

# BE SAFE ONLINE

A guide for women and minority groups





# BE SAFE ONLINE



## **ACKNOWLEDGEMENTS**

This toolkit was developed by TechHerNG with support from the Digital Defenders Partnership (DDP) as part of its efforts to ensure the protection of women, girls and other vulnerable groups from tech-facilitated gender-based violence.

Technical support was provided by digital security experts Andy Madaki and Valerie Oakhu.





# BE SAFE ONLINE

## CONTENTS

1. Why This Toolkit?
2. Defining Online Gender-Based Violence
  - a. Cyberbullying
    - Threats of physical violence
    - Sexual and verbal harassment
  - b. Impersonation and identity theft
  - c. Catfishing
  - d. Cyberstalking
  - e. Threats of revenge & Revenge Porn
  - f. Doxxing
  - g. Sexploitation
  - h. Sextortion
  - i. Deep fakes
3. Cyber threats
  - Malware
  - Phishing
  - Spam
4. How to report abuse across social media
5. Practising good digital hygiene
6. Glossary of Terms





## WHY THIS TOOLKIT?

The internet can be an empowering space for women and girls. On the other hand, it can also be quite dangerous for them. Threats, intimidation, extortion and impersonation are some types of abuse they experience through and within digital spaces.

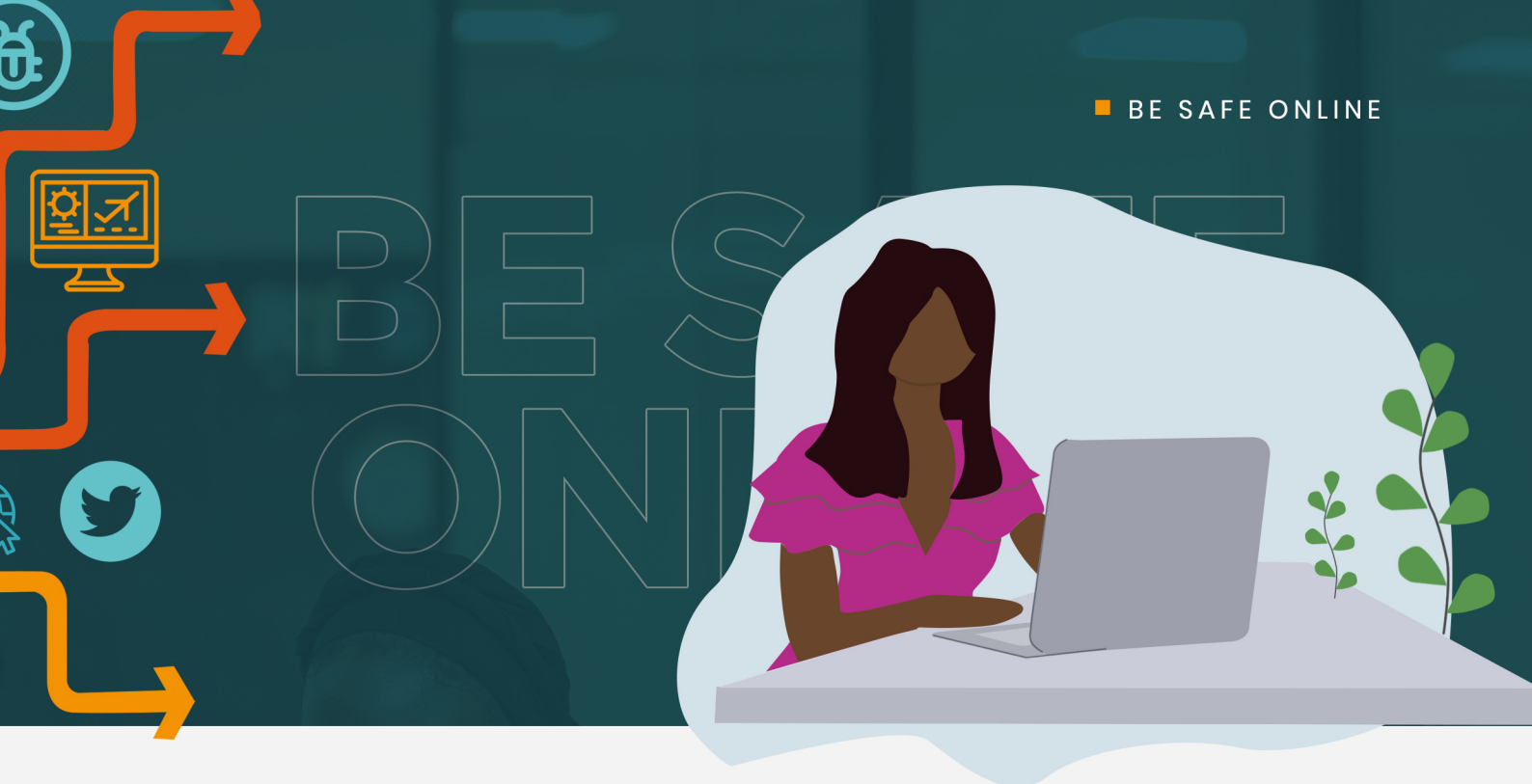
Women and girls can be exposed to these forms of abuse as a result of what they say, groups they belong to, or causes they advocate for, but in many cases, simply because of their gender.

Women are more likely to be victims of severe forms of online violence than men, which has far-reaching and traumatic impacts on their lives. Consequently, this has made many women hesitant about engaging in online discourse and endeavours as a preventive strategy to ensure their safety.

This is not okay.

The right to internet access is a human right, and women should be encouraged to exercise and enjoy such freedoms by taking up space offline and online. However, this cannot be achieved if digital spaces are unsafe for them. Therefore, preventive measures and relevant solutions are required to tackle the unique challenges women face online.

This toolkit was designed to create awareness of the vulnerabilities women and girls are exposed to when they go online. Using case studies, this toolkit shows users what to do when they experience violence online.



## WHAT IS ONLINE GENDER-BASED VIOLENCE?

Online Gender-Based Violence (OGBV) or Technology-Facilitated Gender-Based Violence (TFGBV) is a form of gender injustice and discrimination that occurs within online spaces. This type of gender-based violence can include stalking, harassment, bullying, and unsolicited pornography, among other actions.

### Three Key Facts to Know About Online Gender-Based Violence

- 58% of girls online have reportedly experienced some form of online GBV personally.
- Out of the group mentioned above, 85% said they had experienced multiple forms of harassment.
- 39% of girls across major African cities are concerned about online safety.

*Online violence exists in many forms. This toolkit attempts to cover the most prevalent risks that women and girls face.*

#### Further reading

Plan International (2020) 58% per cent of girls online have experienced some form of online violence – <https://plan-international.org/publications/freetobeonline>

Neema Iyer, Bonnita Nyamwire and Sandra Nabulega (August 2020) 39% of girls across major African cities are concerned about online safety – <https://policy.org/resource/alternate-realities-alternate-internets-feminist-research-for-a-feminist-internet/>

## CYBERBULLYING



*Submission does not come naturally to anybody and definitely not to women. If it did, society would not need to constantly reinforce and force this idea down women's throats.*



*This was the entirety of Efe's post on Twitter or something along those lines, as she had to take it down since it seemingly brought all of Nigeria to her mentions.*

*It's been two weeks since that incident, but yesterday, she tweeted, "Jesus is coming soon". Expectedly, people reacted negatively to the post - calling her a shameless homewrecker and asking people not to buy her products. When will it end?*



1.

### CYBERBULLYING (NOUN)

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



Although men outnumber women in using social media within Nigeria, women are more vulnerable to online violence and cyberbullying. While men are also prone to cyberbullying, targeted women have a different experience because theirs descend quickly into sexualised hate and threats.

Cyberbullying, however, often falls into two main categories:

1. Cyberbullying that women experience because of their gender and online presence. This is unrelated to the content of their posts and is universal to women's experiences of social media use, i.e. sexual objectification.
2. A heightened level of cyberbullying of women who are actively engaged online (feminists championing women's rights, female politicians vying for office, opinionated single or LGBTQ women). This includes threats to their lives or friends/family members and threats of rape, often taken offline.





Cyberbullying is a public health issue, as the effects can be very detrimental to women. It can result in physical, psychological and economic harm.

These effects can be varied and complex depending on the types of harassment women are subjected to. Some commonly observed/reported effects among victims include fear, anxiety and self-censorship, precisely what abusers want.

Although cyberbullying is mainly perceived to be carried out by men on women, it can also be perpetrated by women. This can be in the form of body shaming, negative comments on social media posts or outfit choices, projecting insecurities and lack of support.

While cyberbullying can occur in many forms, threats of physical violence and sexual/verbal harassment continue to be quite prevalent.



#### Further reading

UNICEF (n.d.) *How to stop cyberbullying* - <https://www.unicef.org/end-violence/how-to-stop-cyberbullying>

Plan International (2020). *Free to be online* - <https://plan-international.org/publications/freetobeonline>

UN Women (July 2020) *Take five: why we should take online violence against women and girls seriously during and beyond covid-19* - <https://www.unwomen.org/en/news/stories/2020/7/take-five-cecilia-mwende-maundu-online-violence>

COE (March 2022) *No space for violence against women and girls in the digital world* - <https://www.coe.int/en/web/commissioner/-/no-space-for-violence-against-women-and-girls-in-the-digital-world>

**a. Threats of physical violence:** In Nigeria, just speaking out (as a private individual or public figure) about specific issues online can attract threats of physical violence. These topics could include feminism, gender equality, sexual abuse or specific aspects of women's rights, such as sexual/reproductive health and rights. Female opinions on such topics frequently lead to threats of physical violence, murder, and sometimes, harm to these women's families. These threats are also increasingly spilling offline, sometimes with devastating consequences.

**b. Sexual and verbal harassment:** Sexual and verbal harassment are some of the many forms of cyberbullying. Predominantly, the root cause of violence against women and girls is gender inequality (discrimination, gender stereotypes, sexism). Moreover, women with more than one commonly targeted characteristic – members of minority religions or different sexual orientations – may be attacked more frequently than others.

### What to do if you experience cyberbullying

1. Try not to respond – bullies thrive on attention.
2. Talk to someone you trust – being bullied can feel isolating.
3. Keep evidence of the bullying incident and as much information on the bully as possible. Block and report the bully's account/posts.
4. File a report with the police or relevant authorities.
5. If you notice someone being bullied online, be an active bystander and report the post/account.



## IMPERSONATION AND IDENTITY THEFT

“

*Is this not you?*

”

*This was the summary of the text that started Adaora's problems. She had received this message from her father along with a link to a website notorious for hook-ups in Nigeria. The link opened to a profile containing several pictures she had posted on Facebook and some she had even deleted. It was her in these photos, but it was also not her.*

*She frantically signed up on the website and sent messages to the account, pleading with them to take down the profile as her father was an archbishop in a popular church. This was not just about her.*

### IMPERSONATION (NOUN)

*refers to the act of pretending to be someone else, usually for entertainment or fraud.*

As social media continues to be a critical part of our lives, impersonation across its numerous platforms continues to grow and be a problem. Furthermore, most social platforms require little more than an email or a phone number to set up an account, making it relatively easy to create a fake profile in less than five minutes.

Women's identities in Nigeria are especially targeted for impersonation and used for fraud under a term popularly called “Local.” The plot is simple – pictures of unsuspecting victims are gathered usually from their social media accounts and then used to set up profiles on other social media platforms, especially dating sites. Using these profiles, the criminal lures people into relationships or promises a “hook-up” in exchange for recharge cards, data subscriptions or flight fares. This is problematic as, more often than not, the actual impersonation victim is apprehended for these crimes.

However, in some cases, the impersonation directly attacks the unsuspecting person whose identity is being stolen. Impostors use their identity to attack and harass other people, spread misinformation and defame their character, so the blowback falls on them.

While it can be difficult to completely prevent impersonation, especially if you run a business online or have a large following, you can take steps to protect yourself.



### How to prevent impersonation attempts

1. Create a strong brand. Naming all your accounts and linking them helps spot fakes.
2. Add a disclaimer to your bio – e.g. “Not on Snapchat or TikTok.”
3. Specify a means of contact.
4. Watermark your content with your actual handle.
5. Share as little information about yourself as possible.
6. Enable Multi-Factor Authentication (MFA) on all your accounts.
7. Google yourself routinely.
8. Do not complete “surveys” unless you are sure of their origin.

If you are a regular user who is on social media to keep up with family, friends and trends, consider taking these precautions:

1. Set all your social media profiles to private.
2. Confirm the identity of every follow request, even if you think you know them. Criminals have been known to create fake profiles of friends and families just to access a specific person.
3. Enable MFA on your accounts.

### What to do if you have been impersonated


1. Report the profile as soon as you notice it so it can be taken down. Social media platforms have instructions on how to report these.
2. If you find one fake account, there will be others because criminals tend to set up multiple accounts to create credibility. Check your other platforms as well.
3. Inform your family, friends and online contacts.
4. Impersonation is a criminal offence in Nigeria – file a report with the relevant authorities.





## CYBERSTALKING

Bolu had a few minutes to burn, so she opened her Instagram app. As expected, she had several likes. However, a couple of them stood out – they were from an account that was not one of her followers, but this account was able to consistently like all her photos and her comments on other people's photos.



“Are they following me around and liking all my comments?” she thought. “How are they finding my comments?” This had been going on for weeks...



### CYBERSTALKING (NOUN.)

*is a form of online harassment that uses the internet and technology to harass or stalk a person.*

Cyberstalking occurs in various forms – unsolicited attention, messages, emails, social media posts and requests. This form of harassment is intentional and persistent even after the victim has expressed a desire for it to stop.

However, cyberstalking does not necessarily involve direct communication, and some women may not and may never realise that they are cyberstalking victims. This does not minimise its severity or potential to escalate into a more dangerous situation.

80% of Nigerian women are ill-equipped to fight cybercrime; therefore, sensitisation is the first step to reducing that number.

### Steps to minimise cyberstalking

1. Keep a low profile and keep your social media accounts private.
2. For platforms that don't require your legal names (like LinkedIn), it's best to use a nickname.
3. Minimise the amount of personal information shared online – where you are, who you are with, and where you work.
4. Do not complete “surveys” unless you are sure of their origin.

### What to do when you notice you are being stalked

1. Block the person immediately – you do not have to tell them to stop first.
2. Change your usernames across all platforms.
3. Make a report to the platform on which the stalking occurred.
4. File a report with the police – in Nigeria; cyberstalking is a crime under the Cyber Crime Act.

#### Further reading

Alice Ishang-Ekpan (September, 2021). Vanguard. – <https://www.vanguardngr.com/2021/09/80-of-nigerian-women-girls-ill-equipped-against-cybercrimes-dig-folawiyo/>





## CATFISHING

*Ebiare was a dream come true. Adunni met her on Facebook about two years ago in a group for cat owners, and they immediately hit it off. Ebiare was like the sister she never had. She was funny, smart and always offered a listening ear.*

*It didn't matter that Ebiare never liked to speak over the phone or was always too busy with work and school to make time for them to meet in person. Ebiare was always there for her, and although she often needed help to complete payments at school and buy data for browsing, isn't that what sisters do?*

### CATFISHING (NOUN)

*is when someone uses images and information taken from other people's social media account(s) to create a new identity online - sometimes using an individual's entire identity as their own. The goal is usually to get the victim to fall in love with them.*

In Nigeria, while catfishing for romance scams is incredibly high, some criminals create profiles to gather a considerable following - usually with pictures of pretty women - for a specific purpose. They aim to sell them for thousands of naira to social media influencers or scammers who do not want to work to build their profiles' credibility.

Catfishing can be a traumatic experience for victims, especially if they are emotionally invested in a friendship or romantic relationship with the catfisher. Victims of catfishing can find it extremely difficult to be trusting after their experience. In addition to emotional devastation, victims of catfishing can also face embarrassment and regret after believing & falling for a "non-existent" person.

It can be difficult to prevent being catfished in the first place, but there are a couple of things women can do to minimise the outcome of the experience.

#### How to minimise catfishing attempts

1. Always be careful when talking to strangers online.
2. Never give money/gifts to someone you met online.
3. Trust your instincts - if you think something is off, it will likely be true.

### How to know if you are being catfished

1. They do not have a lot of social media friends, and even if they do, they are more global than local friends. This would suggest that their friends are “fake.”
2. Run a reverse image search of the image they currently have on their profile – this will show you other similar pictures and, more often than not, the source/actual owner of the image.
3. They never want to make voice/video calls.
4. They are reluctant to meet up.
5. They ask you for sensitive information or gifts.
6. They ask you for nudes.
7. They are “too into” you.

### What to do if you think you are being catfished

1. Block them immediately.
2. Report their account on the platform being used.
3. File a report with the police and other relevant authorities.
4. File a report with your bank if you have transferred money.



## THREATS OF REVENGE PORN & REVENGE PORN

“

*I will make sure no man ever wants you, and that no man ever marries you!*

”

Amina frequently got this kind of threat from Hassan before she ended their relationship two weeks ago. He threatened to beat and disfigure her, but he never did hit her. So when she got his text, she rolled her eyes. He would have to find her to do that, right?

Just as she considered blocking his number, another text came in. It contained just one link, and when she opened it, her blood ran cold. “You are about to become very popular,” the text had said.

### REVENGE PORN (NOUN)

*is defined by the U.S. government as “the sharing of private, sexual materials, either photos or videos, of another person without their consent and with the purpose of causing embarrassment or distress.”*

Revenge porn, also known as non-consensual pornography, most commonly happens after a sexual relationship ends. One partner typically posts intimate photos or videos online as revenge. This is where the term “revenge porn” comes from. However, the label “revenge porn” does not cover all cases as it is not always an ex that posts images on the internet after a relationship. Sometimes, the images are obtained by strangers through a hack.

Revenge porn is a crime in a lot of countries, including Nigeria. However, many victims of this form of abuse are unaware that there are legal steps they can take and even when they are, shame and the fear of social stigma prevent them from going ahead.

According to Mary Anne Franks, President and legislative/tech policy director of the Cyber Civil Rights Initiative, “If you look at any revenge porn site, 98% of the people featured are women”. “For a long time, the theory was, ‘Well, women are sending a lot more nude photos than men are.’ Not true. Men send more nude photos than women do . Revenge porn sites do not traffic in men’s pictures.”



In addition to being more likely to be victims of this crime, women also face greater social and cultural retribution than men for taking these types of photos. Should their pictures be made public, women are more likely than men to experience victim blaming, according to research from the Cyber Civil Rights Initiative.

### How to prevent revenge porn

1. If you must take or share intimate photos or videos of yourself, make sure the photos/videos do not show your face, tattoos or any other identifiable features.
2. Use strong passwords on all your devices.
3. Enable MFA on your accounts.
4. Mind the links you click on.
5. Avoid making explicit videos of yourself or with someone else.
6. When you encounter revenge porn, be an active bystander – do not share it and always report the account/post.

### What to do if you are being threatened or are a victim of revenge porn

1. Confide in someone you trust.
2. Report to the police immediately.
3. Visit <https://stopncii.org/>. It is a tool designed to help victims of non-consensual intimate image (NCII) abuse by taking down reported content on Facebook & Instagram.
4. Use this Google tool to report the image and have it removed (<https://support.google.com/websearch/troubleshooter/3111061#ts=2889054,2889099>)



#### Further reading

Tove Marks (April, 2022) Revenge porn: How to prevent and combat it - <https://vpnoverview.com/internet-safety/cybercrime/revenge-porn/>

Jessica Goldstein (2020) Revenge porn was already commonplace. The pandemic has made things even worse

Washington Post. - [https://www.washingtonpost.com/lifestyle/style/revenge-porn-nonconsensual-porn/2020/10/28/603b88f4-dbf1-11ea-b205-ff838e15a9a6\\_story.html](https://www.washingtonpost.com/lifestyle/style/revenge-porn-nonconsensual-porn/2020/10/28/603b88f4-dbf1-11ea-b205-ff838e15a9a6_story.html)



## DOXXING

*Dotun stood and watched as her life savings continued to light up the Lagos night. The firefighters were yet to arrive as they said they were looking for water. That was 3 hours ago. She was numb then, and later, her therapist told her it was because she was in shock.*

*Dotun had always been outspoken about her opinions on marriage and the role women should play in society. She never imagined the hate she would get from men and the women she was trying to help in return.*

*Hate so deep that it had pushed someone to find and release the location of her warehouse online, just a day after she had gotten a lot of products from Turkey in preparation for the busy December season.*

### DOXXING (NOUN)

*is a digital attack that involves publishing personally identifiable, sensitive and secret information about someone on the internet with malicious intent.*

This alarming practice has become incredibly widespread on social media, and in Nigeria, most victims are women. This is because doxxing is part of a more significant issue of men enabled and shielded by a patriarchal society that values and gives men power over women, robbing women of their fundamental rights to privacy and autonomy.

Sometimes, the information gathered and released can be found in public records. However, perpetrators sometimes employ black hat methods - deceptive means of obtaining information - like email/SMS phishing to access a victim's device to gather more personal information.

Doxxing can be life-threatening to women, especially if they are queer, an activist, a journalist, a feminist, or just considered "a problem enough" by the perpetrator(s). However, women can do a couple of things to avoid being doxxed.



## How to avoid being doxxed

1. Use a Virtual Private Network (VPN). It masks your online identity and encrypts your internet traffic.
2. Never use public wifi.
3. Do not reuse passwords/usernames across platforms.
4. Keep your social media profiles as private as possible
5. Educate your family, friends, and colleagues on the tips above. A breach of their security could lead to a breach of yours.
6. Refrain from sharing personal information online, such as where you are visiting, who you are with, and where you work.
7. Google yourself and remove your information from google search engines  
<https://support.google.com/websearch/troubleshooter/9685456>

## What to do if you have been doxxed

1. Document the dox.
2. Report the post/account if it's on a social media platform.
3. If your details were released on a website, reach out to the webmaster, also known as the site manager. A lot of websites have a Contact Us form.
4. Report to the police, especially if the dox contains data that is not already publicly available.



**Further reading**  
Access Now (March 2022) What is doxxing? <https://www.accessnow.org/what-is-doxxing-women-human-rights/>

## SEXTORTION

What do you want from me?

*This was the last text Chioma sent to Ikenna after days of pleading with him not to go through with his threat. He had told her that he was willing to share the video of them having sex online. She had called and texted but never got a response from him. It's been almost a week since her last message, until an hour ago when he responded, "I'll be at Sheraton Hotel today, be there at 9 pm or else..."*

### SEXTORTION (NOUN)

*is an invasive form of extortion that occurs when a perpetrator threatens to release explicit images of you unless you send them a ransom—usually money, explicit images, or even sexual favours.*

Even though illegal, incidents of online sextortion continue to rise. This is not entirely surprising given the increase in online social interactions, especially during the lockdown caused by the COVID-19 pandemic. While perpetrators of sextortion are often past lovers of the victims, sometimes they are bad actors who have obtained intimate content by hacking the victim's device.

However, this does not make a difference in the severity or effects of the crime, especially in a religious and conservative country like Nigeria, where the value of a woman is still hinged on how "pure" she is perceived to be. Sextortion leads to significant financial loss and psychological trauma for the victims. Also, the fear of social stigma and being blamed for their ordeal prevents victims from reporting these crimes and reaching out to relevant authorities for help.

### What to do to reduce the chances of being sextorted

1. Refrain from sharing intimate content with people, especially strangers you meet online
  - a. If you must do the above, make sure the photos/videos do not show your face or any other identifiable feature
2. Do not save intimate content on your devices – they could be hacked.
3. If you have a faulty device, do not leave it with the technician for repair – hang around.
4. Turn off auto sync to services such as iCloud, Google Drive, Dropbox
5. Encrypt your devices
6. Use password managers and strong passwords
7. Enable MFA on all devices and social media profiles where possible.

### What to do if you are being sextorted

1. Do not panic – know this is not your fault
2. Stop all communication with the perpetrator
3. Do not comply with their threat
4. Document the correspondence
5. Report the content/account to the relevant social media website
6. Report to the police – sextortion is a crime in Nigeria.



#### Further reading

Brinton Resto & Aaron Minc (August 2022) How to deal with sextortion on the internet:  
<https://www.minclaw.com/internet-sextortion/>

Calli Tzani (n.d.) Sextortion leads to financial losses and psychological trauma. Here's what to look out for on dating apps: <https://theconversation.com/sextortion-leads-to-financial-losses-and-psychological-trauma>

## SEXPLOITATION



Did you give them permission to use the pictures?



Ene rolled her eyes and sighed at Nkem's question. She didn't even know those pictures were online until some of her followers brought it to her attention. Even more annoying was the fact she had only shared those photos with those on her Instagram close friends' list. Now the pictures were being used to promote a lingerie brand online, and she wasn't entirely sure where to start fighting it – lawyers are not cheap.

### SEXPLOITATION (NOUN)

*is the commercial exploitation of sex, sexuality or explicit sexual material, usually for attention or money.*

There are probably women who are genuinely aroused by the idea of being photographed naked, but it is safe to assume that many more women appear in magazines like Playboy simply because they are paid to, which is fine. However, "because I was paid to" is not the same as "I am taking control of my sexuality."

Women's bodies have historically been used in media and fashion to increase the appeal of a product to the detriment of, or without regard to, the interests of the women portrayed or women in general. However, it has taken a turn for the worse with the advent of the internet and the popularity of social media.

### How to fight exploitation

1. Keep your accounts as private as possible.
2. Use strong passwords on all devices and accounts.
3. Enable MFA for all social media accounts.
4. If sharing content with a large following, watermark your content.

#### Further reading

Female Chauvinist Pigs: Women and the rise of the raunch culture by Ariel Levy



## DEEP FAKES

Gbemi looked at the video again; she knew they were fake. She had never recorded these videos, but that was pointless. Her face was on these naked bodies, and her father's congregation would have much to say about this. The issue of the fake online profile on the hook-up site had barely died down, and here was another one .... "Am I being targeted?"

### DEEP FAKES (NOUN)

*are fake videos created using digital software, machine learning and face swapping. Deep Fakes are computer-created artificial videos in which images are combined to create new footage that depicts events, statements or actions that never actually happened. The results can be quite convincing.*

*Deep fakes differ from other forms of false information by being very difficult to identify as fraudulent.*

Deep fakes are a relatively new player in the social media scene, but this has not limited their usage by bad actors. As the world becomes more technologically advanced and the processing power required to create these fake videos becomes more available, deep fakes will soon become a significantly bigger problem.

### What can we do to prevent this?

- 1) Practice good digital hygiene
- 2) To create a convincing deep fake video, a lot of the victims' images are needed to train the AI - limit the number of pictures you have available online





## CYBER THREATS

### Types of Cybersecurity Threats

Cybersecurity threats target both individuals and devices. A large percentage of cybersecurity threats are a result of human error. A significant way people get attacked online is through social engineering. However, malicious software can be used to hack private and commercial accounts, devices and systems.

### Social Engineering Attacks

Social engineering involves tricking users into providing an entry point for malware. The victim provides sensitive information or unwittingly installs malware on their device because the attacker poses as a legitimate actor.

Here are some of the main types of social engineering attacks:

1. **Baiting** - the attacker lures a user into a social engineering trap, usually with a promise of something attractive like a gift card. The victim then provides sensitive information, such as credentials, to the attacker.
2. **Pretexting** - similar to baiting, the attacker pressures the target into giving up information under false pretences. This typically involves impersonating someone with authority, for example, a police officer, whose position will compel the victim to comply.



3. **Phishing** - the attacker sends emails pretending to come from a trusted source. Phishing often involves sending fraudulent emails to as many users as possible but can also be more targeted. For example, "spear phishing" personalises the email to target a specific user, while "whaling" takes this a step further by targeting high-value individuals such as CEOs.
4. **Vishing (voice phishing)** - the imposter places a call to trick the target into disclosing sensitive data or grant access to the target system. Vishing typically targets older individuals but can be employed against anyone.
5. **Smishing (SMS phishing)** - the attacker uses text messages to deceive the victim.
6. **Piggybacking** - an authorised user provides physical access to another individual who "piggybacks" off the user's credentials. For example, an employee may grant access to someone posing as a new employee who misplaced their credential card.
7. **Tailgating** - an unauthorised individual follows an authorised user into a location - for example, by quickly slipping through a protected door after the authorised user has opened it. This technique is similar to piggybacking, except that the person being tailgated is unaware that another individual is using them.





## MALWARE ATTACKS

Malware is an abbreviation of “malicious software”, which includes viruses, worms, trojans, spyware, and ransomware, and is the most common type of cyberattack. Malware infiltrates a system, usually via a link on an untrusted website or email or an unwanted software download. It deploys on the target system, collects sensitive data, manipulates and blocks access to network components, and may destroy data or shut down the system altogether.

Here are some of the main types of malware attacks:

1. **Viruses** - a piece of code that injects itself into an application. When the application runs, the malicious code executes.
2. **Worms** - malware that exploits software vulnerabilities and backdoors to gain access to an operating system. Once installed in the network, the worm can carry out attacks such as distributed denial of service (DDoS).
3. **Trojans** - malicious code or software that poses as an innocent program, hiding in apps, games or email attachments. An unsuspecting user downloads the trojan, allowing it to gain control of their device.
4. **Ransomware** - a user or organisation is denied access to their systems or data via encryption. The attacker typically demands that a ransom be paid for a decryption key to restore access. Still, there is no guarantee that paying the ransom will actually restore full access or functionality.





5. **Cryptojacking** - attackers deploy software on a victim's device and begin using their computing resources to generate cryptocurrency without their knowledge. Affected systems can become slow, and cryptojacking kits can affect system stability.
6. **Spyware** - a malicious actor gains access to an unsuspecting user's data, including sensitive information such as passwords and payment details. Spyware can affect desktop browsers, mobile phones and desktop applications.
7. **Adware** - a user's browsing activity is tracked to determine behaviour patterns and interests, allowing advertisers to send the user targeted advertising. Adware is related to spyware but does not involve installing software on the user's device and is not necessarily used for malicious purposes. Still, it can be used without the user's consent and compromise their privacy.
8. **Fileless malware** - no software is installed on the operating system. Native files like WMI and PowerShell are edited to enable malicious functions. This stealthy form of attack is difficult to detect (antivirus can not identify it) because the compromised files are recognised as legitimate.
9. **Rootkits** - software is injected into applications, firmware, operating system kernels or hypervisors, providing remote administrative access to a computer. The attacker can start the operating system within a compromised environment, gain complete control of the computer and deliver additional malware.





## HOW TO REPORT ABUSE ACROSS SOCIAL MEDIA

Twitter - <https://help.twitter.com/en/safety-and-security/report-abusive-behavior>

Facebook - <https://www.facebook.com/help/www/181495968648557>

Instagram - <https://help.instagram.com/192435014247952>

TikTok - <https://support.tiktok.com/en/safety-hc/report-a-problem>

Snapchat - <https://support.snapchat.com/en-US/article/report-abuse-in-app>

Youtube - <https://vidiq.com/blog/post/report-youtube-channel/>

Whatsapp - [https://faq.whatsapp.com/2798237480402991/?locale=fi\\_FI](https://faq.whatsapp.com/2798237480402991/?locale=fi_FI)

## PRACTISING GOOD DIGITAL HYGIENE

Good digital hygiene keeps your devices running smoothly and allows you to use them more efficiently. More importantly, it protects you from the ever-growing list of online threats. Poor digital hygiene makes it easier for people to attack you with phishing scams, malware attacks, and other online crimes. It puts your privacy, and potentially the privacy of those you care about, at risk.

1. Use strong passwords.
2. Use a password manager.
3. Use MFA or 2FA.
4. Use an antivirus.
5. Keep your operating systems & other software updated to get the
6. latest security patches.
7. Delete unused software.
8. Regularly review social media accounts' security settings.
9. Regularly review & organise emails (unsubscribe from & block
10. unwanted senders if necessary).
11. Regularly backup your files.
12. Only download software from trusted channels.
13. Use a VPN when possible.
14. Periodically review your information on sites you have signed up to. Delete accounts where necessary.
15. Do not use the same passwords for your social media or email accounts



## GLOSSARY OF TERMS & ABBREVIATIONS

**Blackhat** - A hacker who infiltrates a system or device for malicious purposes

**Dox** - To publish identifying information about a user.

**Encrypt** - To convert data into a code, especially to prevent unauthorised access

**IPV** - Intimate Partner Violence

**LGBTQ** - Lesbian Gay Bisexual Transgender Queer

**Malware** - A malicious program

**MFA** - Multi-factor authentication

**OGBV** - Online gender-based violence

**Power Shell** - A scripting language used for managing Microsoft environments

**TFGVBV** - Technology-facilitated gender-based violence

**VPN** - Virtual Private Network (Provides a layer of anonymity and encryption)

**WMI** - Windows Management Instrumentation

**2FA** - Two-factor authentication

