

digital safety & security

CURRICULUM

POLLICY

Contents

Overview 4

4 Pollicy Digital Safety and Security Curriculum Objectives

4 Extended Outcomes

5 Pollicy Digital Safety and Security Curriculum Components

Module 1 6

6 Digital Literacy and Critical Thinking

Module 2 10

10 Understanding digital safety and security

10 Digital safety

10 Digital security

10 Significance of Digital Safety and Security

Module 3 15

15 Understanding Online Threats

Module 4 24

24 Information Disorder

Module 5 31

31 Data Privacy and Protection

Module 6 **33**

33 Online Identity and Authentication

Module 7 **35**

35 Social Media Safety

Module 8 **37**

37 Internet Shutdown

Module 9 **41**

41 Safe Internet Browsing - Securing Your Digital Life.

Module 10 **43**

43 Mobile Device Security

Module 11 **45**

45 Secure Communication and Encryption

Module 12 **47**

47 Incident Response and Reporting

Module 13 **49**

49 Policy and Advocacy for Digital Rights and Data Governance

51 Source

Overview

Pollicy has proactively led the fight for online safety and a feminist internet for women's organizing in the continent. Our extensive work, especially through the VOTE: Women and Amplified Abuse Research during Elections in Kenya and Uganda, has highlighted the need for a multi-stakeholder approach to combatting Technology Facilitated Gender-Based Violence. As we continue to empower women from different walks of life, we have created the Pollicy Digital Safety and Security Curriculum to equip women (women in politics, human rights defenders, media practitioners, civil society actors, and young individuals) with digital skills to navigate the online world safely and in turn advocate for a safer digital environment within their communities ultimately bridging the digital divide.

Pollicy Digital Safety and Security Curriculum Objectives

The Pollicy Digital Safety and Security Curriculum (PDSSC) key objectives include:

- Empowerment Through Digital Literacy: The PDSSC aims to equip women with a strong foundation in digital literacy and technological competence. Fostering their ability to navigate the digital landscape effectively, empowers them to participate confidently in online activities creating a safe and joyful internet.
- Championing Human Rights and Online Safety: The curriculum cultivates a deep understanding of digital human rights and cybersecurity. Participants learn how to champion the cause of human rights in the online sphere and contribute to efforts that enhance online safety.
- Community Advocacy: PDSSC empowers program participants to take a leadership role in advocating for a safer online environment within their respective communities. By raising awareness and promoting best practices, they contribute to a more secure digital space.
- Capacity Strengthening: The curriculum enhances the capacity of young women and other participants to be effective leaders, educators, and advocates in the field of digital safety and security. It equips them with the knowledge and skills needed to address digital threats and promote responsible online behaviour.

Extended Outcomes

- To provide women with a solid foundation in digital literacy and technological competence.
- To empower program participants to assume leadership roles in advocating for a safer online environment within their respective communities.

The PDSSC serves as a vital resource for empowering women and the next generation of digital citizens who are capable of navigating the internet safely and advocating for a more secure online environment. This curriculum provides a structured pathway for achieving these goals, ensuring that women emerge as effective digital champions and human rights defenders.

Pollicy Digital Safety and Security Curriculum Components

1. Need and Asset assessment

- Identify knowledge gap: The needs assessment survey helps point out the specific areas where the learners lack knowledge and skills, ensuring that the training addresses these gaps effectively.
- Enhancing training: By understanding the exact needs of the learners, the trainer allocates more effort and avoids unnecessary training.
- Align with training objective: The needs assessment ensures that the training aligns with Pollicy`s strategic plan for inclusive and empowering digital access for women and minorities to ensure a safe and joyful internet.

2. Module Design

- Learning Formats: Each module offers content in various formats, catering to different learning preferences. This includes written texts, audio recordings, and video recordings with captions.
- Clear and Concise Language: The curriculum avoids complex jargon and technical terms, focusing on clear and easy-to-understand explanations. Terminologies are broken down into digestible contexts.
- Breakdown of Information: Complex topics are broken down into smaller, more manageable sections, making it easier to process the information depending on the digital literacy level.
- The primary language of instruction and content production is English. However, participants who are not conversant in English, French, and Swahili can be used during the training session.
- Participatory and Engaging: Each module contains a practical activity to engage with the learners. Refreshers will be incorporated into physical training to boost energy, break the ice, and prepare the learners for engagement.

3. Monitoring and Evaluation of Outcomes

- Assess effectiveness: Monitoring and evaluation help determine whether the training achieved its intended outcomes, such as improving digital skills or increasing confidence in using technology.
- Promote sustainability: Understanding the long-term effects of the training to design follow-up programs and ensure that the benefits of the training are sustained over time.
- Ensure accountability: Monitoring and Evaluation provide transparency and accountability to the stakeholders, partners, and participants by showing the impact of the training.

Module 1

Digital Literacy and Critical Thinking

Learning Objectives

I. Understand the importance of digital literacy in the modern age.

II. Explore the fundamentals of digital literacy, including information evaluation and online research.

III. Develop critical thinking skills for navigating the digital landscape.

IV. Engage in practical exercises to enhance digital literacy and critical thinking.

Introduction

In an era dominated by digital technology, the ability to critically evaluate information and navigate the online landscape is essential. This module focuses on digital literacy and critical thinking, empowering women to be discerning consumers and contributors in the digital world.

The Significance of Digital Literacy

Digital literacy is the ability to use, understand, and critically evaluate digital information and technology.

Digital literacy is vital for making informed decisions, staying safe online, and participating in the digital age effectively.

Benefits of Digital Literacy

To Individuals

Digital literacy equips individuals with valuable skills that can significantly enhance their personal development in various aspects:

• Improved access to information and learning opportunities: Individuals and organisations can readily access vast amounts of information online, from educational resources to professional development materials. This empowers them to learn new skills, stay updated in their field, and pursue personal interests.

• Enhanced communication & collaboration skills: Digital tools facilitate communication and collaboration across geographical boundaries. Individuals and organisations can connect with others, share information, and work on projects effectively through online platforms and applications.

• Increased productivity and efficiency: Digital literacy allows individuals and organisations to utilise tools and technologies to automate tasks, manage time effectively, and streamline workflows. This can lead to increased efficiency and productivity in various areas, such as education, work, and personal life.

• Greater access to entertainment and creative outlets: The digital world offers a vast array of entertainment options, from streaming services to online games. Additionally, digital tools can empower individuals to explore their creative potential through platforms for writing, photography, music production, and other artistic endeavours.

To Organisations

Digital literacy goes beyond personal proficiency; it holds immense value for organisations in today's tech-driven landscape. Here are the key benefits:

• Enhanced Operational Efficiency: Digital literacy empowers employees to navigate digital tools and platforms efficiently. Streamlining internal processes through digital solutions enhances overall operational efficiency.

• Improved Collaboration and Communication: Digital literacy fosters effective communication through various online channels. Collaborative platforms enable teams to work seamlessly, breaking down geographical barriers.

• Increased Productivity: Proficiency in using digital tools boosts productivity across tasks and projects. Automation and digital workflows contribute to time savings and resource optimisation.

• Access to Global Markets: Digital literacy opens doors to global markets through online presence and digital marketing. Organisations can reach a broader audience and explore new business opportunities.

• Data-Driven Decision-Making: Digital literacy enables employees to gather, analyse, and interpret data effectively. Informed decision-making based on data insights leads to better organisational strategies.

• Adaptability to Technological Changes: Digital literacy ensures that employees can adapt to evolving technologies. Organisations stay competitive by embracing technological advancements with a digitally literate workforce.

Introduction to different Types of devices

Digital devices are electronic tools designed to process and transmit data, playing a crucial role in our daily lives.

Common types of digital devices include smartphones, computers, tablets, and wearables.

Each device serves specific purposes, contributing to personal, professional, and community development.

Basic Features and Functions of Smartphones

Smartphones are handheld devices with advanced computing capabilities, combining the functions of a phone and a computer.

Key Features

• Touchscreen Interface: Allows users to interact with the device through touch gestures.

• Mobile Operating Systems: iOS, Android, and others provide the platform for applications.

• Internet Connectivity: Enables access to online resources and communication through various apps.

• Camera Functionality: Captures photos and videos for personal and professional use.

•App Ecosystem: Diverse applications cater to entertainment, productivity, and communication.

Basic Features and Functions of Computers

Computers are versatile devices used for processing and storing data, available in desktop and laptop formats.

Key Features

• Central Processing Unit (CPU): Executes instructions and performs calculations.

• Operating System: Manages hardware and software interactions.

• Storage: Hard drives or SSDs store data for long-term use.

• Input and Output Devices: Facilitate communication between users and the computer.

• Software Applications: Programs that enable specific tasks, ranging from word processing to design.

Fundamentals of Digital Literacy

- Information Evaluation: Learn how to assess the reliability and credibility of online information sources.
- Online Research Skills: Develop effective techniques for conducting research and fact-checking online.

Developing Critical Thinking

- Questioning Information: Encourage scepticism and critical questioning of information encountered online.
- Recognizing Biases: Understand how biases can influence information and media.
- Recognizing Misinformation: Identify common types of misinformation, such as fake news, and how to spot them.

Practical Exercises

1. **Participants will engage in practical exercises to enhance their digital literacy and critical thinking skills.**

- Evaluate the credibility of a set of online sources for accuracy and reliability.
- Conduct research on a specific topic and practise effective fact-checking techniques.
- Review case studies of misleading information or online misinformation and discuss strategies for critical thinking.

2. **Activity 1.1: Thinking About Your Digital Self**

   Consider how you use technology in your everyday life, like for entertainment, shopping, sharing photos, and talking to people. Think about who you connect with online and the apps or websites you use for these activities.

   Now, shift your focus to your role as an employee. Make a list or draw a diagram highlighting your digital interactions, including the groups or networks you engage with

   list or draw a diagram highlighting your digital and reflect on how digital technology is incorporated into different aspects of your work life.

   Make a list or draw a diagram of your activities, noting the groups or networks you interact with digitally and thinking about how to use digital technology into various spheres of your life.

By the end of this module, the women will have a better understanding of the importance of digital literacy and critical thinking in the digital age. They will be equipped with practical skills to critically evaluate online information and make informed decisions. The following last module will delve into advocacy for digital rights, empowering them to advocate for responsible data use and privacy protection proactively.

Module 2

Understanding digital safety and security

Learning Objectives

I. Understand the significance of digital safety and security.

II. Define key concepts and terminologies related to online security.

III. Identify the primary objectives and learning goals of this module.

IV. Explore recommended reference materials for further study.

Introduction

In an increasingly digital world, the importance of digital safety and security cannot be overstated. As technology advances, so do the threats and risks associated with the digital landscape. This module serves as an essential foundation for the “Women,” introducing participants to the critical concepts and practices necessary to navigate the online world safely.

Digital safety

Definition: Digital safety is the process of ensuring a safe and positive experience for internet users.

Sensitive information such as personal information identity and passwords are often associated with personal property and privacy and may present security concerns if leaked.

These are also termed as best practices. And it is important for the public but mostly women to be aware of these.

Digital security

Definition: Digital security is the protection of computer systems and data from unauthorised use and harm.

It encompasses the Internet, browser security, website security, and network security as it applies to other applications or operating systems as a whole.

Its objective is to establish rules and measures to use against attacks over the Internet.

These are also termed as best measures. Including VPN,2FA…

Significance of Digital Safety and Security

Digital safety and security are fundamental to protecting individuals, organisations, and societies from a wide range of online threats.

Consider the following statistics:

- In 2022, organisations worldwide identified 493.33 million ransomware incidents, making them a significant cybersecurity concern.
- Phishing, represented by roughly 3.4 billion daily spam emails, continued to hold its position as the most prevalent cyber attack.
- Furthermore, the global average cost of data breaches in 2022 reached $4.35 million while breaches arising from the theft or compromise of credentials incurred an average cost of $4.50 million during the same year.

Why is digital safety and security significant for women to benefit from the use of the internet (social media platforms)

Digital safety and security are crucial for women to fully benefit from the internet and social media platforms. It's not just about being online—it's about being online safely and confidently. That's where the real empowerment starts.

1. Connect, Collaborate, and Amplify: When women feel secure online, they are more likely to engage and connect with others. This enables them to build communities, collaborate on projects, and amplify their voices on issues that matter. Social media can be a powerful tool for advocacy and raising awareness, and safety ensures these voices are not silenced by threats or harassment.
2. Knowledge-sharing and Increased Internet Use: A secure digital environment encourages women to seek and share knowledge freely. This exchange can lead to personal and professional growth, as well as increased confidence in using technology. When safety is a given, the internet transforms into a resourceful space rather than a risky one.
3. Addressing Technology-facilitated Gender-based Violence: Sadly, online spaces can also be venues for gender-based violence. Digital safety measures protect women from harassment, stalking, and other forms of abuse. This protection allows women to advocate for their rights, share their experiences openly, and mobilise support for social change without fear of reprisal.
4. Advocacy for Rights: Digital platforms provide women with a space to campaign for equal rights and opportunities. With secure internet access, they can bring attention to issues like gender inequality, workplace discrimination, and policy changes. These platforms enable women to reach a wider audience, influence public opinion, and put pressure on authorities to take action.
5. Sharing Experiences: When women share their personal stories and experiences, they help to break down stigma and build a sense of solidarity. These narratives can empower others who may be facing similar challenges and encourage them to speak out. It also raises awareness among those who might not understand the issues firsthand.
6. Mobilising Support for Social Change: Secure and inclusive digital spaces allow women to organise and participate in movements for social change. Whether it's through petitions, social media campaigns, or virtual gatherings, these platforms help to galvanise support and coordinate collective actions. By mobilising online communities, women can drive significant societal changes.

The internet, when safe and accessible, becomes a powerful tool for advocacy, storytelling, and activism, amplifying the impact of women's voices.

All these cybersecurity concerns highlight the growing importance of digital safety.

To navigate the realm of digital safety and security effectively, it's important to be familiar with key concepts and terminologies.

Key Concepts and Terminologies

Digital safety is the foundation of your online well-being. It involves practices and strategies to navigate online safely with your personal information, identity, and digital well-being while navigating the online landscape. Here are some essential aspects of digital safety:

- **Cybersecurity:** The practice of protecting systems, networks, and data from digital attacks or unauthorised access.
- **Insider Threat:** Security risks posed by individuals within an organisation who have access to sensitive information and may misuse it.
- **Vulnerabilities:** Weaknesses in digital systems that can be exploited by threats.
- **Data Privacy:** The protection of personal and sensitive information from unauthorised access or use.
- **Authentication:** The process of verifying the identity of users, typically through passwords, biometrics, or multi-factor authentication.
- **Social Engineering:** Manipulating individuals into revealing confidential information or performing actions that may compromise security.
- **Zero-day Vulnerability:** A security flaw in software or hardware that is unknown to the vendor and, therefore, has not been patched.
- **Network Security:** The practice of protecting the integrity and usability of a network infrastructure, which includes devices, data, and communication channels.
- **Penetration Testing:** Ethical hacking is conducted to identify and exploit vulnerabilities in a system or network to assess its security.
- **Data Breach:** Unauthorised access, disclosure, or acquisition of sensitive data, often resulting in the exposure of personal or confidential information.
- **Security Policy:** A set of rules and guidelines that define how an organisation or individual will protect digital assets and respond to security incidents.
- **Cyber Hygiene:** Best practices and habits individuals and organisations follow to maintain good digital security, such as regularly updating software and using strong passwords.

Digital security focuses on protecting digital assets, systems, and networks from a wide range of cyber threats. It involves protecting computers, devices, and the data they contain from unauthorised access, damage, or theft. Here are some fundamental aspects of digital security:

Threats: These are potential dangers or risks to digital systems, including malware, phishing, and hacking.

Incident Response: A structured approach to addressing and managing the aftermath of a security breach or incident.

Encryption: The process of converting data into a code to prevent unauthorised access. It helps protect data confidentiality.

Firewall: A network security device or software that monitors and filters incoming and outgoing network traffic to prevent unauthorised access or malicious activity.

Patch or Update: Regularly releasing and applying patches or updates to software and systems to fix known vulnerabilities and improve security.

Phishing: A type of cyber-attack that involves tricking individuals into revealing sensitive information, often through fraudulent emails or websites.

Two-factor authentication (2FA) and Multi-Factor Authentication (MFA): Enhanced security measures that require users to provide two or more forms of verification to access an account or system.

Computer Worm: A computer worm is a form of malicious software that reproduces itself with the purpose of spreading to other computers.

Vulnerability: A vulnerability denotes a weakness in a system that can make it susceptible to attacks.

Two-Factor Authentication: Two-factor authentication (2FA), often referred to as two-step verification, is a security procedure where the user provides two authentication factors to confirm their identity.

Trojan: A Trojan, also known as a Trojan horse, is a type of malicious software created by hackers to masquerade as legitimate software, enabling access to a target user's systems.

Spyware: Spyware is a category of software that instals itself on a device and covertly observes a victim's online activities.

Ransomware: Ransomware is a form of malicious software designed to block access to a computer system until a ransom is paid.

Malware: Malware, short for malicious software, is crafted to inflict harm on a computer, server, or computer network.

N/B: New concepts and terminology may emerge over time as technology and threats evolve.

Recommended Reference Materials

Global

- Website: StaySafeOnline.org - A resource provided by the National Cyber Security Alliance with tips and information on staying safe online.
- Field manual: PEN America has an online harassment field manual for anyone who is active online to find useful tools and resources for navigating online abuse and tightening digital safety.

Local

- Toolkit: The Internet Society of Uganda Chapter, a part of the Internet Society, has a toolkit, titled 'E-Safety Education Toolkit', to help young Ugandans navigate and stay safe online.

This module sets the stage for a deeper exploration of digital safety and security. In the next modules, we will delve into specific threats, vulnerabilities, and strategies for protection.

Read

1. Securing your digital life like a normal person.
2. Sign up: Join Advocacy Assembly, the world's only free online training platform for human rights activists, campaigners and journalists. To enrol, Click on **'Courses'** to find the online multimedia courses 'Staying safe online and using social media' and 'Secure Communications' by Security First. Send us your certificate: After completing the 2 courses (20 minutes), click on **'View certificate'**, download the pdf.

Module 3

Understanding Online Threats

Learning Objectives

I. Identify and classify common online threats.

II. Understand the motivations and tactics of cybercriminals.

III. Recognize the importance of proactive threat awareness.

IV. Explore practical exercises and case studies to illustrate real-world threats.

Introduction

As we navigate the digital landscape, it's essential to be aware of the threats that lurk in the online world. Cybercriminals are constantly devising new tactics to compromise digital security. This module is designed to help women understand various types of online threats, their motivations, and tactics. By recognizing and understanding these threats, you'll be better equipped to protect yourself and others.

Definition of OGBV

Online abuse refers to a broad range of harmful behaviours, including harassment, bullying, hate speech, and defamation. It can take various forms such as persistent derogatory comments, spreading false information, and cyberstalking. The goal is usually to demean, belittle, or cause emotional distress.

Online threats, on the other hand, involve specific warnings of harm or violence directed towards an individual or group. These can include threats of physical harm, sexual violence, or other forms of danger. The intent is often to instil fear and intimidate the victim.

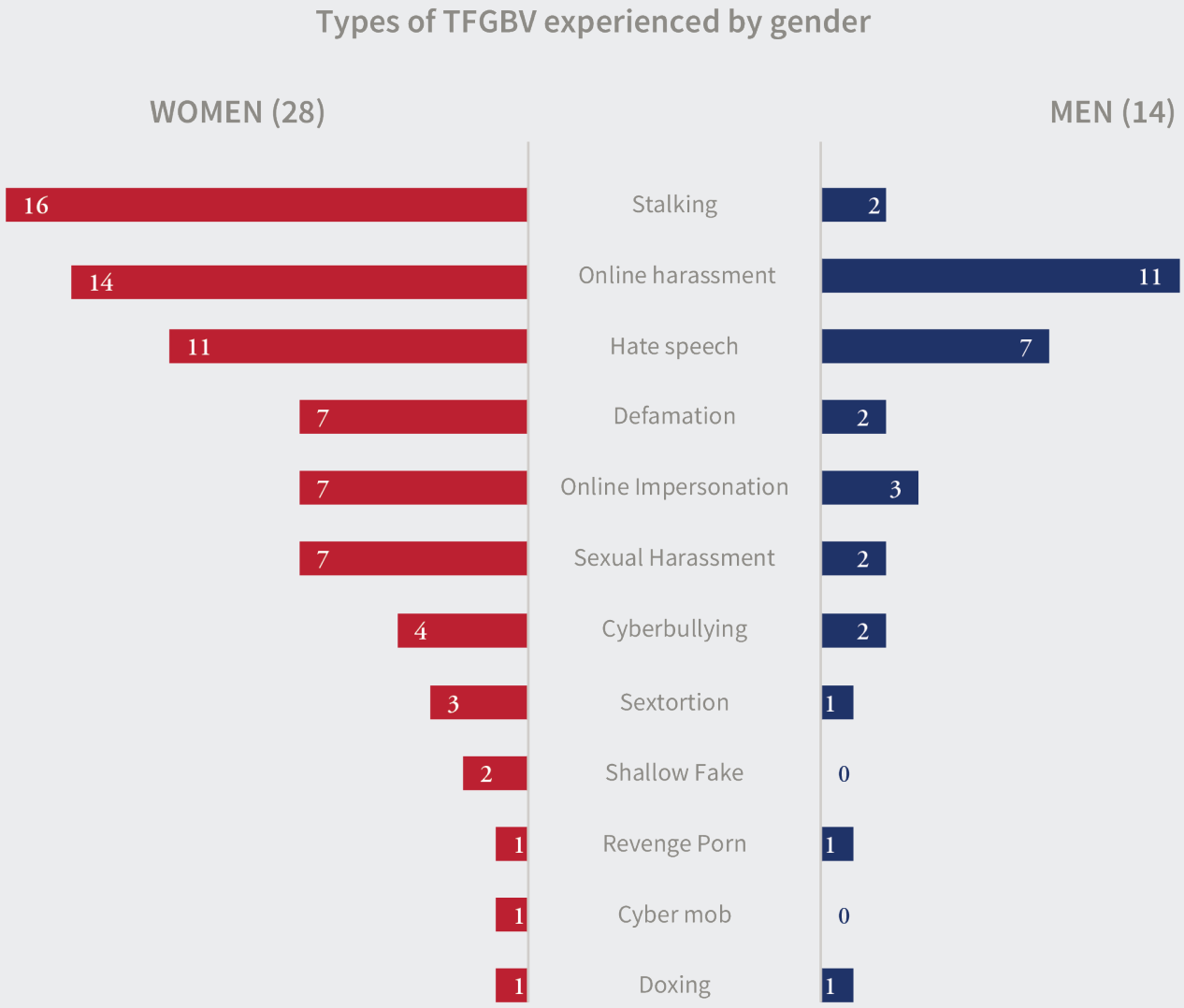
Online gender-based violence is a form of harassment and discrimination against people, especially women, based on their gender, that takes place in online spaces.

TFGBV

Technology-facilitated gender-based violence (TFGBV) refers to acts of violence that are committed, assisted, aggravated, or amplified through the use of information and communication technologies or digital media, targeting individuals based on their gender.

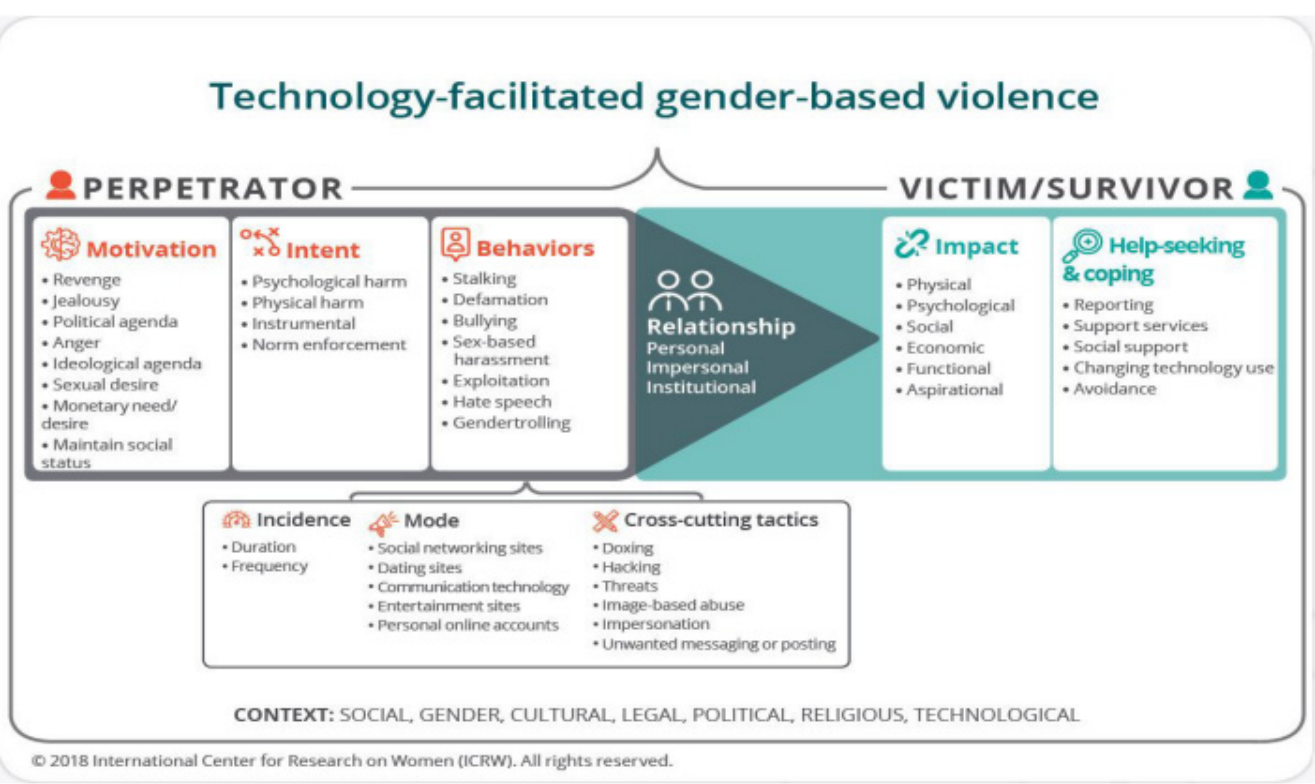
TFGBV is carried out to harm others based on their actual or perceived sex or gender identity. This can include but is not limited to, online harassment, cyberstalking, child sexual exploitation and abuse, online gendered disinformation and misinformation, and nonconsensual image-based abuse. In addition to causing harm, TFGBV can discourage women, girls, and gender-diverse persons from engaging in the digital ecosystem.

The humanitarian organisation Plan International carried out surveys based on online experiences from around the world, indicating that 58% of girls and young women had experienced online harassment, with half saying they faced more harassment online than in the street.



While different reports highlight that girls are being targeted online just for being young and female, it adds that it gets worse for women and girls who are politically outspoken, disabled, Black, or identify as LGBTQ+.

This pushes women and girls out of online spaces, which are at the same time increasingly important for activism and advocating against inequalities and human rights issues, organising movements, speaking up about personal experiences, and finding a community.



Experiences with TFGBV

Female respondents reported significantly more experiences of TFGBV than their male counterparts according to Nendo's online survey findings.

It was also noted that certain forms of TFGBV, such as stalking, defamation, and sexual harassment, are more frequently experienced by women compared to men who experienced online harassment and hate speech.

Types of Online Abuse Against Women

Both women and men can be victims of cyber violence. However, evidence shows that women and girls are highly exposed to it. Not only are they more likely to be targeted by cyber violence; but they can also suffer from serious consequences, resulting in physical, sexual, psychological, or economic harm and suffering.

Some common forms of online GBV include:

1. Cyberbullying: Repeated, aggressive behavior intended to hurt someone. This includes posting harmful or false information, spreading rumors, and making threats.

2. Harassment: Persistent, unwanted contact or attention, often involving abusive messages, threats, and intimidation.

3. Hate Speech: Speech that attacks a person or group based on attributes such as race, religion, ethnicity, gender, or sexual orientation.

4. Doxxing: Publishing private or identifying information about someone without their consent, often with malicious intent.

5. Catfishing: Using a fake identity to deceive someone online, typically to exploit, scam, or manipulate them emotionally or financially.

6. Non-consensual Sharing of Intimate Images: Distributing private, sexual images or videos of someone without their consent, causing significant emotional and social harm.

Trolling: Deliberately posting provocative, offensive, or off-topic messages to incite reactions and disrupt conversations.

8. Stalking: Monitoring someone's online activities obsessively, often coupled with sending intimidating or threatening messages.

These forms of online abuse can have severe psychological, emotional, and sometimes physical consequences.

Types of Online Threats Against Women

1. Physical Harm Threats: Direct threats to someone's physical safety, like messages saying, "I will find you and hurt you."

2. Sexual Violence Threats: Explicit threats of sexual violence, such as someone saying they will assault the victim.

3. Death Threats: Statements that threaten to kill or seriously harm someone.

Impact of OGBV on the use of the Internet by women

Online gender-based violence (OGBV) has a profound impact on women's use of social media platforms,Here are some key effects:

- Reduced Participation: Many women, especially those in public roles, reduce their online presence or withdraw from social media entirely to avoid harassment and threats.
- Self-Censorship: Fear of backlash leads women to self-censor, limiting their expression and participation in online discussions.
- Mental Health Impact: The constant threat of abuse can cause significant psychological distress, including anxiety, depression, and trauma.
- Economic Consequences: Women may face economic losses due to reduced productivity and opportunities, as they may avoid online networking and professional interactions.
- Undermining Democracy: OGBV can undermine democratic processes by silencing women's voices and limiting their participation in public discourse.
- Climate of Unsafety: A pervasive sense of unsafety can deter women from engaging in online activities, affecting their freedom of expression and access to information.
- Addressing OGBV requires concerted efforts from individuals, platforms, and policymakers to create safer online environments for women.

How to mitigate online threats and abuse against women.

Mitigating online threats and abuse against women involves a combination of personal actions, platform policies, and societal changes. Here's a comprehensive approach:

1. Strengthening Personal Security

- Use Strong Passwords: Ensure passwords are strong, unique, and changed regularly.
- Enable Two-Factor Authentication: Adds an extra layer of security to online accounts.
- Review Privacy Settings: Customize settings on social media platforms to control who can see and interact with your content.
- Be Cautious with Personal Information: Avoid sharing sensitive information publicly.

2. Reporting and Blocking

- Report Abusive Behavior: Use platform tools to report harassment, threats, and abusive content.
- Block Abusers: Block individuals who harass or threaten you to prevent further contact.

3. Legal Action

- Know Your Rights: Familiarise yourself with laws and regulations regarding online abuse in your country.
- Document Evidence: Save screenshots, messages, and any other evidence of abuse to report to authorities if necessary.

4. Support Systems

- Seek Support: Reach out to friends, family, or professional organisations for emotional support.
- Online Communities: Join support groups or communities that provide guidance and solidarity.

5. Platform Responsibility

- Advocate for Better Policies: Encourage social media platforms to implement and enforce stronger policies against online abuse.
- Improved Reporting Mechanisms: Advocate for efficient and accessible reporting tools on platforms.

6. Education and Awareness

- Digital Literacy: Educate yourself and others about safe online practices and recognizing abusive behavior.
- Awareness Campaigns: Participate in or support campaigns that highlight the issue of online abuse and advocate for change.

7. Mental Health Support

- Professional Help: Don't hesitate to seek professional mental health support if online abuse affects your well-being.

Tackling online abuse requires collective effort and action at multiple levels. By staying vigilant, informed, and supported, we can create safer online spaces.

Responses to online abuse and threats by women

Women can respond to online abuse in several ways to protect themselves and address the issue:

1. **Report and Block:** Use the reporting tools provided by social media platforms to report abusive behavior. Blocking the abuser can also prevent further contact.

2. **Document Evidence:** Keep records of abusive messages, comments, or posts. Screenshots and saved messages can be useful if you decide to take legal action or report the abuse to authorities.

3. **Seek Support:** Reach out to friends, family, or support groups for emotional support. There are also organizations that specialize in helping victims of online abuse.

4. **Legal Action:** Depending on the severity of the abuse, consider seeking legal advice or filing a complaint with law enforcement. Many countries have laws against online harassment and abuse.

5. **Privacy Settings:** Adjust your privacy settings on social media to control who can see your posts and interact with you. This can help limit exposure to potential abusers.

6. **Self-Care:** Take care of your mental health. Online abuse can be very distressing, so it's important to practice self-care and seek professional help if needed.

7. **Raise Awareness:** Share your experiences and raise awareness about online abuse. This can help others recognize and address similar issues.

8. **Advocate for Change:** Join or support campaigns that advocate for stronger policies and protections against online abuse. Collective action can lead to significant changes in how online abuse is handled.

By taking these steps, women can protect themselves and contribute to a safer online environment for everyone.

Adaptation of Strategies and Programs to Counter TFGBV.

Civil Society

Identify organizations that promote women's political participation and women's rights more broadly, as well as organizations that support survivors of GBV in general.

Collect disaggregated data that acknowledges girls' intersecting identities and tracks the scale and size of the problem.

Technology Sector

Contribute to the creation of technology-based solutions for addressing TFGBV. The mapping should identify popular technology and social media platforms, which are often documented in internet market research reports.

Media Sector

Mapping the journalism media landscape serves multiple purposes. First, given the frequent role of various media outlets in the spread and perpetration of TFGBV, identifying influential media outlets is necessary to understand the problem of TFGBV in a specific context.

Government Sector

The survey of national laws will help to identify which government bodies are empowered to investigate or enforce laws related to TFGBV or electoral violence and will indicate whether national human rights institutions, along with women's affairs ministries, can be helpful depending on their particular focus areas and levels of funding and influence.

Platform Sector

Create effective and accessible reporting mechanisms that target gender-based violence.

Hold perpetrators to account.

Combating Cyber Violence against Women and Girls | European Institute for Gender Equality (europa.eu)

Types of Online Threats against Women

Cyber Harassment and Bullying: This includes name-calling, trolling, and persistent stalking. Women and girls may face derogatory comments and hurtful behaviour online.

Cyber Stalking: It involves unwanted and obsessive attention, monitoring, or tracking of an individual online. Stalkers may use various platforms to harass their victims.

Online Gender-Based Hate Speech: Women and girls are often targeted with hate speech related to their gender. This can perpetuate harmful stereotypes and create a hostile online environment.

Flaming: Flaming refers to heated arguments and aggressive exchanges online. It can escalate into threats and personal attacks.

Image-Based Sexual Abuse (Revenge Porn): Sharing intimate or explicit images without consent can cause immense emotional distress and harm.

Doxing: This involves revealing private information about someone online, such as their address, phone number, or workplace.

General Online Threats

Malware Attacks: Malware, short for malicious software, includes viruses, worms, Trojans, and ransomware. Cybercriminals deploy malware to gain unauthorised access, steal data, or disrupt systems.

Phishing: Phishing involves tricking individuals into revealing sensitive information like passwords and financial data. Phishing attacks often use fraudulent emails, websites, or messages that appear legitimate.

Social Engineering: Social engineering exploits human psychology to manipulate individuals into divulging confidential information or performing actions compromising security.

Denial-of-Service (DoS) Attacks: These attacks overload a network or website with traffic, rendering it unavailable to users. Distributed Denial-of-Service (DDoS) attacks involve multiple devices.

Identity Theft: Cybercriminals steal personal information, such as national ID numbers, credit card information, etc., to commit fraud or financial crimes.

Cyber Espionage: Nations or corporate entities engage in cyber espionage to gain access to sensitive information, trade secrets, or government intelligence.

Motivations of Cyber Criminals

Understanding the motivations behind online threats is crucial for digital safety:

- Financial Gain: Many cybercriminals seek monetary benefits through extortion, stealing financial data, or selling stolen information on the dark web.
- Hacktivism: Some individuals or groups engage in cyberattacks to promote political or social causes.
- State-Sponsored Attacks: Nation-states may engage in cyber surveillance for political, economic, or military purposes.
- Personal Vendettas: Cyberattacks can be used for personal revenge or harassment.

The Importance of Proactive Threat Awareness

Being proactive and vigilant is the first line of defence against online threats. Recognizing the signs of a potential attack, such as suspicious emails or unusual online behaviour, can help individuals and organisations respond effectively.

Practical Exercises and Case Studies

To reinforce the concepts introduced in this module, we will engage in practical exercises and explore real-world case studies. These exercises will include:

- Analysing phishing emails and identifying red flags.
- Investigating a social engineering incident.
- Reviewing a case study of a successful defence against a cyber threat.

Understanding online threats and the motivations behind them is crucial for digital safety. In the next modules, we will explore strategies and best practices for mitigating these threats and protecting digital assets.

Module 4

Information Disorder

Learning objective

I. Definition of Misinformation, disinformation

II. Impact of Gendered Disinformation

III. Measures to gendered disinformation

IV. Recommendations

V. Recognizing fake news and misinformation

VI. Critical thinking and fact-checking online

VII. Interactive exercises and online media analysis

Misinformation is the unintentional distribution of false information.

Disinformation is knowingly, developing, and disseminating incorrect information intended to deceive.

Malformation is information that is based on reality but disseminated with the intent to inflict harm.

Online hate Speech is understood to be bias-motivated, hostile, and malicious language targeted at a person or group.

Fake news or information disorder is false or misleading information presented as news.

Deep fakes are images, videos, or audio that are edited or generated using artificial intelligence tools, and which may depict real or non-existent people.

The spread of misinformation and disinformation has affected our ability for women to express themselves online to improve their experiences as they navigate online spaces creating the term Gendered disinformation.

A 2016 research study by the Association of Media Women in Kenya revealed that 75.4% of Women journalists in Kenya face online harassment due to gender, ethnicity, or their work.

Gendered disinformation is the spread of deceptive or inaccurate information and images against women (political leaders, journalists, influencers, and female public figures) in a way that draws on misogyny and societal stereotypes, framing them as untrustworthy, unintelligent, emotional/angry/crazy, or sexual.

Gender-Based Disinformation: Advancing Our Understanding and Response - EU DisinfoLab

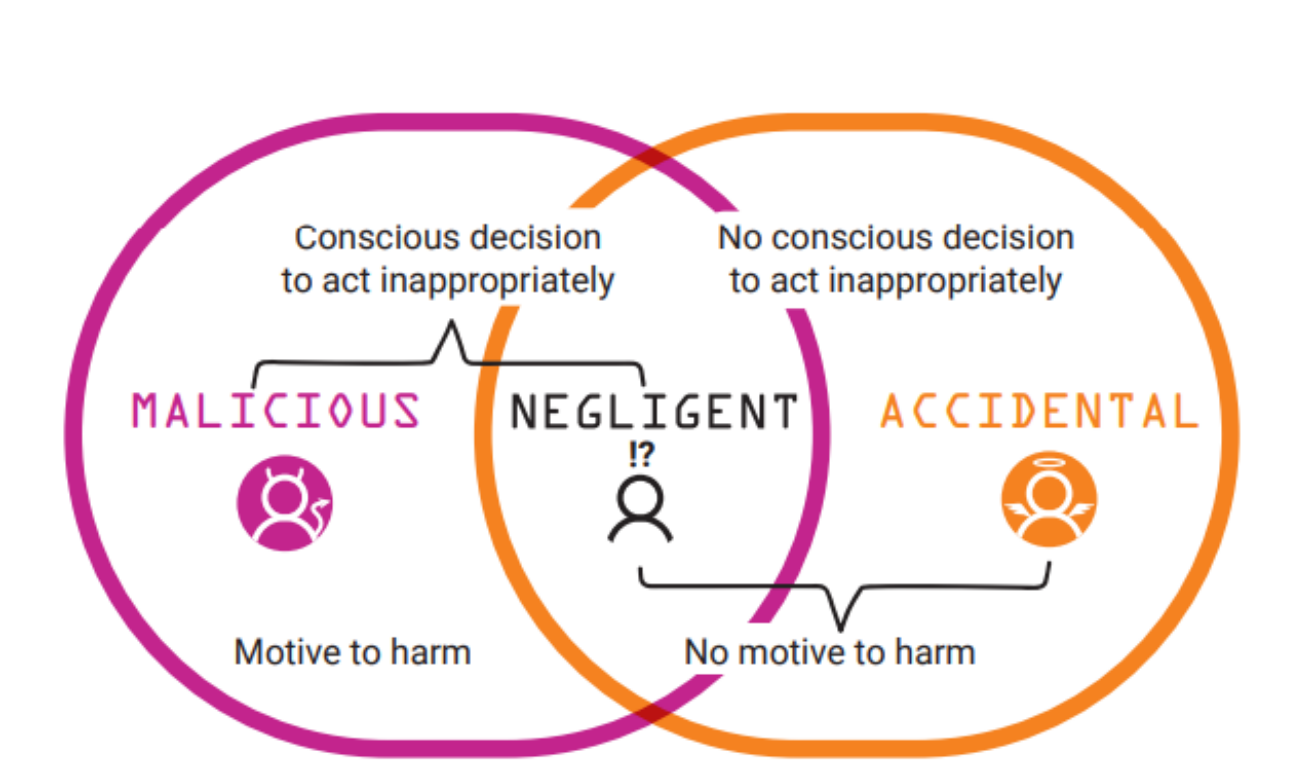
Gendered disinformation is propagated due to patriarchal gender norms that normalise the abuse and harassment of women in general but women in the spotlight in particular. The social expectations, personal attitudes, and behaviours related to gender norms are reflected in the online space and, at their worst, are reaffirmed by disinformation campaigns to attack active women in public positions. Addressing Gendered Disinformation - NDI

Enablers and Intent

This is often then amplified by;

- Media agents (journalists, content creators, influencers, tabloids)
- Religious, Cultural, and Opinion leaders and beliefs (Pastors, Churches, traditional leaders)
- Male and female political opponents (both within their own party and rival parties)
- General population.

Share examples of recent events



Targeted women groups include; Byte bullies

- Women in Politics
- Women Rights defenders
- Journalists
- Content creators
- Social media influencers.
- Public figures

Gendered disinformation is manifested in different forms which include; Strand, C., & Svensson, J. (2021). Disinformation campaigns about LGBTI+ people in the EU and foreign influence.

- Misogynistic comments and posts
- Homophobic sharings
- Dissemination of sexualized content
- Targeted online harassment and demeaning remarks
- Hate speech
- Cyber-attacks

Why is there an increase in Gendered disinformation?

Gendered disinformation strategically aims to evoke emotional responses from its audience. The language used is often exaggerated causing inaccuracy and misleading perceptions.

1. The algorithmic mechanisms employed by social media platforms have in some ways, amplified the spread of misinformation and disinformation content, creating information overload.
2. Emerging technologies like
    - Anonymity, offered by online platforms, has empowered perpetrators with AI-generated deepfakes and fake accounts fueling the spread of gendered disinformation and hate speech online because it shields them from accountability.
    - AI has enabled the automation of social engineering attacks as well as the spread of false or defamatory information for example deepfakes that are targeted at women and are likely to cause harm and damage their reputations.
3. The lack of social media platforms' response mechanisms to complaints about gendered disinformation and hate speech remains inadequate. These accountability challenges are worsened by the lack of transparency regarding the number of complaints reported through the platforms. Wadminw. (n.d.). The Battle Against Misinformation and Disinformation: Unveiling Our Role in Spreading and the Importance of Accurate Information – Cornerstone Institute. Cornerstone. https://cornerstone.ac.za/misinformation-and-disinformation/
4. Neglect of perpetrators accountability but focusing on the victims and survivors leaves no room for actual change or solution to the root cause hence increased gendered disinformation.

Detection tools

Emerging technologies like Artificial Intelligence (AI) can be harnessed to develop detection tools that identify and flag harmful content in real-time, specifically focusing on gendered disinformation and hate speech.

Fact-Checking

- https://tineye.com/
- https://www.invid-project.eu/
- https://who.is/
- https://earth.google.com/web/@0,-1.19719995,0a,22251752.77375655d,35y,0h,0t,0r/data=OgMKATA
- https://toolbox.google.com/factcheck/explorer
- https://scholar.google.com/

Gendered disinformation is used as a tool against women to;

Why is gendered disinformation dangerous for women to succeed in their different fields?

Keep women out of politics since it portrays women as incapable or unworthy of occupying space in the public arena either due to intellectual limits or ulterior motives. Here

Change the views of women and men about women's political participation.

In short, it aims to undermine women's free and equal political participation to the detriment of inclusive, resilient democracy.here

Alter public understanding of female politicians' track records for immediate political gain, as well as to discourage women seeking political careers or leadership roles". Here

Gendered disinformation undermines women's credibility which poses obstacles to their electoral success, and ultimately represents a significant reason why many women abandon political careers.

On some occasions, hate and online threats fueled by gendered disinformation campaigns are followed by physical violence hence life-threatening.

Individual and collective psychological effects are difficult to assess and quantify this is because gendered Disinformation aims to trigger an emotional response in the audience and the victims.

Gender-based disinformation is to remind women that they are inherently vulnerable; this dynamic plays along with the perpetuation of stereotypes, making it more difficult for present and future generations to eradicate these sexist constructs.

Silencing women public figures and deterring women from seeking public roles. here

Undermining democracy and good governance, increasing political polarization, and expanding social cleavages. here

Existing efforts/ measures in Uganda to combat disinformation.

Government bodies - UCC

In March 2018 a directive was issued by UCC ordering all social media pages that produce online content through blogs and live streaming to seek authorisation before publishing any content by April 2018. (Such platforms are believed to be the key disseminators of disinformation) The threat of blocking unregistered service providers by April 2018 was not enforced.

The Computer Misuse Act of 2011 provides for the safety and security of electronic transactions and information systems and prevents unlawful access, abuse, or misuse of information systems including computers, and makes provision for securing the conduct of electronic transactions in a trustworthy electronic environment and to provide for other related matters (Min. ICT & National Guidance, 2019).

Civil Society

Private organisations such as PesaCheck, Code for Africa, and the Debunk Show conduct fact-checking and debunking disinformation.

Digital training and awareness including how to identify disinformation provided by organisations like the African Centre for Media Excellence (ACME).

Social Media Platforms

Suspending users spreading disinformation. The challenge exists with the complexity of catching accounts spreading disinformation, and the business incentives of the companies that run the sites.

Social media companies have begun to require more documentation when creating accounts, for example often requiring a phone number, as a way to combat the fakes. However, this makes it more difficult for new users to join their sites yet their businesses sell more ads if they are known to have more users on their networks.

Warning labels are put in place by Twitter on false and misleading tweets, to prevent its users from accessing and spreading information that is misleading.

YouTube terminates channels that attempt to impersonate.

Media Houses

The editorial process has been strengthened by relying upon in-house professionals, monitoring teams, and well-respected fact-checkers to verify their news stories. Editors and gatekeepers decide which stories to run after they have been verified.

https://drive.google.com/file/d/1cv1jujKgryIGhJGvE9bcSSIPEgkY-a-x/view?ts=6703b886

Recommendations

Enhanced Legal Framework: There's a critical need for stronger legal measures that specifically address TFGBV, alongside more rigorous enforcement of existing laws.

Educational Campaigns: Raising awareness about the nature and seriousness of TFGBV and educating the public on how to report and combat such violence are essential. Integrate personal training on how to protect one's personal information online into project programming,

Platform Responsibility: Social media platforms need to enforce stricter policies and tools to detect and prevent TFGBV, ensuring a safer online environment.

Support Systems: Developing comprehensive support systems, including psychological counselling and legal assistance for victims of TFGBV, is recommended. Build better organisational structures for women affected by gendered disinformation.

Integrate into programming training on protecting one's personal information and mitigating psychological trauma from online disinformation.

Maintain databases of abuse and reports against women employees and affiliates, and share them regularly with platforms.

Individual level; NDI Recommendations

- Integrate personal training on how to protect one's personal information online and mitigate psychological trauma from such attacks.
- Contact specific points for support like organisations, and social media platforms with whom they can escalate their reports of abusive situations.

Institutional level

- Connect their partners with platforms offering training on how to use on-platform tools to mitigate harassment and disinformation campaigns.
- Work with partner organisations' leadership to build better institutional support for women affected by creating a standardised organisational policy for partners on responding to online gendered abuse and disinformation that these partners might deploy within their groups.
- Establish private, country, or region-based support networks of women who have endured or are likely to be subject to gendered disinformation attacks.
- CSOs and political parties should also maintain databases of abuse and reports against their women employees and affiliates. This is critical not only in assessing threats, and if necessary, communicating data to law enforcement, but also in pressuring platforms to enforce their terms of service and protect women users.

Socio-cultural Level - Media Organisation

- Invest in active training and outreach to CSOs, media outlets, academics, political parties, and individual women in politics. Training workshops should ideally help the participants to identify Online VAW-P and gendered disinformation, and be delivered by local platform staff or affiliates with deep knowledge of the sociopolitical context in a particular country or region.

- Media organisations and journalists set the tone for how society conceives of and responds to women in politics. Media should consider adopting a code of conduct for how they cover women candidates to illustratively include: banishing gendered tropes describing women's appearance; and establishing a higher burden of proof for reporting on gendered allegations.

- Platforms and media organisations have a role in challenging such norms as well. In addition to training to identify VAW-P and gendered disinformation, training on recognizing patriarchal gender norms and their societal impact should be mandatory for platform staff and designers, and provided to the other aforementioned stakeholders.

- Platforms should invest in on-platform awareness-building campaigns about the consequences of engaging in gendered abuse and disinformation, in order to educate users.

Module 5

Data Privacy and Protection

Learning Objectives

I. Understand the principles of data privacy.

II. Recognize the importance of data protection laws and regulations.

III. Learn how to safeguard personal and sensitive data.

IV. Engage in real-world examples and exercises related to data privacy.

Introduction

In the digital age, personal and sensitive data are collected, shared, and stored online more than ever before. Protecting this data is not just a matter of good practice but often a legal requirement. This module is dedicated to the critical aspects of data privacy and protection, equipping the women with the knowledge and tools to secure sensitive information.

Principles of Data Privacy

Consent and Transparency: Individuals must be informed about how their data will be used and provide explicit consent.

- **Data Minimization:** Only collect the data necessary for the intended purpose.
- **Data Accuracy:** Ensure that the data is accurate and up to date.
- **Data Security:** Protect data from unauthorised access or disclosure.
- **Data Retention:** Store data only as long as necessary and securely dispose of it when it's no longer needed.

Data Protection Laws and Regulations

Understanding data privacy laws and regulations is crucial, as each country has its own unique set of rules and standards. Here are some local and global as a globally recognized data regulator:

1. Data Protection and Privacy Act (DPPA): Enacted in Uganda, the DPPA governs the collection, processing, and protection of personal data. It provides guidelines for data controllers and processors, as well as data subject rights. For example, individuals have the right to access their personal data, request corrections, and be informed about data processing.

2. The Personal Data Protection Act: Enacted in Tanzania in November 2022,, the data act was a recognition of the right to privacy and personal security enshrined under Article 16 of their constitution.

3. General Data Protection Regulation (GDPR): The GDPR, established by the European Union, serves as a global benchmark for data protection. It mandates strict rules for the processing of personal data and the rights of data subjects. Even for organisations operating outside the EU, GDPR compliance is essential when handling the data of EU residents.

Safeguarding Personal and Sensitive Data

To protect personal and sensitive data, individuals and organisations should:

- Implement strong access controls and encryption.
- Regularly update software and security systems.
- Conduct data privacy impact assessments.
- Train employees and stakeholders on data protection.

Real-World Examples and Exercises

To reinforce the principles of data privacy and protection, participants will engage in real-world examples and exercises:

- Reviewing a privacy policy and identifying its compliance with data protection regulations.
- Conducting a data protection impact assessment for a hypothetical data collection project.
- Participating in a data breach simulation and understanding the response process.

Understanding and implementing data privacy and protection principles are essential for safeguarding individuals' rights and organisations' reputations. In the following modules, we will delve further into topics like online identity, secure communication, and incident response.

Module 6

Online Identity and Authentication

Learning Objectives

I. Explore the importance of managing online identities securely.

II. Understand various authentication methods for online platforms.

III. Learn how to prevent identity theft and unauthorised access.

IV. Engage in interactive role-playing scenarios and hands-on activities.

Introduction

In the digital realm, your online identity is a crucial aspect of your security. Managing your identity effectively and ensuring that you are who you claim to be online are fundamental to your digital safety. This module focuses on understanding online identities, authentication methods, and preventing identity theft.

Managing Online Identities

1. The Significance of Online Identities: Online identities are how you are recognized and interact with others on the internet. They can encompass email addresses, usernames, social media profiles, and more.

2. Digital Footprint: The information you leave behind online is your digital footprint. It's essential to be mindful of what you share, as it can affect your privacy and security.

3. Online Persona vs. Personal Information: Distinguishing between your online persona and personal information is key. Share only what you're comfortable with and consider the implications of oversharing.

Authentication Methods

- Password-Based Authentication: Passwords are the most common method for verifying identity. Emphasise creating strong, unique passwords and consider using a password manager.

- Two-Factor or Multi-Factor Authentication (MFA): These kinds of authentication adds an extra layer of security by requiring something you know (a password) and something you have (e.g., a smartphone) to access an account.

- Biometric Authentication: Biometric methods, such as fingerprint or facial recognition, offer convenient and secure ways to verify identity.

- One-Time Passwords (OTP): OTPs are single-use codes often sent to your phone for authentication.

Identity Theft Prevention

1. Phishing Awareness: Be cautious of phishing attempts, as they often aim to steal login credentials.
2. Privacy Settings: Adjust privacy settings on social media and other platforms to control what information is visible to others.
3. Regularly Monitor Accounts: Regularly review your financial and online accounts for unauthorised activity.

Interactive Role-Playing Scenarios and Hands-on Activities

1. Participants will engage in the following activities to reinforce their understanding of online identity and authentication:
2. Role-play a scenario involving a phishing attempt and demonstrate how to recognize and respond to it.
3. Practice setting up multi-factor authentication on various platforms.
4. Conduct a simulated identity theft prevention exercise, identifying areas of vulnerability.

Securing your online identity is an essential step in digital safety. In the next modules, we will delve into topics like social media safety, safe internet browsing, and mobile device security to build a comprehensive foundation for digital security awareness.

Module 7

Social Media Safety

Learning Objectives

I. Recognize the risks associated with social media use.

II. Understand how to adjust privacy settings and controls on social media platforms.

III. Learn strategies for dealing with cyberbullying and online harassment.

IV. Engage in interactive social media security practices.

Introduction

Social media platforms have become an integral part of our lives, connecting us with friends, family, and a global community. However, along with the benefits come risks, including privacy concerns and the potential for cyberbullying or online harassment. This module is dedicated to social media safety, empowering women to enjoy the benefits of these platforms securely.

Risks Associated with Social Media

1. Privacy Concerns: Oversharing personal information can lead to identity theft or stalking.
2. Cyberbullying: Social media platforms can be used as tools for harassment and bullying.
3. Online Harassment: Individuals may experience harassment or threats online, which can have serious emotional and psychological consequences.

Privacy Settings and Controls

To enhance social media safety, it's crucial to:

- Adjust privacy settings on social media platforms to limit who can see your posts and personal information.
- Review and control the information you share, avoiding the disclosure of sensitive data.

Dealing with Cyberbullying and Online Harassment

1. Recognize Cyberbullying: Understand what constitutes cyberbullying, which includes threats, harassment, and negative comments.
2. Report and Block: Learn how to report abusive behaviour to social media platforms and block users who engage in harassment.
3. Seek Support: Encourage victims to seek support from friends, family, and mental health professionals to cope with the emotional impact of online harassment.

Interactive Social Media Security Practices

- Participants will engage in the following activities to enhance their social media safety:
- Review privacy settings and make necessary adjustments on a sample social media account.
- Role-play a scenario involving online harassment and practice reporting and blocking the harasser.
- Analyse a case study involving the consequences of oversharing on social media.

By the end of this module, the women will have a better understanding of how to enjoy the benefits of social media while safeguarding their personal information and emotional well-being. The following modules will explore safe internet browsing and mobile device security to further enhance their digital safety knowledge.

Module 8

Internet Shutdown

Learning Objectives

- Understanding Internet Shutdowns
- Types of Internet shutdown
- Why Do Governments Shut Down the Internet?
- Gendered Impact of Shutdowns
- Anti-Censorship Tools and Virtual Private Networks
- Network Measurements and Monitoring
- Preparing for internet shutdowns
- Practical exercise

Understanding Internet Shutdowns

An Internet shutdown is an intentional disruption of Internet-based communications, rendering them inaccessible or effectively unavailable, for a specific population, location, or mode of access, often to exert control over the flow of information. This is usually done by the government as a drastic measure.

Types of Internet Shutdown

1. Partial Blocking: blocking access to specific websites, platforms, or services while leaving the rest of the internet accessible.
2. Throttling: Slowing down internet speeds.
3. Social Media Blackouts: Targeting popular social media platforms.
4. Total Shutdowns: Complete cessation of internet access, and civil unrest, usually during elections.

Impact of Internet Shutdown on social, economic, and human rights.

Curtail freedom of expression by limiting individuals' ability to communicate, access information, and express dissenting opinions online.

Economic Disruption: Internet shutdowns disrupt businesses.

Social Isolation and Disruption of Essential Services: Shutdowns disrupt essential services such as healthcare, education, and emergency communication.

Violation of Human Rights: Internet shutdowns violate various human rights, including the right to freedom of expression, assembly, and access to information, as enshrined in international conventions and declarations.

Gendered impact of Internet shutdown

- Access to Information and Communication: Women, LGBTQ+ individuals, and marginalised groups often rely heavily on the Internet for accessing information, social connections, and support networks. Shutdowns deny them these essential resources, exacerbating existing inequalities.
- Economic Opportunities: online platforms for entrepreneurship, remote work, or accessing job opportunities.
- Education and Health: Internet shutdowns impede access to online education resources and healthcare services.
- Silencing Voices: Women often use online platforms to advocate for their rights, share experiences, and organise movements.
- Effects on LGBTQ+ Communities: Marginalisation and Isolation: LGBTQ+ individuals often rely on the internet for community-building, accessing resources, and seeking support.
- Exacerbating the Challenges Faced by People with Disabilities unable to use the transcription app.

Why Do Governments Shut Down the Internet?

Political Motivations

- Control and Censorship: Governments may shut down the internet to control the flow of information and suppress dissenting voices

Social Motivations

- Cultural and Ideological Control
- Mitigating Social Unrest

Economic Motivations

- Protecting Economic Interests

Anti-Censorship Tools and Virtual Private Networks

Anti-censorship refers to actions, principles, or technologies aimed at opposing or countering censorship.

What is a circumvention tool? A circumvention tool is a software or method used to bypass restrictions or censorship imposed on accessing certain content or services on the internet The most widely used anti-censorship tool is the Virtual Private Network (VPN). A VPN establishes a secure, encrypted connection between a user's device and a remote server operated by the VPN provider.

Tor (The Onion Router): Tor is a decentralised network that routes internet traffic through a series of volunteer-operated servers, encrypting data and anonymizing users' identities. Tor enables users to access the internet anonymously and bypass censorship.

Mesh Networks: Mesh networks are decentralised networks of interconnected devices that allow communication between devices without the need for centralised infrastructure. During internet shutdowns, mesh networks enable users to create ad-hoc networks and communicate locally, bypassing restrictions on internet access imposed by governments.

Benefits and Limitations of VPNs in Bypassing Internet Censorship and Shutdowns

Benefits

- Access to Restricted Content: VPNs allow users to bypass geo-restrictions and access content that may be blocked or censored in their region. This includes websites, streaming services, and social media platforms.
- Enhanced Privacy and Security: By encrypting internet traffic and masking IP addresses, VPNs help protect users' privacy and sensitive information from surveillance and cyberattacks.
- Unrestricted Communication: VPNs enable users to communicate freely and securely, even in regions where messaging apps or VoIP services are restricted.

Limitations

- Reliance on VPN Providers: User not all VPN providers may adhere to strict privacy policies or security standards.
- Potential for Slowdowns: The encryption and routing processes involved in using a VPN can sometimes result in slower internet speeds compared to direct connections, particularly if the VPN server is located far away.
- Detection and Blocking: Some governments and organisations actively monitor and block VPN traffic, making it challenging for users to bypass censorship effectively.

Legal measures on the issue of internet shutdowns

Addressing internet shutdowns through legal measures can be complex and challenging due to the involvement of sovereign states and international law.

International Human Rights Framework: Internet shutdowns can violate human rights, including the rights to freedom of expression, assembly, and access to information. Individuals and organisations can leverage international human rights instruments, such as the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, to advocate against internet shutdowns and hold governments accountable.

Preparing for internet shutdowns

Offline Communication: Establish alternative means of communication that don't rely on the Internet. This could include maintaining a list of important phone numbers of family, friends, and colleagues.

Backup Information: Download and save important information, documents, maps, and resources that you may need offline.

Offline Tools: Invest in offline tools that don't rely on internet connectivity. This could include physical maps and compasses.

Stay Informed: Stay informed about potential internet shutdowns or other disruptions in your area. Follow local news sources, sign up for emergency alerts, and stay connected with your community to stay informed about developments and potential risks.

Practical exercise

Case Studies Analysis: Provide case studies of real-life internet shutdown incidents. Divide participants into groups and assign each group a case study to analyse. They should identify the causes, impacts, duration, and responses to the shutdown. Afterward, each group presents their findings to the rest of the participants.

Module 9

Safe Internet Browsing - Securing Your Digital Life.

Learning Objectives

I. Develop secure browsing habits to protect against online threats.

II. Recognize and avoid malicious websites and deceptive content.

III. Utilise browser extensions and tools for enhanced security.

IV. Engage in practical demonstrations and website assessments.

Introduction

The internet is a vast and dynamic landscape, offering an abundance of information and opportunities. However, it's also a playground for cybercriminals seeking to exploit unsuspecting users. Safe internet browsing is critical to mitigate the risks associated with online threats. In this module, the women will learn how to navigate the internet securely.

Secure Browsing Habits

- Keep Software Updated: Ensure your operating system, browsers, and plugins are up-to-date to patch vulnerabilities.
- Use Secure Websites: Look for "https://" and a padlock icon in the address bar to confirm a website's security.
- Beware of Phishing: Be cautious of links in emails and messages. Verify the source before clicking.
- Online Ads: Exercise caution with online advertisements, as they can lead to malicious websites.

Recognizing and Avoiding Malicious Websites

Typo Squatting: Be wary of domains that closely resemble well-known websites but contain typos.

Deceptive Content: Avoid websites that promise unrealistic outcomes, such as "get-rich-quick" schemes.

Pop-Up Windows: Beware of pop-up windows that may contain malware or deceptive ads.

Browser Extensions and Tools

1. Ad Blockers: Install ad blockers to minimise the chances of encountering malicious ads.
2. Password Managers: Use password managers to store and autofill secure, complex passwords.
3. Antivirus and Anti-Malware Extensions: Add browser extensions that can detect and block malicious content.
4. Virtual Private Networks (VPNs): Consider using a VPN to encrypt your internet connection and enhance privacy.

Practical Demonstrations and Website Assessments

Participants will engage in hands-on activities to reinforce their understanding of safe internet browsing:

- Demonstrate how to check if a website is secure by examining the URL and identifying secure and insecure elements on a webpage.
- Assess a sample website to identify potential risks, such as deceptive content or phishing attempts.

By the end of this module, the women will be equipped with the knowledge and practical skills to browse the internet securely and reduce their exposure to online threats. The following modules will delve into mobile device security and secure communication and encryption.

Module 10

Mobile Device Security

Learning Objectives

I. Understand the importance of securing mobile devices.

II. Learn how to protect smartphones and tablets from digital threats.

III. Explore mobile app security best practices.

IV. Participate in app scanning and device security settings.

Introduction

Mobile devices, such as smartphones and tablets, have become integral to our daily lives. They store a wealth of personal and sensitive information, making them prime targets for cyberattacks. This module focuses on mobile device security, equipping women with the knowledge and skills to safeguard their mobile technology.

Securing Mobile Devices

1. Device Passcodes and Biometrics: Use passcodes or biometric authentication (e.g., fingerprint or facial recognition) to secure your device.

2. Remote Lock and Wipe: Enable features that allow you to remotely lock or wipe your device if it's lost or stolen.

3. Keep Software Up to Date: Regularly update your device's operating system and apps to patch vulnerabilities.

4. App Permissions: Review and limit app permissions to protect your personal information.

Mobile App Security

1. App Source: Only download apps from official app stores (e.g., Google Play Store or Apple App Store) to minimise the risk of downloading malicious apps.

2. App Updates: Keep apps updated to receive security patches and bug fixes.

3. App Permissions: Review and understand the permissions an app requests before installing it.

App Scanning and Device Security Settings

1. Security Software: Consider installing mobile security apps that offer antivirus, anti-malware, and anti-phishing protection.

2. Privacy Settings: Adjust privacy settings on your device to control what information apps can access.

3. Device Encryption: Enable device encryption to protect data in case of theft or loss.

Practical Demonstrations and App Scanning

Participants will engage in hands-on activities to reinforce their understanding of mobile device security:

- Demonstrate how to set a secure passcode or enable biometric authentication on a sample mobile device.

- Review app permissions for a selection of commonly used apps and assess their security.

- Explore the settings on a mobile device to enable encryption and review privacy settings.

By the end of this module, the women will have the knowledge and skills to protect their mobile devices and data from digital threats. The following modules will delve into secure communication and encryption, incident response, and advocacy for digital rights.

Module 11

Secure Communication and Encryption

Learning Objectives

I. Understand the principles of secure communication.

II. Explore end-to-end encryption and its importance.

III. Learn about secure messaging apps and encrypted email services.

IV. Engage in practical exercises to implement secure communication practices.

Introduction

In an age of digital communication, protecting the confidentiality and integrity of messages and data is paramount. This module is dedicated to secure communication and encryption, empowering women to exchange information safely and confidentially.

Principles of Secure Communication

1. Confidentiality: Ensuring that the content of a message is kept private and only accessible to intended recipients.

2. Integrity: Verifying that the content of a message has not been tampered with during transmission.

3. Authentication: Confirming the identity of the sender and recipient in a communication.

4. Non-Repudiation: Ensuring that the sender of a message cannot deny sending it.

End-to-End Encryption

End-to-end encryption (E2E) is a method that ensures that only the sender and recipient of a message can decrypt and read its contents. Nobody in between, including service providers, can access the information.

E2E encryption is crucial for protecting sensitive and private communications from interception by unauthorised entities, including hackers and service providers.

Here are some apps and emails having end-to-end encryption:

Secure Messaging Apps

1. Signal: Signal is a secure messaging app that offers end-to-end encryption for text messages, voice calls, and video calls.

2. WhatsApp: WhatsApp also offers E2E encryption for its messages, including multimedia content.

3. Telegram: Telegram provides options for secret chats with E2E encryption.

Encrypted Email Services

1. ProtonMail: ProtonMail offers encrypted email services with user-friendly features.
2. Tutanota: Tutanota provides end-to-end encrypted email and secure calendaring.

Practical Exercises

Participants will engage in hands-on activities to reinforce their understanding of secure communication and encryption:

- Install and set up a secure messaging app (e.g., Signal or WhatsApp) for encrypted communication.
- Create and send an end-to-end encrypted email using a service like ProtonMail.
- Discuss and practise real-world scenarios where secure communication is necessary, such as sharing confidential documents.

By the end of this module, the women will have the knowledge and practical experience to engage in secure communication practices and protect their confidential information. The following modules will explore incident response and advocacy for digital rights, preparing them for reactive and proactive digital security roles.

Module 12

Incident Response and Reporting

Learning Objectives

I. Understand how to respond to security incidents effectively.

II. Learn the importance of reporting security breaches and incidents.

III. Explore the legal and ethical considerations of incident response.

IV. Engage in mock incident scenarios and response planning.

Introduction

In the digital landscape, incidents such as data breaches, cyberattacks, or security vulnerabilities can occur despite best efforts at prevention. Knowing how to respond to these incidents is essential for minimising damage and protecting sensitive data. This module focuses on incident response and reporting procedures.

Responding to Security Incidents

1. Identifying an Incident: Recognize the signs of a security incident, such as unauthorised access, data breaches, or suspicious activity.
2. Containment: Isolate affected systems to prevent further damage.
3. Eradication: Determine the root cause of the incident and remove the threat.
4. Recovery: Restore affected systems and services to normal operation.
5. Lessons Learned: Conduct a post-incident analysis to identify areas for improvement.

Reporting Security Breaches and Incidents

1. Legal Obligations: Understand the legal requirements for reporting security breaches, which may vary by jurisdiction.
2. Ethical Considerations: Reporting incidents is often a matter of ethical responsibility to protect individuals' data and privacy.
3. Internal and External Reporting: Determine who needs to be informed, both within your organisation and relevant authorities or affected parties.

Legal and Ethical Considerations

1. Data Privacy Laws: Comply with data protection laws that require reporting security incidents and breaches.

    a. Key legislation in Uganda

        - The Data Protection and Privacy Act, 2019 (DPPA): DPPA This is the primary law governing data protection in Uganda. It outlines the rights of individuals regarding their personal data and the obligations of data controllers and processors.

        - The Data Protection and Privacy Regulations, 2021: These regulations provide further details on the implementation of the DPPA, including registration requirements for data controllers, data security measures, and procedures for handling data breaches.

2. Transparency: Be transparent with affected individuals and stakeholders regarding the incident and the steps taken to address it.

Mock Incident Scenarios and Response Planning

Participants will engage in practical exercises to simulate incident response:

- Role-play a security incident scenario and practise the steps for incident response.
- Develop an incident response plan for their organisation or institution.
- Discuss and analyse real-world case studies of incident response to better understand the complexities involved.

By the end of this module, the women will be prepared to respond to security incidents effectively, ensuring a timely and appropriate reaction to protect sensitive data and mitigate risks. The following module will delve into digital literacy and critical thinking, empowering them to enhance digital literacy and critical thinking.

Module 13

Policy and Advocacy for Digital Rights and Data Governance

Learning Objectives

I. Understand the significance of digital rights and their intersection with human rights.

II. Explore the role of advocacy in promoting responsible data use and privacy.

III. Learn how to engage in policy and advocacy efforts for digital rights.

IV. Engage in case studies of digital rights activism.

Introduction

In an era of rapidly evolving technology and data-driven decision-making, the importance of digital rights is paramount. Digital rights encompass the principles of privacy, freedom of expression, and the ethical use of data. This module focuses on the advocacy for digital rights and prepares women to become advocates for responsible data use.

Significance of Digital Rights

1. Intersection with Human Rights: Digital rights are closely tied to human rights, including the right to privacy and freedom of expression.

2. Data Ethics: Digital rights emphasise the responsible and ethical use of data and technology.

3. Protection of Vulnerable Populations: Advocating for digital rights is often about protecting vulnerable individuals, such as children and marginalised communities.

Role of Advocacy

1. Promoting Awareness: Advocacy efforts can raise awareness about digital rights and privacy concerns.

2. Policy Influence: Advocacy can shape government policies related to data protection and privacy.

3. Corporate Responsibility: Advocacy can encourage businesses to adopt ethical data practices.

Engaging in Policy and Advocacy Efforts

1. Educate and Mobilise: Educate stakeholders about the importance of digital rights and mobilise them to take action.

2. Collaborate: Collaborate with other organisations and advocates to strengthen advocacy efforts.

3. Engage with Policymakers: Communicate with policymakers to influence legislation and regulations.

Case Studies of Digital Rights Activism

- Participants will explore real-world examples of digital rights activism, such as:
- The campaign for net neutrality and open access to the internet.
- The Data Protection And Privacy Act of Uganda and its impact on data privacy.
- The Implications of Tanzania's Data Protection and Privacy Act on Data Privacy.

By the end of this module, the women will have a deeper understanding of the significance of digital rights and the tools and strategies for advocating for responsible data use and privacy. They will be equipped to take an active role in promoting and protecting digital rights in their communities and institutions.

Source

1. Website: StaySafeOnline.org
2. Digitalisation Training Toolkit
3. Online harassment field manual
4. Toolkit: The Internet Society of Uganda Chapter, a part of the Internet Society
5. E-SAFETY EDUCATION TOOLKIT, to help young Ugandans navigate and stay safe online.
6. Securing your digital life like a normal person
7. Advocacy Assembly, the world's only free online training platform for human rights activists, campaigners and journalists.
8. 'Courses' to find the online multimedia courses 'Staying safe online and using social media' and 'Secure Communications' by Security First.
9. Adaptation of strategies and programs to counter TFGBV. Digital Threats Landscape Assessment
10. Combating Cyber Violence against Women and Girls | European Institute for Gender Equality (europa.eu)
11. Gender-Based Disinformation: Advancing Our Understanding and Response - EU DisinfoLab
12. Addressing Gendered Disinformation - NDI
13. Targeted women groups; Byte bullies
14. The Battle Against Misinformation and Disinformation: Unveiling Our Role in Spreading and the Importance of Accurate Information – Cornerstone Institute. Cornerstone. https://cornerstone.ac.za/misinformation-and-disinformation/
15. Gendered disinformation: Addressing Online Misogyny and Gendered Disinformation: A How-To Guide
    - Understanding the Gender Dimensions of Disinformation.
    - EU Disinformation in Uganda
16. Data Protection Laws and Regulations: Data Protection and Privacy Act (DPPA)
    - The Personal Data Protection Act
    - General Data Protection Regulation (GDPR)
17. Safe Internet Browsing - Securing Your Digital Life.
18. Addressing Gendered Disinformation And Hate Speech On Digital Platforms In The Age Of AI In Kenya.