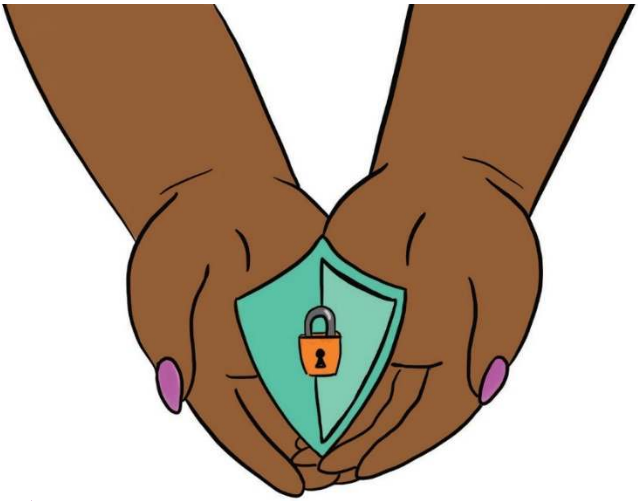
Safe Sisters

A common sense guide to digital safety for women and girls in Sub-Saharan Africa

Download the guide and learn more at **https://safesisters.net**

What is this booklet?

Thank you for picking up our little book! We wrote this booklet to help our sisters learn about problems that we can run into on the internet (like leaked or stolen personal photos, viruses, and scams), how we can make informed decisions every day to protect ourselves, and to help make the internet a safe space for ourselves, our families, and all other women.



Who are we?

This booklet was made possible by the collective effort of Internews, Defend Defenders, and the 2017-2018 Safe Sister fellowship program. Our mission is make digital security less complicated and more relevant to real users and to encourage all women and girls to take online safety into their own hands. We hope this booklet will help readers see that the most effective ways to protect yourself online are common sense strategies we already use offline every day.

A program by:

Internews DEFENDERSTECH
A Project of DefendDefenders

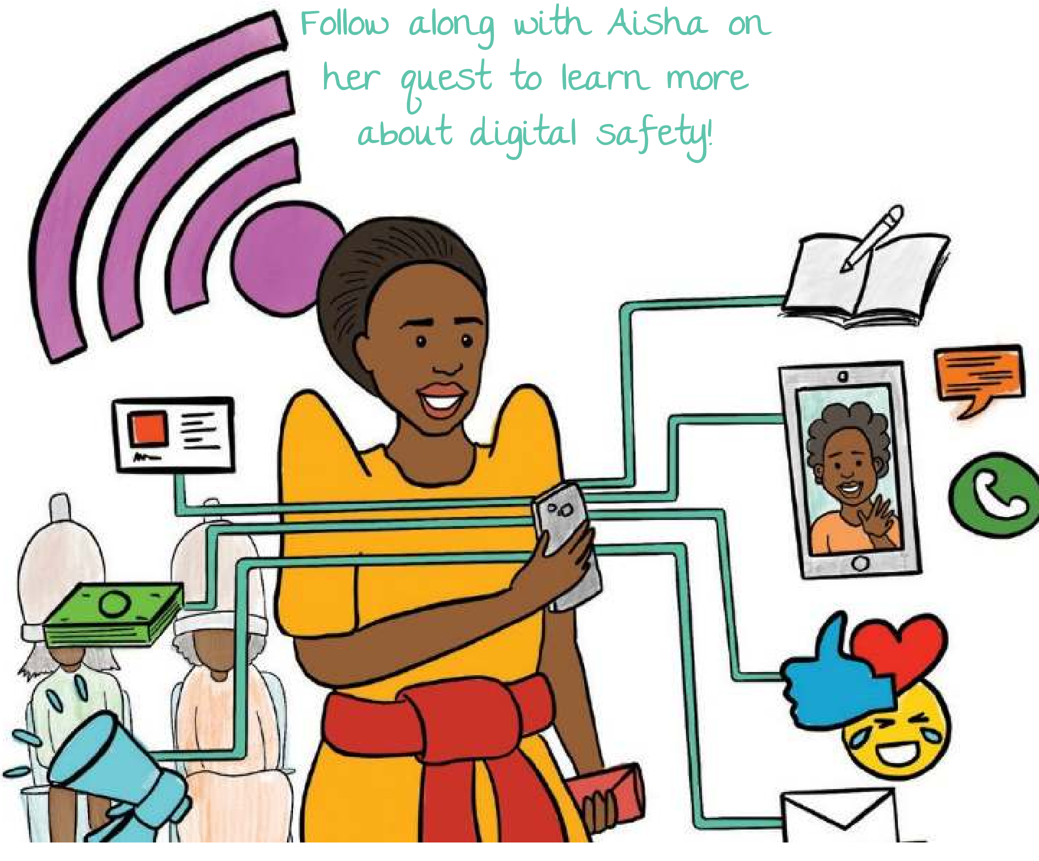
Graphic design and research by: POLLICY

Meet Aisha!

Aisha is a young woman from Kampala, Uganda and for her and her friends, the internet is a part of their lives. They post updates on Facebook, upload photos on Instagram, share thoughts on Twitter, message friends and family on WhatsApp and Messenger, search for things on Google, and send emails for work.

Aisha has a young daughter, Natu, and lives down the road from her mom, dad, and younger sister, Miriam. Aisha has friends who have had their social media accounts hacked, and photos posted of them without their knowledge, and she worries about how safe she and her family are online.

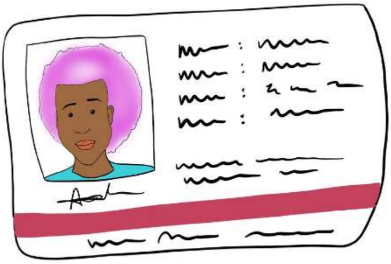
Throughout this booklet Aisha will be asking questions on what happens to her information when she uses the internet and getting ideas on ways that she can be safer online and to teach her daughter and friends how to be safe too.



Follow along with Aisha on her quest to learn more about digital safety!

Aisha Asks...
Can someone hack into my account?

Aisha's cousin, Rachel, had her Facebook account hacked last year, and someone posted things that she didn't write. Rachel contacted Facebook and told them what happened, and they eventually helped her to get back control of her account, but she still didn't know how she got hacked!

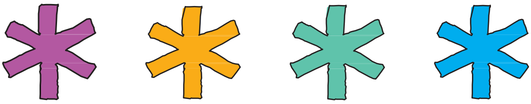


There are many ways that someone could have gotten into Rachel's account. Some of the time its because someone else got her password. Lots of people going around stealing passwords, in fact, this business is booming! Your password is important to hackers because it is the key that unlocks information about you. Why are they succeeding? Well, for one, passwords we use are easily cracked or stolen by computers and used by cybercriminals.

Did you know that **p@ssw0rd** is one of the most commonly used passwords in English?

Consider this:

- A strong password can act as a first line of defense against hackers. Choose it wisely.
- If you're having trouble remembering all of your passwords, try a **password manager**! It will remember all of your passwords for you, so you don't have to, and you only need to remember one thing-- the master password!



Aisha Asks...

How can I make a stronger password?

A little effort can make a huge difference in securing your online accounts from hackers. It is a growing concern that ordinary passwords are not good enough because they are short and easy for a computer to crack quickly. Instead, try a **passphrase**. A passphrase is a kind of password that is made up of a group of words, which when put together, makes sense to their creator and lets them sign into accounts. Passphrases are easy to remember but not easy to crack- even by the most advanced computers.

Aisha's password for Facebook was **`august2013!,`** for the birth month and year of her little sister. That's pretty easy to guess. To make a stronger passphrase, she changed it to **`EyeL1keMyFr1ends&Fam1ly!`** (which to her means, "I like my friends and family!").

Consider this:

- The longer the better! Make your password more than 15 characters, and add symbols, numbers, and uppercase letters, if you can
- Even a very good passphrase isn't always enough. If you want more security for your most important accounts, enable **Two-Factor Authentication (2FA)**. Most of the popular websites (like Facebook, Gmail, Twitter, Instagram) offer 2FA as a more secure way to log in to your accounts. Check it out!
- Whatever you decide to use, remember that passwords and passphrases should not be used for more than one account, because if someone learns that passphrase or password, they can get into many accounts!

Aisha Asks...

What should I post on social media?

If you are like most people, social media is a convenient way to socialize and keep in touch with friends and family. People post and send a lot of information about themselves online, and only find out later that strangers can see their photos and comments. Strangers may be able to find out a lot about you just by looking you up on Facebook.

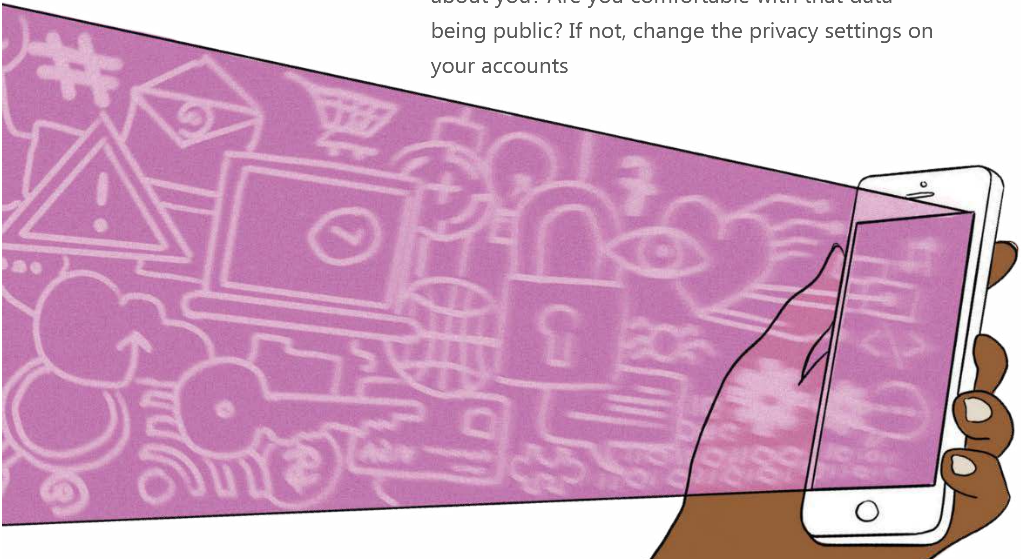
Choose wisely what messages, videos and images you post online. Be careful about what photos your take and what information you send about yourself.

Remember

Nothing online ever really disappears!

Consider this:

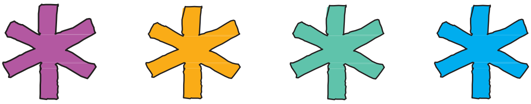
- Do a Google search of your name and check to see how much information about you is available for anyone to look up.
- If your dad went through your social media profile, how much personal information would he find out about you? Are you comfortable with that data being public? If not, change the privacy settings on your accounts



Aisha Asks...

Can someone break into my account without the password?

Do you ever get sent random links from people you don't know? Or perhaps a message congratulating you on winning a prize? Or maybe even a notification telling you that your computer has a virus and you need to download an update right now?



Aside from cracking your password, another way that someone can get into your account without your permission is by sending you a virus (also called **malware**). These viruses are harmful computer programs which can steal information on your computer or your accounts, including your identity and financial information. They become active when you click on a link or download an untrustworthy file that has malware in it.

Consider this:

- Be suspicious! Pay attention to email attachments and links sent to you by people you don't know. Look closely at the sender's information, if it looks weird, don't click on it.
- If you get a notification that your phone or computer has a virus and you need to download an update, be careful, it may not be real. Look at it closely- does it look real? If you're not sure, type the alert message into Google and see if someone else has reported it.
- Don't ignore those messages to update your software. Software updates are important because they contain new features and security updates that protect your computer from viruses! If you are concerned, go directly to the software's website and download it from there.

Aisha Asks...
Is someone watching what I do online?

It's very common to feel that you are being watched online! That doesn't mean that someone is looking at a video of you at all times, though! Most of the time when you use the internet you leave behind digital footprints, or places of information that we collected by our phones, websites we visit, and apps we use. Things like what we like (or dislike), names of friends and families, where you go to school, our political views, and sometimes even what you had for dinner last week!

The major websites that we use every day are owned by businesses who make money by collecting this information and selling it to advertisers. There is a high chance that your digital footprints are being collected right now by these companies, but there are ways to improve your privacy so that you leave less data behind online.

Consider this:

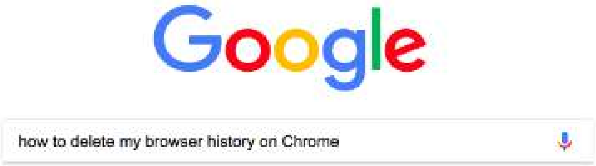
- When an app is free, how does its developer make money from it? Most often, it's through collecting and selling your data to advertisers.
- Review your privacy settings for the social media sites you use, they change all the time.
- Go through your app permissions on your phone and see what your apps have access to. Pay attention to apps that have access to things like your contacts list, your microphone, or your location, and change the app permissions if you want.

Aisha Asks...

What do I do if I share devices with others?

If you use a shared computer, at work, home, or a cybercafe, it is pretty easy for the other people who use it to go through anything that you have on the computer, including look at the websites that you've visited, read your private messages or emails, look at your photos, or even post videos or updates from your accounts.

The best way to ensure that people don't get access to your stuff is to delete your browser history before you leave your computer, sign out of any of your accounts (like your email or social media), and log out of your computer session (if possible). If you're worried about people reading your private documents or seeing your photos, don't download them on the computer, but instead keep them in storage in the cloud (like on Google Drive, or Dropbox), but make sure you sign out before you leave.



how to delete my browser history on Chrome

Even if your computer or phone is shared by other members of your family, it is always important to have a password or number lock (sometimes called PIN code) on it that you can share with them. This helps too if your device is stolen, so the thief doesn't have access to your sensitive information and photos.

Consider this:

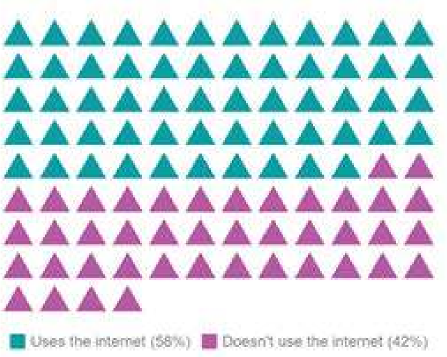
- If you share a computer with someone you don't trust, they may have installed software on it that will track what you do. This software is often called **spyware**. If you suspect that you are using a computer with spyware on it, be careful about what you do on it.
- If someone you know wants to go through your phone to read your private messages, make sure that you delete risky conversations that could be dangerous to have.

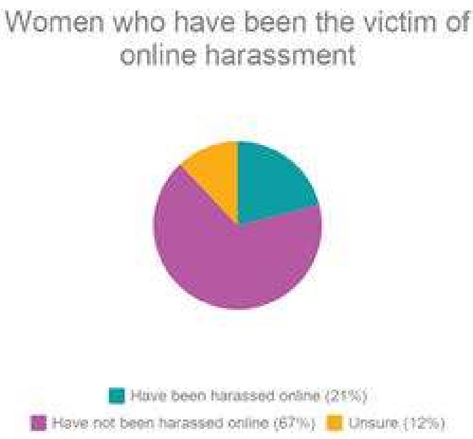
Digital safety by the numbers

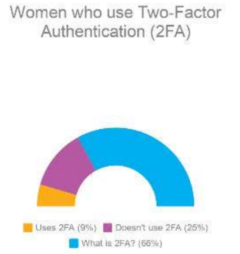
If you think you are the only one who hasn't had much experience with digital safety knowledge, you are not alone!

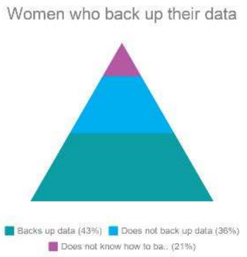
To help tailor this guide, we conducted a survey of 300 women in Kampala, Uganda in February 2018 on their digital safety habits and found the following:

Female internet users in Kampala who use smartphones to access the internet









Aisha's To Do List

Now that Aisha is interested in making changes to improve her digital safety, let's see what she intends to put into practice with her to do list!

1 Make better passwords
Make it fun by creating a strong passphrase from my favorite song lyrics, and add in combination of special characters, numbers and capital letters! Don't use the same password for multiple accounts.

2 Think before you click
Starting right now don't click on suspicious looking links and attachments. Be skeptical of strange emails from people you don't know by paying attention to the sender's info and the contents of the email.

3 Always log off
Review your security settings on your phone and computer, add a password to get into your devices, and always sign out of the account when you leave a shared computer or phone.

4 Be careful with what you post online
It is almost impossible to remove an image or text once you post it on the internet, so think carefully about what you share on social media before you post. Go through your privacy settings on the social media apps and sites, and limit permissions (location, microphone, contacts) and who sees your stuff.

5 Be your sisters' keeper
Photos leaked online bring suffering to a lot of women. Look out for fellow sisters and don't forward inappropriate content on the internet. Delete and report people who use their accounts as a platform for online bullying and violence against women.

Remember: You can do it!

Dedicate time to learn about what being safe online means, and practice caution when using the internet. Your best asset may be the ability to notice strange things and identify problems before they spread to others!