What DSG member data do you share or plan to share with third parties (i.e., implementing organization or a financial service provider)?

    When selecting a vendor, you want to understand who owns client (DSG member) data. Is it the vendor or the implementing organization? If the vendor owns the data, which may be common for DSG solutions, what rights do you as the implementing partner have to access, process or use that data? Will you have access to raw data or only to reports generated by the solution? Will you have access to individual member data (e.g., names or phone numbers) or only group-level data (groups' savings balances)?

    Before signing a contract, it is important to know whether or how the vendor is entitled to share, sell or otherwise use DSG member data, even if they are the ultimate owner of the data. Your vendor should have a data privacy policy that they can share with you.

16. *How does your product ensure user awareness and consent around data collection, processing and sharing?*

    Many DSG platforms are designed to provide data to third parties in order to improve DSG members' access to financial services. But any vendor you work with should have processes in place to request user consent for any data sharing with third parties that includes personally identifiable data, including name, identification numbers, phone numbers or addresses.

    Ask specifics on the consent request, including a copy of their policy on user consent. A blanket data sharing agreement in an applications' 'Terms and Conditions' should not be considered adequate and is often not in compliance with local and global laws, including GDPR. A consent request needs to be presented in a clear and concise way, using language that is easy to understand and be clearly distinguishable from other pieces of information such as terms and conditions. The request must specify what use will be made of personal data and include the name of the company accessing the data. Consent must be freely given, specific, informed and unambiguous.

ANNEX

Acknowledgment: The handouts in this Annex come from GSMA's "Connected Society: Mobile Internet Skills Training Toolkit."

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

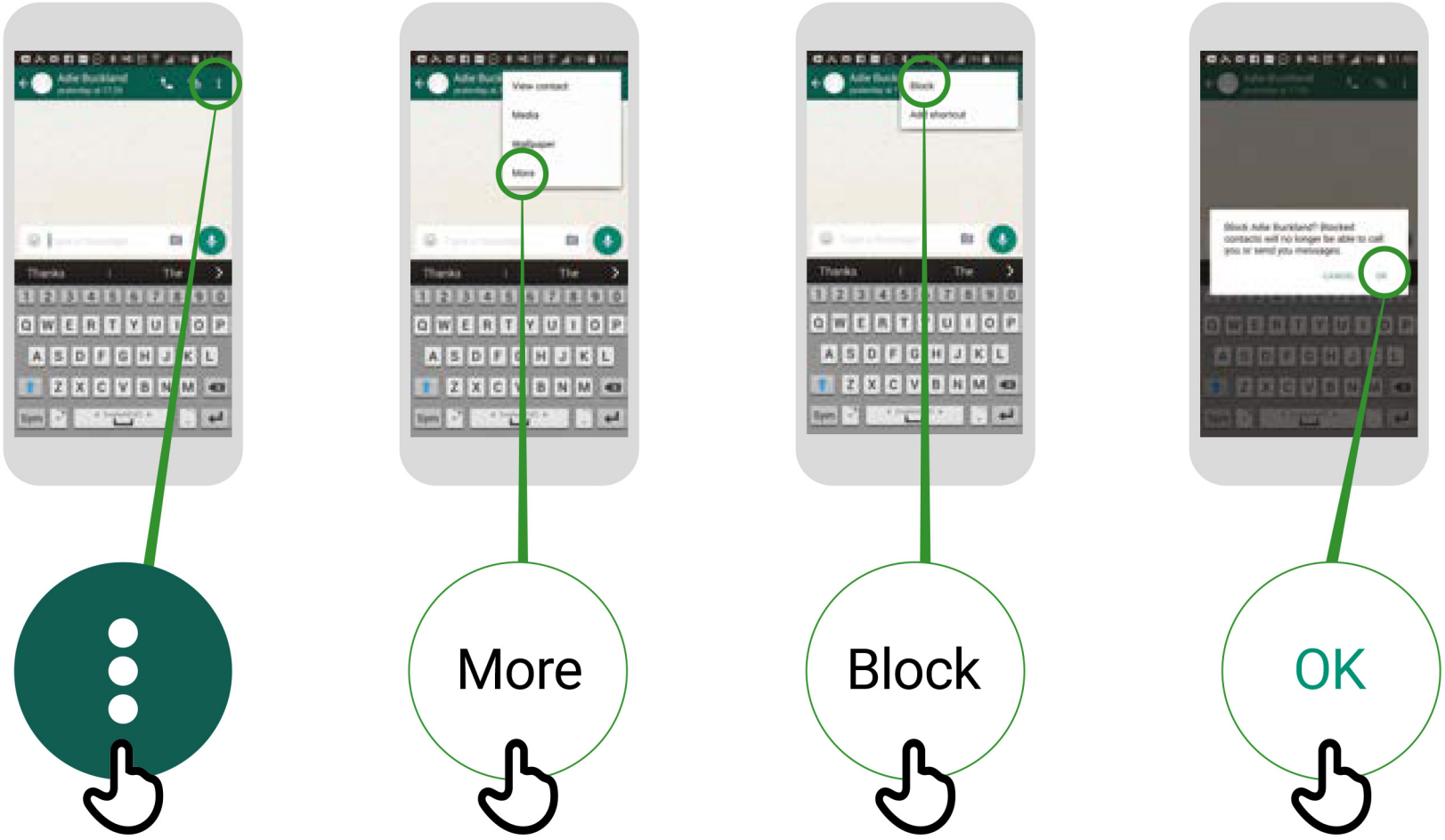
Be polite and respectful to people

WhatsApp

How to use

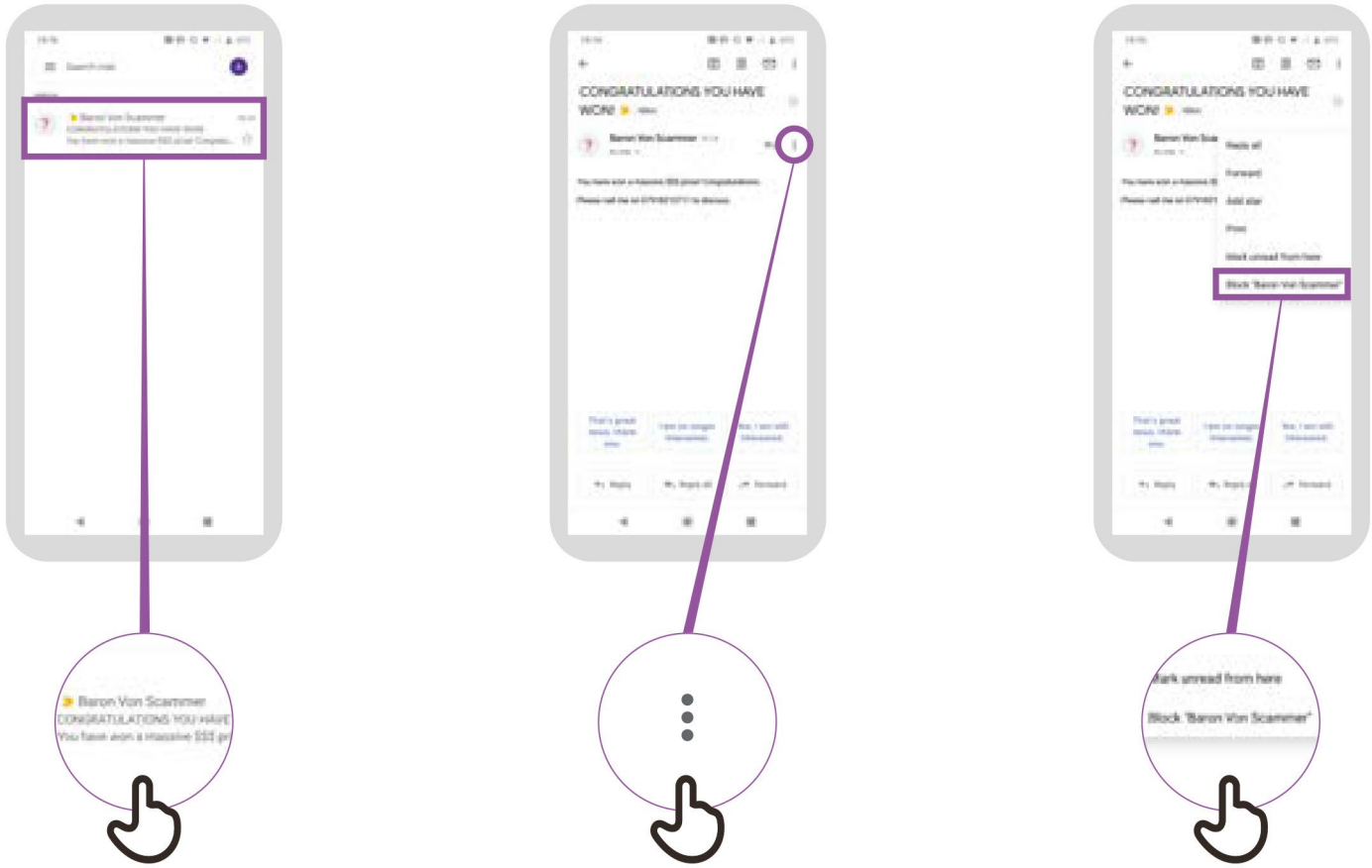
WhatsApp How To ‘Block’

1 → 2 → 3 → 4



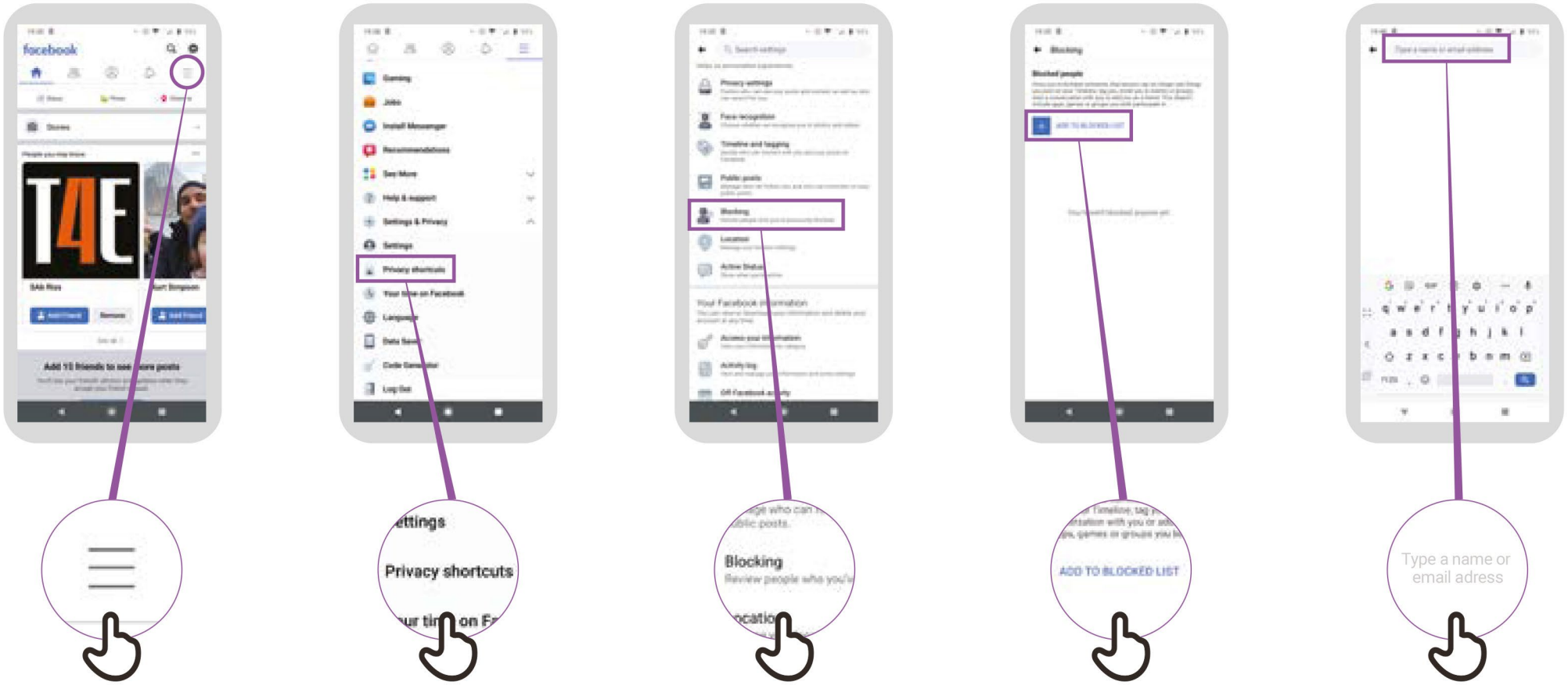
How to ‘block’ on Gmail

1 → 2 → 3



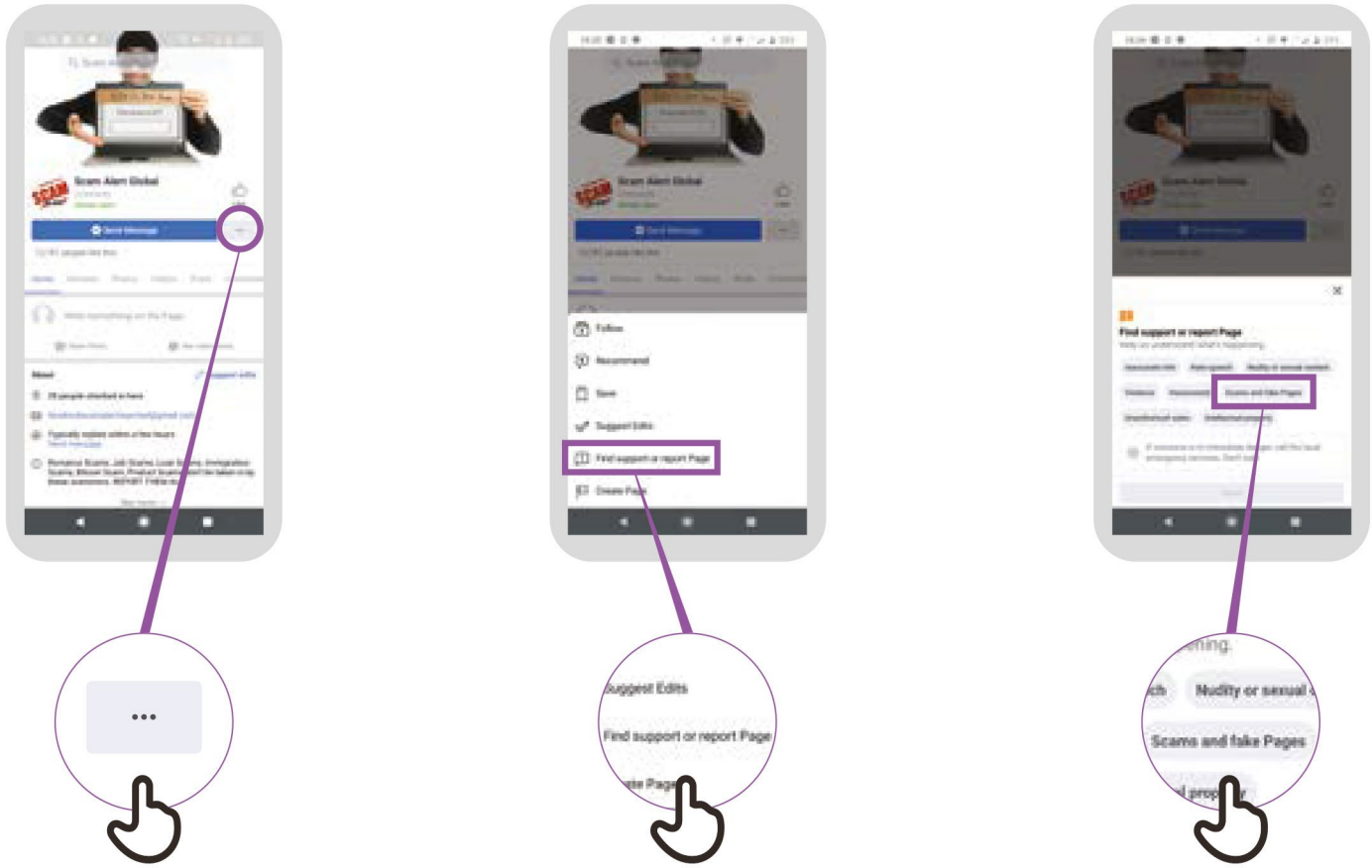
How to ‘block’ on Facebook

1 → 2 → 3 → 4 → 5



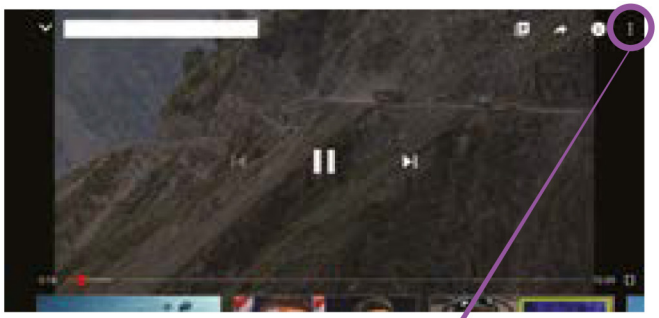
Reporting a page on Facebook

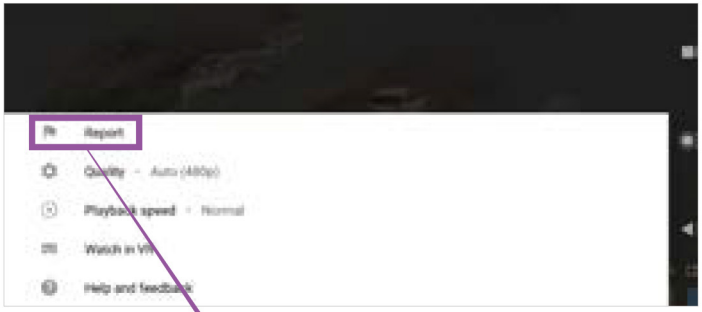
1 → 2 → 3

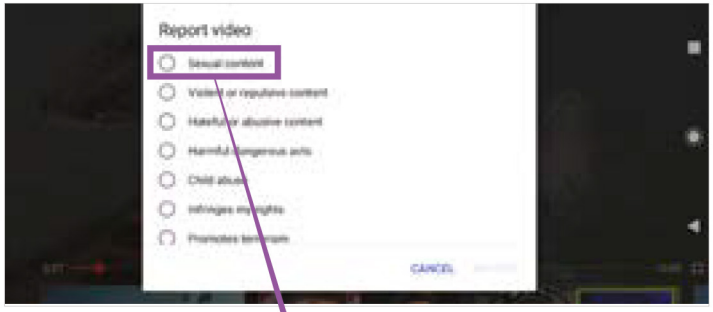


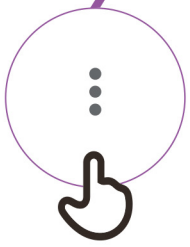
Reporting a video on YouTube

1 → 2 → 3

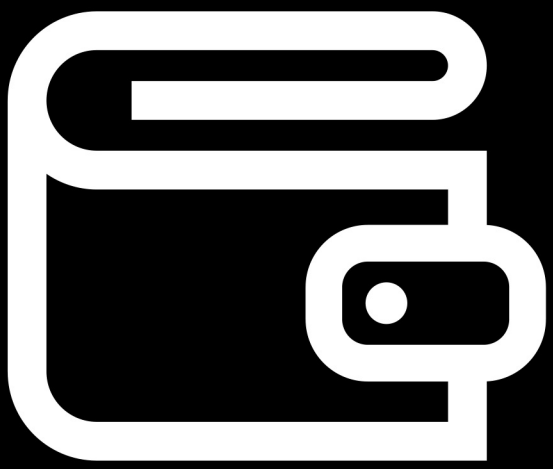




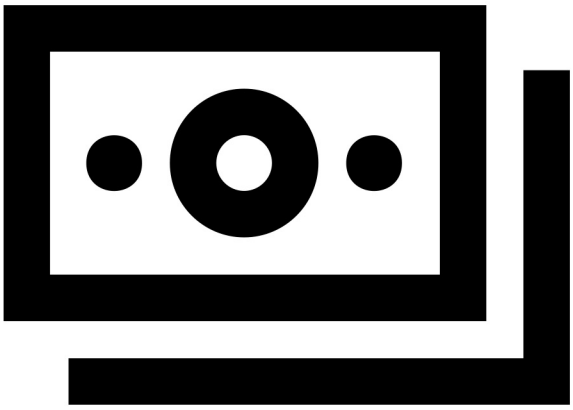




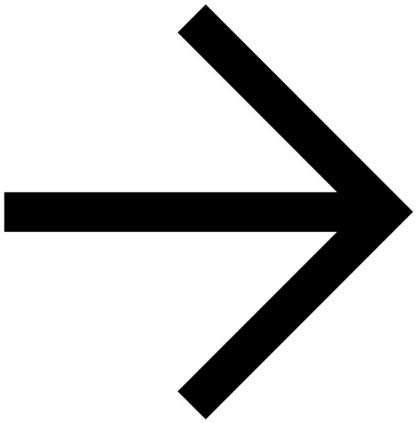
What is mobile money



It's like having a wallet on your phone.



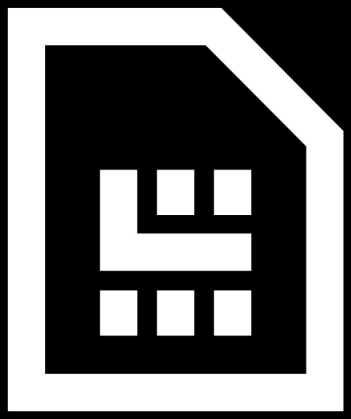
Cash can be deposited and withdrawn from your mobile money account with your agent.



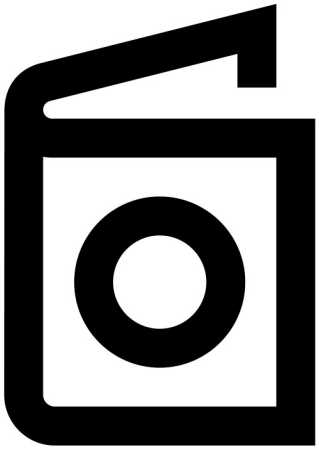
You can send money to other people, pay bills, pay for goods.

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

Registering for mobile money account

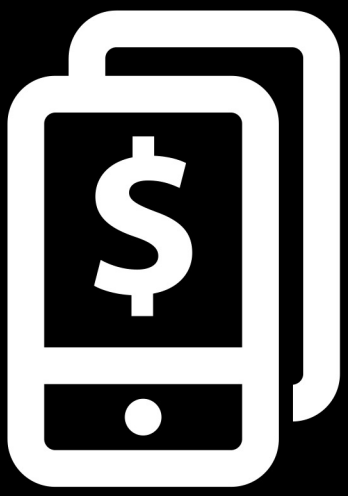


You need a SIM card from your mobile operator. Your money agent will register you for mobile money.



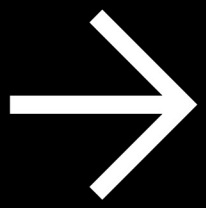
To register for mobile money, you need proof of identity.

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

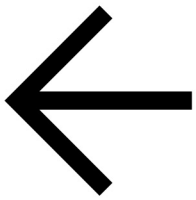


Once these steps have been completed you can start using your mobile money account!

What you can do with mobile money

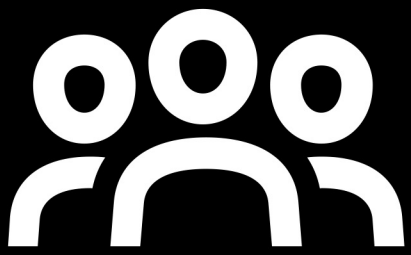


Send money to friends or family



Receive money from friends or family

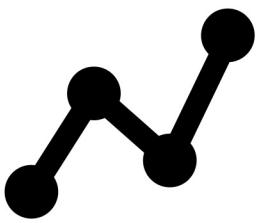
Pay bills or school fees



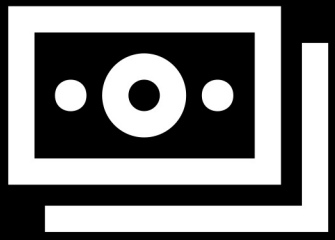
Buy airtime for you or other people

Send / receive money to and from friends and family in other countries

Pay for goods and services

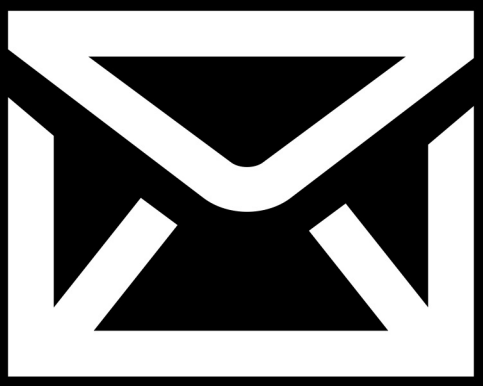


Earn interest on your savings



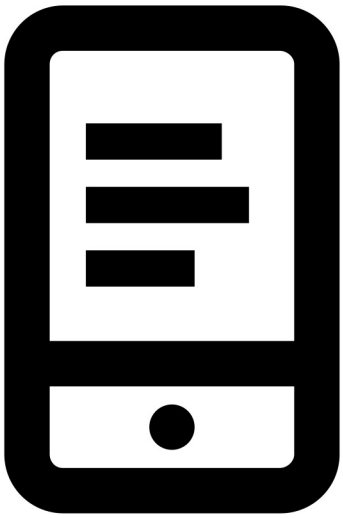
Get a loan

Staying safe using mobile



Message

PIN

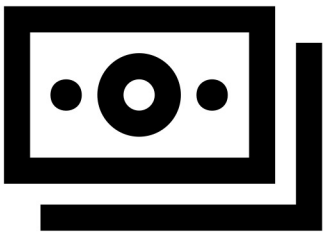


Phone

Agents

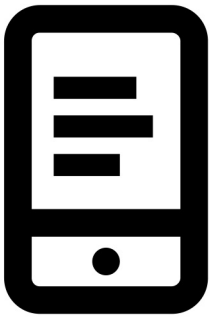
5 key things to know about mobile money

Account registration



Mobile money account

Mobile money agent



Mobile number

PIN number

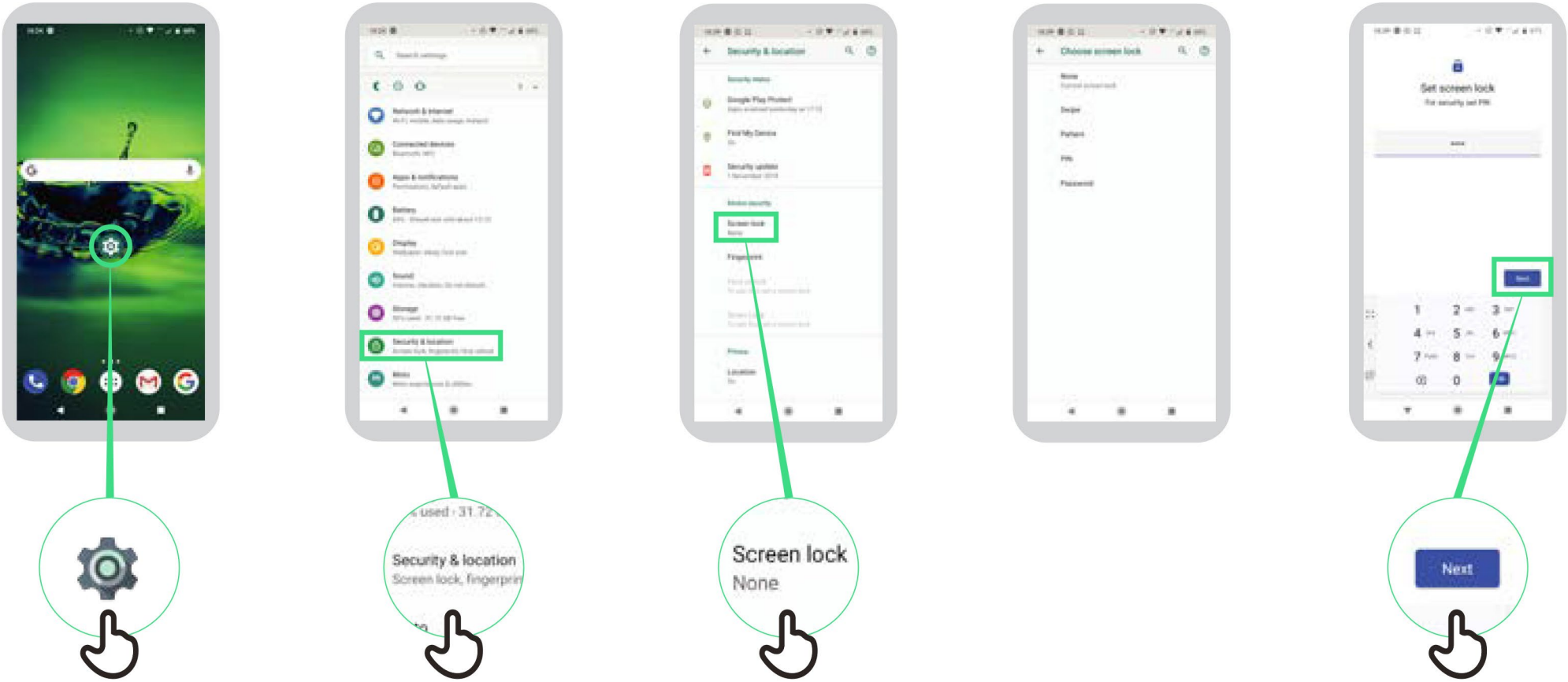
5 key things to know about mobile money

Account registration	To use mobile money you will need to register at a mobile money agent who will help you create an account. To do this you will need a SIM card and some ID documents (like a passport, driving license or voters card)
Mobile money account	A mobile money account is like having a wallet on your phone. With mobile money you can send and receive money from people, and make 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 important for mobile money. When you want to send money to someone using mobile money you use their mobile number. This is the same if they want to send money to you.
PIN number	This is your personal number which helps you protect your mobile money account. You will need to type this into your phone when using mobile money. Keep it safe and don't share it with anyone!

android

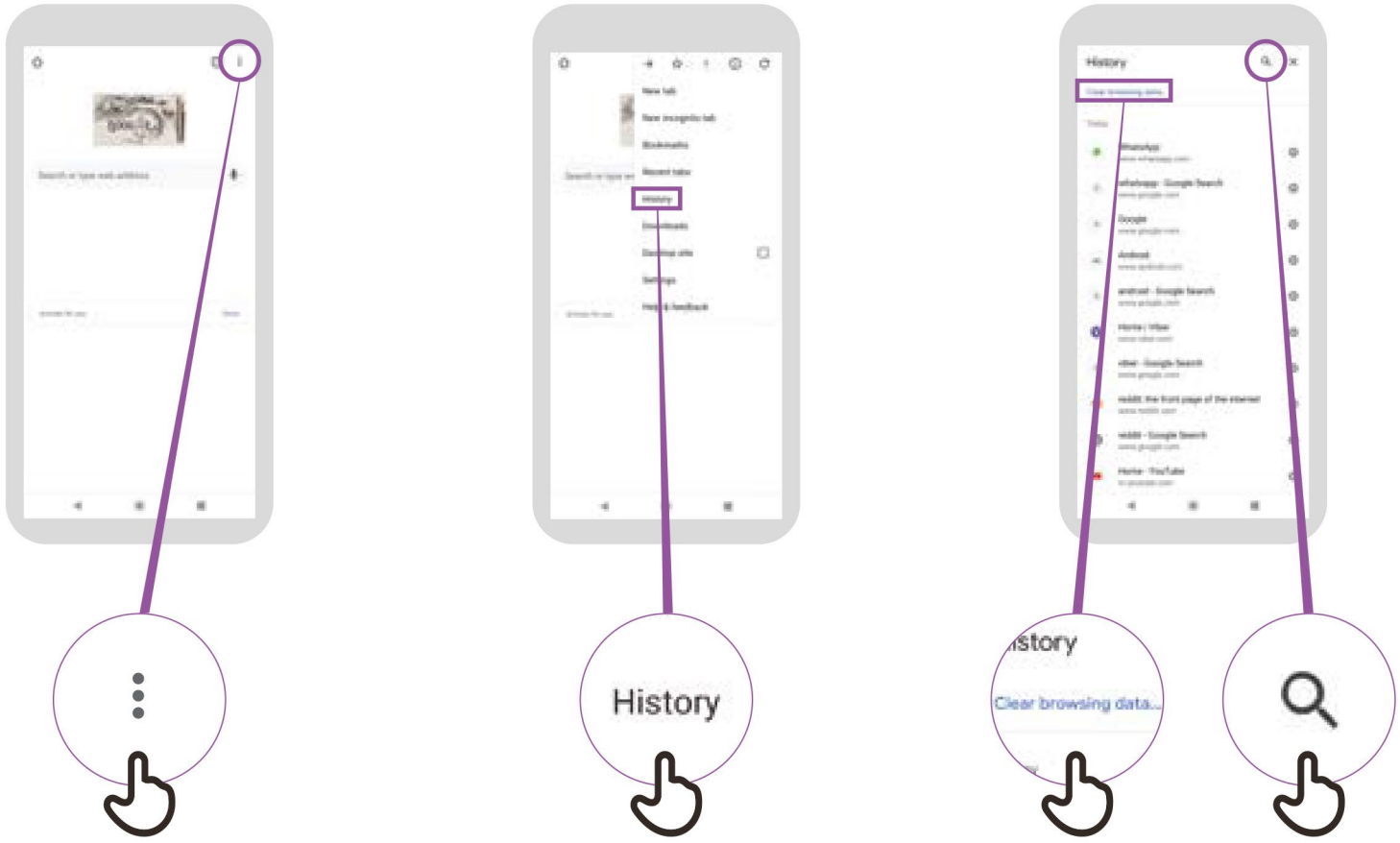
Device Security

1 → 2 → 3 → 4 → 5



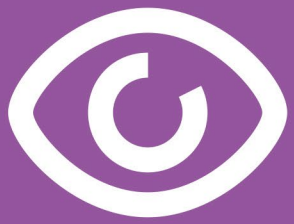
Accessing 'search history' in Chrome

1 → 2 → 3

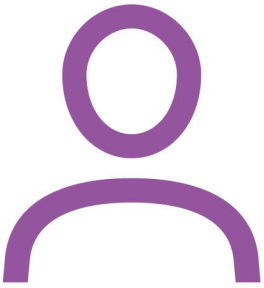


False information

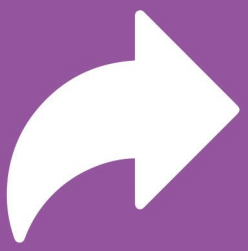
Be careful!



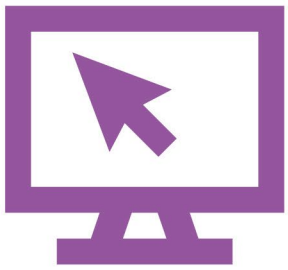
If you are unsure, ask someone you trust!



Don’t share something with other people without thinking first!



Check other sites



Report it

Data Costs

YouTube
facebook

facebook

Google
WIKIPEDIA

WhatsApp