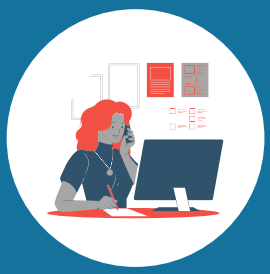
DIGITAL SECURITY AND ONLINE SAFETY MANUAL



Implemented by

WOMEN OF UGANDA NETWORK

in partnership with

digital HUMAN RIGHTS lab

with support from

german cooperation DEUTSCHE ZUSAMMENARBEIT

giz

Authors: Gole Andrew, Sandra Aceng, Isaac Amuku,
Letowon Saitoti Abdi, Esther Nyapendi

Design: Gole Andrew

Photo Credits: Gole Andrew

On Behalf of Women of Uganda Network (WOUGNET)

TABLE OF CONTENTS

PREFACE

Digital Security and Safety of women online has become extremely important, now more than ever. With the rapid adoption of technology and digital platforms, the internet has become a vital resource for all groups of people regardless of age, sex, gender, race, or one’s identity.

Whereas the adoption of the use of the internet and digital technology has sky-rocketed, there has been an increase in threats and challenges related to using these digital platforms. These threats and challenges do not segregate on which group of people are a target. However, women appear to be more of a target when it comes to online threats and this is simply because they are women. According to WOUGNET’s recent study, women face more online threats compared to men while using these online platforms.

In this day and age, Online gender-based Violence (OGBV) has become a force to reckon with and needs to be taken seriously if women's safety online is to be guaranteed.

This Digital Security manual is a step in the right direction in ensuring that women's safety online is something they can give priority to and put in place the necessary measures needed to ensure they achieve it. The manual aims at providing women with basic digital security knowledge and skills that they can implement to take ownership of their online safety and security.

ACKNOWLEDGEMENTS

This digital security manual is a curation of different digital security tips and best practices for women to protect themselves against common digital security threats. It was developed based on the findings from research conducted nationwide on the types, spread, impact, and methods of dealing with OGBV by Women of Uganda Network (WOUGNET) with support from the Digital Human Rights Lab (DHRLAB) which is implemented by Betterplace lab and Future Challenges under a grant agreement with the Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) Programme Strengthening Governance and Civil Society in Uganda, funded by the German Federal Ministry of Economic Cooperation and Development (BMZ) under its Digital Africa Initiative.

ACRONYMS

2FA	2 Factor Authentication
ADIDS	Activity, Discussion, Input, Deepening, and Synthesis
DHRLAB	Digital Human Rights Lab
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
MALWARE	Malicious Software
NCII	Non-consensual Intimate Images
OGBV	Online Gender-based Violence
PIN	Personal Identification Number
USB	Universal Serial Bus
WOUGNET	Women of Uganda Network
WWW	World Wide Web

GLOSSARY

HTTPS	The secure version of HTTP, which is the primary protocol used to send data between a web browser and a website.
Phishing	Is the fraudulent attempt to obtain sensitive information such as usernames and passwords by posing as a legitimate person or entity.
Internet	A vast network that connects computers all over the world. Through the Internet, people can share information and communicate. Derived from international network
Cloud	A cloud is just a server (computer) that's located out of your physical reach but can be accessed with the use of an internet network.
Encryption	This process converts the original representation of the information, known as plaintext, into an alternative form known as ciphertext.
Browser	A web browser is software that navigates websites - Firefox and Chrome are examples.

Password	A string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization.
Antivirus	These are programs created to help protect your device from malware. It mainly looks at data — web pages, files, software, applications.
Malware	An umbrella term for Malicious Software, very likely containing a virus or an otherwise malicious software application.
Password Manager	A computer program that allows users to store, generate, and manage their passwords for local applications and online services.
Data	Refers to any unprocessed information that is retrieved, sent, stored or can be accessed using a web browser or plug-in software.
Digital footprint	This is data that is left behind when users have been online. There are two types of digital footprints which are passive and active.

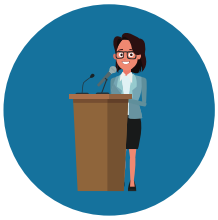
SECTION 1: ABOUT THE MANUAL

1.1: WHY THIS MANUAL

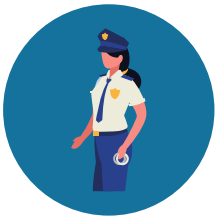
This digital security manual is very vital for women who are experiencing online threats due to their gender. This guide gives them the power to take charge of their online safety and security.

1.2: WHO THIS MANUAL IS FOR

This manual can be used by anyone who is experiencing online gender-based violence and can be used by TOT on digital security and Online Safety. However, it is more focused towards helping the following groups of people below;



Female Politicians



Law Enforcement

Female Journalists

University Students

Female Artists/ Musicians

1.3: HOW THIS MANUAL IS STRUCTURED

- **Section 1:** Provides information about this manual, whom it's meant for, and why it's important.
- **Section 2:** Provides an introduction to digital security and safety for women online.
- **Section 3:** Provides General Digital Security Tips for Women
- **Section 4:** Provides a list of online courses on Digital Security.
- **Section 5:** Provides information on conducting digital security training.

SECTION 2: INTRODUCTION TO DIGITAL SECURITY

2.1: UNDERSTANDING THE COMMON DIGITAL SECURITY THREATS ONLINE

Digital Security is the protection of one's digital personality, as it represents the physical identity on the network you are operating on or the internet service in use.

Digital Security includes the tools which one uses to secure his/her identity, assets, and technology in the online and mobile world. Simply put, let's think of digital personality as the human body.

Under digital security, there are a number of interconnected topics in order to ensure someone who wants to improve their digital security is given all the knowledge and skills to safely do so. Digital Security encapsulates topics related to digital literacy, secure communication, data protection and privacy, password management, device management, and risk assessment.

For this manual, we will briefly explore the common threats faced by women on various digital platforms as we provide practical solutions based on the topics listed above.

2.2: COMMON THREATS FACED BY WOMEN ONLINE

There are quite a number of digital security threats that limit women from fully engaging on digital platforms. These threats can have adverse effects on women in many ways ranging from; feeling upset, embarrassed, stupid, depressed, feeling ashamed, or losing interest in the things they love.

These include threats like;

- Cyber-stalking,
- Trolling,
- Doxing,
- cyber-bullying,
- Impersonation,
- Hate Speech,
- Public Shaming,
- Non-consensual distribution of sexually explicit intimate images (NCII), and
- Online harassment among others.

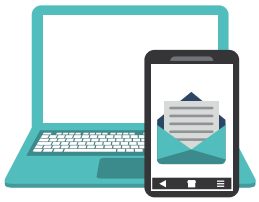
It is important for women to know how to protect themselves from these online threats because they have increasingly become rampant and oftentimes drive women away from digital platforms and the internet.

No one whether woman or man should be driven away from utilizing the internet's full potentials. Let's explore some of these threats in detail and look at the best practices to protect against them.

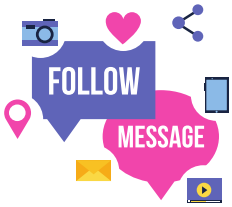
2.2.1: CYBER-STALKING

According to Wikipedia, Cyberstalking is the use of the Internet or other electronic means to stalk or harass any individual, group, or organization. It may include false accusations, defamation, slander, and libel. It may also include monitoring, identity theft, or blackmail.

COUNTERING CYBER-STALKING



Don't leave your devices unattended. It only takes a few minutes for someone to install a tracking device/software on your device.



Practice online safety habits like only accepting friend requests from people you know and keeping your posts private.

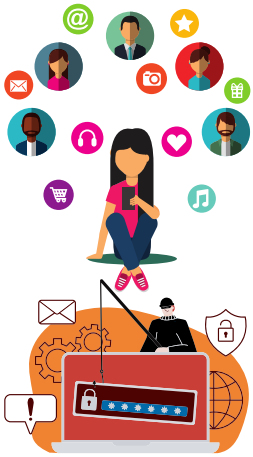
Always log out of social media accounts, and other online accounts after using them. This way, if someone was able to get into your device, they would not have easy access to your accounts.

Make sure you have strong passwords for all your online accounts as well as strong passwords for your devices.

2.2.2: TROLLING

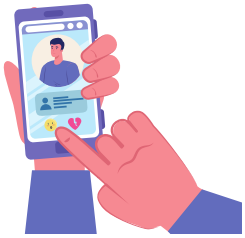
Trolls can be real people or fake accounts run by computer bots. They often aim to shut down discussion on social media threads by leaving so many negative comments that it is impossible for women to engage in conversations. They can also be used to intimidate or threaten female politicians, and in some cases, trolls may try to hack into a person's accounts.

COUNTERING TROLLING



Separate your work from your personal life on your social media accounts.

Protect your accounts from being hacked by using a password manager to create long unique passwords.



Review the privacy settings of your social media accounts and change them for any information that you do not want public.

When trolling occurs, try not to engage with the trolls, as this can make the situation worse.

Block or mute trolls. You should report any trolls that are abusive or threatening to the social media company.

2.2.3: DOXING

Doxing is when personal information on a person – for example, an address or phone number – is made public online. This information is normally taken from public databases or the person's online profile, but adversaries may also hack online accounts to obtain personal data.

COUNTERING DOXING

Review content on your accounts, including emails and private messages on social media, for any information that could put you at risk.

Lock down the privacy settings of your social media accounts.

Consider speaking to relatives about their social media accounts and settings. Adversaries can obtain a lot of information on you through the accounts of family members and friends.

In the event of a doxing attack, Let your contacts know that you have been doxed, including your family, employer, and friends.

2.2.4: CYBER-BULLYING

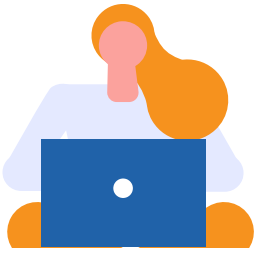
Cyberbullying is bullying with the use of digital technologies. It can take place on social media, messaging platforms, gaming platforms, and mobile phones. It is repeated behaviour, aimed at scaring, angering, or shaming those who are targeted.

COUNTERING CYBER-BULLYING

If the bullying is happening on a social platform, consider blocking the bully and formally reporting their behavior on the platform itself.

Find out as much information about the bully and expose them online. This may make them stop bullying you or someone else.

Ignore bullies. Don't engage with bullies, If they notice you are not giving them attention, they might stop.



If the bullying persists and you feel you are in immediate danger, then you should report to the police immediately.

2.2.5: ONLINE SHAMING

According to Wikipedia, Online Shaming is where a person is publicly humiliated on the internet, via social media platforms (e.g. Twitter or Facebook), or more localized media (e.g. email groups). Online shaming frequently involves exposing private information on the Internet, public humiliation, and "revenge porn".

COUNTERING ONLINE SHAMING

If you find yourself being publicly ashamed on social media, have a break from the platform to avoid breaking down physically, mentally, and emotionally.

Try as much as you can to ignore people who are publicly ashamed of you online especially on social media. If possible, block them and report to the social media platforms.

Protect your devices and online accounts with strong passwords to avoid your sensitive files like photos from getting leaked on social media. These files like intimate photos can be used to publicly ashamed you on social media

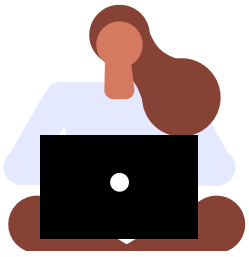
2.2.6: NON-CONSENSUAL DISTRIBUTION OF INTIMATE IMAGES (NCII)

This is when a person's sexually explicit images and videos are shared without their consent or taken without their consent. There has been an increase in the leaking of intimate images on social media recently.

COUNTERING NCII

Take some time off social media to reduce on the negative feedback and consequences resulting from leaked intimate images.

Use strong passwords on devices with sexually explicit intimate images. This will prevent someone from easily accessing its content.



Remove sexually explicit intimate images from the device before taking them for repair. Some phone technicians tend to download files from their clients' devices.

Securely encrypt and backup sexually explicit intimate images in secure locations to avoid them from falling in the wrong hands.

When sharing sexually explicit intimate images or videos with your partner/ loved ones, consider using secure communication platforms like Signal.

2.2.7: HATE SPEECH

Online hate speech is a type of speech that takes place online with the purpose of attacking a person or a group based on their race, religion, ethnic origin, sexual orientation, disability, or gender.

COUNTERING HATE SPEECH

Once you notice someone is spreading hate speech, don't give them the recognition they search for. When you see their provocative comments on social media, the best thing to do is probably ignore them.

Sometimes, hateful messages can also be spread by a real person. In these cases, a direct response could be a more effective way to address the problem, as long as you do it in the right way.

When facing hateful speech, just disconnect., switch your devices off and go for a walk, talk to a friend or do something you like. Get distracted and don't let a bad episode on social media bring you down.

2.2.8: IMPERSONATION/ IDENTITY THEFT

This is the use of someone else's name to send an email, post material, create social networking accounts, or contact other people in any way. Online Impersonation is a big threat to women because sometimes it can be used to promote hate speech or even damage a person's reputation online.

COUNTERING IMPERSONATION/ IDENTITY THEFT

Limit how much information we share on social media. Do not share too much information about yourself on social media.

Review privacy settings of social media platforms. This will help you tweak the settings in a way that limits who has access to information about you on social media.

Use a password manager to create and store complex, unique passwords for your accounts. Don't reuse passwords. Using multi-factor authentication can reduce the risk.

Be alert to phishing and spoofing emails. Scammers can make phone calls that appear to be legitimate attempts to steal your information.

SECTION 3: GENERAL DIGITAL SECURITY TIPS

3.1: GENERAL PASSWORD MANAGEMENT TIPS

Passwords are usually the first line of defense used to protect data and information stored on laptops, social media, and other online accounts, smartphones.

DO NOT USE PERSONALLY IDENTIFYING INFORMATION.

Using your name, birthday, number, etc. is dangerous because these can be easily guessed.

DON'T WRITE YOUR PASWORD DOWN

Use a password manager to help you store long complex passwords as opposed to writing them down on sticky notes

CHANGE PASSWORDS ON A REGULAR BASIS

Passwords should be changed at least once a quarter. Using the same password for longer periods could put your information at risk if a data breach occurs.

DON'T USE THE SAME PASSWORD ON DIFFERENT ACCOUNTS

Don't use the same password on more than one account. If a hacker cracks it, then all the other accounts could also be compromised.

USE PASSWORDS THAT ARE LONG, COMPLEX, AND HARD TO GUESS

The longer the password, the harder it may be to crack. Try for a minimum of 10 characters. Mix numbers, letters(both uppercase and lowercase), and special characters

3.2: GENERAL DEVICE SECURITY TIPS

Passwords are usually the first line of defense used to protect data and information stored on laptops, social media, and other online accounts, smartphones.

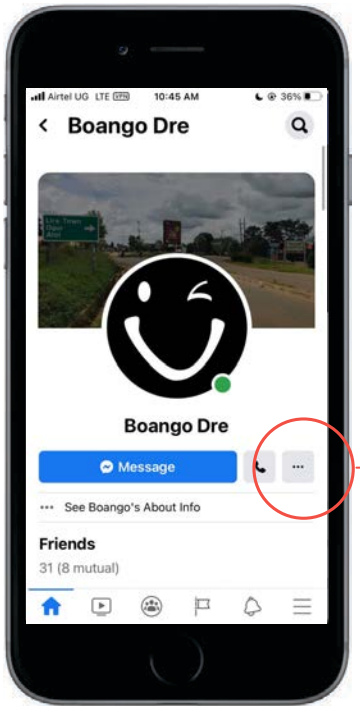
1. Lock devices with a password, code, or PIN. Longer personal identification numbers or passwords are more difficult for others to unlock.
2. Update your operating system, apps, and browsers when prompted. Old software has vulnerabilities that can be exploited to install malware on your devices.
3. Back up your devices regularly in case they are destroyed, lost, or stolen. Store the backup copies securely, away from your regular workstation.
4. Delete sensitive information regularly, including chat messages.
5. Don’t leave devices unattended in public, including when charging, as they could be stolen or tampered with.
6. Don’t plug devices into public USB ports or use USB flash drives that are handed out free at events. These could come loaded with malware that could infect your computer.
7. Set up your devices to allow you to wipe any data remotely if they are stolen. This feature must be set up in advance, and the device will only wipe if it is connected to the internet.
8. Always get devices repaired by reputable technicians.

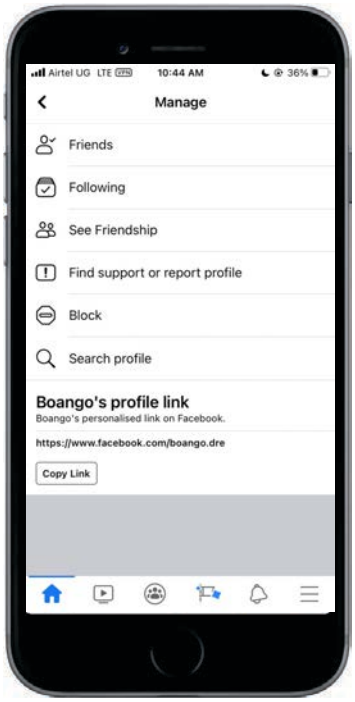
3.3: GENERAL SOCIAL MEDIA SAFETY TIPS

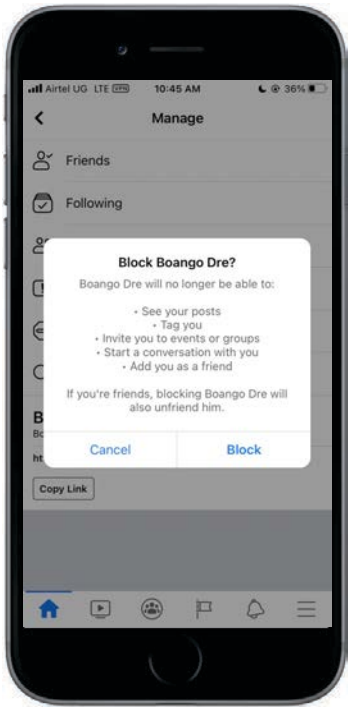
Have you ever been sexually harassed on social media because you are a woman? What did you do? Below are tips on how to boost your safety while on social media.

1. Where possible, create separate work and personal social media accounts. This is to protect you, your family, and your friends.
2. Think carefully about the information that you post on social media and how this could put you and your family at risk.
3. Check the privacy settings of your accounts regularly to ensure that any information you want to be kept private is protected from public view and also to avoid being tagged without your consent.
4. Regularly review comments left on your social media accounts. Pay attention to any particularly hostile or threatening messages as this may help to spot any possible adversaries or disable comments that you don't to be viewed by other family and friends.
5. Speak with friends and family about your social media profile. Inform them if you do not want to be tagged in photos and/or online comments. Set your social media profiles to inform you if you are tagged.
6. Always log out of your social media accounts. This will prevent someone from accessing your information.
7. Use 2FA in addition to a strong password to protect your accounts. See our email guide for further information.

BLOCKING A PERSON OR REPORTING A PROFILE ON FACEBOOK

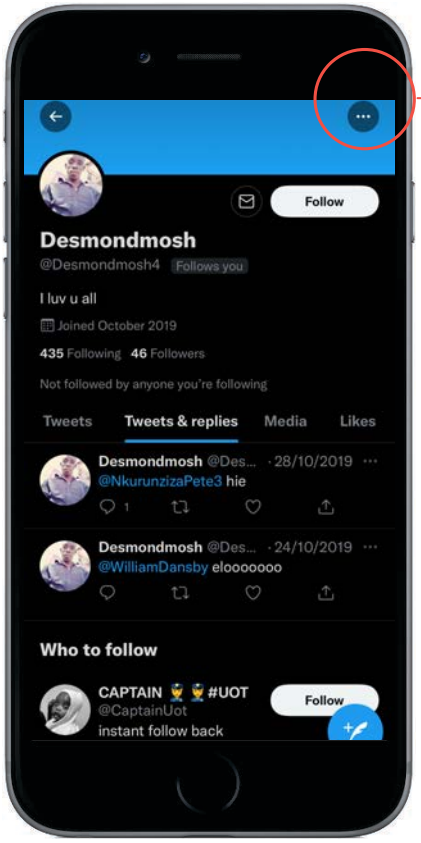


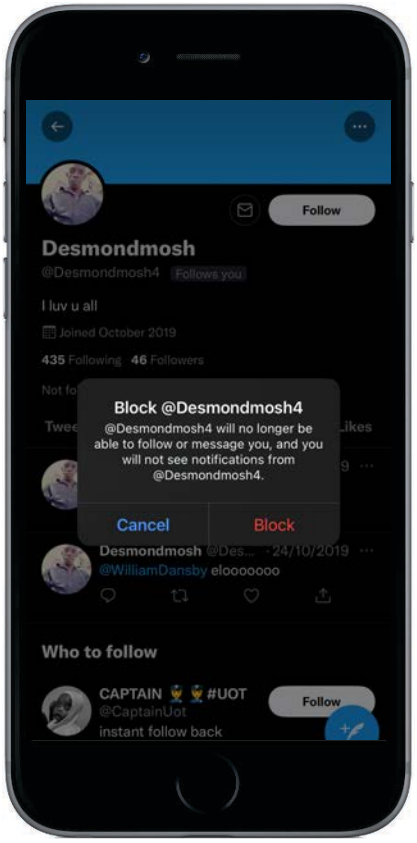




Click the 3-dot menu just below the profile picture. Follow the steps

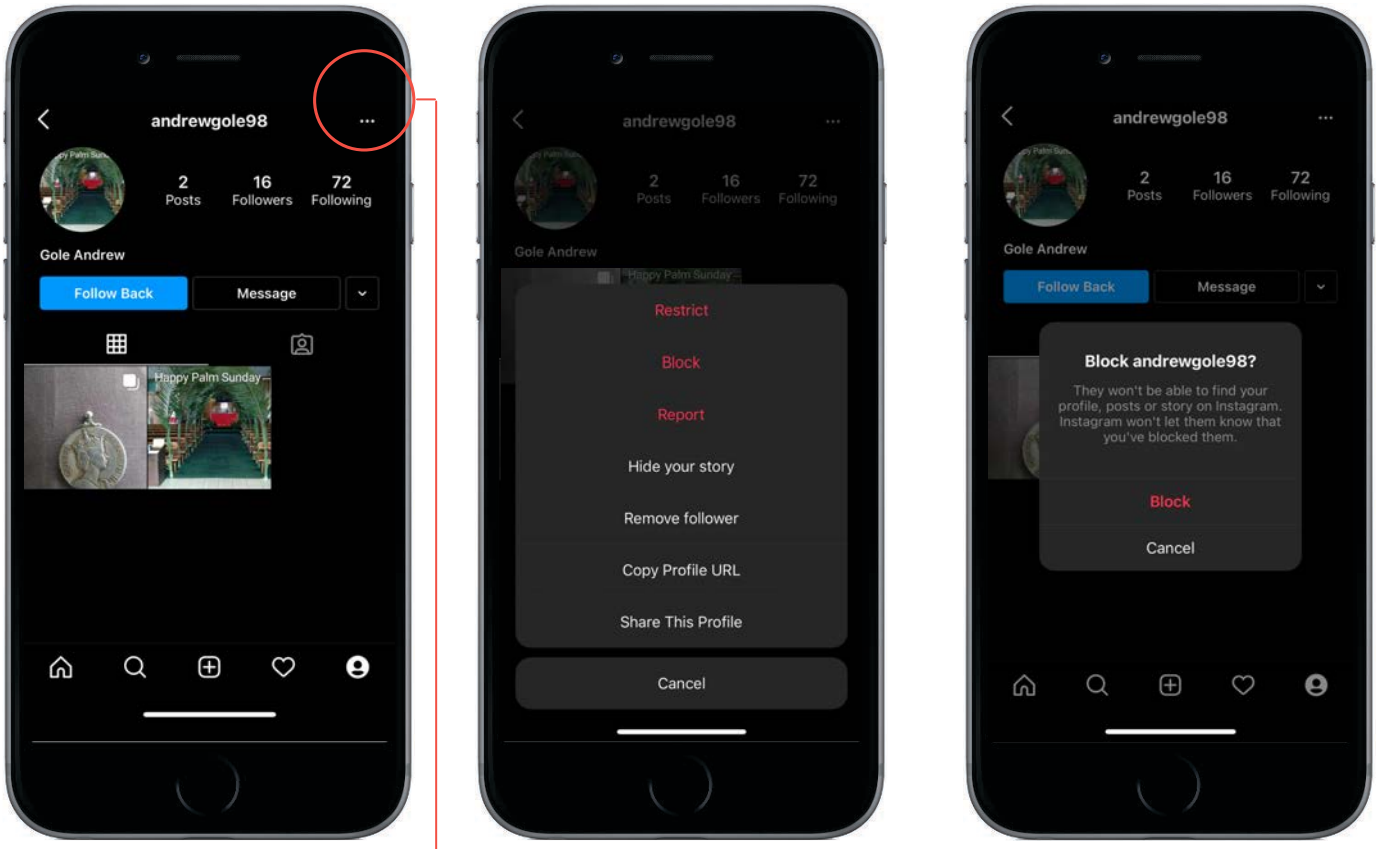
BLOCKING A PERSON OR REPORTING A PROFILE ON TWITTER





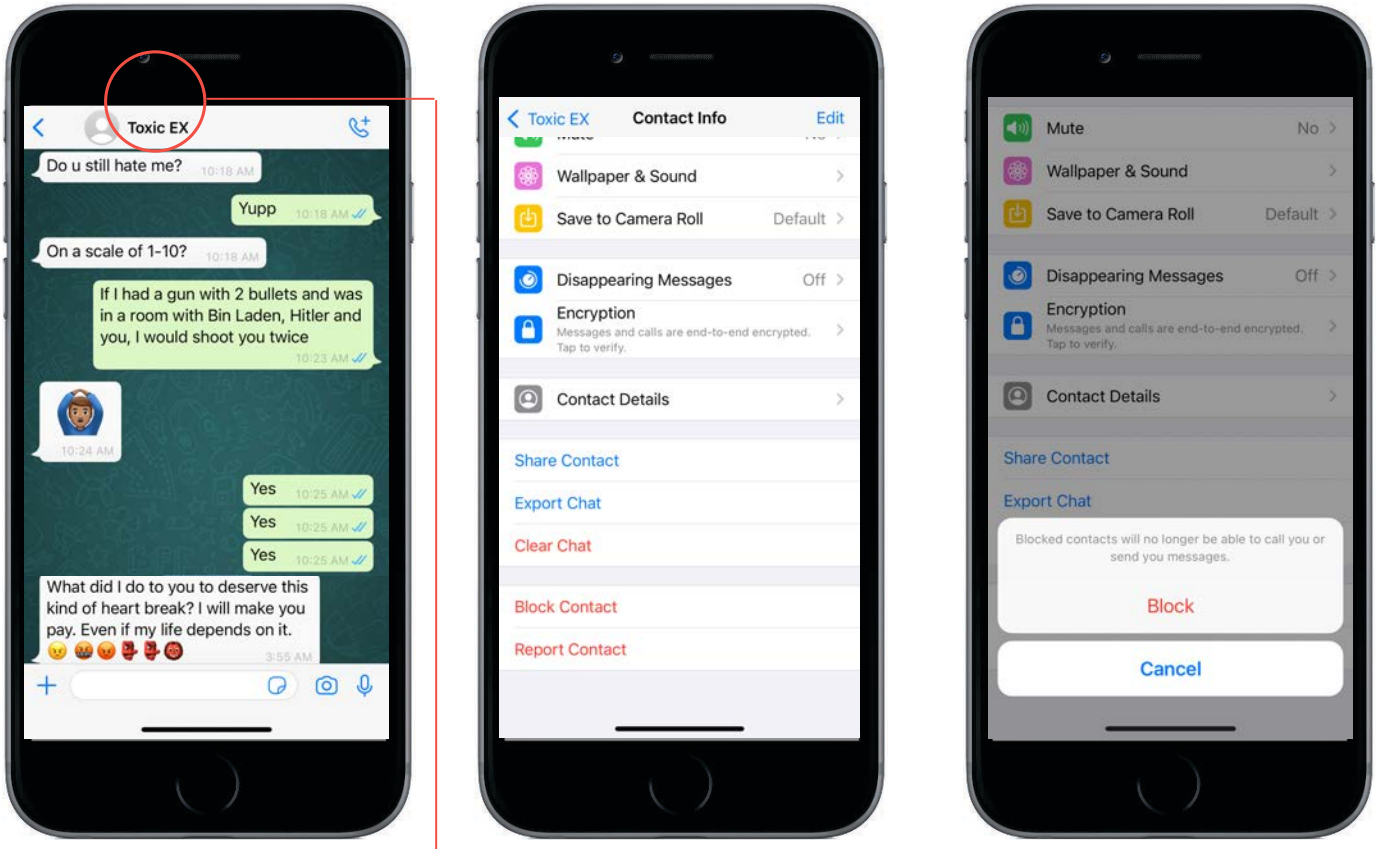
Click the 3-dot menu on the top right of the profile. Follow the steps

BLOCKING A PERSON OR REPORTING A PROFILE ON INSTAGRAM



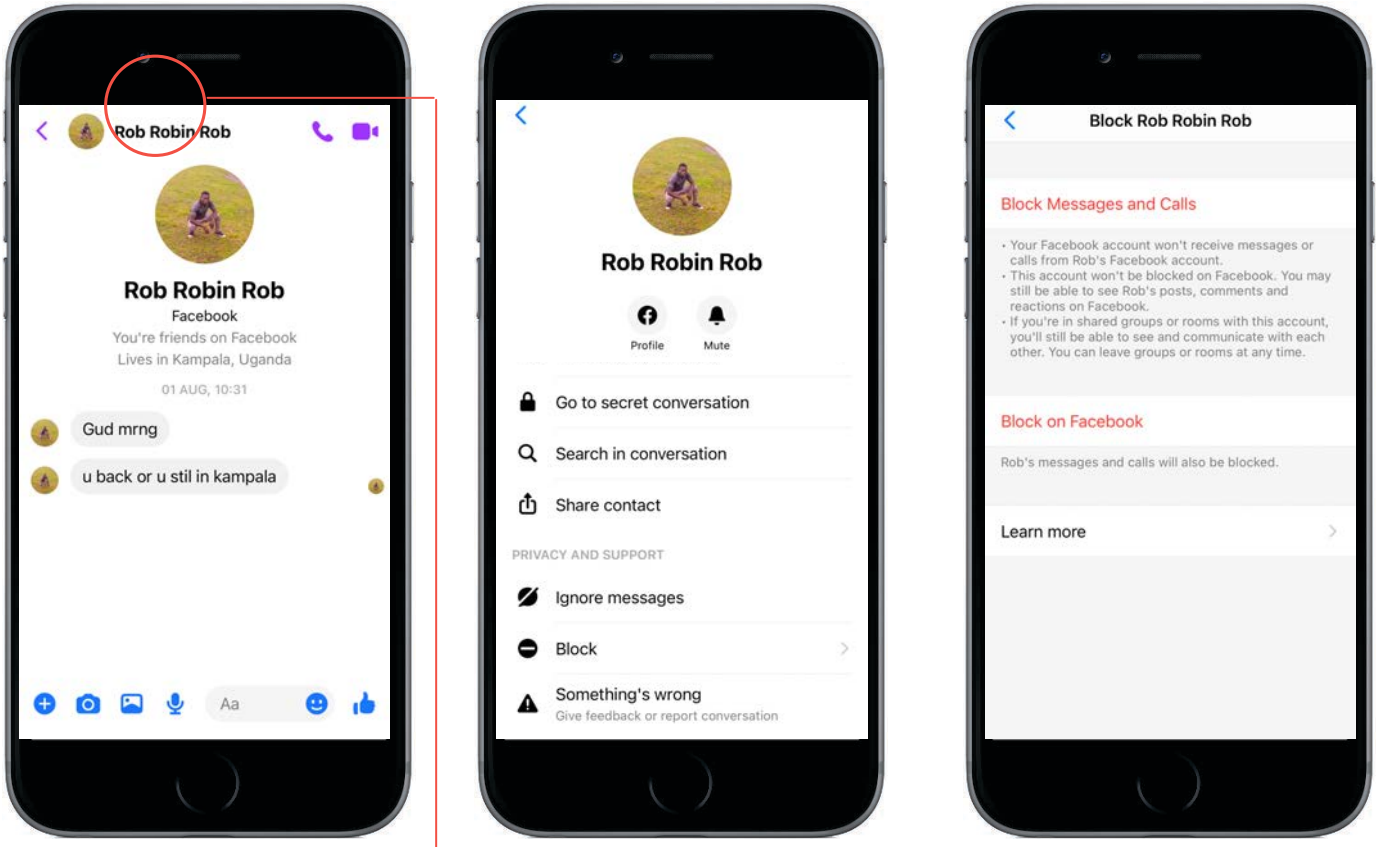
Click the 3-dot menu on the top right of the profile. Follow the steps

BLOCK OR REPORT A PERSON ON WHATSAPP



Click the contacts name at the top of the profile. Follow the steps

BLOCK OR REPORT A PERSON ON FACEBOOK MESSENGER



Click the contacts name at the top of the profile. Follow the steps

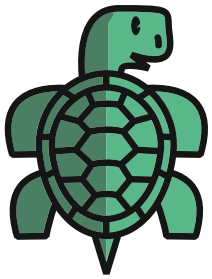
ADDITIONAL RESOURCES ON SOCIAL MEDIA SAFETY FOR WOMEN:

- Resources for Staying Safe on Facebook: https://www.facebook.com/help/122006714548814
- Unfriending or Blocking Someone: https://www.facebook.com/help/1000976436606344
- Twitter Account Security: https://help.twitter.com/en/safety-and-security/account-security-tips
- Community Safety on Instagram: https://about.instagram.com/community/safety
- WhatsApp Safety Tips: https://www.whatsapp.com/safety

SECTION 4: ONLINE COURSES ON DIGITAL SECURITY

There are numerous self-paced online courses that exist on Digital Security. These courses are unique in that they give the learner time to learn at their own pace. They are easy and well structured making it very easy to learn digital security. Below, let us explore some of the courses that exist on Advocacy Assembly and Totem Project.

4.1: ONLINE COURSES ON TOTEM



Developed in collaboration by Greenhost and Free Press Unlimited, Totem is an online learning platform that offers educational courses about digital security and online safety for everyone. Below are some of the Digital Security Courses offered on Totem;

4.1.1: How the Internet Works.

This course teaches you the fundamentals of how the internet works, who owns it, and how you can make informed choices depending on your own privacy and security needs.

Link to the Course:
https://learn.totem-project.org/courses/course-v1:Totem+TP_IP_001+2018/course/

4.1.2: How to Protect your Identity Online

This course aims at helping you adopt effective tools and practical strategies to protect your anonymity and that of your loved ones when using the Internet.

Link to the Course:
https://learn.totem-project.org/courses/course-v1:Totem+TP_IO_EN+001/course/

4.1.3: Know your Trolls

This course is aimed at helping journalists identify who is behind the abuse they are receiving online so that they can better protect themselves online

Link to the Course:
https://learn.totem-project.org/courses/course-v1:IWMF+IWMF_OH_EN+001/course/

4.1.4: Secure your Devices

This course is aimed at helping you understand some of the key threats to your digital devices and explore strategies to help mitigate the risks.

Link to the Course:
https://learn.totem-project.org/courses/course-v1:Totem+TP_SD_EN+001/course/

4.2: ONLINE COURSES ON ADVOCACY ASSEMBLY

Advocacy Assembly is a free learning community for human rights activists and journalists. It's a collaborative space where training organizations from around the world can upload their best training material and reach new audiences. Below are some digital security courses on Advocacy Assembly;

4.2.1: Staying Safe Online and Using Social Media

This course is designed to help journalists and activists prevent themselves from becoming the victim of the most common reasons for digital security breaches.

Link to the Course:
https://advocacyassembly.org/en/courses/32/

4.2.2: Cyber Harassment: Concepts and Prevention

This course covers what cyber harassment is, discusses myths and misconceptions, and provides you with tools to run safer online campaigns

Link to the Course:
https://advocacyassembly.org/en/courses/43/

4.2.3: Recognizing and Responding to Online Gender-Based Violence

This course teaches the different types of online gender-based violence, and shares case studies that show how such violence affects people e.g. women online.

Link to the Course:
https://advocacyassembly.org/en/courses/34/

4.2.4: Secure Passwords and Encryption of Data

This course is aimed at helping you understand how to create secure passwords and use different techniques to encrypt your data.

Link to the Course:
https://advocacyassembly.org/en/courses/31/

4.2.5: Phishing, Malware, and Social Engineering

This course is aimed at helping you identify a phishing email, social engineering attempt, how malware works, and which tools can best protect you.

Link to the Course:
https://advocacyassembly.org/en/courses/30/

SECTION 5: CONDUCTING DIGITAL SECURITY TRAININGS

This section is aimed at digital security trainers and seeks to provide them with the basic information needed to conduct successful digital security training. How a trainer structures their digital security training is vital for the participants because they are the recipients of the training

5.1: CONDUCTING DIGITAL SECURITY TRAINING FOR ADULTS

Digital Security Training is unique because usually they are not designed for everyone. When digital security training is organized, a specific group of people is in mind. In most cases, participants of digital security training are adults and therefore the training is geared towards an adult audience.

5.1.1: What it Means to Teach Digital Security

When we teach adults digital security, we have to ensure at the end of the training it was worth their time. Adults are people who do not have the whole day just to sit and attend training. Usually, they are there not because they have time or need to be there but because they want to learn something new.

Therefore, as trainers;

1. We have a responsibility and duty of care towards the participants.
2. We have to foster different groups and cultures and above all make sure our training is as inclusive as possible and welcoming to all regardless of their age, sexual orientation, or gender identity.
3. We have to encourage further learning when it comes to digital security because it's a constantly evolving field and new threats and challenges come up as technology advances. Also, you can't train participants on everything when it comes to digital security because of many factors like time, financial resources, and the availability of the participants.

5.1.2: The Do's and Don'ts of Teaching Digital Security

As a trainer, when you train adults on digital security, below are some of the things you should and should not do;

THE DO's

- Keep in practical. Make topics as practical as possible so that participants can see how something is done.
- Use real-life examples or case studies that participants can relate to.
- Get to know your participants' digital habits and behaviors, relating the training to those.
- Connect the training sessions to the work that your participants do on a daily basis.
- Encourage participants to ask questions or seek clarity on any of the topics covered

THE DONT'S

- During the training, don't use too much technical jargon and when you do, explain the meaning
- Don't use too many slides during your training. Too many slides make it hard for participants to follow the training.
- Don't take over the participant's mouse when showing them how to do something on their device.
- Don't use too many scare tactics during your training. This can put some participants off.

5.1.3: Understanding ADIDS: An Effective Adult Learning Approach

The operating principle behind the ADIDS approach is that adult learners benefit most from the information presented in stages, and in a variety of formats – i.e., group activities, case studies, slides, and audio-visual presentations, facilitated discussions, group work, hands-on practice, and reflection.

This approach creates a comprehensive learning environment by taking into consideration the needs of kinesthetic learners (who need to do something physically to understand), as well as visual learners (who rely on pictures, diagrams, and video) and auditory learners (who learn through hearing material such as lectures).

Let's briefly look at the five steps under the ADIDS Approach

Activity (easing into the topic):

Each module begins with an Activity that illustrates the material that is to follow. These act as “icebreakers” for new participants and will ease them into thinking about a topic that may be new to them.

Discussion (providing context):

Discussion sessions follow each of the Activity sessions. These sessions are designed to engage participants in a conversation about the topic (and the preceding session).

Input (interacting):

After the two previous steps, the participants will be guided through an effective Input session in which participants are engaged with a range of materials, including case studies, that will facilitate a give-and-take in knowledge sharing between the trainer and the participants.

Deepening (hands-on activities):

This session includes the application of skills, software, and learning to use them. This is possibly the most important session in the training, as this is where participants learn new skills by doing them.

Synthesis (reflection):

Lessons benefit from practice and review, and learning is reinforced by reflecting on the knowledge acquired. In this session, the knowledge and skills that have just been addressed are summarized, with the participants encouraged to ask questions and seek clarification.

According to Malcolm .S. Knowles, **adults learn best when they take responsibility for their own learning.**

These five statements summarize Knowles' theory:

1. Adults need to understand and accept the reason for learning a specific skill.
2. Experience (including error) provides the basis for learning activities.
3. Adults need to be involved in both the planning and evaluation of their learning.
4. Adult learning is problem-centered rather than content-oriented.
5. Most adults are interested in learning what has immediate relevance to their professional and social lives.

ADDITIONAL RESOURCES ON ADULT LEARNING

- https://www.umsl.edu/~henschkej/articles/a_The_%20Modern_Practice_of_Adult_Education.pdf
- https://granite.pressbooks.pub/teachingandlearninginadulthood/chapter/adult-learning-in-the-digital-world/
- https://chrissanders.org/2020/06/toward-applied-andragogy/
- https://komentoolkits.org/wp-content/uploads/2015/03/Introduction-to-Adult-Learning-Principles-B-AA-Comm.pdf
- https://marciaconner.com/resources/adult-learning/

5.2: General Tips for Digital Security Trainers

- Limit your Slides. 7 to 8 slides per presentation should be enough. If you use more than that, it might indicate that you are speaking more than the participants.
- Use your PowerPoint presentation to facilitate a discussion by ending each slide with questions that you want the participants to discuss.
- Be patient. Not everyone will learn to do things at the same speed. Give your participants time to practically do things by themselves.
- During a training, if you sense the energy in the room is low, and the participants are not paying attention, address it and do something about it like taking a quick break.
- During a training, Use graphics more than text. If you really want to use your presentation to address visual and auditory learner needs, use images on your slides coupled with a spoken lecture.
- Use Metaphors, and use them often. Think about the topic you are teaching and try to find practical, common-place analogies that can illustrate the concepts in a clearer way

ADDITIONAL RESOURCES FOR DIGITAL SECURITY TRAINERS

- https://level-up.cc/you-the-trainer/roles-and-responsibilities-of-a-digital-security-trainer/
- https://level-up.cc/you-the-trainer/be-a-better-trainer/
- https://level-up.cc/you-the-trainer/golden-rules-of-effective-training/

APPENDICES

APPENDIX 1: Additional Digital Security Resources for Women

For women to enjoy the full benefits of the internet, they need to adopt the different digital security and safety tips and techniques shared in this guide. Below are additional digital security resources available on the internet;

- Advanced DIY Privacy for Every Woman: https://chayn.gitbook.io/advanced-diy-privacy-for-every-woman/
- Feminist Internet: https://feministinternet.org/
- Tactical Tech's Me and My Shadow: https://myshadow.org/
- Surveillance Self Defense: https://ssd.eff.org/
- Safe Sisters: https://safesisters.net/
- Take Back The Tech: https://takebackthetech.net/
- Securing your Digital Life Like a Normal Person: https://medium.com/@mshelton/securing-your-digital-life-like-a-normal-person-a-hasty-and-incomplete-guide-56437f127425
- Rory Peck Trust Digital Security Guide for freelance journalists: https://rorypecktrust.org/freelance-resources/digital-security/

APPENDIX 2: References

- Simplified Guide on Digital Security Best Practices. https://digitalhumanrightslab.org/resources/simplified-guide-on-digital-security-best-practices/

- Digital Security Training Curriculum. https://digitalhumanrightslab.org/resources/digital-security-training-curriculum/

- Digital Safety Trainers Assistant. https://safesisters.net/wp-content/uploads/2019/09/Digital-Safety-Trainers-Assistant-smaller.pdf

- Modern Practice of Adult Learning. https://www.umsl.edu/~henschkej/articles/a_The_%20Modern_Practice_of_Adult_Education.pdf

- Level-Up Trainer's Curriculum. https://level-up.cc/curriculum/

- Security Education Companion: https://sec.eff.org/

APPENDIX 3: Summary of Training Schedule for the Training of Trainers

No.	Estimated Duration	SESSION/TOPIC
DAY ONE		
1.	15mins	**Welcome/Introductions/Registration**
2.	1hr	**Introduction to Digital Security** • Introduction • Common myths and misconceptions • Important Digital Security Topics for Survivors of Online Gender-based Violence - Digital Literacy - Secure Communication - Password Management - Device Management - Data Protection and Privacy - Risk Assessment **What it means to Teach Digital Security** • We have responsibility and a duty of care • We foster groups and culture • We encourage further learning
3.	**15mins**	**HEALTH BREAK**
4.	1hr:30 mins	**Group Exercise: Do's and Don'ts of Teaching Digital Security** • Groups discuss dos and don'ts using post-its • Presentation from each group • Discussion
END OF DAY ONE		
DAY TWO		
1.	15mins	**Recap of Day One**
2.	1hr	**Understanding the Common Digital Threats faced by Women Online** • Impersonation • Non-consensual Sharing of Intimate Images • Doxing • Cyberstalking • Hacking
3.	**15mins**	**HEALTH BREAK**
4.	1hr:30mins	**Introduction to Adult Learning** **Adult Learning Theory:** **1. How adults learn is different from kids** - Understand and accept reasons for learning - Experience (incl. failure) is a great tool - Involve participants in planning - Need immediate relevance to work/life **2. Different modalities** - Auditory/hearing, Visual/seeing, Kinesthetic/doing **3. Barriers to learning** - Pride, Shame, Priorities, Gender roles, social status, Trauma
END OF DAY TWO		

DAY THREE		
1.	15mins	**Recap of Day Two**
2.	1hr	**Effective Adult Learning Methods** **ADIDS Methodology** - Activity: exercise, game, experiment - Discussion: reflection on the Activity - Input: lesson, lecture - Deepening: hands-on experimentation - Synthesis: reflection on the module
3.	**15mins**	**HEALTH BREAK**
4.	1hr:30mins	**Multi-modal presentation** - Doing, seeing, hearing—find a balanced mix **Personal context considerations** - How you organize and conduct a digital security training depends on the category of participants **Self-generating workshops** - Start with risk assessment exercises - Let results guide content - Great for short trainings with one or two organizations
END OF DAY THREE		
DAY FOUR		
1.	15mins	**Recap of Day Three**
2.	1hr	**GROUP EXERCISE: WHAT'S MY LEARNING STYLE?** **Discuss your individual learning styles** - What has worked for you? - What hasn't worked for you? **How do you like to teach?**
3.	**15mins**	**HEALTH BREAK**
4.	1hr:30mins	**GROUP EXERCISE:** TOP 5 DIGITAL SECURITY TIPS FOR SURVIVORS OF ONLINE GENDER-BASED VIOLENCE - Quick brainstorm - Discuss and rank in groups. - Present ranking to full group and collectively figure out top 5
END OF DAY FOUR		

DAY FIVE		
1.	30mins	**Recap of Day Four**
2.	1hr	**Planning a Digital Security Training** **Guide questions for curriculum design** - What are the learning goals? - What topics will you cover? How are they organized? - Is there an activity to introduce the topic? - How will you debrief? What questions will you ask? - How will you deepen the understanding? - If you're running a hands-on exercise: what are the steps? **Planning details** - Time: what's your participants' availability? - Location: online, near the participants or remote - Logistics: pre-arrange as much as possible - Internet connectivity! Get LTE modems if you need to - Writing materials, post-its, pens, flipcharts, etc. - Power outlets! - Accommodations: any participants with disabilities? Single parents with small children?
3.	**15mins**	**HEALTH BREAK**
4.	1hr:30mins	**GROUP EXERCISE**: ORGANIZE A DIGITAL SECURITY TRAINING FOR SURVIVORS OF ONLINE GENDER-BASED VIOLENCE • Using everything we've learned so far, outline how we'd go about creating this digital security training for survivors of online gender-based violence in Uganda
END OF DAY FIVE		

Plot 360 Kansanga - Gaba Road off at UBA Bank. Sali Road Warade Close
P.O. Box 4411, Kampala (Uganda)
Tel: +256 394823109, +256 414532035
info@wougnet.org
@wougnet1
@wougnet
Women of Uganda Network
https://www.wougnet.org