MODULE 4

PROMOTING DIGITAL SAFETY

PUBLICATION DETAILS PAGE

First published in March 2020

PUBLISHED BY :
MinorMatters an initiative by the National Christian Evangelical Alliance of Sri Lanka

WEB : **www.minormatters.org**

EDITOR: Nalaka Gunawardene

PROJECT COORDINATION BY:

Yamini Ravindran, *Director, Legal and Advocacy*
Shalomi Daniel, *Legal and Advocacy Coordinator, Religious Liberty & Social Justice Commission*
Akshina Palihawadana, *Media Strategy Officer, Religious Liberty & Social Justice Commission*

COVER DESIGN: Sanjayan Ariadurai

PAGE LAYOUT AND DESIGN: Shenal Jesudian

PROMOTING DIGITAL SAFETY

As noted earlier, cybersecurity is about systems and devices; cyber safety is about people who use them.

This module covers the basics of digital and cyber safety, i.e. the personal safety of human beings when they use digital technologies and web services.

Many people equate security with safety. But the two concepts are not the same. It is important to understand the difference.

A common approach is to secure digital devices, data and even digital identity. All this is necessary -- but not sufficient. Safety is addressed only when the needs and realities of human users are factored in.

To be safe can mean to be secure, but to be secure does not necessarily mean a person is safe. The ways we talk about safety and security are important as we think about the healthy digital ecosystem we hope to create.

To create a healthy digital ecosystem, we need to promote qualities like trust, good relationships and collaborations. We also need progressive laws and regulations as well as effective law enforcement.

Research that analyses and identifies key trends and recommends policy and regulatory responses provides the knowledge base for such action.

Collaborations can emerge from alliances between the tech industry, law enforcement agencies, civil society groups and individual users.

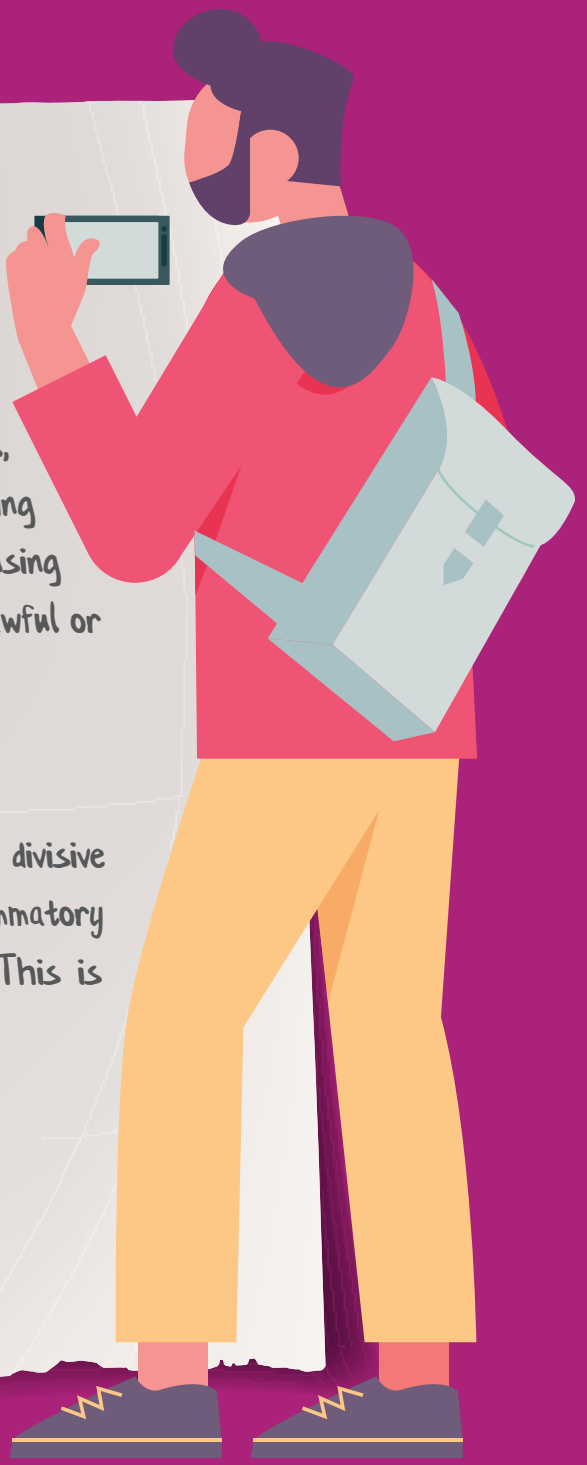
KEY TERMS

Cyberbullying: Cyberbullying is bullying that takes place over digital devices like mobile phones, computers, and tablets. It can occur through SMS and apps, or online in social media, forums or gaming where people can view, participate in, or share content. Cyberbullying includes sending, posting or sharing negative, harmful, false or mean content about someone else. It can include sharing personal or private information about someone else causing embarrassment or humiliation. Some cyberbullying crosses into unlawful or criminal behaviour.

Source: https://www.stopbullying.gov/cyberbullying/what-is-it/index.html

Troll is a member of an internet community who posts offensive, divisive and controversial comments. Often, a troll will make obviously inflammatory statements that are meant to bait other users into reacting. This is called trolling.

Source: https://www.techopedia.com/definition/429/troll v



DIGITAL SAFETY AND HUMAN RIGHTS

We need to approach digital safety based on human rights: everyone, everywhere has a right to a safe and secure internet experience without any discrimination or harassment.

As mentioned in Module 1, the same human rights that people have offline must also be protected online.

The relevant human rights includes online aspects of the following: right to freedom of expression (which includes the right to information); right to privacy and data protection; rights of people with disabilities; and gender rights.

These rights are cross-cutting and interlinked. For example, the freedom of expression and information is related to access to the internet and net neutrality. Protection of minority rights is influenced by multilingualism and promotion of cultural diversity. Ensuring the protection of privacy is important in dealing with cybersecurity as well as cyber safety.

[1] Net neutrality is the principle that internet service providers (ISPs) must treat all internet communications equally, and not discriminate or charge differently based on user, content, website, platform, application, type of equipment or method of communication. More: https://www.eff.org/issues/net-neutrality

TECHNOLOGY-RELATED VIOLENCE AGAINST WOMEN

Digital safety is a concern for everyone who uses digital technologies. However, as women and children are disproportionately targeted online for harassment and cyber exploitation, their needs merit priority attention.

The Association for Progressive Communications (APC), a global network of civil society organizations, works to strengthen women's rights activists to use technology tools in their work. When it comes to violence against women, they highlight how that violence is increasingly linked to technology.

According to APC, the most common cases of technology-related violence against women are cyberstalking, sexual harassment, surveillance and the unauthorized manipulation of women's personal information including images and videos.

Even as these violations are rising, many women and girls who fall victim do not know what to do to stop the abuse, what they can report to whom, and what help they can expect.

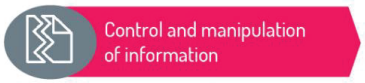
Many countries do not yet have policies, regulations or services to respond to these new forms of violence, or they are inadequate. Together with Mexican campaigners Luchadoras and SocialTic, APC has developed a longer list of 13 types of online gender-based violence.

For a more detailed discussion on human rights online, see:
[2]https://dig.watch/baskets/human-rights
[3] https://www.genderit.org/resources/13-manifestations-gender-based-violence-using-technology

https://www.genderit.org/resources/13-manifestations-gender-based-violence-using-technology

Unauthorised access and controlling access

Unauthorised attacks to gain access to a person's accounts or devices. These can imply unauthorised information gathering and/or blocking access to a person's account.

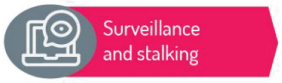


Control and manipulation of information

Information gathering or theft that can imply a loss of control over such information, and any unauthorised attempt at modifying it.

Impersonation and identity theft

The use or forgery of someone's identity without their consent.

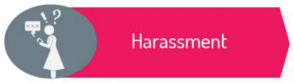


Surveillance and stalking

The constant monitoring of a person's activities, everyday life, or information (be it public or private).

Discriminatory speech

Speech reflecting cultural models that assign women and gender-non-conforming bodies a secondary, sexualised or strictly reproductive role. Such speech may or may not incite violence.

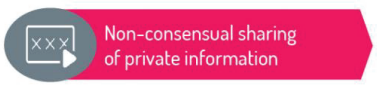


Harassment

Repeated and unsolicited acts against a person that are perceived as intrusive, disturbing or threatening. These acts may or may not be sexualised.

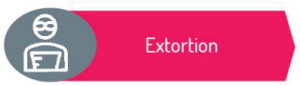
Threats

Speech and content (verbal or written, in images, etc.) with a violent, sexually aggressive or threatening tone that express an intention to harm a person, their family or friends, or their belongings.



Non-consensual sharing of private information

The unauthorised sharing or publication of any kind of information, data or private details regarding a person.



Extortion

Forcing a person to act according to another persons' will, through threats and intimidation regarding something of value (e.g. personal information, intimate images, etc.)

Disparagement

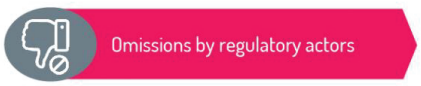
Defamation, smearing and/or undermining of the credibility, professional career, work or public image of a person, group or initiative, through the spreading of false, manipulated or off-topic information.

Technology-related sexual abuse and exploitation

The act of exercising power over someone based on the sexual exploitation of their pictures and/or body against their will, where technology is a fundamental means.

Attacks on communications channels

Deliberate tactics and actions aimed at putting a person's or group's communication or information channels out of circulation.



Omissions by regulatory actors

Contempt or lack of interest, acknowledgment or action by actors (authorities, internet intermediaries, institutions, communities) who have the possibility of regulating, resolving, and/or penalising technology-related assaults.

13 MANIFESTATIONS OF GENDER-BASED VIOLENCE USING TECHNOLOGY

CYBER EXPLOITATION AND VIOLENCE

Cyber exploitation and violence (CEV) is the use of ICTs to bully, blackmail, harass, victimize, stigmatize, discriminate, coerce or in any way cause harm to a person's mental, physical or emotional well-being.

CEV can manifest itself in many ways, according to the Bakamoono.lk website managed by the Grassrooted Trust, a Lankan organization working on creating safe spaces for marginalized communities both online and in the real world.

- **Trolling** (in terms of the internet) is the deliberate act of someone making random unsolicited and/or controversial comments online – usually to provoke an emotional reaction from readers to engage in an argument.

- **Cyberstalking** is a criminal practice where an individual uses the internet to systematically harass or threaten someone. This crime can be perpetrated through email, social media, chat rooms, instant messaging and any other online medium. Cyberstalking can also occur alongside offline stalking.

- **Identity theft** is the unauthorized collection of personal information and its subsequent misuse to open credit cards and bank accounts, redirect mail, obtain a mobile phone subscription, etc. Impersonating another person online or offline is a criminal activity.

- **Cyberbullying** is when someone bullies or harasses others on social media. Harmful bullying behaviour can include posting rumours, threats, sexual remarks, publishing a victim's personal information or use of racist or sexual insults (hate speech).

- **Revenge Porn** (also known as Girlfriend Porn, or Collecting and Exchanging Nudes, or Slut Shaming) involves pictures and videos of a sexual nature being shared online by former partners who have since fallen out and are now using such material – once exchanged in confidence - for public revenge.

There have been very few studies on CEV in the Sri Lankan context, even though anecdotal evidence suggests that the issues are very much present in society. A recent study conducted jointly by researchers from three advocacy groups -- the Centre for Policy Alternatives (CPA), Ghosha and Hashtag Generation – looked at how women are discussed on Facebook, the most popular social media platform in Sri Lanka with over 6 million monthly active users.

Their report includes findings from focus group discussions conducted with members of the Lesbian, Bisexual and Transgender (LGBT) community on their experiences relating to technology-based violence, as well as views gathered through interviews with female politicians and activists outside Colombo.

Researchers in this study monitored 52 Facebook accounts over a period of 6 months in English, Sinhala and Tamil. Apart from meme pages and public Facebook groups dedicated to specific special interests or hobbies, the pages monitored included those of public figures such as politicians and local celebrities. The study notes: "What emerged was a clear pattern of speech that was sexist, or objectified, harassed or otherwise targeted women and members of the LGBT community. The non-consensual dissemination of intimate photos and videos was another disturbing trend found in the lead-up to this study, with entire pages dedicated to such content, or alternatively linking to such content on third-party websites. The findings of this report indicate the normalisation of sexist commentary, escalating to and including violence against women and LGBT communities, both online and offline."

This study has highlighted the culture of sexism and misogyny that exists on Facebook which was common across Sinhala, Tamil and English languages. Researchers believe this is an extension of the casual sexism that already exists on Facebook and in Lankan culture in general. This is often packaged (and justified) as 'humour'. There were also instances where the page or poster seemingly defends women whilst, in fact, propagating violence against them.

The internet's anonymity is being exploited by many followers or commentators using fake identities, the researchers found – this makes it difficult to report such pages to Facebook administrators. The study also discovered that those involved have found ways to work around Facebook's community standards, using tactics such as posting only links, or placing text over images, or only liking posts without sharing them.

[4] https://groundviews.org/2019/06/27/opinions-btch-technology-based-violence-against-women-in-sri-lanka/

"OUR RESPONSE AS PARENTS, TEACHERS, AND CONCERNED ADULTS, CANNOT BE TO BAN THE USE OF SOCIAL MEDIA, OR THE USE OF HANDHELD ONLINE DEVICES. THE BENEFIT OF BEING ONLINE IN TERMS OF KNOWLEDGE GATHERING AND KNOWLEDGE SHARING IS IMMEASURABLE. THE ONLINE WORLD IS ANOTHER SPACE WHERE WE COMMUNICATE WITH EACH OTHER, WHERE WE BUILD RELATIONSHIPS. WE MUST BE CONSCIOUS OF RESPECT FOR SELF, RESPECT FOR THE OTHER, AND RESPECT FOR DIFFERENCE IN ALL OUR INTERACTIONS, BOTH ONLINE AND OFF IT." –

BAKAMOONO.LK

"IT IS INCREASINGLY POSSIBLE TO CHALLENGE THE FALSE DICHOTOMY OF ONLINE VS. OFFLINE VIOLENCE. TECHNOLOGY-RELATED VIOLENCE DOES NOT EXIST IN ISOLATION AND IS AN EXTENSION, AND OFTEN FORMS AN INTEGRAL PART OF, THE VIOLENCE EXPERIENCED BY WOMEN, GIRLS AND LGBT PEOPLE... TECHNOLOGY-RELATED VIOLENCE DOES NOT OCCUR ENTIRELY ON THE INTERNET – TEXT MESSAGES OR PHONE CALLS ALSO FALL INTO THE SPECTRUM. THE CONSEQUENCES, SUCH AS VIOLATIONS OF WOMEN'S RIGHT TO PRIVACY, EDUCATION, WORK AND HEALTH, DO NOT EXIST SOLELY ONLINE. THE SAME DISCRIMINATIONS, VIOLATIONS AND SURVEILLANCE FACED IN PUBLIC AND PRIVATE SPHERES ARE REPLICATED ONLINE AND IN SOME CASES, EXACERBATED." –

OPINIONS, B*TCH: TECHNOLOGY-BASED VIOLENCE AGAINST WOMEN IN SRI LANKA (CPA, Ghosha and Hashtag Generation, 2019)

SOCIAL MEDIA COMMUNITY STANDARDS

All key social media platforms have rules for their users. These are widely known as community standards. Everyone agrees to abide by these rules when starting an account.

For example, the world's largest social media network Facebook had 2.38 billion monthly active users as of 31 March 2019. These users generate or react to billions of items of content every day and night. For the most part this global chatter is harmless. But not everyone plays by the rules. Facebook's Community Standards outline what is allowed or not on their platform. See: https://www.facebook.com/communitystandards/

"The goal of our Community Standards is to encourage expression and create a safe environment. We base our policies on input from our community and from experts in fields such as technology and public safety," says its introduction.

Facebook says its rules are built around three pillars: Safety (removing content that harms others), Voice (the ability for users to express diverse views and ideas), and Equity (applying the same standards to all users).

The rules don't allow content that encourages violence or criminal behaviour including terrorist and hate groups, human trafficking and organized crime. It also forbids trading in "regulated goods" like drugs or firearms. Facebook will remove posts that encourage self-harm or suicide, and those involving sexual exploitation (of children or adults).

Additionally, the rules list content deemed objectionable, which includes graphic violence and hate speech, defined as "a direct attack on people based on what we call protected characteristics — race, ethnicity, national origin, religious affiliation, sexual orientation, sex, gender, gender identity, and serious disability or disease."

Rule breakers face consequences. First breach could draw a warning, and repeated violations can lead to restrictions in the user's ability to post. Serial offenders will see their profile (account) disabled. "We may also notify law enforcement when we believe that there is a genuine risk of physical harm or a direct threat to public safety," say the rules.

Other platforms like Instagram, YouTube and Twitter also have their own rules. We encourage you to read and understand these rules which are attempts to self-regulate social media.

HOW TO REACT TO CYBER EXPLOITATION AND VIOLENCE

Raising awareness and promoting user level precautions are the first steps.

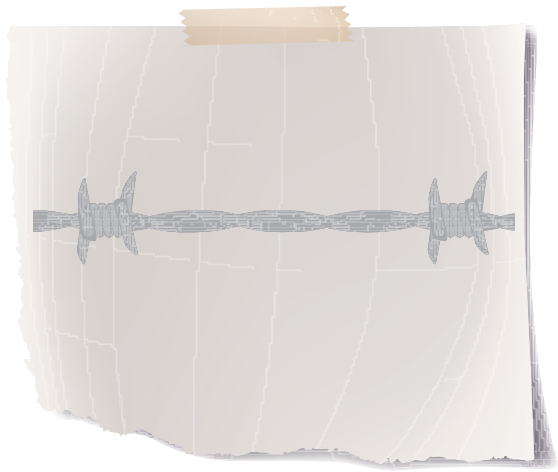
There are many helpful online resources as well as campaigns and self-help groups. Here are two international examples:

- **Take Back The Tech!** is an initiative by APC. It is a call to everyone, especially women and girls, to take control of technology to end violence against women. It's a global, collaborative campaign project that highlights the problem of tech-related violence against women, together with research and solutions from different parts of the world. The campaign offers safety roadmaps and information and provides an avenue for taking action. Take Back the Tech! leads several campaigns at various points in the year, but thier biggest annual campaign takes place during 16 Days of Activism Against Gender-Based Violence (25 November to 10 December). https://www.takebackthetech.net/

- **Safer Internet Day (SID)** is an international day of awareness for the risks involved in using the internet. Originally created in 2004 by the European Union, it is observed on the second day of the second week of February each year. SID has become a landmark event in the online safety calendar. It is now celebrated in approximately 140 countries worldwide. From cyberbullying to social networking, each year Safer Internet Day aims to raise awareness of emerging online issues and chooses a topic reflecting current concerns.
https://www.saferinternetday.org/

In Sri Lanka, several civil society and advocacy groups offer information, advice or support that are related to digital safety and/or digital responsibility.

- **The Grassrooted Trust** was set up to provide a safe space for marginalized communities, online and in the real world. http://www.grassrooted.net/
- **Bakamoono.lk** is a trilingual website managed by the Grassrooted Trust and its partners. Its work is focused on issues related to sex and relationships and includes information on consent, gender, cyber exploitation and violence. http://www.bakamoono.lk/en
- **Women in Need (WIN)** is dedicated to addressing issues of gender based violence faced by women and girls in Sri Lanka. It has a team of lawyers and counsellors. https://www.winsl.net/
- **Shilpa Sayura** Foundation promotes responsible ICT use by youth. It implements the 'Respect Girls on Internet', a voluntary initiative to address cyber harassment of girls on social networks (see also Case Study 1 in this module) http://www.shilpasayura.org



[5] http://counterpoint.lk/violence-is-violence-offline-or-online/

HOW TO REPORT CASES OF CYBER EXPLOITATION AND VIOLENCE

Three state institutions are involved in the official responses to cyber harassment:

- National Child Protection Authority (NCPA) leads the response for victims and perpetrators under 18.
- Cyber Crimes Division of the Police Criminal Investigation Department (CID) handles the matter if victims are over 18.
- Sri Lanka Computer Emergency and Readiness Team (SL-CERT) also records complaints they receive, and refers to both the CID Cyber Crimes and NCPA response mechanisms.

The NCPA is also working with policy makers to review and strengthen our existing laws for responding to all forms of child abuse, including CEV.

If a picture or video of you, or someone you know is online, e.g. on a website, inform Sri Lanka CERT on 011 2 691 692 immediately. If you do not receive the support you need and/or expected, get in touch with Women in Need on 011 471 85 85 to report the incident.

If the victim is over 18, you may also contact the CID Cyber Crime Unit directly on 011 232 6979 and email details of the incident to BOTH <dir.cid@police.lk> and <telligp@police.lk>

if the victim is under 18, approach the National Child Protection Authority on their hotline 1929 or visit their website: http://www.childprotection.gov.lk/

Here are some tips shared by the Grassrooted Trust on its website with regard to preserving evidence and information.

- If you are being blackmailed, ensure that any communications with the perpetrator are not deleted regardless of the platform that it is on. The police may require you hand in your phone to confirm the evidence first hand, ensure it is not doctored, etc. This could include messages, call logs, etc.
- We recommend for your records and information you take and store screenshots as well, as with some platforms like Instagram, Direct Messages can be unsent. When you make a complaint to the police speak to your lawyer or the person who accompanies you about asking if the police can take the screenshots on their computer or to certify the validity of the screenshots taken.
- If a phone is being handed over to the Police, you should have saved screenshots of all evidence. Ideally, you should create a list of all related material that can be found on the phone and give a copy of it along with the phone so that there is a clear acknowledgment of what was given.
- Keep a record of everything that has happened, for example if threatening phone calls/texts were received over the period of time, you should keep a written note of dates/times or approximate date/times and nature of the call/text. Keeping a chronological account is helpful when making a police complaint, will help them remember the order of events, and be clearer and more consistent when you are giving evidence or making a complaint.

[6] http://www.bakamoono.lk/en/article/2600/how-to-report-cases-of-cyber-exploitation-and-violence

LEGAL PROTECTION AGAINST CYBER HARASSMENT

Up to mid-2019, Sri Lanka did not have specific laws that criminalize cyber harassment.

However, some sections of the Penal Code could be used to address some aspects of it:

- Section 345 deals with sexual harassment (defining it as the use of words or actions to cause annoyance or harassment to a person)
- Section 372 deals with extortion (defining it as the intentional act of putting another person in fear of injury, inducing a person to deliver property or valuable security)
- Section 483 addresses criminal intimidation or threatening a person to act or omit an action in order to avoid some sort of punishment.

Of these, sections 372 and 483 can be used to tackle blackmail over the sharing of personal photos or videos captured using digital media and/or stored online.

Under the Obscene Publications Act (of 1927 and later amendments), the sharing personal, intimate images without consent, or sharing of images which have been explicitly altered using editing software, can be challenged. Section 2 of this Act makes it offences to possess, distribute or publicly exhibit of "obscene photographs".

In the Payment Devices Frauds Act (No 30 of 2006) section 3 (r) makes it an offence to obtain money or goods through a payment device with intent to defraud -- this can be used to tackle blackmail.

Section 7 of the Computer Crimes Act No 24 of 2007 makes it an offense for people to obtain information from a computer or a storage medium of a computer without permission. It also criminalizes downloading, uploading or making copies of such illegally acquired content.

DESPITE THESE LEGAL PROVISIONS, IT IS NOT EASY FOR VICTIMS TO ACCESS JUSTICE FOR CRIMES COMMITTED AGAINST THEM ONLINE. MOST VICTIMS DO NOT PURSUE LEGAL ACTION DUE TO FLAWS IN THE SYSTEM OF REPORTING ONLINE VIOLENCE TO AUTHORITIES. IN ADDITION, NOT ALL SURVIVORS MIGHT BE ABLE TO AFFORD LAWYERS TO SUPPORT THEMSELVES.

CASE STUDIES

CASE STUDY 1: RESPECT GIRLS ON INTERNET

A few years ago, Poornima Meegammana was busy preparing for her GCE Advanced Level (university entrance) exam. The day before the exam was to start, she received some 'really nasty' messages -- seemingly from a trusted male friend's Facebook account.

"I was stunned by these messages and didn't know what to make of them. I least expected such a thing from this friend, and I was psychologically very affected. It was only later that I found out that someone else – also known to both of us – had accessed my friend's account without authorisation and sent those messages."

Poornima coped with the trauma with the understanding and support from her family and close friends. But she realised that the phenomenon was widespread and how girls and women were especially being targeted.

Turning her bitter experience into a positive action, she founded 'Respect Girls on Internet', a voluntary initiative to address cyber harassment of girls on social networks, including extreme cases of self-harm. The effort is anchored within the non-profit Shilpa Sayura Foundation.

Poornima says many teenagers typically start using the internet without any knowledge about cyber safety or privacy. Young persons who experience cyber bullying tend to withdraw from social life and digital activities while the physical and/or psychological effects impact their studies or work.

"There are laws and procedures for protection, but there is a lack of awareness, advice and resources available – especially in local languages -- for victims to seek justice. Respect Girls project creates digital content to raise awareness about the problem, advocate for safe and respectful online discourse and promote empathy. One of the project's key outputs is a Cyber Privacy e-Handbook for teenagers new online, as well as for teachers and parents.
Respect Girls also acts as a network of youth for preventing cyber harassment, and as a support group for victims.

In 2017, the Internet Society selected Poornima for a 25Under25 Award recognising young people around the world who are taking action and using the Internet as a force for good.

More: http://respect-girls-on-internet.blogspot.com/
https://www.internetsociety.org/25th/25-under-25/awardees
https://www.bbc.com/sinhala/sri-lanka-41218095

CASE STUDY 2: REVENGE PORN IN SRI LANKA

'Revenge porn' is a commonly used term for the non-consensual distribution or publication of intimate images or videos online. This practice has been growing in Sri Lanka, even though most victims choose not to report or seek legal help.

Feminist activist and researcher Sharanya Sekaram from the Grassrooted Trust describes one of the many revenge porn networks her organization had unearthed in their research: a WhatsApp group, and to be a part of the group each individual had to submit five explicit pictures of nude females.

"The question is: what has made these boys come to consider a naked picture as some form of currency? How do they think they have ownership over these?" she asks.

She relates another incident in which a girl had been asked by an ex-boyfriend to "get on video call" and "please" him, or risk having her intimate pictures circulated. When the girl refused, the perpetrator had responded saying that she had better consent if she values her life, because once her pictures are released, her life would be ruined.

"This shows that the perpetrators are often perfectly aware of the repercussions their victims will face if these explicit images or videos are ever released. They know how our society works and where the blame will invariably lie. They know what damage they can do."

Sharanya believes that the problem is one rooted in culture, patriarchal notions and societal attitudes rather than technology. She says revenge porn should be viewed through the same lens as intimate partner violence and gender-based violence.

"People view online violence as an isolated problem, but they haven't been connecting the dots," she says. She adds that existing laws in Sri Lanka can be invoked when reporting such crimes, e.g. Section II of the Obscene Publications Act deals with the distribution, exhibition, and possession of obscene images.

However, public institutions with the mandate to act are ineffective, and victims are often treated with insensitivity – discouraging those who seek justice. The widespread culture of victim-shaming, which blames the victim rather than the perpetrator, also makes victims reluctant to come forward.

Adapted from: https://roar.media/english/life/in-the-know/cyber-exploitation-and-violence-the-darker-side-of-cyberspace/

DISCUSSION POINTS

Here are a few questions and discussion points for further exploring this topic.

- How much can a user take precautions to guard herself against cyber harassment, exploitation and online violence? What user level actions are possible and practicable?
- "Online violence against women is an overt expression of the gender discrimination and inequality that exists offline." Do you agree or disagree? Discuss.
- Digital and cyber safety are major concerns for children and women, but other marginalized groups are also vulnerable. Who or what are these groups? In what ways are they targeted online?
- Consensual sharing of intimate photos and videos between two persons in a relationship has become easier with smartphones and the web. Is this an inherently unsafe practice? What precautions are possible and advisable? Discuss.
- Don't feed the trolls! As they thrive on attention and engagement, the best way to discourage trolls is to ignore them. But it doesn't always work, so what other actions can be taken?
- The internet's anonymity is being exploited by those who engage in cyber harassment as they use fake identities. Should everyone be compelled to use online services only under their real identity? What implications can such a requirement have for vulnerable groups?

- Recent research found a culture of sexism and misogyny that exists on Lankan pages of Facebook which was common across all three languages. Is this a reflection of offline society? Is Facebook a mirror of our society?

- Have you reported about any problematic content to a social media platform like Facebook? If so, what was your experience?

- What do you think of community standards of social media platforms: are they adequate? Is there proper monitoring by the platforms? What more can be done?

- Why is it so difficult for victims to access justice for crimes committed against them online? How can law enforcement and justice process be more supportive and sensitive?

- Does Sri Lanka need new laws to strengthen digital and cyber safety? Or is it more a case of properly enforcing existing laws and increasing proactive action to tackle rising levels of cyber exploitation? Discuss.

LEARNING OUTCOMES

By the end of this module, you will have an understanding of the following:

- To create healthy digital ecosystem, we need to promote qualities like trust, goodwill, good relationships and collaborations. We also need progressive laws, regulations and effective law enforcement.
- Internet and digital safety are concerns for everyone who uses these technologies. Cyber exploitation and violence threaten this safety.
- Preventing technology-related violence against women is an important component in ending violence against women in general: it contributes to creating a safe and secure environment for women and girls in every sphere of life.
- Facebook and other social media platforms, as they are used in Sri Lanka, are a reflection of disparities and inequalities that exist in society. For example: the culture of sexism and misogyny.
- All major social media platforms have their own rules, known as community standards. However, violators keep finding ways to get around these rules. Stronger vigilance and action are needed by both platforms and the user community.
- Victims of cyber exploitation and violence find it hard to access legal relief or justice. Most victims do not pursue legal action due to flaws in the system of reporting online violence to authorities.
- In this situation, it is various self-help groups and civil society organizations that offer advice, guidance and support.

FURTHER READING

Facebook Community Standards
https://www.facebook.com/communitystandards/

YouTube policies
https://www.youtube.com/yt/about/policies/

Twitter Rules
https://help.twitter.com/en/rules-and-policies/twitter-rules

Instagram Community Guidelines
https://help.instagram.com/477434105621119

Beyond the Report Button: Tackling Cyber-Violence in Sri Lanka.
A detailed discussion by Amalini De Sayrah, published on Bakamoono.lk
http://www.bakamoono.lk/en/article/2136/beyond-the-report-button-tackling-cyber-violence-in-sri-lanka

OPINIONS, B*TCH: Technology-based Violence Against Women in Sri Lanka
Centre for Policy Alternatives, Ghosha and Hashtag Generation, 2019
https://groundviews.org/2019/06/27/opinions-btch-technology-based-violence-against-women-in-sri-lanka/

Cyber-Exploitation and Violence: The Darker Side of Cyberspace.
Article by Radhia Rameez on Roar Media, April 2018
https://roar.media/english/life/in-the-know/cyber-exploitation-and-violence-the-darker-side-of-cyberspace/

Children's Rights and the Internet: From Guidelines to Practice. Unicef, 2016
https://www.unicef.org/csr/files/Childrens_Rights_and_the_Internet_Guidelines_to_Practice_Guardian_Sustainble_Business_English.pdf

Take Back the Tech! A call to take control of technology to end violence against women
https://www.takebackthetech.net/

Online gender-based violence: A submission from the Association for Progressive Communications to the UN Special Rapporteur on violence against women, its causes and consequences, November 2017
https://www.apc.org/sites/default/files/APCSubmission_UNSR_VAW_GBV.pdf