In the recent years, Kenya has steadily increased its number of internet users, and with this growth there has also been an evident increase in cyber violations. With support of the Ford Foundation, iHub conducted a research study on women’s online experiences in Kenya, which shed light on the darker and more unfortunate effects of a more accessible internet. In this document we outline different types of online violence and identify simple procedures and tools that can be used by all to have a safer online experience.

Online Harassment/Bullying

In the recent years, Kenya has steadily increased its number of internet users, and with this growth there has also been an evident increase in cyber violations. With support of the Ford Foundation, iHub conducted a research study on women’s online experiences in Kenya, which shed light on the darker and more unfortunate effects of a more accessible internet. In this document we outline different types of online violence and identify simple procedures and tools that can be used by all to have a safer online experience.
Types Of Online Violence
Doxxing

Doxxing – named for “documents” or “docs” – is the act of release of someone’s **personal and/or identifiable information** without their consent. This can include things like their full legal name, social security numbers, home or work addresses and contact information.

There’s no set format for a “dox”; the doxxer simply publishes whatever information they’ve managed to turn up in their searches. Sometimes this even includes the names and details of their target’s family or close friends.

As a tactic of harassment, doxxing serves two purposes: it intimidates the people targeted by invading and disrupting their expectations of privacy; and it provides an avenue for the perpetuation of that person’s harassment by distributing information as a resource for future harassers to use.

Non-consensual Dissemination of Intimate Images

This is the distribution of sexually explicit images or video of individuals without their permission. The sexually explicit images or video may be made by a partner of an intimate relationship with the knowledge and consent of the subject, or it may be made without his or her knowledge. The possession of the material may be used by the perpetrators to blackmail the subjects into performing other sex acts, to coerce them into continuing the relationship, or to punish them for ending the relationship.
Cyberstalking

This is the use of the Internet or other electronic means to stalk or harass an individual, group, or organization. It may include false accusations, defamation, slander and libel. It may also include monitoring, identity theft, threats, vandalism, solicitation for sex, or gathering information that may be used to threaten, embarrass or harass.

Cyberstalking is often accompanied by realtime or offline stalking. Both are motivated by a desire to control, intimidate or influence a victim. A stalker may be an online stranger or a person whom the target knows. He may be anonymous and solicit involvement of other people online who do not even know the target.

Trolling

A troll is a person who starts quarrels or upsets people on the Internet to distract and sow discord by posting inflammatory and digressive, extraneous, or off-topic messages in an online community (such as a newsgroup, forum, chat room, or blog) with the intent of provoking readers into displaying emotional responses and normalizing tangential discussion,[3] whether for the troll’s amusement or a specific gain.
Catfishing and Impersonation

Catfishing is a type of deceptive activity where a person creates a sock puppet social networking presence, or fake identity on a social network account, for attention seeking, bullying or as a romance scam.

A “catfish” is someone pretending to be someone they are not on the internet. A catfish usually targets a victim or has someone they are pretending for. Usually people intend catfishing as a romance scam on dating websites or seeking online relationships. People use fake profile pictures, names, and often genders. Catfishers create fake profiles to trick people into thinking they are someone else. Usually, the fabricated life displayed is the one they wish was their own, making it easy to act as if it is really them.

Catfishing is similar to impersonation, except that the perpetrator is not pretending to be a person who really exists (like a celebrity or public figure) He or she usually steals photos from acquaintances or strangers off the Internet for their accounts. In order to minimise the effects of impersonation, social media platforms e.g. Twitter, Instagram have introduced a verification procedure common amongst public figures, that’s illustrated by a ‘blue tick’.

Swatting

Swatting is the harassment tactic of deceiving an emergency service (via such means as hoaxing an emergency services dispatcher) into sending a police and emergency service response team to another person’s address. This is triggered by false reporting of a serious law enforcement emergency, such as a bomb threat, murder, hostage situation, or other alleged incident.

More often than not the different forms of online violence just like *aspect of online violence being perpetrated by people that we have been intimate with
We may think online violence has no real life consequences, however just like physical violence, online violence can have negative long lasting or even permanent effects on victims.
Mental and Emotional Upheaval

Online violence may have a semi-permanent or even permanent effect on its victims' emotions, ranging from anger, fear, sadness, frustration, low self-esteem that then result in mental disorders such as anxiety, depression and suicidal ideation. Without effective and consistent interventions to deal with these effects, victims may suffer permanent emotional degradation.

Leaving online spaces (permanently or semi-permanently)

A negative effect of facing online violence is altogether leaving online spaces and choosing not to engage online via various platforms due to the perceived risk and fear of repeated violence. The impact of this is having a significant number of people not accessing social, educational, networking, economic benefits that can be gotten from being online, thus foregoing the right to be online.

Self censorship

Often speaking out on controversial topics online attracts attention from all corners of the internet. This attention may result in positive and even negative interactions from other online users. During our research we discovered that women we have undergone online violence may sometimes opt to avoid talking about certain sensitive topics in order to avoid repeated harassment online as a result in other users disagreeing with their opinions and taking it a step further and harassing them for their views and opinions.

Pseudonym Accounts / Separate identities

It is not uncommon to see some internet users use pseudonym accounts in order to enable them keep their offline persona separate from their online persona. This is usually in fear of being persecuted for their online views, their gender, identity (e.g. individuals from the LGBTQI community) which may attract hostility from society or the industry in which is the target of their work.
How To Deal With Online Violence
01 DOCUMENT! DOCUMENT! DOCUMENT! COLLECT ANY EVIDENCE AGAINST THE PERPETRATOR THAT WOULD HELP PUSH YOUR CASE

02 REPORTING TO LAW ENFORCEMENT, THE RECEPTION MAY NOT BE VERY 1

03 CONSULTING A LAWYER

04 SEEKING MENTAL HEALTHCARE

05 SEEKING YOUR SUPPORT SYSTEM - THIS INCLUDES FRIENDS AND GUARDIANS.

06 SEEKING OTHERS WHO HAVE EXPERIENCED ONLINE VIOLENCE WITH WHOM YOU CAN SHARE YOUR EXPERIENCE WITH, LISTEN TO THEIR EXPERIENCES AND FINDING A WAY
What to do in the event of online violence

Record or document all and any evidence from the incident (including context that may lend clarity to the incident)

Immediately report the incident to the authorities in your country as well as by using the reporting function on the platform you are currently using. Usually, online platforms have a code of conduct and individuals who are responsible in ensuring they are upheld.

Share this information with a close friend or guardian who can help you come to terms with any negative emotional effects that may result after the incident.

If necessary, do not hesitate to seek professional help e.g. from a counsellor in order to help you process the emotional effects if any.
General Tips for Staying Safe Online
01 Password Management

Always use a strong password that you regularly update your passwords, and because this can be challenging use Password Manager applications such as ‘1 Password’. However, passwords are not enough, add an extra layer of protection with 2 Factor Authentication.

Two-factor authentication, or 2FA as it’s commonly abbreviated, adds an extra step to your basic login procedure. Without 2FA, you enter in your username and password, and then you’re done. The password is your single factor of authentication. The second factor makes your account more secure, in theory.

02 Devices

Do not log into your social media platforms using devices that are not yours (as mentioned previously, more often than not several instances of impersonation, hacking, Non-consensual Dissemination of Intimate Images etc are done by past intimate partners or people we once considered friends and know us relatively well.

03 Click Smart

Do not click on links or run programs you do not trust as they may be some form of malware.
**Software Updates**

Always install current updates as soon as they are available to ensure your devices are always up to date with the current security software your devices require to keep security breaches at bay.

---

**Network Use**

These days it is not uncommon to encounter free access wifi in public places such as restaurants, airports and various community centres. However, when connecting to these networks you need to exercise caution to only connect to official networks.

---

**Secure Websites**

When using websites to process sensitive information such as payment transactions, ensure that your address bar indicates that it is “HTTPS” aka Hypertext Transfer Protocol Secure which basically means that secure communication is occurring over a computer network. It is equally important to login to authentic websites, to avoid phishing.
A great example of this is DuckDuckGo which does not store a record of your search meaning it doesn’t collect or share your personal information, has an ad free search experience. Understand which applications you are logging into and whether these application can geolocate you. Everytime you download an application understand the settings you are complying to. For instance, ().

For some of us today social media is akin to breathing and any moment of free time will have us scrolling through the pages of different social media pages. It is very easy to get carried away to share private information that could very easily give away our physical location, our home address or its environs, day itinerary, personal identifiable information etc. Unfortunately, this poses a huge risk and may result in stalking, impersonation or even physical confrontation. Do not share personal information online for instance, your KRA PIN, passwords, financial information.

It is important that we continually seek to improve our levels of digital literacy and that of those around us, to reduce the risk of being prone to encountering harm online and further to take advantage of opportunities online such as networking,
References

https://hackblossom.org/cybersecurity/

https://longreads.com/2018/03/28/who-does-she-think-she-is/

https://rad.cat/


https://cyber.harvard.edu/node/99714

https://onlineharassmentfieldmanual.pen.org/resource-guide-to-combat-online-harassment/defining-online-harassment-a-glossary-of-terms/

https://feministinternet.org/sites/default/files/FPI_brochure.pdf

https://dataprivacyproject.org/learning-modules/risk-assessment/#jo

https://datadetox.myshadow.org/en/detox/day1/5-challenge

https://myshadow.org/tracking-so-what