Digital Safety Handbook for Women

siasa PLACE
We the people..inventing the future

DW Akademie

german cooperation
DEUTSCHE ZUSAMMENARBEIT

Table of contents

Foreword

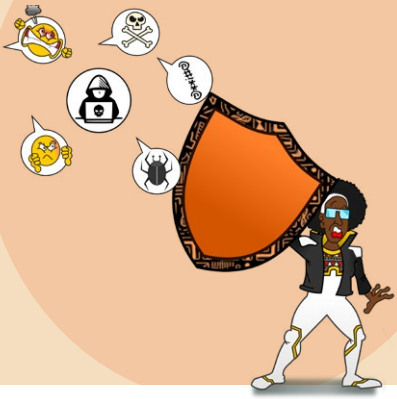
Siasa Place is a non-governmental organization based in Kenya that focuses on engaging young people who normally shy away from politics. We recognize the importance of their participation not just in electoral processes but in accountable governance as well.

We are also part of the Women@Web regional network, a project initiated by DW Akademie in 2017 that aims to enhance women's rights and help them move more skillfully and securely in the digital sphere. DW Akademie is Deutsche Welle's center for international media development and carries out projects that strengthen the human right to freedom of opinion and promote free access to information.

The Women@Web network includes civil society organizations and individual advocates in Kenya, Rwanda, Tanzania and Uganda. The network holds regular training sessions for women in all four countries and has developed modules on topics such as digital rights, digital resilience, digital storytelling and digital security. Women@Web also organizes peer-to-peer meetings, raises awareness of issues facing women online, and works toward legislation promoting women's digital safety.

A survey among more than 200 women attending Women@Web workshops showed that 60% had experienced online harassment, that 90% believed women need more digital training, and that more than 90% believed women are particularly vulnerable online.

This handbook is a tool to help other women who are active in the digital sphere. We are convinced that it is only when women can navigate the Internet securely that we will all be able to take advantage of the myriad of opportunities it offers and make an impact in our fields of expertise.



10 Golden Rules of Digital Safety

1 Limit the personal information shared online

Social media runs a significant portion of people's social lives. We use it to connect with far-flung friends and family, send quick messages to co-workers, and announce major (and minor) events in our lives. Many businesses use social media sites to collaborate or share information—for instance, you might discuss a project with co-workers via a Facebook messaging session or plan a conference on a LinkedIn forum.

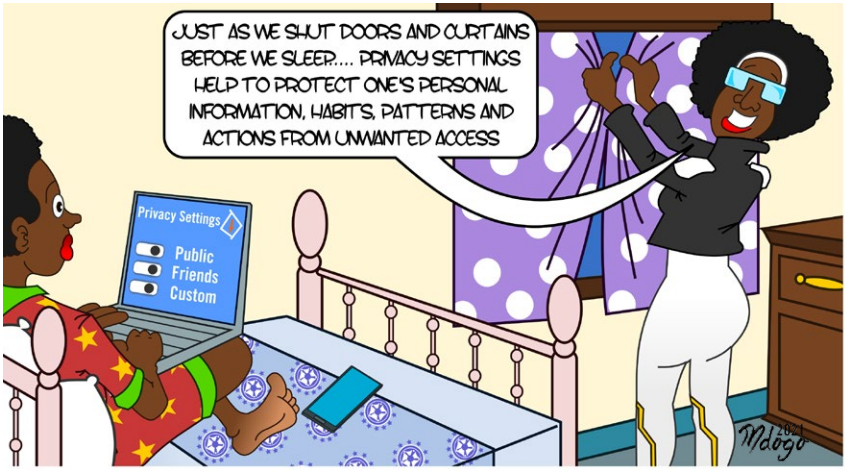
Avoid sharing personal numbers like ID numbers, account numbers, passwords, as well as specific information about yourself like your address on public platforms. Facebook gives you the option to fill in a great deal of information about yourself, from your date of birth to

where you went to high school. Just because these fields are offered, however, doesn't mean you must fill them out. Consider offering a general version of the information requested or simply leaving the field blank. For instance, listing only your county of residence, instead of both city and town, can make it harder for others to figure out exactly where you live.

Clean up your personal information. Have you ever given your phone to a friend or a relative to send a message or make a call? You might not have thought about it then, but you gave them direct access to your browser history and chat history from your messaging apps.

To avoid other people putting their nose into your private life, regularly erase your call and message histories. If there are conversations you would like to keep, just archive and encrypt them. You will keep them forever for your eyes only!

2 Turn on your privacy settings



All social media sites give you the option to limit post viewing to specific audiences. Take the time to explore these settings, try different options, and become a master of their use. For instance, Facebook,

Twitter and Instagram let you create custom lists of people who are allowed to view specific posts.

As you get better at using the privacy settings, bear in mind that not all privacy settings "translate" between websites. For instance, some Facebook users have reported that photographs they set to "private" on Facebook were still indexed publicly in Google Image Search—and could be found by searching for their names. If you don't want it found publicly, don't post it!

3 Practice safe browsing

Safe browsing is a combination of various activities to safeguard your online presence. This can be done by limiting the information you share online, using secure networks to access the internet and using tools like DuckDuckGo and TOR to surf the internet.

Make use of VPN (virtual private networks) to safeguard your connection. You wouldn't choose to walk through a dangerous neighbourhood—don't visit dangerous neighbourhoods online. A VPN creates a secure connection between you and the internet. When you connect to the internet through a VPN, all your data traffic is sent

through an encrypted virtual tunnel. There are various VPN apps such as Surfshark and IPVanish VPN which allow you to connect with various devices. A VPN allows you to have more online security, privacy, browse the internet with more freedom and make public WI-FI safer.

In order to deactivate tracking from websites use the following steps:

- **Chrome** > Settings > Show Advanced Settings > > Privacy > Send "Do Not Track" request with your browser traffic
- **Firefox** > Options > Privacy > Manage your "Do Not Track" settings
- **Safari** > Menu > Preferences > Privacy > Website tracking > Ask websites not to track me
- **Explorer** > Tools (Alt + X) > Safety > Turn on tracking protection > Enable

Cybercriminals use sensationalist content as bait. They know people are sometimes tempted by such content and may let their guard down when searching for it. The internet is filled with hard-to-see pitfalls, where one careless click could expose personal data or infect your device with malware. By resisting the urge, you reduce the risk of exposure to malware.

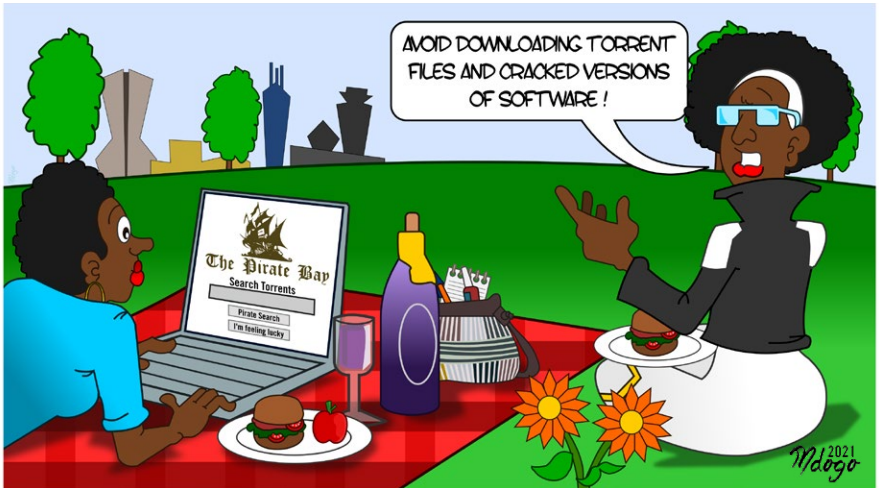
If you're using a public computer, make it a ritual to log out—but log out of private devices from time to time as well. Logging out helps ensure that other people won't "commandeer" your social media profile and use it to attack your friends, change your personal information, post embarrassing or slanderous comments, or worse, change your password and lock you out of your own account entirely.

While surfing the web, you are unknowingly sharing information. Websites use trackers and cookies to learn where you are located, what other websites you visited, what products you bought, and what keyword searches you made. You can change that by using browser extensions to block tracking cookies. You can turn off cookies on the browser settings. Also, where that may not be possible, only enable necessary cookies when asked for such permissions. DO NOT be quick to click the "I Agree" button without reviewing what you have agreed to as you could expose yourself.

DID YOU KNOW

While in private mode or Incognito mode, none of your browsing history is permanently stored on your computer. However, this **does not mean you are anonymous on the internet.** Each page you visit still recognizes your IP address. If someone has the ability to view your IP address history for legal purposes, an ISP (Internet Service Provider), website or even a search engine server log could be used to track you.

4 Be careful what you download



Avoid downloading torrent files especially if you cannot confirm its source. Avoid using cracked versions of apps and software. A top goal of cybercriminals is to trick you into downloading malware—programs or apps that carry malware or try to steal information. This malware can be disguised as an app: anything from a popular game to something that checks traffic or the weather. As PCWorld advises, don't download apps that look suspicious or come from a site you don't trust.

5 Choose strong passwords

A strong password uses a combination of words, numbers, upper- and lowercase letters, and special characters that is easy for you to remember, but tough for other people to guess. Skip common password elements like birthdates, anniversaries, and the names of your children or pets. Keep passwords private by memorizing them—and never write them on the device itself. The longer your password, the harder it is for a computer or person to hack. Insert symbols, letters, numbers and capital case characters in between to solidify the strength of the password. Then again, don't make life so difficult for yourself that you can never remember your passwords.

Passwords are one of the biggest weak spots in the whole Internet security structure, but there's currently no way around them. And the problem with passwords is that people tend to choose easy ones to remember (such as "password" and "123456"), which are also easy for cyber thieves to guess. Select strong passwords that are harder for cybercriminals to demystify. Password manager software can help you to manage multiple passwords so that you don't forget them. A strong password is one that is unique and complex—at least 15 characters long, mixing letters, numbers and special characters.

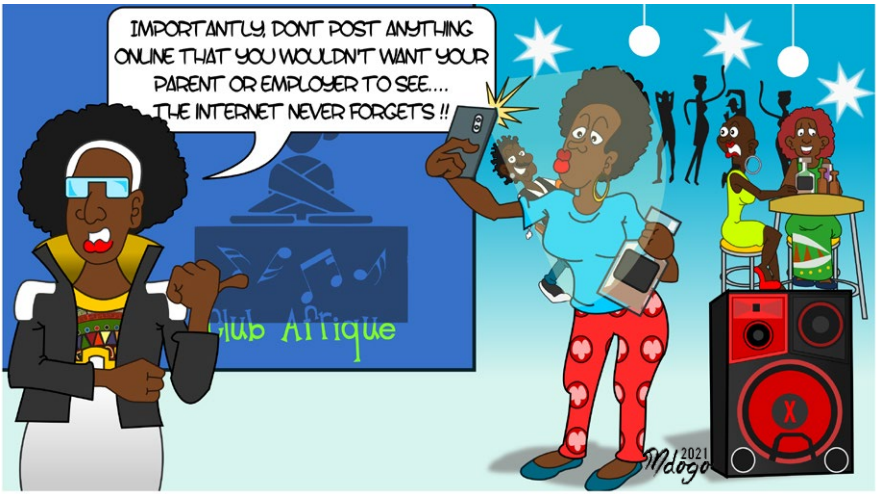
6 Make online purchases from secure sites

Opt for payment on delivery when purchasing items. If a purchase has to be made, make sure it's from a secure site to avoid sharing your card information with mirror sites.

If you must transact online, get a pre-loaded card which is loaded with the amount you wish to transact. Any time you make a purchase online, you need to provide credit card or bank account information—just what cybercriminals are most eager to get their hands on. Only supply this information to sites that provide secure, encrypted connections.

7 Be careful what you post online

The internet never forgets and some have lost job opportunities due to their timeline posts. The Internet does not have a delete key. Any comment or image you post online may stay online forever because removing the original (say, from Twitter) does not remove any copies that other people made. There is no way for you to "take back" a remark you wish you hadn't made, or get rid of that embarrassing selfie you took at a party. Don't put anything online that you wouldn't want your mom or a prospective employer to see.



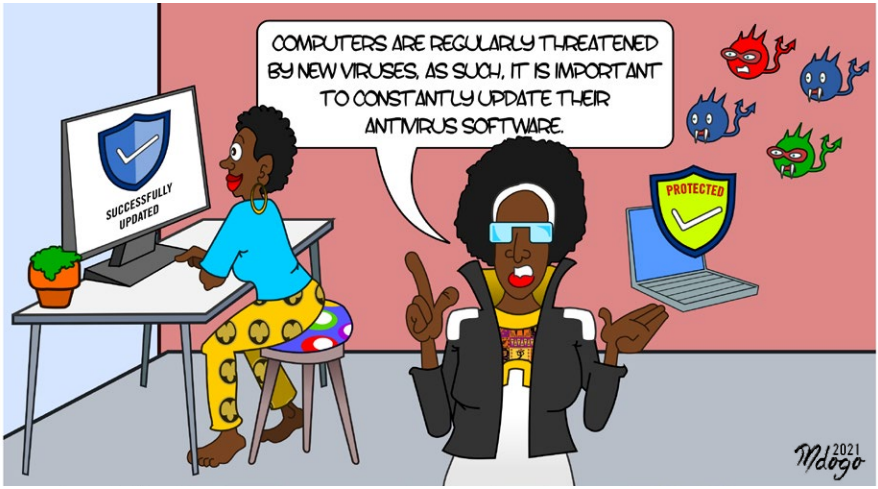
8 Be careful who you meet online

Vet the people on online dating sites like Tinder. People you meet online are not always who they claim to be. Indeed, they may not even be real.

As InfoWorld reports, fake social media profiles are a popular way for hackers to cozy up to unwary Web users and pick their cyber pockets. Be as cautious and sensible in your online social life as you are in your in-person social life.

Today, smart social media users know that the more people you're connected to, the harder it is to control what happens to the information you post. Be careful about befriending people you don't know in real life. Don't hesitate to use the "block" feature when the situation seems to call for it.

9 Keeping your antivirus and operating systems up to date



Antivirus software works best when they are up-to-date. Internet security software cannot protect against every threat, but it will detect and remove most malware—though you should make sure it's up to date. Be sure to stay current with your operating system's updates and updates to applications you use. They provide a vital layer of security.

10 Make use of a password manager

Most antivirus software come with a password manager as part of the package such as McAfee or Kaspersky among others. They allow you to manage your passwords and directly login to accounts with complex passwords. Password managers allow you to create and remember strong passwords.

Self-Care

Digital safety is not complete without including self care. Self-care is the practice of consciously doing things that preserve or improve your mental or physical health.

When people talk about self-care they are generally talking about the conscious and deliberate choice to do something that enhances your well-being. Self-care covers the mental and physical aspects, and is a regime that improves the way you feel in body and mind.

Self-care is an important part of living a healthy and happy lifestyle. Looking after yourself both mentally and physically is crucial to taking control of your health. We lead increasingly busy lives and it can be easy to forget to put yourself first, especially if you have multiple responsibilities and other people to care for.

Self-Care Tips

1 Take a break

Social media is a tool we use to communicate and sometimes your message fails, at times your message is misunderstood, and there will be times when you don't understand others. Do not take social media validation as a sign of your value, worth or contribution to society.

If you've realized that spending time on any social media platform makes you feel tired or irritable, consider taking a break. It can be liberating to eliminate unnecessary stresses from your life. This is especially true if your feed is filled with posts about police shootings, sexual assault cases or other emotionally demanding topics. Don't feel bad about taking care of yourself. It's ok to take a step back. If you're spending more time online and less time hanging out with friends or family or doing other activities, it may also be time to take a break.

Check out online tools that can help you track your social media usage, some will even allow you to limit the amount of time you spend on different apps such as Offtime, Moment and Breakfree App.

2 Find balance by limiting consumption

We find ourselves constantly checking our phone, reading the paper and refreshing our feeds, and this turns us into media addicts. Try to use social media to learn and not just to mindlessly entertain yourself. Look at social media alternatives as well: Read books, listen to a podcast, go for a walk, have conversations, check in on local news regularly and have broad interests.

3 Be mindful

As you're looking through social media feeds, take a second to check in with yourself. Do you feel happy and energized? Or tried and preoccupied? Why do you feel this way? Are certain people's posts stressing you out? Is this how you want to be spending your time at this moment? Adjust your social media habits to fit your needs. Your mental health takes priority. Make use of the block, unfollow and unfriend buttons.

4 Prioritize your creative output

Generating new and creative ideas often requires psychological distance, i.e. the ability to think abstractly and about the bigger picture. If you're constantly consuming information, without taking time to process or analyze, you'll likely spiral into confusion and disorientation. By giving yourself the space to create, you may need to limit the amount of input you receive. Remind yourself that this is normal and feel comfortable turning sources of inspiration off.

Overall, everyone has a unique way of incorporating self care towards their online routine. It is important to add selfcare to the routine that is positive to both your physical and mental health.

Acknowledgements

We thank

- DW Akademie for their support in making the Women@Web program a success
- Mrs. Mutitu Munene for her input in the digital safety training at the Women@Web masterclass webinar 2021 and for compiling the ten golden rules to digital safety for women
- Dr. Frida Kameti for input on the mental and psycho-social support training at the Women@Web masterclass webinar and input on the self-care section
- Bwana Mdogo for creating the illustrations in this handbook

Links and Resources

Norton Life Lock Employee (2021).How to keep your personal information safe on social media.Norton. https://nr.tn/3b59buB

Bradley, T. (2011, November 14). Five timpe to avoid malware in mobile apps. PC World. https://bit.ly/2RvP95b

Chayn. (2019). How to protect your browser. Basic DIY Online Privacy. https://bit.ly/3vMv4H0

Chayn. (2019). Social media and devices. Basic DIY Online Privacy. https://bit.ly/3elsbqA

Hervey, JC. (2018, March 21). Nine self care tips. Forbes. https://bit.ly/3th2ziQ

Mount Sinai. (2018, April 11.) 6 ways to practise self care on social media. Mount Sinai. https://bit.ly/33guBR9

Amnesty International. (2018, March.) Online violence against women. Amnesty. https://bit.ly/3xlDHcQ

Contacts

SIASA PLACE

Development House, 8th Floor
Moi Avenue, Nairobi
@SiasaPlace
Siasa Place
support@siasaplace.com
www.siasaplace.com

DW AKADEMIE

DWAkademie
@dw_akademie
dw.com/newsletter-registration
dw.com/mediadev
dw-akademie.com