AMWIK
ASSOCIATION OF MEDIA WOMEN IN KENYA
Committed to Enhancing the Status of Women in Kenya and Africa

DW Akademie

german cooperation
DEUTSCHE ZUSAMMENARBEIT

Handbook on
Digital Safety & Security

A publication of the Association of Media Women in Kenya (AMWIK)

December, 2021

Handbook on Digital Safety and Security
© The Association of Media Women in Kenya,
December, 2021

TABLE OF CONTENTS

1.0 INTRODUCTION ---------- 5

2.0 SHORT GLOSSARY OF TERMS ---------- 6

3.0 DIGITAL RISK ASSESSMENT ---------- 9

4.0 ASSESSING YOUR DIGITAL FOOTPRINT---------- 10

5.0 HOW VIOLENCE AGAINST FEMALE JOURNALISTS MANIFESTS ONLINE, AND MITIGATION STRATEGIES -----12

6.0 BEST PRACTICES: KEEPING ONLINE SPACES SAFE --- 19

7.0 PSYCHOSOCIAL SUPPORT ---------- 30

8.0 LEGAL FRAMEWORK ---------- 35

9.0 ABOUT AMWIK ---------- 38

ACKNOWLEDGEMENTS

This handbook has been produced by The Association of Media Women in Kenya (AMWIK), with financial support from Deutsche Well Akademie in partnership with the German Cooperation (GIZ).

Special thanks to the developer Lourdes Walusala, Editor Lorna Sempele and Graphics/Inforgraphics designer Joe Ngari.

Thank you AMWIK staff, led by Executive Director Judie Kaberia, for your relentless efforts in ensuring all information in the booklet is accurate and appealing to readers.

EXECUTIVE SUMMARY

The Internet has opened avenues of communication for journalists with different ways of utilizing them. These avenues can be used for news dissemination and online interaction with audiences and sources. Unfortunately, the Internet is now being used for online harassment, and it became worse when the COVID 19 Pandemic plunged the world into a new normal, which drove people, including journalists, in all countries, to explore news models of interaction.

Many women and girls ventured into the digital world for business or work, completely unaware of the dangers that loomed regarding working and communicating majorly online. Most are now shying away due to experiencing online violence. A large proportion of media practitioners also lack digital skills, and especially women journalists.

This handbook is a response to the various research recommendations, and it is focused on journalism, the protection of freedom of expression, and how women journalists, both novice and experienced, can be digitally savvy and safe. This handbook includes frequently asked questions and it will serve as a sustainability measure of sensitizing the public on online harassment.

1.0 INTRODUCTION

According to the Communications Authority of Kenya (CAK), Internet subscriptions in Kenya between April and June 2021 stand at 46.7 million. These figures show that online platforms have become popular and available, transforming how people communicate and share information.

The COVID Pandemic has made journalists dependent on digital communications services and social media channels. Unfortunately, as dependence on digital communication increases, so do online violence patterns and frequency, especially against female journalists and content creators.

Online attacks have real-time consequences for you as a journalist or as a content creator, as well as for your colleagues and sources. Therefore, failing to protect yourself and your information from growing online threats could mean putting yourself and others at risk of harm.

This handbook will equip you with the requisite skills for digital safety and protection management while in the line of duty.

2.0 SHORT GLOSSARY OF TERMS

A detailed Glossary of Terms can be found at https://cyberbullying.org/social-media-cyberbullying-online-safety-glossary.pdf developed by Sameer Hinduja, Ph.D. and Justin W. Patchin, Ph.D., for the Cyber Bullying Research Centre, however, we have also endeavoured to develop a short glossary of terms that are normally used in discourses about digital safety and security, and these are enumerated herebelow:

Algorithms: A set of computations that use data as their main ingredient and transform these data (input) into desired outputs.

Browser: A program that lets you find, see, and hear material on web pages. Popular browsers include Mozilla Firefox, and Google Chrome, Safari.

Cache: A unique high-speed storage mechanism. It can be either a reserved section of main memory or an independent high-speed storage device.

Ciphertext: The encrypted form of a sent message.

Cookie: A piece of information about your visit to a website that some websites record automatically on your computer. By using a cookie, a website operator can determine a lot of information about you.

Cybercrime: A form of Internet-related illegal activity.

Cybersecurity: A technique or software used to protect computers and prevent online crime.

Data Mining: A technique that analyses existing information and

pursues new business avenues.

Decryption: The process of transforming an encrypted message into its original plaintext.

Deep fake: Using a form of artificial intelligence called deep learning to make manufactured images, audio, and video that appears natural. These images, audio, and video mimic speech or facial expressions to make it appear as if someone has said or done something they have not.

Denial of Service: The act of preventing authorised access to a system resource or delaying system operations and functions.

Digital Footprint: A trail of the activities that cyberspace users leave behind, for example, website visits.

Digital Security: Refers to tools and tactics we can use to protect our digital data and devices from anyone or anything that might want to harm or hurt us.

Domain Name: The name that locates an organisation or other entity on the Internet.

Encryption: The transformation of data into a form that hides its original meaning to prevent it from being known or used.

Filtering: Blocking certain types of content from being displayed. Some of the things you can screen for include obscene language, nudity and violence.

Firewall: A security system used to block hackers, viruses, and other malicious threats to your computer.

Internet Service Provider (ISP): Any company that can connect you directly to the Internet.

Malware: Malicious software that includes any harmful code designed to damage the computer or collect information.

Netiquette: Rules for interacting respectfully with others online.

Parental controls: Specific features or software that allow parents to manage children's online activities.

Password: A secret word or number that must be used to access an online service.

Password Cracking: The process of attempting to guess passwords.

Password Sniffing: Passive wiretapping, usually on a local area network, to gain knowledge of passwords.

Phishing: A popular form of social engineering where a hacker sends you a professionally designed email pretending to be a website or service, including a website link for you to follow. When you click the link, it will take you to a seemingly legitimate website that asks for your password, ATM pin, or other information. But in reality, the website is a fake that collects the private data you mistakenly hand over.

Search engine: An Internet service that helps you search for information on the web.

Sexting: Creating and exchanging provocative messages and sexual images using a cell phone or computer with a built-in digital camera and text messaging capabilities.

Social Engineering: Involves psychological manipulation of targets to reveal sensitive information. The common case is when the perpetrator contacts you and pretends to be a representative of a company or service.

Spam: Unsolicited email or junk mail.

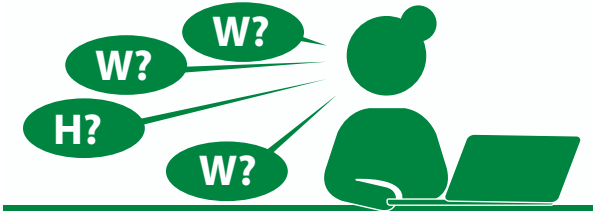
Spoof: Attempt by an unauthorised entity to access a system by posing as an authorised user.

URL (Uniform Resource Locator): The unique address of a site on the Internet.

VPN (Virtual Private Network): An internet security service that allows users to access the Internet as if they were connected to a private network.

Virus: A kind of malicious computer program, which when executed, replicates itself and inserts its own code. When the replication is done, this code infects the other files and program present on the computer system. These various types of computer viruses can infect a device in different ways.

3.0 DIGITAL RISK ASSESSMENT



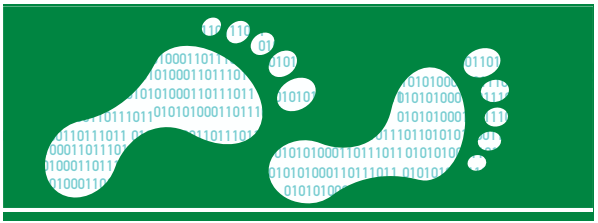
In this era of nonstop privacy breaches, getting a handle on one's digital security matters more than ever. It is therefore paramount to understand digital risks. In addition, some safety risks have been moved from the offline world to the online world. For example, death threats in response to web-based content, or audio and visual broadcast content, are now emailed or sent via social media handles...

It is crucial for you to ask yourself the following questions when embarking on online interaction:

i. What do you want to protect?
ii. Who do you want to protect it from?
iii. How will you protect it?
iv. What are the consequences if what you want to protect falls into the wrong hands?

Digital security is more than just downloading new apps. It is about knowing your online presence and practice well, and making informed decisions to build a safer environment for yourself.

4.0 ASSESSING YOUR DIGITAL FOOTPRINT



A digital footprint is also referred to as a digital shadow or electronic footprint.

It is the trail of data you leave behind when using the Internet and it can be used to track your online activities and the devices that you use to access the Internet. For example, for trail leads to the websites you visit, the emails you send, and the information you submit online.

As an Internet user, you create a digital footprint either actively or passively.

An active digital footprint is where you deliberately share your information through posting or participating on social networking sites or online forums. If you are logged onto a website through a registered username or profile, any posts you make through it form part of their active digital footprint. You also contribute to active digital footprints by subscribing to a newsletter or accepting cookies on your browser.

On the other hand, a passive digital footprint is created when information is collected about you without you being aware that this is happening. For example, social networking sites and advertisers use your likes, shares, and comments, to profile you and target you with specific content regarding their products and services.

Since employers and other people can check your digital footprint, it is good practice to protect it by:

Searching yourself up online to get a sense of information about you that is publicly available. If any of the results show you negatively, contact the site administrator to see if they can remove it.

Limiting the amount of data you share about yourself. Any personal information you provide to any organisation expands your digital footprint and increases the possibility of misusing that data. Before submitting any form to an organisation, consider if it is worth it, and whether there are any other ways for it to obtain that information or service without you sharing your data.

A good rule of thumb is to only give personal information that is absolutely necessary. Do not be afraid to make things up! You can always give a fake name, a fake address, and all sorts of other made-up information when it is not absolutely necessary for you to provide personal information to obtain a service, and where you will not be penalised in any way with regards to integrity-issues, for concealing specific and true, personal information.

5.0 HOW VIOLENCE AGAINST FEMALE JOURNALISTS MANIFESTS ONLINE, AND MITIGATION STRATEGIES

Online violence is real violence that needs to be addressed because it limits the right to full participation, freedom of expression, and right to safety and privacy, for online users.

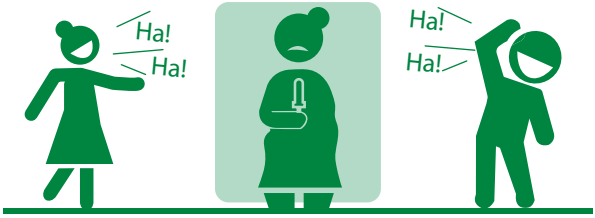
Female journalists and content creators are regularly subjected to the following forms of online violence:

Non-Consensual Distribution of Intimate Images (Revenge Porn)

This is the act of sharing private and sexually-explicit images or videos of someone without their consent.

This form of online violence can be highly traumatic and requires legal intervention. Ensure that you flag the explicit image or video for removal, report to the police and your employer, and turn to your support system for help during that trauma-filled period.

2. Body Shaming



This type of online abuse manifests itself through negative comments about the online user's body size or shape. This form of online violence can especially wreck a woman's mental health.

Remember that body positivity starts with you. Just keep at reminding yourself that you are more than just your body, and say no to body shaming. Over and above that, ensure you report and flag the message.

3. Trolling

A perpetrator intentionally publishes offensive remarks online to upset an individual and incite a response. The most common type of trolling is referred to as concern trolling. This is when abusers pose as fans or supporters but make harmful and demeaning messages or comments disguised as constructive feedback.

When targeting women, concern trolling is most often done through 'helpful' suggestions on improving one's appearance when such comments are designed to undercut or demean the recipient.

Most of the time, concerned trolls want to get your attention, therefore, counter speech may be counterproductive, and blocking could escalate the abuse. So, it is often advised 'don't feed the trolls', but you need to judge for yourself whether or not it is worth engaging/confronting the trolls.

The best mitigating strategy that has worked for most victims of trolling is muting. This enables you to hide specific abusive content, so that you do not have to see it. While at it, do not forget to report any annoying or offensive content to the platform where it appears, and to document all instances of trolling from repeat offenders. Take screenshots of the message, timestamps, and ensure that the offender's name is visible.

4. Doxing

This is a short form for the phrase dropping docs. It is the searching for, and publishing of sensitive personal information online including one's home address, email, phone number, or national identification number etc., to harass, intimidate, extort, or stalk someone, or to steal their identity all with malicious intent.

To protect yourself from doxing, search for yourself on Google. First, make sure you are logged off from your Google account and use different search engines. This will give you an idea of the information about you that is online, and where it is cropping up.

Make sure you also alter the privacy settings of your social media accounts to ensure that private information is not accessible to the public. This is because abusers comb through social media accounts looking for confidential information that they can leverage against you.

Set up Google alerts that will notify you if your full name, phone number, home address, or other private data about you suddenly pops up online, as this may mean that you have been doxed.

5. Hacking

Intrusion into a device or network to attack or harm the victim by stealing their data, violating their privacy, or infecting their device with viruses.

The best way to protect yourself from hackers is to practice rigorous cyber security, which will be explained later in this handbook.

6. Impersonation

This is when someone creates a hoax social media account using the target's name and photo, in order to post offensive or inflammatory statements to defame and discredit the target, or to instigate further abuse.

Should you become a victim of online impersonation,

report this to the platform on which it appears and remember to ask your support system to report on your behalf as well. Ensure you make a statement on your real social media accounts alerting your online communities about the impersonation. Facebook and Twitter now allow one to 'pin' posts to the top of their profile. Ensure you do so for quite a long time. Be sure to report to your employer as well regarding the issue, especially if the offensive statement published by the imposter involves your work as a journalist.

7. Online sexual abuse

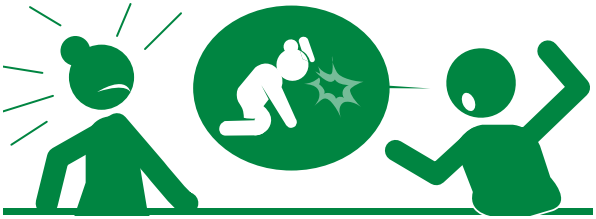
This form of abuse occurs in the form of sextortion, unsolicited pornography, or unwanted sexualisation.

Sextortion is a form of blackmail in which an abuser threatens "to expose a nude or sexually explicit image" unless the target does something to or for them.

Unsolicited pornography is when one sends sexually explicit or sexually violent images and videos to a target. Unwanted sexualisation is defined as sending unwelcome sexual requests, comments, and content, to a target.

The first thing to do is report any form of online sexual violence to the platform on which it was received and document the abuse. You can also press charges against the abuser. Reaching out to others for support can go a long way in ensuring your mental health.

8. Threats



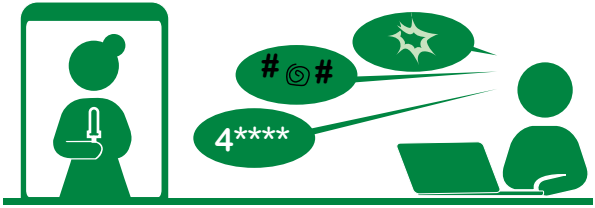
A statement to inflict pain, injury, damage, or other hostile action, on or against a target. This includes death threats, threats of physical violence, and often for women, threats of sexual violence.

Threats can be implied. For example: 'people like you should be shot', or they can be explicit, for example, 'I am going to kill you'.

Legally, an implied threat may not be considered a threat therefore, choose not to engage with the person, block them, mute them and report them to the platform.
Explicit threats are serious. You need to lock down your physical location by relocating temporarily or by developing a home security plan. Be sure to report to the police and inform your employer and allies of the threats.

Whether implied or explicit, take all threats seriously.

9. Abusive comments



Do not bite the hook! Being ambushed by an abusive comment may leave you feeling hyper-aroused and eager to strike back instantly. Do not do this. Press the pause button: take a few deep breaths first or, better still, come back to considering whether or not to respond to abusive comments, later.

6.0 BEST PRACTICES: KEEPING ONLINE SPACES SAFE

Social networks are great fun and can be advantageous. Still, you need to understand that this is a complicated world that you need to manage wisely.

i. Before you sign up for an online service, find out:
ii. Who owns the service you are using?
iii. What data about you do they keep?
iv. Do they share the data with anyone else?
v. Has the company been hacked before?

Your Internet Service Provider has access to the following information about you:

vi. Personal sign-up details
vii. Browsing history
viii. Location
ix. Content you watch
x. How long do you spend looking at things on the Internet

Below are the best practices to help you maintain digital safety and security:

1. Create Strong Passwords

Passwords are your first line of defence. To keep your data safe/confidential, reduce the chances of viruses attacking your computer/phones, keep hackers from accessing your computer, and make your password strong, complex, and too

difficult for hackers to crack it.

Passwords are commonly compromised when:

xi. They are shared with others
xii. Someone witnesses a password being entered on your screen
xiii. Through "Save My Password" or "Remember Me" settings saved on websites via a browser
xiv. Malware, such as a keylogger
xv. Social Engineering

What makes a good password? It should be:

xvi. Long- at least 14 characters
xvii. Unique- make it alphanumeric, containing upper and lower case letters, as well as numbers and symbols
xviii. Do not include personal, identifiable information such as your birthdate
xix. Change it often
xx. DO NOT REUSE PASSWORDS ACROSS MULTIPLE PLATFORMS

Writing down your passwords on a scrap of paper that you keep in your drawer or wallet or stick on your computer monitor is never a good idea. Storing all your passwords in a password manager is a smart move.

A password manager is:

i. A service that stores and creates passwords
ii. Stores passwords in one place
iii. May sync between devices

A password manager is not:

i. The option to store passwords on your browser

Pros of a password manager:

i. Currently, the most secure option
ii. Remembers passwords
iii. Creates long, unique passwords
iv. Shares passwords securely
v. Protects you from phishing attacks

Cons of a password manager:

i. Can malfunction
ii. You need a password for the password manager, so if you lose it, you lose all your other passwords.

An excellent example of a password manager is LastPass. It uses a combination of browser extensions, phone apps, encryption, two-factor authentication, and many other technologies to ensure your passwords are stored safely and accessibly for you alone. It can also randomly generate extremely strong passwords for you to use.

1. Enable Two-Factor Authentication (2FA)

2FA is an extra layer of security for your accounts

Once this feature is enabled, you will be prompted for your password and a code. The code could either be a one-time code sent via a short messaging service (SMS), or it can be generated by a dedicated mobile app that stores a secret (e.g. Google Authenticator) or a hardware key.

The process of enabling 2FA differs from platform to platform, and so does the terminology used. However, to enable 2FA on most platforms, you only need a mobile phone through which to receive an SMS.

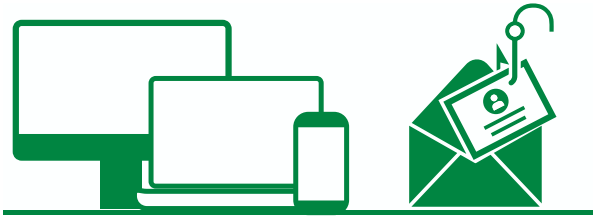
2. Stick to App Stores

Should you want to download any app, get it from the Play Store if you use Android or App Store if you use IOS. The official App stores vet apps for potential security or privacy issues.

Downloading apps from unsafe sites makes you easy prey, to malware and potential online abuse. Also, only download the apps you need and use as apps mine data from you.

Update your software and apps regularly.

3. Watch out for Phishing Scams.



Phishing is an act of luring unsuspecting users into revealing private account or login information.

To be safe, if you receive an email that includes a link to a website, make sure that the website is legitimate before you click on the link. For example, instead of clicking through to the site, from within the email, open a different Web browser and visit the business's website directly to perform the necessary actions. You can also verify an email from a legitimate company or individual by calling the business, agency, or individual directly.

4. Clear your Browser History

Browsers keep records of every site you visit.

Ensure you clear browser history for all the devices you use in a day – your home and work computers, or your own or friend's iPad. Internet browsers like Firefox or Chrome keep track of where you have been and what you have done online. They keep records of every site you visit. Information about what you sent from or saved on your computer can be kept for days or weeks. To be safe, always clear your browsing history.

5. Use HTTPS

HTTPS is officially known as "hypertext transfer protocol secure." It is similar to HTTP, which is used to enter Internet addresses. However, HTTPS adds an extra layer of security and encryption while online. Communication between users and sites that support HTTPS is encrypted and authenticated. That means that HTTPS can determine whether or not a website is genuine.

6. Use VPN

A Virtual Private Network (VPN) is an Internet security service that allows users to access the Internet as though they were connected to a private network. This encrypts Internet communication and provides a substantial degree of anonymity.

This means your IP address will be masked, ensuring no one can trace back to your devices and geo-location, and you can search and browse the Internet without anything or anyone keeping digital records of your activity and history.

A user connecting to the Internet using a VPN service has a higher level of security and privacy. You should, however, be aware that your VPN has access to the following:

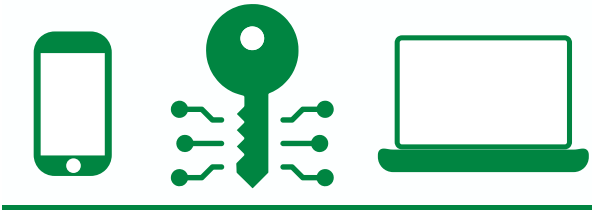
i. Personal sign-up details
ii. IP address and location
iii. Browsing history
iv. Content you watch
v. How long you spend looking at things on the Internet

Therefore, think about the following:

i. Who owns it?
ii. Where are its servers located?
iii. Does it encrypt your data?
iv. Does it have a history of sharing data with others?

Examples of VPN include tunnelbear or Cloudflare.

7. Encrypt your Data and Devices



Do you want to keep outsiders from listening in on your chats, phone calls, and more? Then encrypt them. Encryption involves converting human-readable plaintext into incomprehensible text, known as ciphertext.

It is the simplest and most important way to ensure a computer system's information cannot be stolen and read by someone who wants to use it for malicious purposes.

Nothing is 100 per cent secure. However, a lot of digital security software incorporates encryption to varying degrees. If encryption is an essential feature for you, Open-source software (OSS) like Signal, is recommended

because the community can audit it to ensure no backdoor entry is allowed.

8. Review your Privacy Settings

Most phones have a settings page where you can see which apps have access to everything, so it is here that you can review which apps have access to what, and disable permissions you do not remember granting.

The same applies to your social media accounts; review your privacy setting to limit access to select information. While at it, be careful who you add as a friend or choose to follow.

Block/unfriend anyone you feel is a threat or with whom you feel uncomfortable; otherwise, you will be making yourself more of an onlinetarget.

In addition, think before you send that tweet or post anything controversial to reduce your chances of being violated online. Do not, however, self-censor while at it.

9. Beware of Public Wi-Fi

When you are on a Wi-Fi network, anyone else using that network can watch or intercept your Web traffic (even if it is a password-protected network).

The absolute best protection is to use a Virtual Private Network (VPN) to encrypt your Web traffic so it cannot be intercepted. A great alternative is to use the Tor Browser to send your browsing over the Tor network, thus making you anonymous while encrypting your data. Please note that it will be slower than using your usual browser, but it is worth the effort.

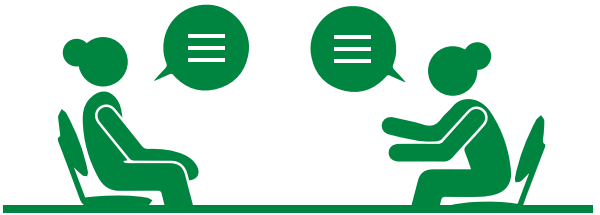
10. Self-Dox

Develop a habit of searching for yourself on Google to discover what information is there about you, especially from your social media accounts. Try doing that using the link below.

https://lmgtfy.app/#gsc.tab=0

What information pops up about you? Do you like what pops up?

7.0 PSYCHOSOCIAL SUPPORT



Online harassment is more than just unpleasant. Its effects are far-reaching for journalists. It affects their mental health and prevents them from doing their job effectively. Therefore, accessing support can be an essential step to helping journalists who are violated online.

Below is a recommendation on what to do If you are being targeted online because of your journalistic work:

Seek Help

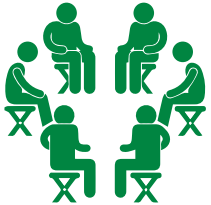
Reach out to the organisations that help journalists targeted online with psychosocial support, for example, The International Women's Media Foundation (IWMF), The Black Journalists Therapy Relief Fund, The Committee to Protect Journalists, The Rory Peck Trust, among others.

1. Speak with your Employer or Colleagues at Work

You may want to speak to your editor or newsroom manager about the abuse you are facing and see whether they have a policy to support staff facing online harassment. If you are a freelance journalist or work in a

newsroom without support, reaching out to colleagues elsewhere, or journalist' networks can be a helpful way of finding support or resources.

2. Create a Support Group



Building your own formal or informal support network of colleagues can be a helpful way of managing the stress of being abused online. Having a network will allow you to reach out to others for emotional and practical support. This can include setting up group chats to share strategies and tips for dealing with the online abuse.

This supportive community can also help amplify the content of the person being abused, drawing attention away from an abuser via funny or unrelated content, or reporting the abuse to the platform where it happened – and it can help tag the platform to draw extra attention.

3. Go Offline

Staying offline is self-care. Step away from an online platform, computer, or smartphone for a while to focus on your mental and physical well-being. While offline, reach out to a colleague or friend to monitor your social media accounts for threats, hate speech, impersonation, and doxing, and request them to document them on your behalf, as well as take screenshots and save hyperlinks.
Psychologists have advised the following additional options of practising self-care after an episode of online harassment:

i. Keep a journal about your online experience; Journaling will help you process your trauma and distance yourself from your experience.
ii. Relieve stress by reading your favourite book, or just write.
iii. Get a body massage to relieve the physical stress related to your emotional stress.
iv. Take a walk; if you can go for nature walks, it is even better
v. Maintain your religious or spiritual practice if you have one
vi. Listen to music

vii. Turn off your phone notifications, especially at night, and ensure you get uninterrupted sleep.
viii. Sip some hot beverage - with an attitude!
ix. Spend some time with a loved one
x. Practice breathing exercises
xi. Meditate

What about supporting others?

It can be intimidating to intervene when you witness another person being targeted by online hate or harassment.

When considering whether or not, and how, to support a victim of online harassment, ask yourself the following questions:

i. Will you worsen the harassment?
ii. What if tables turn and you become the target of such harassment?
iii. What if the harassment traumatises you in some way, making you leave the online platform, or something else?

if you feel compelled to help someone who is being abused online, and believe you can do so without risk to yourself, it is advisable to do the following:

i.

Tighten your cybersecurity to protect yourself from doxing, hacking and impersonation and while at it. Trust your instincts.

ii. Take time to identify the abuse that is taking place. Being in the know will help you prepare for the best way to respond. In addition, different forms of violence require different tactics of dealing with it.

iii. Contact the target of online harassment and inquire from them about the support they would require. If the victim has no idea what kind of support they need, you can give them available options.

8.0 LEGAL FRAMEWORK

1. The Kenya Constitution, 2010

The Bill of Rights in Chapter 4 of the Kenya Constitution, 2010, provides several fundamental rights and freedoms for Kenyan citizens. These include the rights to privacy; access to information; to property; to consumer protection; to fair administrative action; to access to justice and fair hearing; to freedom of conscience, religion and opinion; to freedom of expression; and to freedom of the media.

According to Article 21 of the Constitution, the State and every State organ is required to observe, respect, protect and fulfil the rights and fundamental freedoms in the Bill of Rights. It further requires the State to enact and implement legislation to meet its international obligations regarding human rights and fundamental freedoms.

Should a right or fundamental freedom in the Bill of Rights be denied, violated or infringed, or be threatened, Article 22 grants every person the right to institute a court proceeding.

2. Computer Misuse and Cybercrimes Act, 2018

This Act of Parliament came into force on 30 May 2018.

The Act aims to: protect the confidentiality, integrity and availability of computer systems, programs and data; prevent the unlawful use of computer systems; facilitate the prevention, detection, investigation, prosecution and punishment of cybercrimes; protect the rights to privacy, freedom of expression and access to information as guaranteed under the Constitution, and facilitate international co-operation on matters covered in the Act. Any person who commits an offence as defined in this Act,

will be liable to a fine not exceeding five million shillings (USD10,000), imprisonment for a term not exceeding three years, or both.

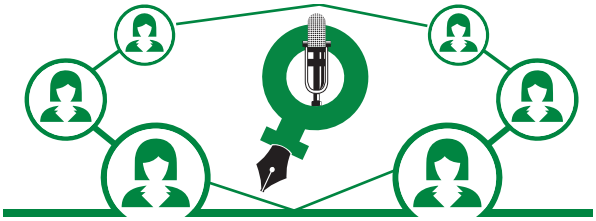
3. Data Protection Act, 2019

The Act enumerates comprehensive laws that protect the personal information of individuals. It establishes the Office of the Data Protection Commissioner and makes provisions for regulating the processing of personal data in Section 25.

The Act further protects the privacy of individuals; establishes a legal and institutional mechanism to protect personal data, and provides data subjects with rights and remedies to protect their personal data from processing that is not as per the Act.

A person who commits an offence as defined in this Act, shall be liable to a fine not exceeding three million shillings (USD 30000), or to an imprisonment term not exceeding ten years, or to both. In addition, the Court may order the forfeiture of any equipment or any article used or connected in any way with the commission of the offence.

9.0 ABOUT AMWIK



The Association of Media Women in Kenya (AMWIK) is a National Media Association established in 1983 and registered under the Societies Act as a non-profit membership organisation for women journalists from print, electronic media and other areas of communication.

AMWIK's vision is a just society where the media embraces and promotes equitable development, human rights, and women's rights. AMWIK's mission is to use the media to promote an informed and gender-responsive society through professional and transformative media in Kenya and Africa.

10.0 REFERENCES

Sameer Hinduja, Ph.D. and Justin W. Patchin, Ph.D of the Cyber Bullying Research Centre, and accessed at: *https://cyberbullying.org/social-media-cyberbullying-online-safety-glossary.pdf*

DIY Feminist Cybersecurity (hackblossom.org)

https://ijnet.org/en/story/new-hub-offers-support-journalists-facing-online-violence

https://www.kaspersky.com/resource-center/definitions/what-is-a-digital-footprint

https://rorypecktrust.org/freelance-resources/digital-security/navigating-the-internet/

https://onlineharassmentfieldmanual.pen.org/defining-online-harassment-a-glossary-of-terms/

https://onlineviolenceresponsehub.org/journalism-psychosocial-support

Kenya Gazzette Supplements Act, 2018, and 2019

https://www.passwordmonster.com/ to check the strength of your password

https://www.lastpass.com/ to get LastPass password manager

https://lmgtfy.app/#gsc.tab=0 to check what information is online about you

https://stopncii.org/ to get support for non-consensual distribution of intimate Images

https://philome.la/jace_harr/you-feel-like-shit-an-interactive-self-care-guide/play/index.html to assess your emotional wellbeing.

Association of Media Women In Kenya

(AMWIK)

Mbaruk Rd , Off Muchai Drive Opp.
Awash Ethiopian Restaurant
P.O Box 10327-00100

0722-201958/0737-201958

info@amwik.org

Website www.amwik.org