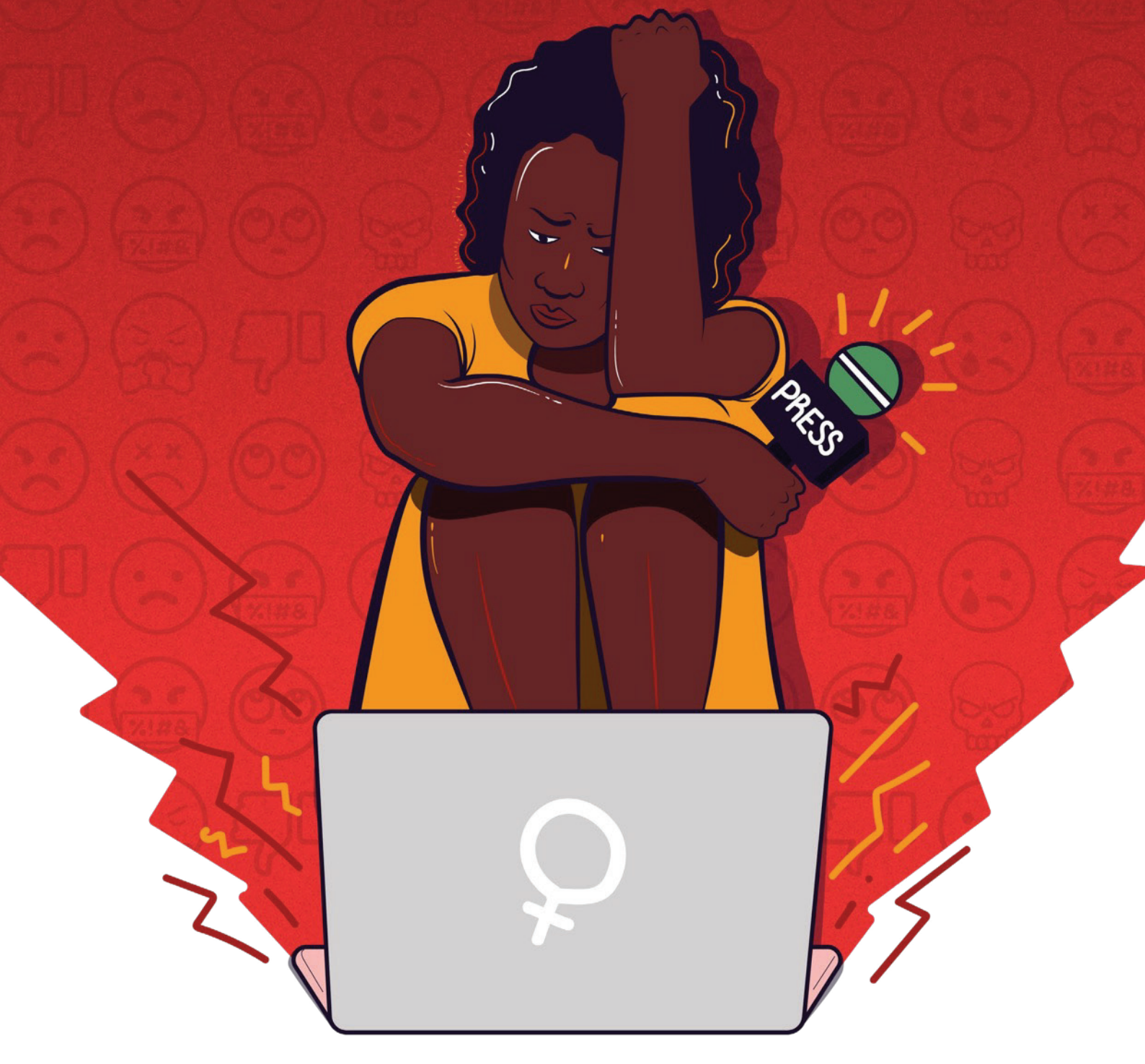
Digital Security Toolkit for Female Journalism Students

Written by Cecilia Mwende Maundu



Overview

Module 1: Background and Introduction

Purpose of the toolkit
Brief on the current digital landscape and challenges female journalists face.
The importance of digital security and its intersection with gender issues

Module 2: Online Gender-Based Violence

Definition and types of online gender-based violence
The psychological, social, and professional impacts on victims Recognizing and responding to signs of digital harassment Real-life examples and case studies

Module 3: Digital Security and Safety

Importance of digital hygiene
Best practices for secure online communication Creating and managing strong passwords
Recognizing and countering phishing attempts and social engineering Privacy settings on major platforms and understanding digital footprints

Module 4: Data Protection

Introduction to data protection laws and regulations
Best practices for data minimization, anonymization, and de-identification The intersection of FemTech and Data Privacy
Importance of VPNs and encrypted communication tools

Module 5: Disinformation and Misinformation

Basics of digital literacy
Recognizing misinformation and biases online Strategies for verifying information and fact-checking
Real-life examples of misinformation campaigns and their impacts

Module 6: Role of Media of Main Streaming Countering OGBV

Definition and difference between misinformation and disinformation Recognizing and countering gendered disinformation tactics
Strategies for fact-checking and media literacy tailored to gendered disinformation
Ethical considerations when reporting or countering disinformation

Module 7: Cyber Communities

Importance of online communities for support and advocacy Strategies for building a positive and supportive digital presence
Navigating and participating in online forums, social media platforms, and professional net- works
Recognizing and countering echo chambers and filter bubbles

Module 8: Legal Rights and Reporting Mechanisms

Overview of international and regional laws addressing online harassment Steps for reporting online violence and harassment on major platforms Understanding rights as a digital citizen
Navigating legal recourse in cases of severe online harassment
*Role of law enforcement in countering OGBV

Module 9: Psychosocial/Selfcare

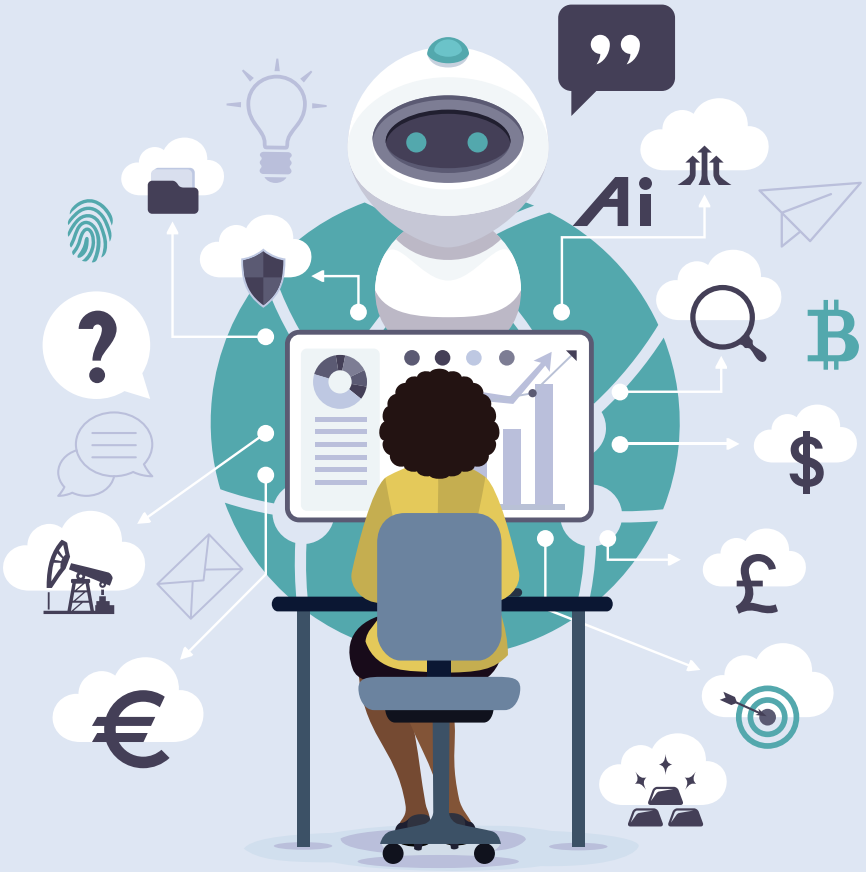
The toll of digital harassment on mental and emotional well-being Importance and strategies for digital detox
Resources and tools for mental health support tailored for journalists Balancing online engagement with offline well-being

Module 10: Stories of Resilience

Personal narratives of female journalists overcoming online violence Lessons learned, coping mechanisms, and strategies employed
The role of community and support networks in navigating online spaces Inspiring examples of positive change through resilience

Module 11: Resources

Comprehensive list of tools, platforms, and organizations for digital security Relevant literature, courses, and workshops on digital literacy and security Organizations and helplines for online harassment victims
Directory of legal resources and agencies focused on digital rights



Module 01:

Background & Introduction

In a world where every click, every share, and every tweet can broadcast one's thoughts to a global audience, the digital realm has become a vast ocean of information. Yet, lurking beneath its vastness are challenges and vulnerabilities that can turn this space of opportunity into a treacherous terrain for many, especially female journalism students.

Imagine Sarah, an aspiring journalist. She's determined, talented, and on her way to breaking a significant story. Yet, one misstep, one tweet taken out of context, and she's inundated with threats, doxxing attempts, and online harassment. A scenario not too distant from reality for many female journalists, where the line between criticism and harassment is often blurred.

This isn't to scare you, but to emphasize a reality: the digital landscape, with all its promise, holds potential pitfalls that female journalism students need to be aware of and defend against. It's not just about knowing the right tools; it's about understanding the terrain.

Let's embark on this journey together, delving into the very essence of the digital realm and why it's essential for female journalists to be equipped and aware. Ready?

Purpose of the Toolkit:
This toolkit isn't just a guide; it's an ally. A bridge between knowledge and application. The aim? To empower female journalism students like you to navigate the digital space with confidence, ensuring your voices are heard, unhindered and unthreatened.

Unpacking the Current Digital Landscape

The Global Digital Awakening:

The 21st century has witnessed a dramatic increase in global internet connectivity. By April 2023, a staggering 5.18 billion people were online, accounting for 64.6% of the world's population. Remarkably, 4.8 billion of these individuals, representing 59.9% of the global populace, engaged with social media, paving the way for instantaneous communication, rapid dissemination of information, and the formation of a global community. While this vast digital network presents numerous opportunities, it also poses distinct challenges, particularly for women journalists navigating the through the internet.

Africa's Digital Surge Amidst Global Connectivity:

In the context of global digital connectivity, Africa is showcasing a striking trajectory in its digital expansion. Between 2024 and 2028, the continent is projected to welcome an additional 280.2 million internet users, marking an impressive growth of 45.81%. By 2028, after fifteen years of consistent growth, it's estimated that the number of online users in Africa will peak at 891.93 million. This trend underscores a consistent and remarkable rise in internet users across the continent over the past years, reflecting the number of individuals actively accessing the internet in the region.

The Promise and the Peril:

The digital realm is a double-edged sword. On one side, it acts as a platform of empowerment, particularly for marginalized voices. Conversely, it can also amplify misinformation, harassment, and digital violence. In African nations, female journalists grapple with both universal and unique local challenges. They face smear campaigns, doxxing, and gender-based cyberbullying among other adversities

Challenges in Focus:

A global study highlights the perils of this digital era, revealing that 38% of women have encountered online violence, with 85% having witnessed such behavior towards other women. The field of journalism, revered for truth and accountability, isn't shielded from these threats. Half of female journalists face gender-based digital threats, according to the International Federation of Journalists (IFJ). The International Center for Journalists (ICFJ) paints an even more concerning picture: 73% of female journalists have been targets of online violence. Within this, 25% faced threats of physical harm, and 18% encountered threats of sexual violence.

Popular platforms like WhatsApp, Facebook, and Twitter can be both a boon and a bane. They promote news dissemination and public discourse but can also become conduits for misinformation and harassment. The challenge for African female journalists lies in harnessing the benefits of these platforms while safeguarding their own security and integrity.

Understanding these dynamics and challenges is the first step. As we progress through the upcoming modules, you'll be equipped with practical strategies, tools, and insights. With this knowledge, you're not just a passive observer but an empowered actor shaping the future of digital journalism

Module 02:

Online Gender-Based Violence

In the age of digital connectivity, the internet is a double-edged sword. While it offers a platform for voices to be heard, it also harbors dark corners where violence, especially gender-based, thrives.
Online Gender-Based Violence is a broad term that encompasses a variety of harmful acts or threats committed online, which are based mainly on gender, often targeting women.

Understanding the Different Forms of OGBV:

Cyberstalking: It's more than just following someone online. Victims feel like they're under surveillance. Their every move is watched, and every post dissected. Perpetrators often send persistent, unwanted, intimidating, or threatening messages.

Doxxing: Beyond revealing one's name or location, doxxing can lead to massive breaches of privacy, pushing personal details into the public domain, often inciting others to harass or threaten the victim.

Revenge Porn: A grave breach of trust, where intimate photos or videos, shared in confidence, are disseminated without consent, leading to humiliation and trauma.

Hate Speech: Aggressively discriminatory remarks, ranging from body-shaming to threats of physical violence, which can be especially venomous when targeting gender or sexual orientation.

Trolling: Not always innocent or harmless, the intention here is to humiliate, anger, or provoke the victim, often escalating to more severe forms of harassment.

Harassment: Unsolicited, often repetitive, malicious behaviors that may include threats, derogatory comments, or other forms of intimidating online actions.

Digital Abuse: The use of technologies to bully, harass, stalk or intimidate another person.

Sextortion: A form of blackmail in which sexual information or images are used to extort sexual favors or money from the victim.

Impersonation/Catfishing: Creating fake profiles on social platforms to deceive others, sometimes leading to emotional or financial exploitation.

Misogynistic abuse: Explicit gendered threats and discriminatory comments, often sexualized, that target women based on their gender.

vNon-consensual sharing of personal content: Beyond revenge porn, this includes any non- consensual sharing of pictures, videos, or information that might not necessarily be intimate but can harm one's reputation, personal life, or career.

Technology-facilitated violence: This may involve the use of spyware or other malicious software to monitor or control a victim's device, especially in intimate partner violence situations.

Exclusion: Intentionally excluding someone from digital platforms or online spaces because of their gender, gender identity, or sexual orientation.

Gender-based cyberbullying: A form of cyberbullying particularly focused on an individual's gender or gender identity.

Psychological, Social, & Professional Impacts on Victims

Victims of OGBV bear significant scars:

Psychological: Beyond anxiety and depression, many victims experience intense fear, leading to self-imposed isolation, or even self-harm. The trauma can linger, affecting trust and intimacy in personal relationships.

Social: Personal relationships can be strained. Friends or family may distance themselves, either out of fear of being targeted themselves or misunderstanding the severity of the situation.

Professional: Harassment and threats can affect one's ability to work. Women in visible roles, especially journalists, might self-censor or entirely withdraw from their professions.

Recognizing and Responding to Signs of Digital Harassment

i. **Identifying Warning Signs:** Recognizing patterns like unsolicited messages, activities from anonymous accounts, or consistent negative interactions.
ii. **Safety Measures:** Implementing actions like tightening privacy settings, employing two-factor authentication, and practicing good digital hygiene.
iii. **Reporting Mechanisms:** Making use of platform reporting tools, understanding the legal avenues available, and documenting evidence of abuse.
iv. **Support Channels:** Reaching out to organizations or professionals that specialize in digital safety, mental health, and well- being.

Real-life Examples and Case Studies

Case Study A:
Maria Ressa

Maria Ressa, a Nobel Peace Prize and UNESCO/ Guillermo Cano World Press Freedom Prize Laureate of 2021, is the CEO of Rappler in the Philippines and previously worked as a CNN war correspondent.

After Rodrigo Duterte's election as the Philippine President in 2016, Ressa became a target of intensified online hate, with government propagandists propelling a campaign to arrest her.

By 2022, she faced a cyber libel conviction and seven other legal challenges, all following years of threats, attacks, and dehumanizing tactics that were state-sponsored.

Analysis from "The Chilling" examined 2.5
million posts targeting Ressa and journalist Carole Cadwalladr, indicating the attacks were instigated by their identities as female journalists.

Despite these ordeals, Ressa's resilience and global backing highlighted the dangers of online gender-based violence against journalists.

Case Study B:
Carole Cadwalladr

Carole Cadwalladr, a British journalist, is celebrated for unveiling the Facebook- Cambridge Analytica scandal linked to Trump's 2016 campaign and the Brexit referendum.

Following the initial release of her investigative series in The Guardian and Observer, Cadwalladr was engulfed in an online hate campaign, leading to persistent legal challenges by political figures.

The abuse was predominantly gender-specific, attempting to erode trust in her work. Beyond online harassment, she was physically stalked in 2018 and confronted numerous defamation claims, recognized as SLAPPs by entities like Reporters Without Borders.

An analysis of 2.1 million tweets sent to Cadwalladr between December 2019 and January 2021 confirmed the intention to discredit her.

However, she remained undeterred, continuously seeking solutions and actively challenging disinformation.

These two case studies, along with other examples, will be examined further in Module 10: Stories of Resilience.

Module 03:

Digital Security & Safety

Importance of Digital Hygiene

Mastering digital security isn't just an option in the face of rising digital threats, especially for high-risk groups like female journalists. It's a necessity to ensure stories, sources, and personal security remain uncompromised.

address, avoid clicking on unsolicited links, and never download attachments from unknown sources.

Software Updates: They aren't just about new features. Most updates patch security vulnerabilities that hackers could exploit. Staying updated means staying protected.

Digital Security Basics

- **Encryption:** It isn't just tech jargon but a way to turn data into an unreadable format, resembling a coded language decipherable only by its intended recipients.
- **Authentication:** A mechanism ensuring users are who they claim to be, much like security officers verifying IDs.
- **Firewall:** Visualize it as a filter, keeping threats at bay while permitting regular data flow.

Digital Security Tools

- **Password Managers** (e.g., LastPass, Dashlane): Store and retrieve complex passwords seamlessly.
- **VPNs** (e.g., NordVPN, ExpressVPN): Beyond encrypting data, VPNs mask your digital footprint, making it difficult for potential attackers to trace activities back to you.
- **Encrypted Communication Tools** (e.g., Signal, Telegram): They guarantee that your messages are read only by the intended recipient, not by prying eyes lurking in the digital shadows.
- **Two-Factor Authentication:** A dual security layer, combining a password with an additional verification step.

Digital Safety Practices

- **Password Discipline:** Don't reuse passwords. Regularly rotate through strong, intricate passwords, avoiding obvious choices like birthdays or sequential numbers.
- **Guard Against Phishing:** Be wary of suspicious emails. Check the sender's

Privacy Settings on Major Platforms & Understanding Digital Footprints

The Role of Digital Platforms in User Security: Online platforms have transformed from mere interaction spaces to ecosystems where users invest significant time. Recognizing their responsibilities, these platforms now act as custodians of user safety;

The Mechanisms in Play Automated Monitoring and AI: These digital sentinels are ever-watchful. They automatically detect and act on suspicious activities, be it an attempted hack, a spammy link, or a harmful file.

User Feedback Systems: Empowering users to be the eyes and ears. Platforms rely on users to report malicious activities, which are then reviewed and acted upon.

Regular Safety Updates: Just as a city adapts to new challenges, platforms evolve. They constantly roll out safety updates, making it harder for malicious entities to exploit them.

Enhanced Authentication Protocols:
Beyond the password, platforms are using biometrics, two-factor authentication, and more to ensure that a user's space isn't breached.

Education and Awareness:
They often provide resources, tutorials, and guidelines on digital safety, ensuring users know how to protect themselves.

Examining the Giants: How They Uphold Security

Facebook: One of the pioneers in using AI for content moderation, Facebook swiftly detects suspicious activities. The platform offers tools such as login approvals and aids in recognizing unauthenticated logins. Their collaborations with external safety organizations further enhance their security measures.

Twitter: Prioritizing user safety, Twitter has integrated features like two-factor authentication and advanced reporting mechanisms. Their proactive stance against online harassment is reflected in their continually evolving policies and quick response mechanisms.

Instagram: Catering to a younger audience, Instagram ensures that safety isn't compromised. Features that allow users to limit comments, filter specific words, and curate their audience are testimony to their commitment. Their "Close Friends" feature and private account options further offer users choices in how they want to engage.

LinkedIn: Holding the flag high for professional interactions, LinkedIn is vigilant against any form of harassment. They've embedded tools for blocking, reporting, and, importantly, AI-driven content moderation mechanisms that ensure the platform's professional integrity remains uncompromised.

Case Study:

Piers Morgan's Twitter Hack

Background: Piers Morgan, a renowned British journalist and television personality, has a significant online presence, with millions of followers on platforms like Twitter. Given his often-polarizing opinions, Morgan's digital presence attracts both avid supporters and vocal critics.

Incident: In December 2022, as reported by the New York Post, Piers Morgan became the target of a cyberattack. Hackers infiltrated his Twitter account, renaming it "Piers Moron" and posting a slew of offensive tweets. Among these, several misleadingly invoked Queen Elizabeth II's name in an inappropriate manner. While the Queen had passed away in September 2022, any misuse of her name, especially in such a manner, was considered deeply offensive and hurtful to many.

Impact
Disrespect to a National Figure:

By bringing the recently deceased Queen lizabeth II into the narrative, the hackers created a heightened sensitivity around the incident. The tweets were not only seen as an attack on Morgan but also as a show of profound disrespect to a national symbol.

Potential Damage to Reputation: The false tweets, given their offensive nature and the misuse of the Queen's name, risked serious damage to Morgan's reputation. Those unaware of the hack could mistake these posts as Morgan's own, leading to a potential backlash against him.

Data Privacy Threat: The infiltration of Morgan's account raised concerns about the exposure of his private conversations or direct messages, potentially containing confidential information.

Doubts on Platform's Security: The incident brought forward pressing questions about Twitter's security mechanisms, especially when it comes to safeguarding high-profile accounts.

Resolution and Countermeasures

Immediate Account Recovery: Recognizing the breach, Twitter swiftly intervened, restoring Morgan's account to its original state and erasing the derogatory content.

In-depth Investigation: Following the cyberattack, an internal investigation would have likely been launched by Twitter to discern how the security breach occurred and to ensure similar incidents are prevented in the future.

Enhanced Security Protocols: Morgan would have been advised to ramp up his account's security, using features such as two-factor authentication, secure password practices, and regular security checks.

Transparent Communication: Upon regaining control of his account, it was crucial for Morgan to communicate openly with his audience, explaining the situation, assuring them of heightened security measures, and clarifying any misconceptions stemming from the unauthorized tweets.

The cyberattack on Piers Morgan's Twitter, coupled with the inappropriate evocation of Queen Elizabeth II's name posthumously, emphasizes the complex challenges of the digital age. The episode underscores the importance of robust digital security measures, especially for prominent public figures, and the necessity for platforms like Twitter to continually refine and fortify their security mechanisms.

Module 04:

Data Protection

In today's digital age, personal data has become a new currency. Whether it's the social media platform you browse, the news portal you frequent, or the online shopping site you use, every click, every view, every purchase is recorded, analyzed, and often sold. As female journalism students, it's imperative to understand the significance of these digital footprints, especially when pursuing stories, making contacts, or even expressing opinions online.

Several international, regional, and country-specific laws and regulations have been enacted to protect the rights of individuals and their personal data. The European Union's General Data Protection Regulation (GDPR) is a notable example, setting stringent guidelines on how data must be handled, stored, and protected. Closer to home, countries in Africa, like South Africa's Protection of Personal Information Act (POPIA) and Kenya's Data Protection Act, are making strides in ensuring digital data safety.

Best Practices for Data Minimization, Anonymization, and De-Identification

Protecting data isn't just about complying with laws; it's about fostering trust and ensuring ethical standards. Here's a look at some best practices:

Data Minimization: The less data you hold, the less risk there is. Always question if you need the specific piece of data before collecting or storing it. For journalists, this means being judicious about what details are crucial for a story or contact.

Anonymization: This involves stripping data of personally identifiable information where identification of data can not occur without additional information that is held separately.

De-Identification: It's a broader term than anonymization, where data might not be entirely anonymous, but is modified to eliminate or reduce the risk of unintentional disclosure of personal information.

For a female journalism student, utilizing these practices can ensure that the sources they interact with or the people they report on are protected from potential harm.

The Intersection of FemTech and Data Privacy

FemTech, a term coined to describe technology geared towards women's health, is revolutionizing how women understand and take control of their bodies. Apps that track menstrual cycles, fertility, and even menopause symptoms have gained significant popularity. However, with such intimate data being shared, concerns over privacy become paramount.

For aspiring female journalists, it's a sector ripe for investigation and reporting, but understanding the data dynamics is crucial. How are these apps storing menstrual cycle data? Who has access? Are they being monetized? These are hard-hitting questions that need answers in today's age.

Importance of VPNs and Encrypted Communication Tools

VPNs (Virtual Private Networks) and encrypted communication tools have become essential tools in a journalist's toolkit, especially for women in regions or countries where freedom of speech may be suppressed.

VPNs: They help mask your online activities, making it difficult for third parties to track your actions or access your data. For journalists working on sensitive stories, a VPN can be a lifeline, ensuring that their research or sources aren't compromised.

Encrypted Communication Tools:
Platforms like Signal or WhatsApp provide end-to-end encryption, ensuring that only the sender and receiver can read the content. For female journalists, this ensures that communications, whether with sources, editors, or peers, remain confidential.

As female journalism students prepare to enter a world where the boundaries between the physical and digital are blurring, understanding data protection and privacy becomes not just a professional requirement but a personal necessity. Stay safe, stay informed, and always be empowered with knowledge.

Module 05:

Disinformation & Misinformation

Basics of Digital Literacy

In a world dominated by digital devices, algorithms, and instantaneous news cycles, discerning between information and misinformation has become increasingly challenging. Digital literacy, at its core, is not merely about knowing how to use a computer or smartphone. It's the ability to find, evaluate, utilize, share, and create content using information technologies and the internet. This understanding extends to comprehending the vast digital landscape, discerning credible sources from non-credible ones, and navigating online content responsibly and ethically.

In an era where stories emerge on platforms like Twitter before reaching mainstream news and where viral TikTok content can shape global narratives, mastering digital literacy is paramount. For upcoming female journalists, it's not just about wielding digital tools, but also grasping the implications these digital domains have on their narratives and potential biases they might face.

Recognizing Misinformation and Biases Online

The internet is rife with misinformation, and biases often lurk in the shadows. These biases can range from gender, race, political leanings, to even more subtle forms like confirmation bias, where individuals unconsciously interpret information in a way that confirms their pre-existing beliefs.

For instance, in 2019, a study found that certain algorithms on social media platforms tend to push polarized content, further deepening societal divides. As female journalists, understanding and recognizing these biases is the first step in ensuring balanced reporting.

Strategies for Verifying Information and Fact-Checking

In the era of 'fake news,' verifying information has become more critical than ever. Here's a strategy that budding female journalists can adopt:

1. Source Verification: Always check where the information originated. Is the source reputable?
2. Cross-Reference Facts: Before trusting a source, check the same information across multiple reputable platforms.
3. Check Dates and Timelines: Old news can often be recycled and represented as current.
4. Reverse Image Search: Tools like Google's reverse image search can track the origin of photos, helping debunk doctored images.
5. Consult Experts: When in doubt, consult with experts in the field.
6. Use Fact-Checking Websites: Platforms like Snopes or FactCheck.org can be incredibly valuable.
7. Analyze the website: Look at the URL. Does it end in ".com.co"? This might be a fake version of a reputable source.

Real-Life Examples of Misinformation Campaigns and Their Impacts

Misinformation isn't just about a stray false news article. Organized misinformation campaigns have swayed political elections, jeopardized public health (as seen with COVID-19 misinformation), and amplified gender biases.

For instance, during the 2016 US Presidential Elections, misinformation campaigns played a pivotal role, with fabricated stories receiving significant traction. Closer to home for our African audience, misinformation about health remedies and political unrest has often spread like wildfire on platforms like WhatsApp, leading to dire consequences.

Digital literacy isn't just about discerning truth from fiction; it's about equipping oneself with the tools to navigate the complex digital landscape confidently. For female journalism students, this journey is interspersed with unique challenges, but armed with knowledge and critical thinking, they can rise above and lead with credibility.

Module 06:

Role of Media of Main Streaming Countering OGBV

Online gender-based violence (OGBV) casts a dark shadow over the digital landscape, particularly for women and marginalized communities. It's a problem intensified by the rapid spread of misinformation and disinformation, which can perpetuate harmful stereotypes and beliefs. At the forefront of this battle stands the media, wielding significant influence and responsibility. How exactly does the media counter OGBV, especially in the misinformation era? This module delves into that pivotal role.

Difference between Misinformation and Disinformation

Misinformation and disinformation, while often used interchangeably, are not the same. Understanding the nuances is crucial for media practitioners:

Misinformation: False or misleading information shared without harmful intent. It often spreads due to lack of knowledge or misinterpretation.

Disinformation: False information shared with the explicit intention to deceive, often weaponized for political, commercial, or other malicious objectives like perpetuating OGBV.

When gendered biases infiltrate these misleading narratives, they can exacerbate OGBV, making the media's role in discerning and combating such narratives all the more essential.

Recognizing and Countering Gendered Disinformation Tactics

Disinformation, particularly when gendered, can be subtle and cunning, often preying upon deeply entrenched societal norms and prejudices. Recognizing its signs involves:

Stereotyping: Exaggerated or false claims based on gender norms. For instance, suggesting that all women are overly emotional or that all men are aggressive.

Impersonation: Using fake profiles, often of women, to spread falsehoods. This can exploit societal tendencies to trust or believe women in certain contexts, or to discredit women in others.

Trolling: Deliberate attempts to provoke or harass, often gender-specific. This can be done by individuals or organized groups.

Image-Based Abuse: Using manipulated or real images to harass or blackmail. This might include tactics like "revenge porn" or digitally altered photos to defame someone.

Countering such tactics requires:

Media Literacy: Understand the source of information and its potential biases.
Example: Sarah notices a website consistently portrays women in a negative light. Recognizing its gender bias, she seeks more balanced sources.

Critical Thinking: Question the content before accepting or sharing.
Example: James sees a post claiming men can't be emotionally sensitive. He reflects on contrary real-life examples and hesitates to share the post.

Fact-Checking: Rely on trusted platforms and tools to verify information.
Example: Maria finds a claim that "95% of tech jobs are held by men." Before sharing, she consults reliable databases and finds the statistic is exaggerated.

Strategies for Fact-Checking and Media Literacy Tailored to Gendered Disinformation

A fact is a powerful antidote to deception. Here's how the media can equip itself:

Questioning Sources: Use advanced digital tools to verify images, video footage, or claims.

Collaborative Efforts: Share information with other media houses. A collective counter-narrative is more potent.

Training: Regular workshops to upgrade skills and stay abreast of the latest gendered disinformation tactics.

Ethical Considerations When Reporting or Countering Disinformation

Protect Identities: Especially crucial when discussing OGBV. Victims' identities must be protected unless they choose to go public.

Double-Check Facts: Before publishing, always double-check. Misinformation can harm credibility.

Transparency: If a mistake is made, acknowledge it transparently and correct it.

Avoid Amplifying: Sharing even to debunk can give it more visibility.

The Pivotal Role of Media in Countering OGBV

The media doesn't just reflect society—it shapes it. Here's how the media actively challenges OGBV:

Awareness & Education:
By spotlighting OGBV incidents and highlighting gendered misinformation, media educates and creates a more informed public.

Challenge Norms & Stereotypes:
Actively debunk myths and portray women in empowered roles.

Provide a Platform for Voices:
Allow OGBV victims to share their stories.

Collaboration & Partnerships:
Join forces with NGOs and tech companies to amplify efforts.

Policy Influence: Persistent, sensitive reporting can influence and drive policy changes.

The media's role against OGBV, especially in the age of misinformation and disinformation, is multifaceted and indispensable. Recognizing and acting upon its responsibilities, the media can significantly impact how society perceives and confronts OGBV.

Module 07:

Cyber Communities

In an increasingly digital world, communities have transitioned from physical spaces to online platforms. For female journalism students, these online spaces not only offer avenues for professional growth but also provide essential support systems. This module will guide you through the realm of digital engagement, emphasizing the creation and nurturing of positive communities and understanding the potential pitfalls.

Importance of Online Communities for Support & Advocacy

Professional Growth: Online communities can be treasure troves of resources, mentorship, and opportunities tailored for budding female journalists.

Emotional Support: They offer spaces where individuals can share experiences, seek advice, and find solace among peers who understand their challenges.

Amplification: Collectively, these communities can amplify issues, driving them to the forefront of public discourse, essential for advocacy efforts.

Strategies for Building a Positive and Supportive Digital Presence

Consistent Branding: Maintain a consistent persona across platforms, reflecting your professional aspirations and values.

Engage Actively: Comment, share, and engage in discussions that align with your interests and values.

Be Authentic: Authenticity builds trust. Share your journey, the highs and lows, to connect genuinely with your audience.

Build Your Network: Connect with mentors, peers, and industry professionals to broaden your horizon and opportunities.

Navigating and Participating in Online Forums, Social Media Platforms, and Professional Networks

Platform Etiquette: Understand the unwritten rules and norms of each platform.

Privacy Settings: Familiarize yourself with and regularly update your privacy settings to safeguard your information.

Join Groups & Forums: Participate in niche groups that resonate with your interests and career goals.

Engage Respectfully: Online discussions can become heated. Engage with empathy and understanding, avoiding online spats.

Recognizing & Countering Echo Chambers & Filter Bubbles

Echo Chambers: Places where individuals are only exposed to information that aligns with their current beliefs, leading to a narrowed worldview. Example: Jake joins a Facebook group where everyone opposes climate change. Over time, only seeing posts doubting climate science, he becomes more entrenched in his skepticism.

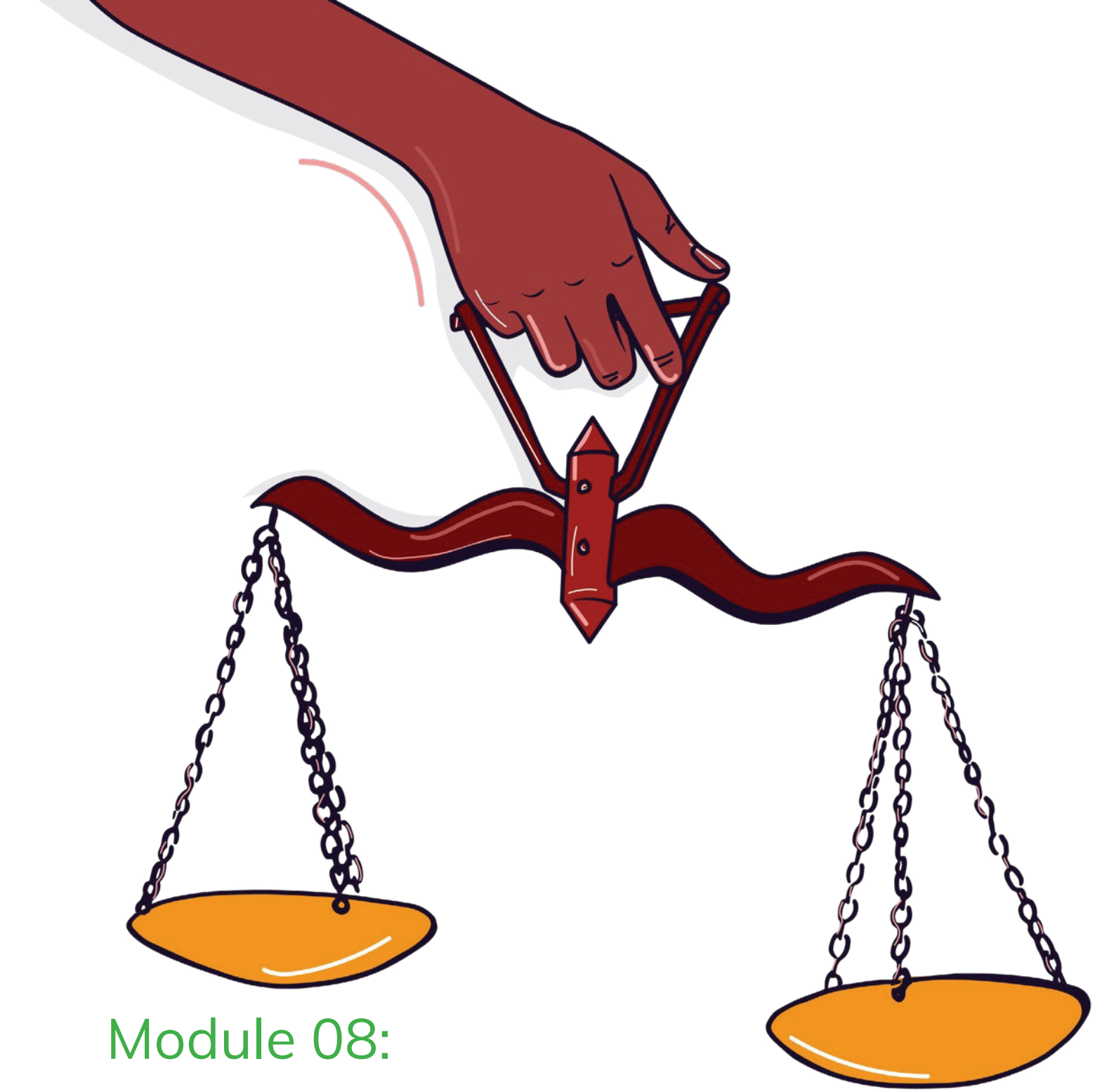
Filter Bubbles: Algorithm-driven content that aligns with a user's preferences, limiting exposure to diverse perspectives. Example: Lisa always clicks on celebrity gossip articles. Soon, her news feed is dominated by similar content, pushing out varied topics like global news or scientific discoveries.

Strategies to Counter:

Diversify Sources: Deliberately seek out and follow diverse voices and sources of information.

Engage in Constructive Debate: Engage in discussions outside your comfort zone, understanding other perspectives.

Fact-Check: Verify the information before sharing, especially in insular communities.
The digital realm offers unparalleled opportunities for engagement and community building. However, it's crucial to approach it with intention, understanding both its potential and pitfalls. As budding journalists, your online engagements can shape not only your career but also the broader digital discourse. Engage wisely and constructively, building a community that uplifts and supports, while always remaining open to diverse perspectives.



Module 08:

Legal Rights & Reporting Mechanisms

In the sprawling digital universe, the protection of rights is paramount. This is even more pertinent for female journalists, who may disproportionately face online threats and harassment. While the digital challenges are abundant, the evolution of legal structures and platform-specific mechanisms offers hope.

Overview of International and Regional Laws Addressing Online Harassment

Globally, nations and regional bodies are acknowledging the pressing issue of online harassment. The UN's Resolution on Cyber Violence marks a milestone in recognizing online harassment as a violation of human rights. Meanwhile, regions like the EU have their framework, such as the Digital Services Act, to protect online users.

In Africa, the African Declaration on Internet Rights and Freedoms sets a standard, emphasizing the importance of countering online gender-based violence.

Reporting Online Violence on Major Platforms

Twitter: Navigate to the offensive tweet > Click on the dropdown arrow > 'Report Tweet.'

Facebook: Choose the post or profile > Click on the three dots > 'Find support or report.'

Instagram: Select the offensive post or profile > Tap on the three dots > 'Report.'

Each platform has its nuances, but the priority is user safety.

Rights of a Digital Citizen:

Digital Privacy: Every individual deserves to be shielded from unsolicited data collection and surveillance.

Digital Expression and Information: A space to voice opinions, share ideas, and access information without intimidation or censorship. Digital Education: The right to comprehend and navigate the online world securely and responsibly.

Digital Protection and Security: Every netizen deserves protection from cyber threats.

Redressal and Access to Justice: Clear avenues for justice and remediation when digital rights are breached.

Digital Decent Work: Assurance of rights and fairness in the digital working environment.

Navigating Legal Recourse in Cases of Severe Online Harassment

Facing severe harassment? Consider:

Evidence Collection: Retain screenshots, URLs, and date stamps; they can be invaluable evidence.

Legal Consultation: Engage with a legal expert to comprehend if there's a solid ground to initiate legal proceedings.

Jurisdictional Understanding: It's pivotal to recognize that laws addressing online harassment might vary regionally.

Role of Law Enforcement in Countering OGBV

Threat Investigation: Address and probe into credible online threats.

Collaboration with Platforms: Work in tandem with digital platforms to identify perpetrators.

Public Awareness: Disseminate knowledge about digital threats, preparing the public for potential online challenges.

In the digital domain, arming oneself with knowledge and understanding the plethora of rights and tools available can pave the way for a safer and more inclusive online environment for all.

Module 09:

Psychosocial/ Selfcare

In an age where being connected is the norm, our digital well-being has become as crucial as our physical health. For female journalism students, who often face the brunt of online harassment, understanding and prioritizing mental and emotional health is paramount.

The Toll of Digital Harassment on Mental & Emotional Well-being

Digital harassment extends far beyond virtual inconveniences; it causes genuine psychological trauma.

The global study of online violence against women journalists revealed that 26% of female journalists surveyed who experienced online violence identified mental health impacts as the most significant consequence. Additionally, 12% sought medical or psychological assistance, and 11% took leave from work to recover. Gendered harassment, in particular, deeply ingrains feelings of self-doubt, fear, and isolation.

Importance and Strategies for Digital Detox

The digital realm is vast and engaging, but stepping back is essential. Here's a comprehensive look at the importance of digital detox and the strategies to effectively implement it.

Importance of Digital Detox

Reduces Stress: Constant notifications and the barrage of news updates can be overwhelming. Taking a digital break can help recalibrate emotions and reduce anxiety.

Improves Sleep: Allocating screen-free time, especially before bedtime, can significantly improve sleep cycles, leading to more restful nights.

Enhanced Focus: The distractions that come with digital devices can scatter our attention. Disconnecting can allow for deeper concentration on tasks and can increase productivity.

Better Physical Health: Extended device usage can contribute to physical issues such as eye strain, headaches, and poor posture. A detox can alleviate some of these problems.

Improved Social Connections: While digital communication is convenient, face-to-face interactions often foster deeper, more meaningful connections.

Decreased Dependency: Lessening our time on digital devices can curb the feeling of "needing" to constantly check them, promoting a more balanced lifestyle

Strategies for Digital Detox:

Scheduled Breaks: Designate specific times during the day or week to disconnect from all digital devices. This can be during meals, the first hour after waking up, or the last hour before bedtime.

App Limitations: Utilize built-in smartphone features or third-party apps to set daily or weekly limits on app usage, especially for particularly distracting apps.

Offline Activities: Allocate time for non-digital activities such as reading physical books, taking nature walks, journaling, or practicing a hobby.

Digital Sabbatical: Consider dedicating a full day weekly or monthly where you go entirely offline, disconnecting from all digital platforms.

Notifications Management: Turn off non-essential notifications. This reduces the frequency of interruptions and the urge to continually check your device.

T**ech-Free Zones:** Designate areas in your home, such as the dining room or bedroom, where devices are not permitted, promoting quality family or personal time.

Mindful Consumption: Rather than mindlessly scrolling through feeds, be intentional about the content you consume. Engage with quality content and avoid excessive digital multitasking.

Resources and Tools for Mental Health Support Tailored for Journalists

ICFJ Mental Health Toolkit:
Resources to address mental issues, from post-traumatic stress disorder to digital wellness.

Journalist Trauma Support Network:
An international community of qualified therapists trained to care for trauma-impacted journalists.

International Women's Media Foundation:
A Mental Health Guide for Journalists Facing Online Violence.

Support Groups: Forums where journalists can discuss their experiences and seek advice.

Balancing Online Engagement with Offline Well-being

It's crucial to understand that while the digital space offers opportunities, real life remains primary.

Set Boundaries: Decide on specific hours when you won't check social media.

Physical Activity: Regular exercise can counteract the stress of online negativity.

Mindfulness Practices: Activities like meditation can ground you in the present.

As female journalism students brave the digital landscape, the shield of self-care and psychosocial awareness is their strongest ally. Prioritizing mental health isn't just an act of self-love; it's a professional necessity.

Module 10:

Stories of Resilience

Resilience in journalism is evident in the journey of a journalist fraught with challenges, especially for women journalists who find themselves at the intersection of their professional calling and their gender. These women not only bear the responsibility of accurate reporting but also have to navigate a digital minefield of gendered abuse, harassment, and threats. This module shines a light on their journeys, the challenges they overcame, and the mechanisms they employed to continue their mission.

Personal narratives of female journalists overcoming online violence:

Case Study A:

Maria Ressa - The Intersection of Journalism, Gender, & State- Sponsored Online Harassment.

Background: Maria Ressa, celebrated as a Nobel Peace Prize Laureate and UNESCO/ Guillermo Cano World Press Freedom Prize Laureate of 2021, stands tall in the world of journalism. The CEO of Rappler, a digital news platform in the Philippines, Maria has previously carved a reputation as a CNN war correspondent over two decades.

Incident: Post the election of Rodrigo Duterte as the President of the Philippines in 2016, Maria became the center of a whirlwind of online abuse. This intense attack was not just on her identity as a woman but also on her professional role as a journalist. Her decision in 2017 to address this online violence only intensified the attacks on her, with orchestrated campaigns, notably by government propagandists to push the hashtag #ArrestMariaRessa.

Impact: By 2019, she found herself arrested twice in a single month. At the time she penned her foreword in "The Chilling" in July 2022, Maria was grappling with a cyber libel conviction, one of the eight legal cases instigated by the Philippine government. Over these six tumultuous years, she was subjected to an array of threats, including rape and murder.

Revealing investigations tied these online attacks directly to the state, further empowered by technological platforms. They also correlated with the real-world legal challenges she faced.

Analytical insights from "The Chilling" studied over 2.5 million social media posts targeting Maria and her colleague Carole Cadwalladr. It became evident from the study that their roles as women journalists drove the attacks.

Resolution: Maria's story, with all its challenges, resonates with courage and an undying spirit. Her resilience, bolstered by global recognition and support, brings to the fore the deep-seated issue of online harassment and its tangible repercussions. By persistently highlighting these concerns and not succumbing to the pressure, Maria emerges as a beacon of hope and resilience in the fight against online gender- based violence in the journalistic world.

Case Study B:

Carole Cadwalladr - Exposing Scandals and Facing the Wrath of Disinformation

Background: Carole Cadwalladr has been recognized globally for her remarkable investigative journalism that brought the Facebook-Cambridge Analytica scandal into the limelight. Her insights connected the data misuse to significant global events, including the 2016 U.S. election and the Brexit referendum.

Incident: Upon the publication of her groundbreaking series in The Guardian and Observer, Carole was immediately thrust into a virulent online harassment campaign. This gender-specific attack subsequently led to continuous legal troubles spearheaded by political figures.

Impact: Online Harassment: Carole's major platform of abuse was Twitter. Amplified by pro-Brexit groups, right-wing media, and even established media figures, the objective was clear

– discredit Cadwalladr and consequently, erode trust in her reportage. The abuse distinctly carried a gendered tone, often reducing her to derogatory labels.

Physical Threats: The intimidation was not confined to the digital realm. In 2018, an individual, informed by a military and cyber espionage background, stalked Cadwalladr. Initial friendly approaches morphed into menacing threats.

Legal Harassment: Carole was confronted with multiple defamation claims, most notably by Arron Banks, a pivotal figure in her investigations. Some tweets from Banks bordered on direct intimidation, resonating with clear gendered undertones. Such defamation claims have been characterized as Strategic Lawsuits Against Public Participation (SLAPPs) by bodies like Reporters Without Borders (RSF).

Analysis: A comprehensive study analyzed around 2.1 million tweets directed at Carole between December 2019 and January 2021. Out of these, 10,400, determined through Natural Language Processing, were unabashedly abusive. Delving into data and interviews, the intent became evident – undermine Cadwalladr and her revelations, especially concerning platform-related misinformation.

Resolution: In the face of adversity, Carole Cadwalladr's spirit remained unbroken. Continuously delivering on her journalistic commitments, she also established support groups for fellow women journalists. Her proactive approach towards addressing social media accountability and countering political actors sets her apart. For Carole, the aim remains clear – combat disinformation, rather than remain a passive victim.

Case Study C:

Women Journalists of Daily Maverick - Courage Amidst Hostility

Background: The Daily Maverick is an influential South African news platform known for hard-hitting investigative journalism. Their journalists, especially women, have often faced backlash for their relentless pursuit of truth.

Incident: "Section 16" throws light on the harrowing experiences of four stalwart journalists from the Daily Maverick - Pauli van Wyk, Ferial Haffajee, Caryn Dolley, and Marianne Thamm.

The documentary contrasrs their personal narratives with findings from a UNESCO and ICJ study, vividly portraying the gendered threats and hostility they face in their line of work.

Impact: Marianne Thamm: After her incisive reportage on "the dangerous contestation for power in the key Crime Intelligence division of the SAPS", Thamm's house was burgled, with her work computer stolen. The timing, immediately after she was alleged to possess classified material, made her suspect foul play linked to Crime Intelligence.

Caryn Dolley: A journalist known for her in- depth exposes on corruption within the South African Police Service, Dolley has penned significant works like "The Enforcers" and "To the Wolves". Delving into treacherous terrains such as police-gang connections, she received life-threatening warnings while probing into gun smuggling cases. Her haunting words in the documentary, "I ask when is it going to happen to me or my colleagues? Not if, but when," underscore the imminent dangers she faces.

Ferial Haffajee: With a reputation for her relentless investigative journalism, particularly around State Capture, Haffajee has faced gruesome online backlash. In retaliation to her exposures, particularly regarding the Bell Pottinger campaign, social media platforms were inundated with morphed, derogatory images of her, from being portrayed as a dancer and a cheerleader to being demeaned as an animal.

Pauli van Wyk: At the heart of exposing the VBS scandal, van Wyk meticulously traced how the

bank's funds, trusted to them by the working class, were misappropriated by senior EFF members for their opulence. She highlighted the organized nature of the attacks she faced, noting the eerie similarity in the way trolls went about their abuse.

Resolution: Despite the threats, cyberbullying, and harrowing experiences, the women journalists of the Daily Maverick persevere. Their stories, now immortalized in "Section 16", serve as both a warning and an inspiration, underlining the importance of press freedom and the gendered dimensions of its violation in contemporary society. Their resilience continues to inspire many, reaffirming the importance of press freedom and shedding light on its continuous, gendered violation.

Case Study D:

Rana Ayyub Journalism in the Face of Nationalistic Fury

Background: Rana Ayyub, an Indian investigative journalist, has been lauded internationally for her courageous reportage, especially concerning issues of minority rights, government corruption, and nationalist politics in India.

Incident: Due to her hard-hitting investigations, Ayyub has consistently found herself in the crosshairs of extensive online abuse campaigns, often orchestrated by right-wing nationalists and trolls. These campaigns have been relentless in their attempt to silence her, utilizing both threats and character assassination attempts.

Impact: The nature of the abuse hurled at Ayyub has been alarmingly gendered, involving threats of sexual violence, doctored videos, and targeted misinformation campaigns to malign her reputation. This online harassment has, on several occasions, spilled over into real-world threats, requiring her to seek police protection.

Resolution: Ayyub continues her journalistic endeavors, refusing to be silenced. With international recognition and the support of various journalism bodies, she remains a formidable voice in Indian journalism, continuously shedding light on contentious issues despite facing personal threats.

Case Study E:

Ghada Oueiss - Journalism Under the Shadow of International Politics

Background: Ghada Oueiss is a prominent Al Jazeera anchor and journalist. Her reportage has spanned across several countries and touched upon sensitive geopolitical issues.

Incident: Given her reach and the sensitivity of her topics, Oueiss has been at the receiving end of targeted online harassment campaigns, which are believed to be politically motivated. These campaigns often involve doctored images, fake news, and orchestrated attempts to discredit her journalistic integrity.

Impact: Ghada has faced gendered insults, threats, and extensive online trolling due to her reportage. These online attacks not only question her credibility as a journalist but also consistently reduce her to derogatory gendered stereotypes, often reflecting the deep-seated misogyny prevalent in online spaces.

Resolution: With the backing of Al Jazeera and several international journalism bodies, Ghada Oueiss continues her journalistic journey. She constantly counters the misinformation spread about her with facts, maintaining her stand as a fearless journalist in the volatile landscape of global politics.

Each of these case studies serves as a testament to the unyielding spirit of women journalists across the globe, who, despite facing adversities, persist in their commitment to truth and integrity.

Lessons Learned, Coping Mechanisms, & Strategies Employed

Harnessing Community Support:
Journalists like Maria Ressa and Carole

Cadwalladr found strength in collective actions and global community support, demonstrating that solidarity can counter targeted campaigns.

Documenting and Publicizing Threats:
The Daily Maverick journalists, by participating in "Section 16", showed the world the risks they face daily. By doing so, they not only spread awareness but also made it more difficult for their harassers to operate in the shadows.

Navigating Legal Challenges:
Seeking legal protection and recourse, as seen with Ayyub's case, is crucial when online harassment transitions to real-world threats.

Utilizing Technology for Safety:
From encrypted communication to tracking online misinformation campaigns, many journalists employ tech solutions to protect themselves and counter false narratives.

Leveraging Supportive Platforms:
Journalists facing backlash can benefit immensely from having a supportive platform. Daily Maverick, as an organization, stands firm behind its journalists, providing them with a foundation to continue their work amidst adversity.

Building and Relying on Networks:
This was evident with the Daily Maverick journalists, where internal support and camaraderie provided strength during trying times. Furthermore, global bodies like the Committee to Protect Journalists, UNESCO, and others play crucial roles in supporting journalists under threat.

The Role of Community and Support Networks in Navigating Online Spaces

Whether it's the global acclaim of Maria Ressa or the grassroots support for the Daily Maverick journalists, it's evident that community plays an essential role. Here are some:

Mentorships & Guidance:
Senior journalists often mentor younger colleagues, guiding them on how to navigate online spaces safely.

Professional Networks:
Bodies like the Committee to Protect Journalists, UNESCO, and others have shown support, rallying behind journalists facing undue online pressure.

Personal Communities: Families, friends, and local communities become safe spaces where journalists find solace and rejuvenation to continue their work.

Inspiring Examples of Positive Change through Resilience
Each of these journalists represents a beacon of hope, demonstrating that resilience can lead to broader societal awareness and change:

Changing Narratives: By continually highlighting their experiences, these journalists have brought the issue of online gendered harassment to global limelight, pushing tech giants and policymakers to rethink digital safety.

Educational Impacts: Their stories are now part of curriculum and workshops, training the next generation on the importance of digital security.

Inspiring Others: Their determination and refusal to be silenced inspire countless other journalists and women to raise their voices against online violence and harassment.

It's evident that the resilience of these female journalists is not just about personal triumphs. It's about changing the global narrative around online gendered violence and ensuring that the digital space is inclusive, safe, and empowering for all.

Resources

Digital Security Tools, Platforms, and Organizations:

Tools:

Password Managers: Tools like LastPass and 1Password, which help manage and generate secure passwords.
Encryption Tools: VeraCrypt for encrypting sensitive files and Signal app for encrypted messaging.

Platforms:

Tor Browser: For anonymous browsing and protecting user location and usage from network surveillance or traffic analysis.
Online Safety: Platforms like HTTPS Everywhere, which ensures encrypted connections to websites.

Organizations:

Digital Defenders: An organization offering tools and strategies for journalists facing digital threats.
International Women's Media Foundation (IWMF): A foundation supporting women journalists globally through initiatives, grants, and training.
International Center for Journalists (ICFJ): A non-profit promoting journalism worldwide through professional exchanges, fellowships, and training.
Article19: An organization dedicated to defending freedom of expression and information, named after Article 19 of the Universal Declaration of Human Rights.

Literature, Courses, and Workshops:

Book: "Digital Literacy for Dummies" by Faithe Wempen - An introduction to the digital landscape. :The Smart Girl's Guide to Privacy" by Violet Blue offers a deep dive into online privacy specifically tailored for women. :ONLINE HARASSMENT FIELD MANUAL by PEN AMERICA

Course: "Online Violence Response Hub Training" by Coalition Against Online Violence - A self-paced online course with interviews of women journalists who have been targeted by online abusers "Online Harassment: Strategies for Journalists' Defense" offered by Knight Center - Global con text of online harassment and hearing from women journalists who will speak about the strategies they have used to deal with it.

Workshop: Monthly workshops by CyberSecure Journalists on emerging threats and mitigation techniques. :Local universities and journalism schools often host digital literacy and security workshops. Check event calendars for opportunities.

Organizations and Helplines for Online Harassment:

TrollBusters: Designed for women journalists, this service offers just-in-time rescue services for those under digital attack.

HeartMob: Provides real-time support for those experiencing online harassment and helps document and report it.

Online SOS: Provides emergency assistance to those facing online harassment.

Online Violence Response Hub: https://onlineviolenceresponsehub.org/

Directory of Legal Resources and Agencies:

Media Defence: Global NGO that helps defend the rights of reporters across continents and across platforms.

The Digital Rights Foundation: Advocates for digital rights and offers legal aid for online harassment cases.