TFGBV Training: Learning about the digital world of gendered-disability-based violence

TFGBV Training: Learning about the digital world of gendered-disability-based violence

An education guide for women with disabilities, caregivers and loved ones, and service providers

EUNICE TUNGGAL; BABALWA TYABASHE-PHUME; LIEKETSENG NED; AND KAREN SOLDATIC

Contents

Family and Caregivers

Frontline Service Providers

EXIT SITE

This project was made possible with funding from:

- The Canada Excellence Research Chair (CERC) in Health Equity and Community Wellbeing;
- The Stellenbosch University Division of Disability and Rehabilitation Studies, and;
- The Sexual Violence Research Initiative (SVRI).

EXIT SITE

This resource provides an overview of technology-facilitated gender-based violence (TFGBV) as it's experienced by women with disabilities. Particularly, we highlight stories of women with disabilities living in South Africa. However, there are some important things to know before we continue.

Important things to know:

1. This resource was made to be Easy to Read and uses plain language.

---

2. The information found in this book does not only apply to women with disabilities in South Africa. While our stories and content may highlight this community, we encourage people of all nationalities, genders, and disability status to learn online safety.

---

3. While we let a lot of other women with disabilities and other professionals review this book, we know that we may have missed some things. If we did, we want to know! Please let us know in the comment section located at the bottom of the webpage.

---

4. If you are reading this resource, we want you to stay safe. We have provided an easy exit button on each page. That way, you can click off the page to the Google Search Engine quickly, in case someone unsafe is nearby. However, please keep in mind that this button **does not erase browser history**. Please use this resource safely.

The safe exit button is located on the righthand side of the page. It is a red rectangle, which says "EXIT SITE". Look for it now!

South African Support and Resources Page

Please review the following support services and resources available for South African residents. This information has been adapted from the **South African Government** (source linked here), and the UNHCR Refugee Agency (UNHCR source linked here).

We also recommend viewing the following document provided by the **National Council of & For Persons with Disabilities** (NCFPD), which details a list of gender-based violence (GBV) supports. Click here to view the resources listed by the NCFPD.

South African Police Service

The police will assist in cases of domestic violence or sexual assault, and can help you access medical attention, shelter, and victim counselling.

SAPS emergency number, call: 10111

National Helplines

- **Gender-Based Violence Command Centre; call:**
  - 0800 428 428
  - *120*7867# (free from any cellphone)
- **STOP Gender Violence Helpline; call:**
  - 0800 150 150
  - *120*7867#
- **Halt Elder Abuse Line (HEAL) – helpline for elderly people; call:**

    - 0800 003 081
    - E-mail: action@actiononelderabusesa.co.za
- **Human Trafficking helpline; call:**
    - 08000 737 283 (08000 rescue)
    - 082 455 3664
- For **Persons living with disabilities;** SMS “help” to 31531

Support Organisations

People Opposed to Woman Abuse (POWA):

Support for women affected by violence, including counselling (telephonic and in-person), legal support, and temporary shelter.

- Website: http://www.powa.co.za
- Tel: 011 642 4345
- E-mail: info@powa.co.za
- Social media: link to Facebook and link to Twitter/X

Childline South Africa:

Support for children and families dealing with abuse, trafficking, and behavioural issues.

- **Website**: https://www.childlinesa.org.za/
- **Toll-free helpline**: 116
- **E-mail**: olcadmin@childlinesa.org.za
- **Social media**: link to Facebook and link to Twitter/X

Child Welfare South Africa:

Focuses on child protection, family development, and child abuse reporting.

- **Website**: http://childwelfaresa.org.za/
- **Tel**: 074 080 8315
- **E-mail**: info@childwelfaresa.co.za
- **Social media**: link to Facebook and link to Twitter/X

Families South Africa (FamSA):

Provides support for domestic violence, trauma counselling, and divorce and family mediation.

- **Tel**: 073 213 3831
- **E-mail**: national@famsa.org.za
- **Social media**: Link to Facebook

Sonke Gender Justice:

Place to **anonymously and safely report** any incident experienced, seen or heard about.

- **Website**: Sonke Gender Justice
- **Tel**: 0800 333 059 (toll-free whistleblower hotline)
- **SMS**: 33490
- **E-mail**: sonke@whitleblowing.co.za.

Tears Foundation:

Assists survivors of domestic violence, sexual assault, and child sexual abuse.

- **Website**: http://www.tears.co.za/
- **Free SMS helpline**: *134*7355#
- **Tel**: 010 590 5920
- **Email**: info@tears.co.za
- **Social media**: link to Facebook and link to Twitter/X

Thuthuzela Care Centres:

These are one-stop facilities for victims of sexual violence, offering medical care, counselling, and legal services. Link to Website for Thuthuzela Care Centres (TCCs) for more information about province-specific supports.

Tshwaranang Legal Advocacy Centre (TLAC)

Facilitates access to justice for women who have experienced or are at risk of experiencing GBV.

- **Tel**: **011 331 0088**
- **Email**: tshwaranang@tlac.org.za
- **Website**: www.tlac.org.za

EXIT SITE

Global Support and Resources Page

Please review the following resources for global support services and crisis response networks.

No More Global Directory

No More Global Directory is an international directory of domestic and sexual violence resources in nearly every UN-recognized country and territory. You can navigate to this link to access the *No More Global Directory*, or explore the embedded page below.

An interactive H5P element has been excluded from this version of the text. You can view it online here: https://pressbooks.library.torontomu.ca/tfgbvsafetytraining/?p=1002#h5p-28

Chayn

Chayn (meaning “solace” in Urdu), is a global nonprofit, run by survivors and allies from around the world, creating resources to support the healing of survivors of gender-based violence. You can navigate to the *Chayn* global directory for support in your region by going to this link.

GENERAL INFORMATION ABOUT TFGBV

Chapter 1: What is technology-facilitated gender-based violence?

Learning Objectives

By the end of this chapter, we hope you:

- Know what technology-facilitated gender-based violence (TFGBV) is.
- Know what counts as TFGBV.

"**Technology-facilitated violence**" (**TFV**) is when someone uses technology like phones, computers, or the internet to hurt, scare, or control another person.

"**Gender-based violence**" (**GBV**), is when someone is hurt or bullied because they are a woman or gender-diverse. There are many forms of GBV.

"**Technology-facilitated gender-based violence**" (**TFGBV**), is when someone uses technology to hurt, scare, or target women and gender-diverse people. It happens online or through digital devices.

The word "violence", is used to describe a lot of different behaviours and actions that humans can do to hurt others. There are many forms of violence that can occur, such as physical violence, sexual violence.

Physical violence: this means punching, slapping, cutting, kicking or hurting the body.

Sexual violence: this means any type of sex or sexual touch that is not wanted. For example, rape or sexual assault.

Psychological or emotional violence: this means using words or behaviours to hurt or scare someone.

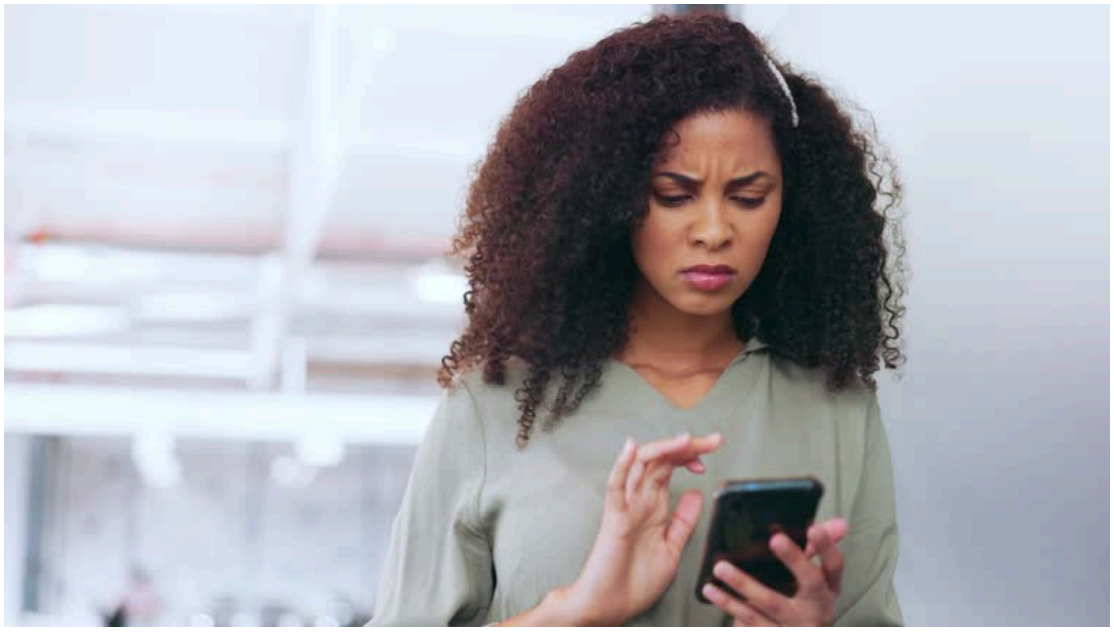
Many types of violence can that happen offline can also occur in online spaces or through using technology, which makes them forms of TFGBV. However, not all TFGBV leaves behind visible marks, injuries, or other physical evidence. Because of

this, many people do not recognize TFGBV as actual “violence”, and not treated as seriously.

So... *Is technology-facilitated violence **actually** violence?*

Question: Is “technology-facilitated” violence actually violence?

Answer: Yes. TFGBV is real violence because it causes real harm. Even though it happens through phones, social media, or online platforms, it can still affect a person’s safety, mental health, dignity, relationships, access to services, and overall wellness.



TFGBV can be very distressing. Many survivors of TFGBV are left unsure about what to do, who to tell, or how to keep the violence from happening again.

TFGBV is real but it can look different than offline violence. There is often a digital device (like a phone, computer, iPad/tablet, video game system, etc.) that physically separates the person being hurt from the person committing the violent act (the **perpetrator**).

Sometimes, **what starts as online violence can lead to offline violence.** For example, a perpetrator may begin cyberstalking someone, but eventually, begin stalking them in-person using the location they shared on social media. In many cases, online violence has led to femicide or physical abuse.

The reverse can also be true. **What begins as offline abuse** (such as domestic violence) **can then start happening using technology as weapon.** For example, a perpetrator has been committing **intimate partner violence** through emotional abuse, but soon begins controlling their partner's ability to use her phone and computer.

Activity

An interactive H5P element has been excluded from this version of the text. You can view it online here:
https://pressbooks.library.torontomu.ca/tfgbvsafetytraining/?p=30#h5p-1

What Counts as Violence?

Violence isn't always physical. It can happen with words, actions, or technology. To help you understand whether an action or event is violent, ask yourself two questions:

1. **"Is it harmful?"**
2. **"Is the harm on purpose?"**

Let's talk more about these two questions.

---

1. Is it harmful?

This question is asking if the action or event is **hurting** or **intruding on** someone's **body** (including digital images/media/content that involves your body), your **privacy**, your **feelings**, or **things that belong to you**?

Violence causes *real harm*, even if it happens online or through digital technology.

Harm can be...

- Emotional (fear, anxiety, shame, sadness);
- Social (ruined relationships, employment, education, reputation);
- Physical (threats, doxxing, stalking, stealing physical devices);
- Financial (stealing money, pressuring you to pay, ruining your career);
- Digital (hacking into accounts, sending unwanted images), or;
- Threatening to do things that will cause other forms of harm.

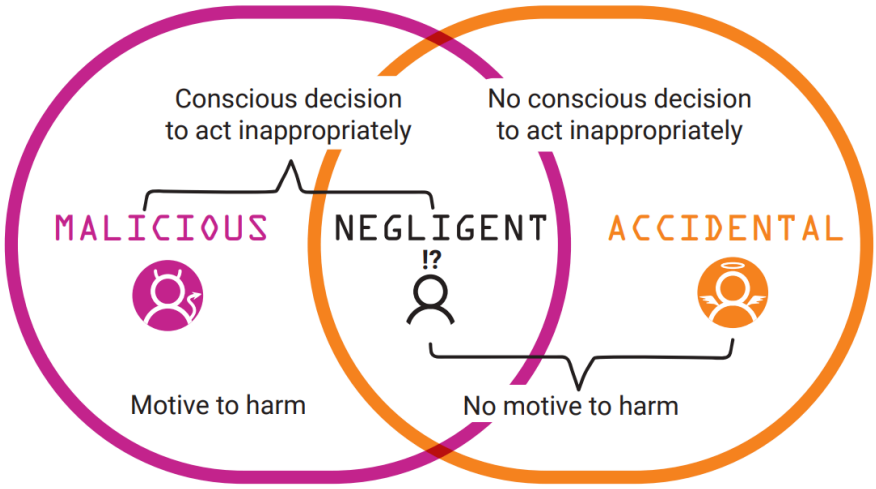
---

2. Is the harm on purpose?

Violence is intentional, not an accident. Violent actions are when someone is doing or saying something because they wish to...

- Scare;
- Hurt;
- Control;
- Embarrass;
- Pressure;
- Intimidate, or;
- Steal from someone else.

Sometimes, it's difficult to identify when something is violence, especially if it isn't a well-known form of violence. TFGBV still not well-known or recognized as violence by many people. This is why it is vital to understand the definition of TFGBV, and to be able to recognize different forms of TFGBV.



"Types of Actors" (Taken from UNFPA, 2023).

Another way to look at TFGBV and the "what is violence?" question, is by viewing threats of violence as being malicious (or, intentionally bad, or inappropriate), negligent (where there was a conscious inappropriate behaviour, but without any bad intent), or accidental (where there was no intentionally inappropriate behaviour and no bad intent).

Other terms used to refer to TFGBV

We want to make you aware of the other ways that people might refer to TFGBV. **Other terms might include:**

- Being harassed online
- Online bullying / cyberbullying
- Social media abuse
- Being "dragged" online
- Technology-facilitated violence
- Digital abuse
- Online violence
- Cyber-harassment

This list is not complete, and you may come across other terms or phrases that people use to talk about TFGBV. The important part is that you understand that these terms mean similar things.

Before we learn about about the different types of TFGBV, **check your existing knowledge with the quiz below.**

Activity

An interactive H5P element has been excluded from this version of the text. You can view it online here:
https://pressbooks.library.torontomu.ca/tfgbvsafetytraining/?p=30#h5p-2

Resources

- UNFPA. (2025). *An Infographic Guide to Technology-facilitated Gender-based Violence (TFGBV)* [Infographic Guide]. United Nations Population Fund. https://www.unfpa.org/sites/default/files/pub-pdf/An%20Infographic%20Guide%20to%20TFGBV.pdf
- UNFPA. (2023). *Guidance on the Safe and Ethical Use of Technology to Address Gender-based Violence and Harmful Practices: Implementation Summary* [Implementation Summary]. United Nations Population Fund. https://www.unfpa.org/sites/default/files/pub-pdf/UNFPA_SafeEthicalGBVTechGuide_Summary_2023.pdf

Chapter 2: Where does TFGBV happen?

TFGBV can occur across many digital spaces, and using various different technologies. In this chapter, we will **overview common digital platforms and devices** which can facilitate or become settings for TFGBV.

Learning Objectives

- Know the different places and ways that TFGBV can happen.
- Be able to identify TFGBV as it presents in different forms.

Sometimes, when we hear the terms “online abuse” or “technology-facilitated violence” we make assumptions about what they mean.

For example, many people may only think these terms apply to cyberbullying (such as strangers making mean comments on social media posts); or even non-consensual image sharing (like a bully sending out an embarrassing photo of you to the whole school through an email blast).

Mobile Devices

Mobile phones, laptops and PC computers, tablets, and wearable technology (like Apple watches) etc.) can be used to facilitate TFGBV.

This can happen through calls, texts, video chats, image sharing, and apps. TFGBV can also be facilitated by the forced restriction of access to these devices.

Everyday mobile devices can become channels for harassment, isolation, coercion, or monitoring.

Online and Social Media Platforms

Online and social media platforms allow people to **create profiles, share content, and interact with others.** TFGBV can occur through comments, messages, impersonation, or unwanted contact.

To help you think broadly, here are different types of online platforms where TFGBV can occur, with examples for each. But remember, this list is *not* exhaustive. As we have seen in the last 10 years, new platforms appear all the time!

Reflect

Think of different platforms that “online and social media platforms” might refer to. How many can you list?

Social Media Platforms

Social media platforms focus on personal networking, where users create profiles to connect with one another. **Examples include:** Instagram (Threads), Facebook (Facebook Messenger), YouTube, TikTok, Twitter/X, WhatsApp, Snapchat, LinkedIn.

How TFGBV shows up: Harassment in comments or DMs, impersonation, non-consensual image sharing, monitoring through “last seen” or story views.

Online Chatrooms and Forums

Online chatrooms and forums are digital spaces for real-time or asynchronous communication, ranging from specialized support groups and niche communities to random video chats. **Examples include:** Twitch, Omegle, Discord, reddit, 4chan.

How TFGBV can show up: Targeted harassment, doxxing, grooming, coordinated attacks, pressure to share personal information.

Dating Apps

Dating apps are mobile apps or websites where users can create profiles with the goal of creating sexual, romantic or even platonic relationships. **Examples include:** Tinder, Hinge, Facebook Dating, Grindr, Badoo, OKCupid, Bumble.

How TFGBV can show up: Coercive messaging, catfishing, threats after rejection, pressure to share intimate images, location-based stalking.

Online Gaming

Online gaming is the use of console games, PC games, or mobile games which include online, interactive elements. **Examples include:**

- **Multiplayer** online games such as League of Legends, Call of Duty, Fortnite, or Minecraft.
- **Social and interactive worlds** such as Club Penguin, Second Life.
- Online, **user driven games** such as Roblox.

How TFGBV can show up: Voice-chat harassment, targeted attacks, grooming of younger players, coercion through in-game relationships, monitoring through shared servers.

Online gaming is a common place for TFGBV to occur, particularly against female gamers.

Rideshare and Delivery Apps

These are mobile-based platforms that connect users with others for transportation (rideshare) or delivery services (food, groceries, packages). These platforms can be used by the user or the service providers to track and stalk locations, or carry out other harms. **Examples of these can include** Uber or UberEats, Bolt, KROOZ, and Mr D.

A white Bolt rideshare car, with signage on the side with the "Bolt" logo.

Monitoring and Tracking Technologies

Tools designed for convenience or safety can be misused to **track, monitor, or control** someone's movements or activities. **Examples include:**

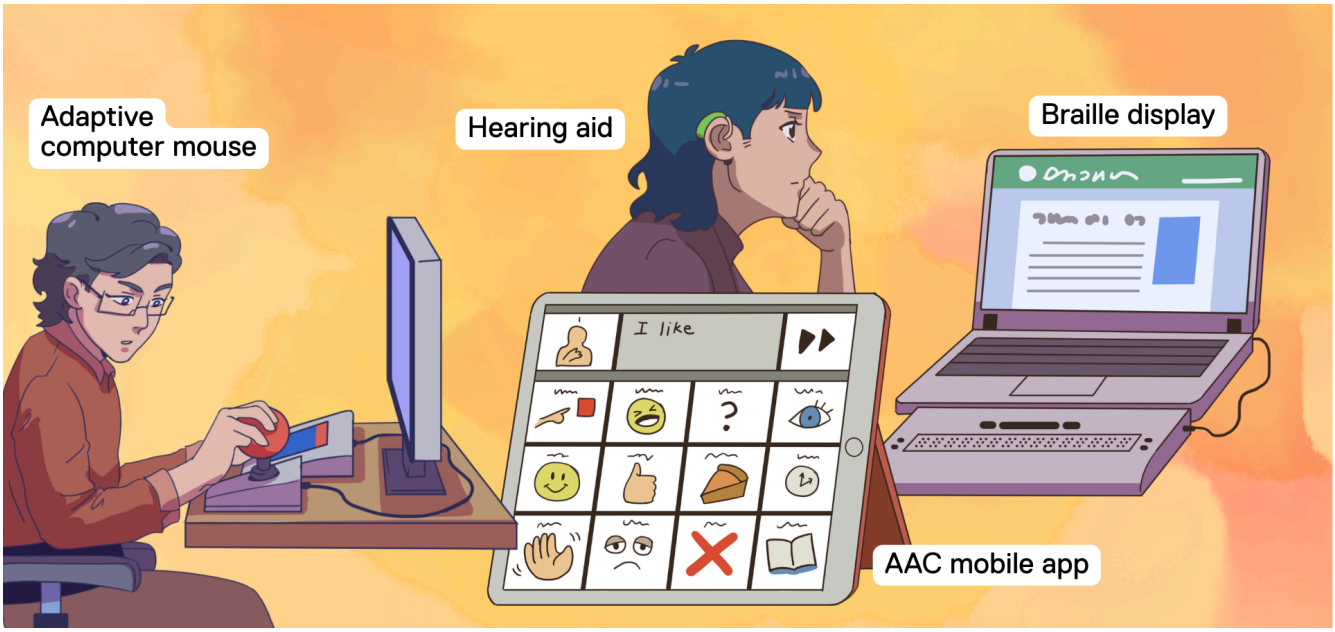
- **Computers and mobile devices:** Accessing accounts, browsing history, or installed apps.
- **GPS and trackers:** Monitoring location through phones, vehicles, wearables, or standalone devices.
- **Home security cameras:** Viewing footage from doorbell cameras, nanny cams, or hidden cameras.
- **Smart home systems:** Controlling lights, locks, alarms, or appliances to intimidate or restrict movement.

While convenient, location-tracking and surveillance systems and tools can be used for TFGBV.

Assistive Technology

Assistive technologies are designed to support independence, communication, and access. When misused, **they can become tools of surveillance, coercion, or control.** This form of abuse is often invisible because the technology is assumed to be "helpful" and innocuous. **Examples include:**

- **Screen-readers:** Monitoring what someone reads or accesses.
- **Vision-support apps:** Accessing camera feeds or location data.
- **Hearing aids with apps:** Remotely adjusting or disabling devices, tracking usage.
- **Augmentative and Alternative Communication (AAC) devices:** Restricting access, deleting vocabulary, or monitoring communication.



Examples of assistive technologies used by people with disabilities.

Digital and Online Services

Everyday **digital services hold sensitive personal information** and can be used to commit TFGBV. Many services are not designed with accessibility or digital safety for people with disabilities in mind, and put people with disabilities at a **greater risk of experiencing TFGBV.**

Banking and Financial Services

Mobile and online banking platforms store financial data, transaction histories, and identity information. This is very private personal information.

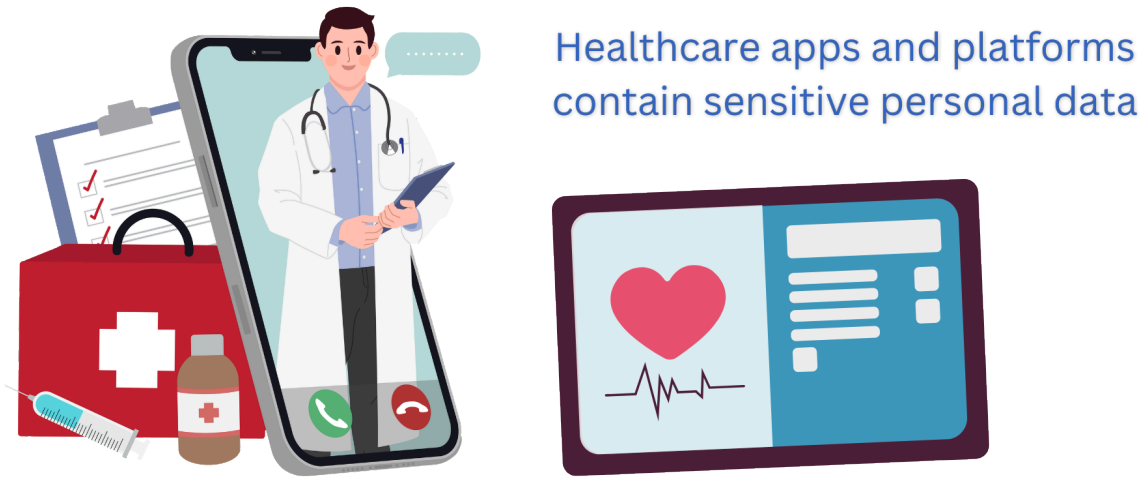
How TFGBV can show up: Unauthorized access, financial control, monitoring spending or travel, coercion to share login details.

Healthcare, eHealth, and Telehealth Platforms

Healthcare is transitioning into online spaces, which is a great option for many people with disabilities who struggle to attend in-person appointments due to barriers in their physical environments. However, digital health systems contain sensitive information, which, if misused by the wrong people, can be dangerous.

How TFGBV can show up: Accessing private health records, tracking

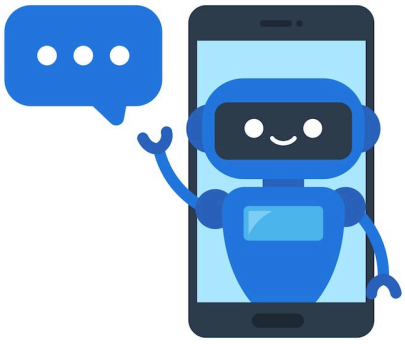
appointments or medications, impersonating someone to cancel care or obtain information.



AI Chatbots and Generative Tools

Artificial intelligence (AI) is growing more powerful and prevalent in everyday life.

How TFGBV can show up: Creating fake messages or images, generating manipulated sexual content, automating harassment through bots.



Email Services

Email services such as **Gmail, Yahoo!, Hotmail, Microsoft Outlook** (et cetera), remain a very important central communication tool.

How TFGBV can show up: Account takeover, monitoring other linked services, resetting passwords to gain control.

Video Conferencing Platforms

These apps or platforms are used for **video conferencing** or calls, to facilitate digital communication. **Examples include:** Zoom, Google Meets, Microsoft Teams, Slack.

How TFGBV can show up: Joining calls without consent, recording or screenshotting meetings, harassing participants within calls, monitoring who someone speaks to.

Zoom and other web conferencing and video streaming platforms can be used to perpetrate TFGBV, or settings for TFGBV.

Reflection

What other examples of TFGBV can you think of? Leave them in the comments below to educate us and others!

Activity

An interactive H5P element has been excluded from this version of the text. You can view it

online here:
https://pressbooks.library.torontomu.ca/tfgbvsafetytraining/?p=88#h5p-3

Chapter 3: Forms of TFGBV

In this chapter, we will focus on the ***forms of TFGBV.*** This means, the actual behaviours and tactics that perpetrators use. The same harmful behaviours can appear across many different platforms, and that the same platform can be misused in several different ways. Separating the forms of TFGBV from potential places where TFGBV can occur makes it easier to **recognise patterns, understand risks, and connect what you learn to real-life situations.**

When we listed platforms and devices in Chapter 2, our goal was to help you understand where tech-facilitated gender-based violence can take place. People use many different apps, websites, and digital tools every day, and any of them can be misused. But knowing the platforms alone doesn't give the big picture story.

Learning Objectives

- Learn how TFGBV can be committed in different forms and with different tactics.

This chapter builds on the foundation from Chapter 2 by showing **how digital spaces can be used to harm someone.** It gives you a clearer picture of what TFGBV can look like in practice, no matter which platform or device is involved.

There are hundreds of recognized forms of TFGBV, and TFGBV is constantly evolving. As a result, this list is not totally comprehensive. However, **we will discuss the following common categories of TFGBV forms:**

- Control-based abuse

- Cyber-grooming
- Economic and financial abuse
- Hacking and account takeovers
- Hate speech
- Image-based abuse
- Impersonation and identity theft
- Online harassment and cyberbullying
- Stalking, tracking, and digital surveillance
- Threats and intimidation

Control-Based Abuse

Control-based abuse happens when someone **restricts your** ability to use phones, computers, the internet, or other technology. This can isolate someone from support or limit their independence. **This may look or sound like:**

- Taking away devices without consent or permission.
- Logging into accounts to monitor or restrict communication.
- Controlling devices under the excuse of "helping" or saying things like: "you don't understand technology."
- Limiting access to assistive technology needed for independence.
- Discouraging online presence with statements such as: "You'll embarrass yourself online.

Control-based TFGBV can occur by the control of access to technology, or through controlling actions committed via technology.

Cyber-Grooming

Cyber-grooming occurs when someone builds trust online to exploit another person sexually, financially, or emotionally. Grooming usually happens over time and often involves someone older or in a position of power (for example, a teacher, caregiver, or community leader). **Cyber-grooming can include:**

- Pretending to be a friend, romantic partner, or supportive figure.
- Using trust to pressure someone into harmful or abusive behaviour.
- Manipulating someone into giving money or access to financial resources.

Economic and Financial Abuse

Digital platforms can be used to control or **exploit someone's finances**. **Examples of financial abuse may include:**

- Accessing online banking without permission.
- Threatening harm unless money is sent.
- Offering "help" with finances as a way to gain control.
- Controlling disability payments or benefits.
- Forcing mobile money transfers.
- Locking someone out of financial or work-related apps.

Hacking and Account Takeovers

Hacking involves **accessing someone's accounts, devices, or personal information without permission.** This can include guessing passwords, using saved logins, or exploiting security weaknesses. **Once inside an account, they may:**

- Read private messages.
- Lock someone out.
- Impersonate them.
- Monitor activity.

Hacking often leads to other harms, such as financial abuse or impersonation.

Hate Speech

Hate speech targets someone's identity, like their gender, disability, sexuality, or race. Hate speech can be used to shame, intimidate, or silence them. It can happen in online comments, messages, posts, gaming chats, or group discussions. Because it spreads quickly and publicly, it can cause significant emotional harm and reinforce discrimination.

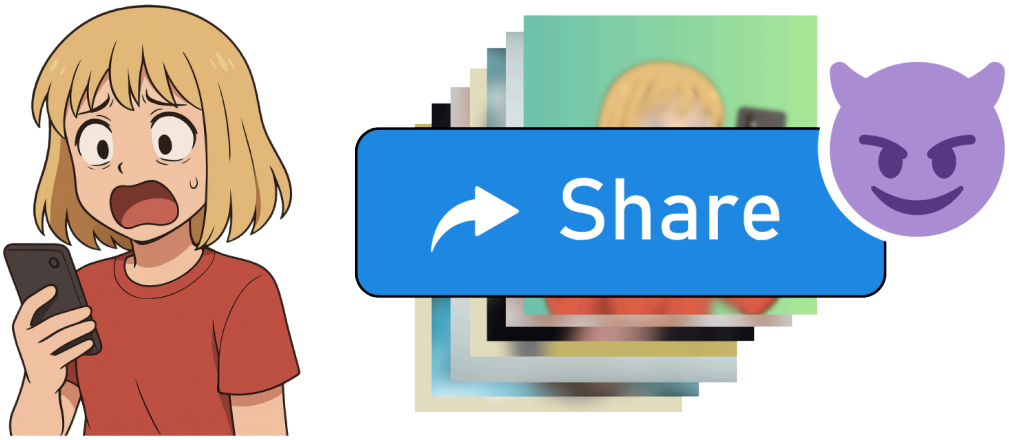
Image-Based Abuse

Image-based abuse involves creating, sharing, or threatening to share intimate or personal images without consent. **Image-based abuse can include:**

- Sharing someone's intimate images without permission.
- Threatening to release personal images to coerce or control.

- Pressuring someone to send sexual images.
- Creating manipulated or deepfake images to shame or intimidate ("deepfakes").
- Sending unwanted sexual images.

If you have experienced image based abuse, the StopNCII.org is a site that specifically provides resources and information for people who have experienced Non-Consensual Intimate Image abuse. For resources specific to South Africa, you can check our Support and Resources Page.

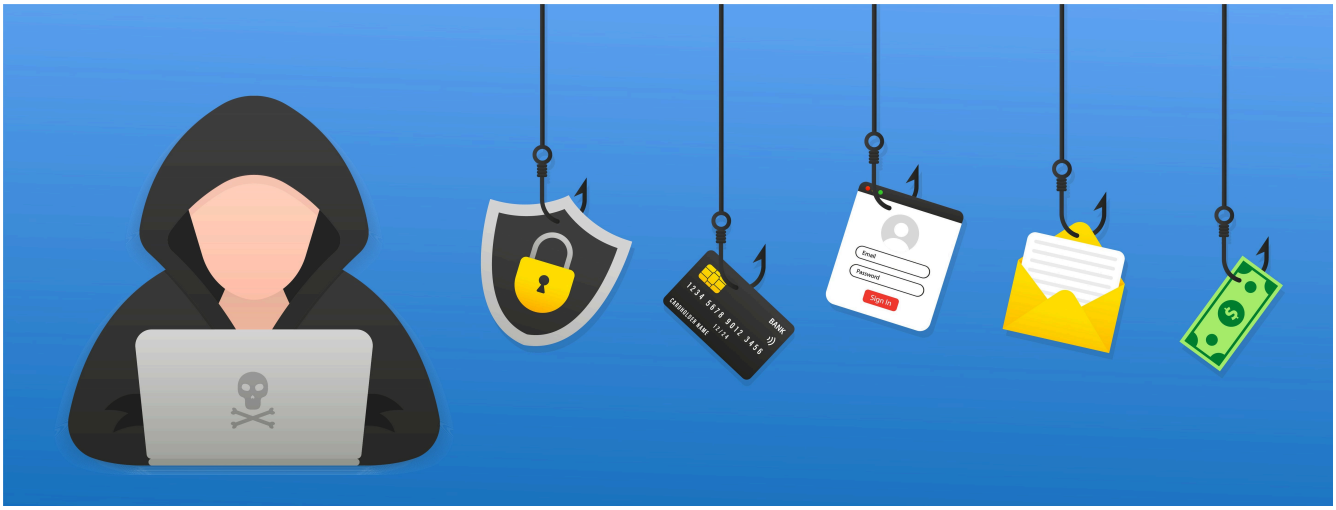


See Case Study 2 to learn about Maya's experience with image-based abuse.

Impersonation and Identity Theft

Online impersonation occurs when someone pretends to be another person online, often to harm, deceive, or exploit them. **Impersonation or identity theft may look like:**

- Creating fake accounts using someone's name or photos.
- Posting harmful or offensive content while pretending to be them.
- Messaging a target's family or friends to request money under false pretenses.
- "Catfishing" by pretending to be someone else for romantic or financial gain.

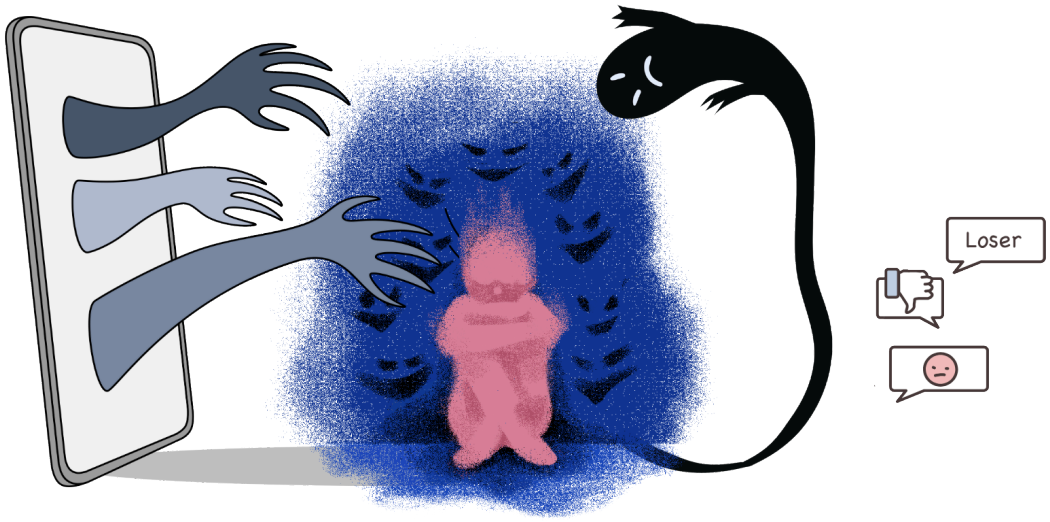


Online Harassment and Cyberbullying

Online harassment includes repeated or targeted behaviour intended to cause emotional, social, or psychological harm. Cyberbullying often involves individuals or groups using their power to target someone. **Examples include:**

- Threatening or harassing messages.
- Disability-based hate speech and ableism.
- Gendered hate speech, misogyny, homophobia, or transphobia.
- Spreading false information to damage reputation or cause distress.

See Case Study 1, to learn about Thandi's experience with cyberbullying and harassment.



Stalking, Tracking, and Digital Surveillance

Digital tools can be misused to **monitor someone's movements, communications, or daily activities.** These behaviours often involve repeated, unwanted contact or observation that causes fear or distress. **Examples of surveillance or stalking include:**

- Installing spyware under the guise of "helping."
- Tracking location through phones, apps, or social media features.
- Monitoring home cameras, doorbell cameras, or other connected devices.
- Using vehicle GPS systems to follow someone's movements.
- Justifying surveillance with statements such as "I need to keep an eye on you."

Cyberstalking can lead to in-person threats and stalking behaviour. (Cyberbullying Research Center, 2025)

Front door cameras give a view of a whole neighbourhood, and might be used as a way to monitor and control people. (The New York Times, 2020)

Abusers may be monitoring and spying on victims through their car GPS system. (DomesticShelters.org, 2024)

Threats and Intimidation

Threats can be sent through any digital channel. They may involve threats of physical harm, threats to release personal information, or threats to damage someone's reputation. Even without physical contact, digital threats can create fear, isolation, and ongoing emotional distress.

Reflection

Have you heard these forms of TFGBV before? Have you ever experienced them? Which form of TFGBV do you think is most hidden for disabled women?

Resources

- Herrman, J. (2020, January 19). Who's Watching Your Porch? *The New York Times*. https://www.nytimes.com/2020/01/19/style/ring-video-doorbell-home-

security.html.
- Hinduja, S. (2025, December 29). Cyberstalking. *Cyberbullying Research Center*. https://cyberbullying.org/cyberstalking.
- Fontes, L. A. (2024, August 7). *Abusers Are Monitoring and Spying on Victims Through Their Cars*. DomesticShelters.Org; DomesticShelters.org. https://www.domesticshelters.org/articles/identifying-abuse/abusers-are-monitoring-and-spying-on-victims-through-their-cars.

Chapter 4: Gender, Disability and TFGBV

Learning Objectives

- Understand how disability and gender can create unique experiences of TFGBV.

Technology-facilitated violence impacts everyone... So why do we need to talk about gender and disability?

While it is true that technology-facilitated violence is experienced by people of all gender, disability status and other identities, women with disabilities may encounter unique harms, that are made worse because of other unique experiences of vulnerability.

Let's think about a different scenario to understand how vulnerabilities are created.

An example scenario:

Someone physically attacks you. What do you do?

Scenario A: You are visiting a new country where you do not speak the main language. Suddenly, a stranger approaches you and attacks you, then runs off. However, no one witnessed this happen. You want to ask someone for help, but no one can understand you. You want to go to the police, or to a hospital, but you can't read the directions.

Scenario B: You are living in your home country where you speak the main language. You are suddenly attacked by a stranger while walking home from work. Thankfully, your neighbor sees it happen, so you have a witness. You know how to call for help, and you can go see your family doctor to tend to your injuries.

In both scenarios, the same crime was committed against you. However, the context you were in changed how you were able to respond, receive support, and heal. While this is an imperfect example of offline violence, it shows how certain contexts can enable or disable people.

This remains true in online violence scenarios.

For women with disabilities, the context of a misogynistic and ableist society impacts daily life. Digital technology and online worlds replicate existing offline misogynistic and ableist systems.

Disability and Technology-Facilitated Gender-Based Violence

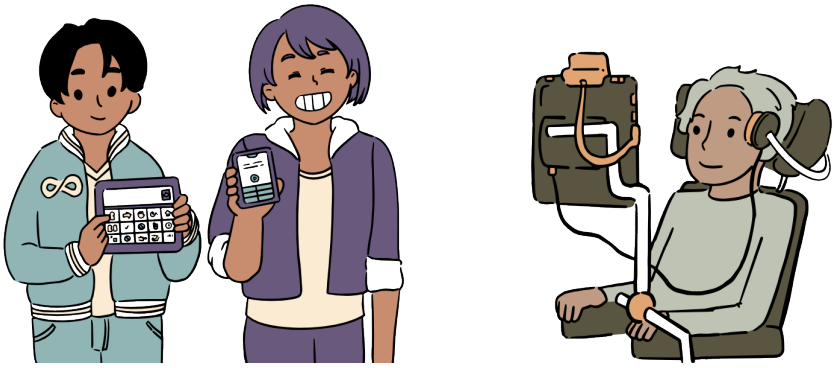
Women with disabilities may face different structural or systemic barriers. These barriers can include things like:

More physical and digital isolation. Often, inaccessible or unwelcoming spaces will prevent women with disabilities from participating in many areas of society. This means that there are fewer witnesses to violence, and can increase vulnerability.

Being isolated can make you feel like you have no one to support or help you, even if this is not the truth.

More dependence on caregivers and loved ones. Many people with disabilities rely on support from paid or unpaid caregivers, making them at risk for abuse by these people.

More dependence on technology. Often, people with disabilities use technology to support their navigation through daily life (such as communication, mobility, access to work or school). However, this increased reliance on tech can be used to exploit, manipulate, or control people.

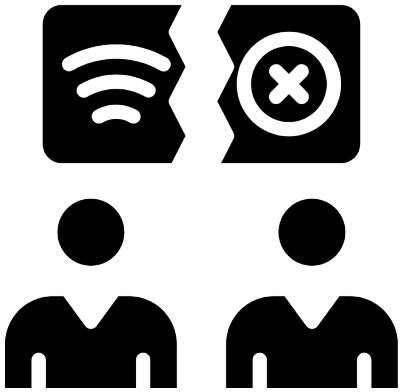


Technology supports daily life for many people with disabilities, but dependence on it can also create risks.

More risk of devices being taken, monitored, or misused. Women with disabilities may rely on caregivers or family members for certain daily tasks, or have less physical autonomy to use their own devices. Because of this, "care" might be used as an excuse for taking away or monitoring devices.

Limited private time or private space. Disabilities can create situations that create constant surveillance for health-related reasons. Often, this lack of privacy can be used against people.

Lower digital literacy or education. Women with disabilities have historically lower levels of digital competency due to inaccessible education and devices, which overall compromises their online safety.



The digital divide creates unequal access to opportunities and community participation. It can also increase vulnerability to violence.

Inaccessible and non-inclusive reporting, safety and education. While tools to report and protect against TFGBV exist, many of them are not accessible for people with disabilities, or poorly explained. Therefore, people with disabilities are less likely to benefit from these tools.

Gendered-disability stigma. Women, people with disabilities, and women with disabilities often encounter societal stigma that creates inequality. These groups are frequently infantilized, fetishized, and/or degraded and demeaned. This carries over into TFGBV.

TFGBV in South Africa

In South Africa, the barriers mentioned above are very common. This is because there are many existing stigmas and discrimination around disability and gender.

For example, infantilization of women with disabilities is common. This further disables women by assuming that they are powerless or have no autonomy, or cannot make wise decisions (Capri & Swartz, 2018; Olkin et al., 2019). These assumptions may lead to increased risk of coercive control being masked as "helping".

Overall, there is a disproportionately high rate of gender-based violence in South

Africa, with **35.8% (1 in 3) of women** having experienced some form of gender-based violence in their lifetime (Govender, 2023; Masiko-Mpaka, 2024; Mkwananzi & Nathane-Taulela, 2024). Moreover, levels of proper documenting, reporting, intervening and preventing gender-based violence is currently a major health challenge (Govender, 2023)

General view during the Gender-Based Violence (GBV) protest march organized by the Office of The Premier in collaboration with Phepha Foundation on April 26, 2021 in Durban, South Africa. © 2021 Darren Stewart/ Gallo Images via Getty Images (Taken from Human Rights Watch).

South Africa often has undereducated reporting systems about technology-facilitated violence for women with disabilities, making it difficult to report and find help for technology-facilitated violence. For example, disability-specific forms of violence such as taking away assistive technology, or abuse by caregivers may be less likely to be believed because they are not "generic" forms of TFGBV.

Technology-facilitated gender-based violence is often not taken seriously by law enforcement or by others. Because of this, many survivors will wonder if they are being "too sensitive" or making a big deal of nothing... and many times they will not report violence.

In addition, many people have misconceptions about TFGBV, for example, saying "Oh it's not so bad. Just turn off your computer!" However, TFGBV has huge implications and impacts on survivors that go far beyond the screen.

TFGBV can lead to both online and offline harms.

How Can Different Forms of Disability Shape Risks?

Disability does not *cause* tech-facilitated gender-based violence (TFGBV), but different access needs can change **how** abuse shows up and **what makes someone more at risk or harder to reach for support.** The following examples are not exhaustive, but they can illustrate common patterns associated with different access needs.

Vision (blindness or low vision):

- Reliance on audio or screen readers can make harassment or harmful content harder to detect quickly.
- Scammers may exploit trust in screen-reader output or offer “help” navigating devices as a way to gain access.
- Perpetrators may send sexual or harmful images knowing the recipient cannot

safely preview them.

d/Deaf or Hard of Hearing:

- Abusers may remove or restrict access to hearing aids or communication devices.
- Reporting TFGBV can be harder when services rely on voice calls or are not accessible in sign language.

Learning or Intellectual Disabilities:

- Threatening or manipulative tones in messages may be harder to interpret.
- Shame can be used as a tool ("You won't understand," "Let me do it for you").
- Fraud, grooming, and manipulation may be harder to identify due to unclear or shifting boundaries.
- Consent can be exploited when information is not communicated in accessible ways.

Mobility Disabilities:

- Technology may be a primary link to independence, so when it becomes unsafe, mobility and freedoms can become limited.
- Caregivers, partners, or support workers may have easier access to devices and accounts, increasing opportunities for control.

Psychosocial Disabilities:

- Abusers may use messages or posts to encourage self-harm or undermine self-worth.
- Threats of self-harm can be used to coerce someone into giving money,

images, or compliance.

Speech or Communication Disability

- Reporting abuse may be more difficult when systems rely on audible verbal disclosure.
- Abusers may exploit the likelihood that authorities or services will not take disclosures seriously, or that they will misunderstand disclosures due to communication differences.

If you think of others, leave them in the comment section below (online version)!

Reflection

Which of these vulnerabilities have you witnessed? How did they show up in your life or the life of someone you know of?

Resources

- Capri, C., & Swartz, L. (2018). 'We are actually, after all, just children': Caring societies and South African infantilisation of adults with intellectual disability. *Disability & Society*, *33*(2), 285–308. https://doi.org/10.1080/09687599.2017.1409102.
- Govender, I. (2023). Gender-based violence – An increasing epidemic in South Africa. *South African Family Practice*, *65*(1), 5729. https://doi.org/10.4102/safp.v65i1.5729.
- Masboungi, C., & Quarterman, L. (2025, June 12). When will we listen? –

Centering girls' voices in our efforts on technology-facilitated gender-based violence (TFGBV). *Sexual Violence Research Initiative*. https://www.svri.org/when-will-we-listen-centering-girls-voices-in-our-efforts-on-technology-facilitated-gender-based-violence-tfgbv/.

- Masiko-Mpaka, N. (2024, November 25). Confronting South Africa's Crisis of Gender-Based Violence. *Human Rights Watch*. https://www.hrw.org/news/2024/11/25/confronting-south-africas-crisis-gender-based-violence.
- Mkwananzi, S., & Nathane-Taulela, M. (2024). Gender-based violence and femicide interventions-perspectives from community members and activists in South Africa. *Frontiers in Global Women's Health*, *5*, 1199743. https://doi.org/10.3389/fgwh.2024.1199743.
- Olkin, R., Hayward, H., Abbene, M. S., & Van Heel, G. (2019). The Experiences of Microaggressions against Women with Visible and Invisible Disabilities. *Journal of Social Issues*, *75*(3), 757–785. https://doi.org/10.1111/josi.12342.
- South Africa: Broken Promises to Aid Gender-Based Violence Survivors. (2021, November 24). *Human Rights Watch*. https://www.hrw.org/news/2021/11/24/south-africa-broken-promises-aid-gender-based-violence-survivors

Chapter 5: What Are Your Rights Online as an Adult?

Everyone deserves to feel safe, respected, and in control when using technology. **Your phone, your accounts, and your online spaces belong to you.** This does not change dependent on gender or disability status.

As an individual, a caregiver, a friend, a family member, or a frontline service provider, understanding adults' rights with regards to online safety and wellness is essential to getting and giving the right support and protecting against violence.

Learning Objectives

- Learn about your rights as an adult when using digital technologies.
- Learn about the laws in place to protect you as a person living in South Africa.

This chapter explains everyone's basic digital rights in clear and accessible language.

These rights apply whether you are using a phone, computer, tablet, assistive device, or any online platform. Understanding your rights can help you recognize when someone is crossing a line. It can also help you **speak up, set boundaries, and reach out or even provide for support** when it is needed.

Your Rights in Everyday Digital Life

You have the right to use technology in ways that support your independence, safety, and wellbeing. These rights apply to everyone, including people who rely on caregivers, support workers, partners, or family members for daily tasks. **You have the right to:**

- Use your own phone and devices.
- Have privacy when using technology.
- Keep your passwords secret.
- Say no when someone asks to check your device.
- Use social media and online platforms.
- Report abuse or harmful behaviour.
- Get help without asking for permission.
- Ask someone safe to help you manage your technology.

These rights are about **choice and control**. No one should pressure you to give up your privacy or independence.

Your Right to Choose

Choice is at the heart of digital safety. As an adult, you can decide what feels safe and comfortable for you. You decide who gets access to your information and who does not.

You can say, "I have the right to choose..."

- "Who helps me with my technology."
- "Who knows my passwords."
- "Who can see my photos."
- "Who can view my social media."
- "If I want to share my location."

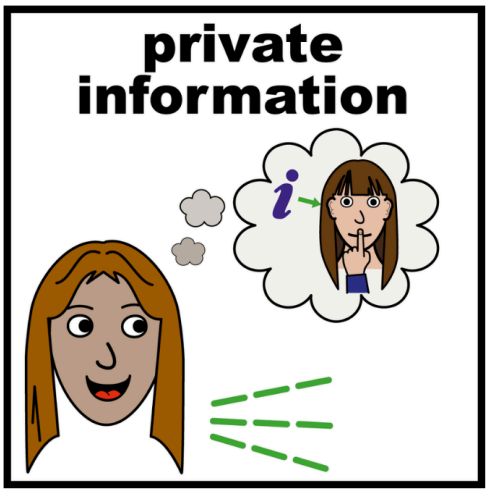
As an adult, these choices belong to you. They are not rewards that someone can take away. They are not privileges that depend on someone else's approval. They are your rights.

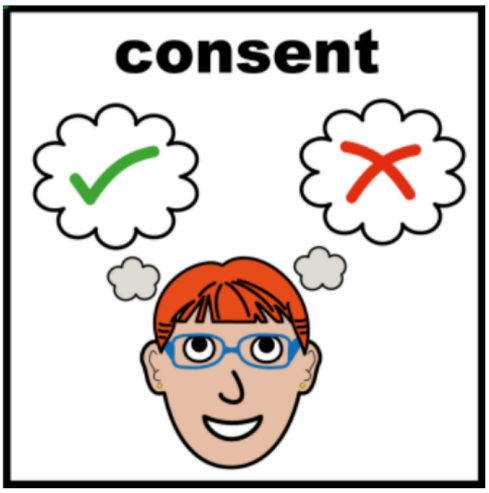
Your Right to Consent

Understanding Privacy and Consent Online

Privacy means having control over who can access or see your information. Consent means choosing to do, or not do something. Consent applies to what you want to share and who you want to share it with. Private information should not be shared

with many people, and you should think about who you are giving consent to access your information.





You have the right to:

- Decide who sees your photos
- Decide who can message you
- Decide who can help you with your technology
- Change your mind at any time

If someone pressures you to share information, photos, or passwords, that is not consent. **Consent must be freely given, without fear or guilt.**

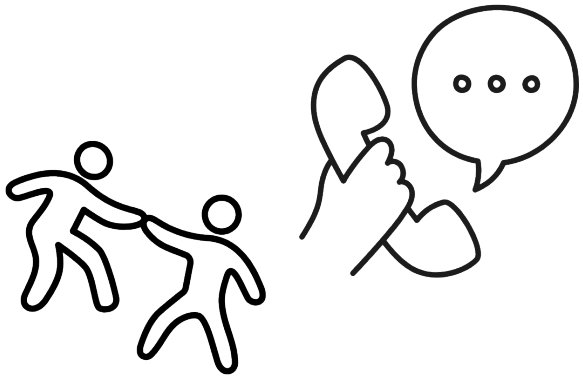
Your Right To Get Help

You have rights to not be harmed or targeted for violence, and you have the right to be protected and seek support. **You have the right to:**

- Report online abuse to law enforcement (like police, security officers, et cetera).
- Apply for a protection order or receive other support.

- Speak about abuse with a support worker, healthcare provider, social worker, or trusted person.
- Ask someone safe to help you gather evidence.
- Receive support.

You do not need to wait for the situation to “get worse.” If something feels wrong, you are allowed to reach out for support.



Your Rights Under South African Law

People in South Africa have strong legal protections when it comes to online safety. These laws exist to protect your privacy, your identity, your personal information, and your freedom to use technology without fear. They apply **whether the harm happens online or in person.** They also apply **no matter who is causing the harm**. It could be a partner, family member, caregiver, friend, stranger, or anyone else.

South African law is clear that digital abuse is real abuse. Online harassment, cyberstalking, impersonation, and the sharing of harmful content are recognised as serious offences.

Key Laws That Protect You

South Africa's **Cybercrimes Act of 2020** makes many forms of TFGBV illegal. This includes harmful messages, threats, image-based abuse, and any attempt to access your accounts without permission. The Act also allows you to apply for protection orders and requires certain cybercrimes to be reported to the police.

To help you navigate the **Cybercrimes Act of 2020**, we recommend you review an Easy Access website created by Michalsons. This website reviews the whole cybercrimes act and provides excellent South Africa-based resources to support South African residents. To learn more, visit the website by accessing this link to the Cybercrimes Act Website.

Other laws, such as the **Protection from Harassment Act**, the **Domestic Violence Act**, and the **Criminal Law (Sexual Offences and Related Matters) Amendment Act**, also protect people from digital forms of harm.

We have created a folder containing PDF formats of the **Cybercrimes Act of 2020** , the **Protection from Harassment Act**, the **Domestic Violence Act**, and the **Criminal Law (Sexual Offences and Related Matters) Amendment Act**. If you wish to download or view these documents, you can follow the link here to access the folder.

Having access to copies of these documents may be useful when reporting violence to authorities, and ensure they take your concerns seriously.

What the Law Says About TFGBV

<u>You are protected under South African law from the following behaviours:</u>

- No one may harass you or harm you on purpose. This includes online harassment, repeated messages, or harmful posts.
- No one may threaten to share your photos or share them without your permission. This includes intimate images, edited images, or deep fake images ("deepfakes").
- No one may stalk you. This includes tracking your location, monitoring your online activity, or using technology to follow you.
- No one may pretend to be you. Creating fake accounts, impersonating you, or using your identity to harm you is a crime.
- No one may access or control your devices without your permission. This includes logging into your accounts, installing spyware, or taking your phone away.
- No one may steal your money, your information, or anything that belongs to you. Financial abuse through online banking or mobile money is illegal.

These protections apply whether the abuse happens on social media, through messaging apps, on gaming platforms, or through everyday devices.

Knowing your rights helps you recognise when something is not okay. It also helps you understand that digital abuse is not "just online drama." It is a form of violence, and the law should take it seriously.

However, please be aware that even though these laws are in place and you should have certain rights, many times, online violence is still not taken seriously. That does not mean it isn't serious. This is why it is important that you **know your rights and know the law**.

Chapter 6: Online Safety How-To's

This chapter will **review online safety tips and ways to set up your accounts and devices for safe use** across different types of technology. This chapter will only discuss specific tips and ways to navigate settings for online and digital safety.

Safety Note:

Changing any of your typical digital behaviour (changing passwords, logging out of or deleting accounts, turning off location, uninstalling apps) may alert your abuser. If you believe you are in danger, find support from a local service or use a safer device before making any changes.

Learning Objectives

This chapter reviews the following topics, which are important for online safety measures:

- App Permissions and Mobile Privacy Settings
- Detecting and Removing Spyware/Stalkerware
- Device Safety
- Location Sharing and Preventing Unwanted Tracking
- Messaging Apps and Secure Communication
- Password Security Basics
- Smart Home Devices and Webcam Privacy
- Social Media Privacy Settings and Audience Control
- Two-Factor Authentication (2FA)

App Permissions and Mobile Privacy Settings

On your mobile devices and in different applications, you have some degree of control over what functions are enabled at different times. We have outlined some **considerations for mobile privacy settings:**

- Only give apps the permissions they need.
- Set access to “While Using the App” or “Never” for most apps. Turn off location, camera, or microphone access entirely for apps you don’t trust.
- Delete apps you don’t use or don’t recognize.
- Review permissions regularly, especially after updates.

For Android Devices

How to check and change app permissions:

1. Open the **Settings** app.
2. Tap **Security and Privacy** or **Privacy**.
3. Tap **Privacy Dashboard**.
4. See which apps have accessed your location, camera, microphone, etc.
5. Tap an app to change its permissions (allow, deny, or allow only while using the app).

For iPhone Devices

How to check and change app permissions:

1. Open the **Settings** app.
2. Tap **Privacy & Security**.
3. Tap **Location Services** to see which apps can access your location.
4. Tap each app to set permission to **Never**, **Ask Next Time**, or **While Using the App**.

5. Check permissions for camera, microphone, contacts, and more in the Privacy settings.

Example: Sam finds that a game app has access to his microphone and location, even though it doesn't use them in-game. He changes the settings to deny these permissions.

Checklist: App Permissions

Task	Done?
Review app permissions for location, camera, microphone	Yes/No
Remove permissions from apps that don't need them	Yes/No
Delete unused or suspicious apps	Yes/No

Apps often ask for more access than they need. Limiting permissions protects your privacy and reduces the risk of someone spying on you through your device.

Detecting and Removing Spyware/Stalkerware

Spyware or stalkerware is software secretly installed on your device to monitor your messages, calls, location, and more. It is often used by abusers to control or watch their victims.

Warning signs of spyware/stalkerware being installed:

- Your device is slow, hot, or the battery drains quickly.
- You see unfamiliar apps or settings.
- Your abuser knows things only someone watching your device would know.
- The device lights up or makes sounds when not in use.

How to check for spyware:

Android: Go to Settings > Apps > See all apps. Look for apps you don't recognize, especially with generic names like "System Service." Go to Settings > Security > Device admin apps.

- Only expected entries should be there. Use anti-stalkerware apps like Norton 360, Malwarebytes, or Certo AntiSpy.

iPhone: Check for "jailbreak" apps like Cydia or Sileo. Go to Settings > General > VPN & Device Management.

- Look for unknown profiles. Use security apps like Clario Anti Spy or Norton Mobile Security.

How to remove spyware:

- Delete suspicious apps or profiles.
- Run a security scan with a trusted app.
- As a last resort, do a factory reset (erase all data and set up as new).
- Change all passwords from a clean device.

Checklist: Spyware Detection

Task	Done?
Check for unfamiliar apps or settings	Yes/No
Run a security scan with anti-stalkerware tools	Yes/No
Remove suspicious apps or profiles	Yes/No
Change passwords from a safe device	Yes/No
Get support before making changes if at risk	Yes/No

Spyware is a serious threat to your privacy and safety. Regularly checking your

device and knowing the signs can help you act quickly. Always consider your safety before removing spyware, as it may escalate the situation.

Device Safety: Choosing and Using a Safer Device

If you think someone is monitoring your device, it's safest to use a different one that they have never accessed in order to contact help. This could be a friend's phone or computer, a public computer at a library or community center, or even a new phone with a new account (not linked to your old cloud accounts).

Tips for safer device use:

- Set a strong passcode or PIN (at least 6 digits, not a birthday or easy pattern, like 123456).
- Don't link your new device to old accounts or cloud backups.
- Turn off Bluetooth and location sharing when not needed.
- Keep your device's software up to date.
- Use a device not accessed by an abuser.

Example: Maria suspects her ex has installed spyware on her phone. She buys a pay-as-you-go phone, sets a new PIN, and only uses it to contact support services and trusted friends.

Location Sharing and Preventing Unwanted Tracking

Sharing your location can put you at risk if someone wants to track or harm you. Many apps and devices can share your location without you realizing it. To turn off location sharing or better manage it, try these steps:

- **On Android:**
  Settings > Location > Toggle off “Use location” or manage app permissions individually.
- **On iPhone:**
  Settings > Privacy & Security > Location Services > Toggle off or manage per app.
- **Google Maps:**
  Open the app, tap your profile, tap “Location sharing,” and stop sharing with others.
- **Find My (iPhone):**
  Open Find My, tap “Me,” and turn off “Share My Location.”
- **Messaging apps:**
  Check app settings to turn off location sharing.

Tips for stopping location tracking:

- Don’t “check in” to locations on social media.
- Delete location history, especially before or after visiting safe places like shelters.
- Turn off Bluetooth when not in use (Bluetooth can be used for tracking).

Example: Taylor turns off location sharing in all her apps and deletes her location history before moving to a new apartment.

Checklist: Location Privacy

Task	Done?
Turn off location services when not needed	Yes/No
Stop sharing location in apps and with contacts	Yes/No
Delete location history regularly	Yes/No
Turn off Bluetooth when not in use	Yes/No

Controlling your location settings helps prevent someone from tracking your movements. Regularly reviewing and updating these settings keeps you safer.

Messaging Apps and Secure Communication

Not all messaging apps are equally safe. Some are better for private, secure conversations.

Best Apps for Secure Messaging

App	End-to-End Encryption	Metadata Protection	Open Source	Notes	Reporting System?
Signal	**Yes** (default)	**Yes**	**Yes**	Best for sensitive chats.	**Yes**. To report abuse on Signal, use the "**Block and Report**" feature directly within a chat by tapping the user's name or group header
WhatsApp	**Yes**	**No**	**No**	Owned by Meta, collects metadata	**Yes**. To report abuse on WhatsApp, open the chat with the user, tap the contact or group name to view their profile, scroll down, and select "**Report"**.
Telegram	Only in Secret Chats	**No**	**Partial**	Default chats are not encrypted	**Yes**. To report abuse on Telegram, use the built-in report feature in the app's menu (three dots) to flag specific messages, users, groups, or channels for violations like spam, violence, or illegal content.

Tips for all messaging apps:

- Don’t share sensitive information or content in group chats, or to people you don’t know.
- Turn off message previews in notifications.
- Be very cautious with accessing links and attachments.

Checklist: Secure Messaging

Task	Done?
Use Signal or another secure app for sensitive chats	Yes/No
Enable disappearing messages	Yes/No
Verify contacts’ safety numbers	Yes/No
Turn off message previews	Yes/No

Signal is the gold standard for secure messaging. It encrypts messages so only you and the recipient can read them. WhatsApp is better than SMS but collects more data. Telegram is only secure in Secret Chats. Always use the most secure option for sensitive conversations.

Password Security Basics: Passwords and Password Managers

Strong passwords are key to ensuring you protect yourself from people accessing your accounts and devices without your permission. Weak or reused passwords make it easy for someone to break into your accounts. If you use the same password everywhere, one breach can put all your accounts at risk.

How to create a strong password:

- Use at least 12 characters (longer is better).
- Mix uppercase and lowercase letters, numbers, and symbols.
- Avoid using names, birthdays, or common words.
- Use a passphrase (a sentence or group of random words).

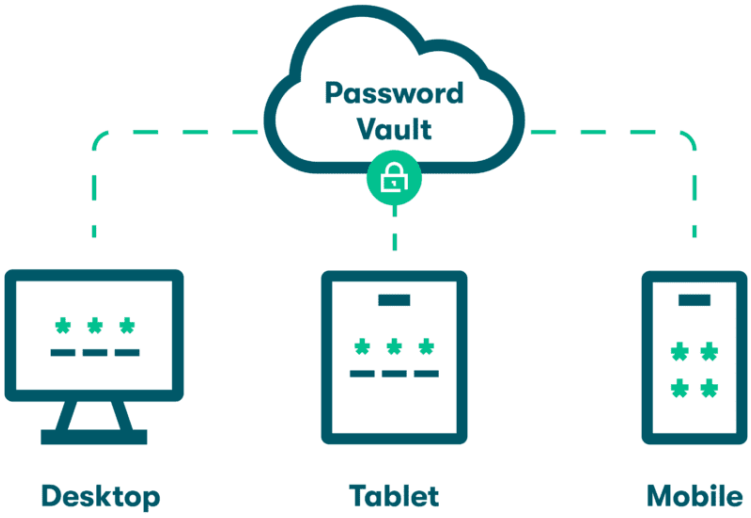
Example: Instead of “jasmine123”, use “Sunshine!River$Pineapple2026”.
(Please do not use this password. This is just an example of a potential password.)

Using a Password Manager

A password manager is a tool that stores all your passwords securely. You only need to remember one master password. Examples of good, secure password managers include Bitwarden, 1Password, and KeePassXC.

Password managers can ensure that you have **strong, unique passwords** for each of your linked accounts, while providing convenience of using **only one password as the main user.**

It remembers your passwords, so you don’t have to. Many password managers are also able to **detect if your chosen passwords are weak,** or if your privacy has been breached.



Structure of password management by a password manager or "Password Vault".

Checklist: Password Safety

Task	Done?
Change all passwords to strong, unique ones	Yes/No
Use a password manager	Yes/No
Don't share passwords with anyone	Yes/No
Don't use social media accounts to sign in to other services	Yes/No

Strong passwords and password managers are your first line of defense. They make it much harder for someone to guess or steal your login information. Changing passwords regularly and not reusing them keeps your accounts safer.

Smart Home Devices and Webcam Privacy

Smart home devices (like Alexa, Google Home, Ring Security cameras, smart cameras, or smart thermostats) can be used to monitor or harass you if someone else has access.

Tips for smart home safety:

- Change default passwords on all devices.
- Review who has access to your smart home accounts.
- Regularly check and delete voice recordings (see device settings).
- Use the physical mute button on smart speakers when not in use.
- Place smart speakers in common areas, not bedrooms.
- Cover webcams when not in use (a piece of tape works).

How to delete voice recordings:

Alexa: Open the Alexa app > Settings > Alexa Privacy > Review Voice History > Delete recordings.

Google Assistant: Go to myaccount.google.com > Data & Privacy > Web & App Activity > Uncheck “Include voice and audio recordings.”

Checklist: Smart Device Safety

Task	Done?
Change passwords on smart devices	Yes/No
Review and remove unwanted account access	Yes/No
Delete stored voice recordings regularly	Yes/No
Use mute buttons and cover webcams	Yes/No

Smart devices can make life easier, but they also create new risks. Taking control of your devices and who can access them helps protect your privacy.

Social Media Privacy Settings and Audience Control

Social media is a common place for TFGBV. Protecting your privacy on these platforms is essential.

Key settings to check across all social media platforms:

- Set your account to private. If you wish to keep it public, then aim to do regular checks of your following, and limit interactions.
- Only accept requests from people you know.
- Ignore or delete requests from strangers.
- Block or report suspicious accounts.
- Limit who can comment or message you.
- Turn off location tagging.
- Review tagged photos before they appear on your profile.
- Regularly audit your followers and remove suspicious accounts.

Social media privacy settings help you control who sees your information and interacts with you. Regularly reviewing and updating these settings keeps you safer from harassment and unwanted contact.

Checklist: Social Media Safety

Task	Done?
Set accounts to private	Yes/No
Limit comments and messages	Yes/No
Turn off location tagging	Yes/No
Review tagged photos and followers	Yes/No

Social media privacy settings help you control who sees your information and interacts with you. Regularly reviewing and updating these settings keeps you safer from harassment and unwanted contact.

Two-Factor Authentication (2FA) and Authenticator Apps

What is Two-Factor Authentication?

Two-factor authentication (2FA) adds an extra step when you log in. After entering your password, you'll need to enter a code sent to your phone or generated by an app. This makes it much harder for someone to break in, even if they know your password. Many apps use 2FA for online security.

Tips for 2FA Apps:

- Use an authenticator app instead of SMS if possible.
- Save backup codes in a safe place in case you lose your phone.
- Don't share your 2FA codes with anyone.

Please keep in mind that 2FA requires you to have more than one device, or for you to be able navigate multiple apps. Sometimes, people with disabilities have a difficult time using these systems because they are not built with access in mind.

Types of 2FA include authentication using **SMS codes**, where a code sent by text message (which less secure, as it can be intercepted through text), and using **authenticator apps.** Apps like Google Authenticator, Microsoft Authenticator, Authy, or 2FAS generate codes on your phone (more secure).

How to set up 2FA:

1. Go to your digital (email, social media, etc.) account's security settings (look for "Two-Factor Authentication" or "2-Step Verification").
2. Choose to use an authenticator app.
3. Scan the QR code with your app.
4. Enter the code from the app to confirm.

Example: When logging into her email, Priya enters her password and then a code from her authenticator app. Even if someone knows her password, they can't get in without her phone.

Checklist: 2FA Setup

Task	Done?
Enable 2FA on all important accounts	Yes/No
Use an authenticator app, not just SMS	Yes/No
Save backup codes securely	Yes/No

2FA is like adding a second lock to your door. Even if someone has your key (password), they can't get in without the code from your phone. Authenticator apps are safer than SMS because texts can be intercepted or stolen.

Reflect

Based on this chapter, do you have secure devices and accounts?

What can applications and organizations do to make online security more accessible for you? For other women with disabilities?

Leave suggestions in the comments below!

After this general information about TFGBV, we want to provide specific training for different audiences. To accompany this general information, we have designed resources for **three different audiences:**

1. Women With Disabilities;
2. Family and Caregivers; and,
3. Frontline Service Providers.

Please select the training which applies to you:

Women With Disabilities

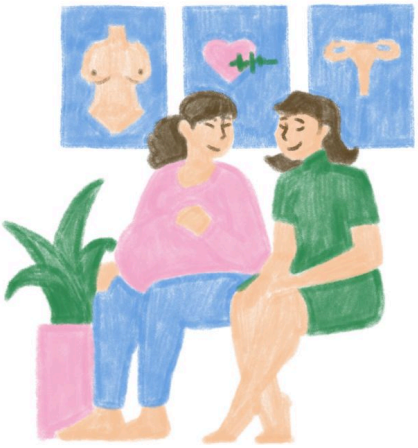
If you wish to learn about TFGBV as a woman with a disability, click here to start.

Women with disabilities include anyone who identifies as a woman (cis or trans), and who has a diagnosed or undiagnosed disability of any kind (physical, mental, neurological, sensory, et cetera).

Family and Caregivers

If you wish to learn about TFGBV as a family member or caregiver click here to start.

Family and caregivers include loved ones (family members, friends, romantic partners) or daily care providers (such as parents, hired caregiving staff) of women with disabilities, who are part of their immediate support system.



Frontline Service Providers

If you wish to learn about TFGBV as a frontline service provider, click here to start.

Frontline service providers are those delivering direct care, support, and services to citizens, particularly in health (nurses, community workers), social services, and education.

WOMEN WITH DISABILITIES

Women with disabilities include anyone who identifies as a woman (cis or trans), and who has a diagnosed or undiagnosed disability of any kind (physical, mental, neurological, sensory, et cetera).

Chapter 7: Recognizing TFGBV when it's happening to you

People often notice **changes in how they feel or behave** before they recognize the abuse itself. These signs are not proof on their own, but they can be important signals that something is happening that deserves your attention.

In this chapter, we will focus on **how you may feel and behave differently** according to your experiences. Please use this information along with what you learned in Chapters 1, 2 and 3.

Learning Objectives

- Recognize emotional, psychological, and behavioral signs of online harassment.
- Learn how to step back and assess situations that feel uncomfortable.

How do you know if you're experiencing TFGBV?

Emotional and Psychological Signs

Take a moment and think about how your body and mind have been feeling. Have you been more nervous, depressed, irritable, or tired than normal? Have you felt heavily conflicted about an online experience?

These are some possible **emotional and psychological signs** that you may be experiencing TFGBV:

- Sudden anxiety when receiving messages, notifications, or calls.

- Feeling nervous about posting online or checking your accounts.
- Feeling embarrassed, ashamed, or like you are “overreacting.”
- Blaming yourself for someone else’s harmful behaviour.
- Feeling watched, monitored, or “on edge” even when you’re alone.
- Feeling confused because the person harming you also says they are “helping.”

Reflect

What do you notice in your body when you feel anxious? When you feel scared? When you feel angry?

How do you regulate these feelings when they arise? If you aren’t sure how to regulate these feelings, see Chapter 8: Responding Safely to TFGBV.

Behavioural and Daily Life Signs

Sometimes people change their daily routines or actions without thinking about it, to protect themselves. Have you found yourself changing your daily life or behaviours in response to some online or technology-related event?

For example:

- Avoiding certain apps, platforms, or devices because they no longer feel safe.
- Deleting posts or changing how you communicate to avoid upsetting someone.
- Difficulty sleeping, concentrating, or enjoying things you normally like.
- Withdrawing from friends, family, or online communities.
- Changing passwords repeatedly or checking your devices for signs of tampering.
- Feeling pressure to respond immediately to messages, even when you don't want to.

Recognizing When Someone May Be Committing TFGBV

Many people do not realize they are being targeted until the situation escalates. Recognizing early warning signs helps you protect your **safety, privacy, and wellbeing.**

TFGBV can involve harassment, monitoring, impersonation, threats, or the misuse of devices and apps. It can also often involve a person engaging in manipulation, false promises, or attempts to steal money or personal information. In both cases, **the person causing harm can be anyone**: a stranger, a romantic partner, a caregiver, a family member, or even someone you met online.

Signs that someone may not be trustworthy

People who scam others or commit TFGBV often use **pressure, secrecy, control, and manipulation**. These behaviours can come from strangers, online contacts, partners, ex-partners, caregivers, family members, or people in your home or community.

Common signs include:

- **Asking for money**, airtime, gift cards, sexual favours or images, or financial help, especially early in the relationship.
- **Creating a sense of urgency**, such as “I need help right now” or “Don’t tell

anyone."

- **Encouraging secrecy** or requesting that you not tell anyone. Saying things like, "This is too special, we don't want anyone to know about it and ruin it."
- **Refusing video calls** or making excuses for why they cannot meet in person.
- **Stories that change over time**, or details that don't add up.
- **Requests for personal information**, such as ID numbers, passwords, or banking details.
- **Messages that feel scripted**, overly romantic, or too intense too quickly. This is sometimes called "lovebombing".
- **Threats or guilt-tripping** if you hesitate to help them or give them what they want.
- **Pretending to be someone else**, including using fake profiles or impersonating people you know, or even legal officials.

We have made a master list of different forms of TFGBV which you can read about in **Chapter 3: Forms of TFGBV, which are linked here.**

TFGBV often affects your **sense of safety**, **privacy**, and **control**. These feelings show up in your body and behaviours long before you might identify the event or situation as being violent or abusive. Recognizing these early signs, and connecting them to your knowledge of different forms of TFGBV, may help you understand what's happening and decide what support you may need and want.

Self-Reflection Checklist: Noticing When Something Feels Wrong

This checklist is designed to help you pause and reflect on your experiences, after reviewing the forms of TFGBV in Chapter 3, linked here. **You do not need to answer "yes" to everything for your feelings to be valid.** Even one "yes" can be a sign that something deserves your attention.

Emotional and Psychological Checklist:

- **Do you feel anxious or tense** when you receive messages, notifications, or calls?
- **Do you feel nervous about posting online**, even when you used to enjoy it?
- **Do you feel embarrassed, ashamed, or "at fault"** for someone else's behaviour?
- **Do you feel watched or monitored**, even when you're alone?
- **Do you feel confused** because the person harming you also says they are "helping"?
- **Do you feel pressured to respond immediately**, even when you don't want to?

Behavioural Checklist:

- **Have you changed how you use your phone or apps** because someone's interactions make you uncomfortable?
- **Do you avoid certain platforms or conversations** because they no longer feel safe?
- **Do you delete posts or messages** to avoid upsetting someone?
- **Do you check your devices repeatedly** for signs of tampering or monitoring?
- **Do you feel the need to hide your online activity** from someone who might react negatively?

Social and Relationship Checklist:

- **Have you pulled away from friends or family** because someone makes you feel guilty for talking to them?
- **Do you feel isolated**, even when you're connected online?
- **Has someone told you that you "don't understand technology"** and should let them control your devices?

- **Has someone discouraged you from using assistive technology** or made you feel incapable of managing it?
- **Have you felt like being alone more often**, because someone has made you feel sad or scared?

Physical and Daily Life Checklist:

- **Are you having trouble sleeping**, focusing, or enjoying things you normally like?
- **Do you feel tired or overwhelmed** after interacting with someone online?
- **Do you notice physical reactions,** like a racing heart, stomach discomfort, or shaking, when you use your technology, or when receiving certain notifications?

Technology-Related Checklist:

- **Has someone logged into your accounts** without your permission?
- **Do you notice settings changed** on your phone, apps, or assistive devices?
- **Do you notice money missing** from your bank accounts?
- **Do you notice that there are messages sent** from your device or accounts, that you don't remember sending?
- **Do you feel unsure whether your location or messages are being monitored?**
- **Has someone taken away your device**, or insisted on "managing" it for you?

Also check through Chapter 3: Forms of TFGBV, linked here, which highlights the different forms of TFGBV that you can watch out for in your digital life.

Activity

We have created a PDF file with this checklist in case you wish to keep it for personal use. You can download the checklist if you access the link here.

Chapter 8: Finding Safe Support

Many people need help with technology. This can include reading messages, understanding apps, managing passwords, or staying safe online. There is nothing wrong with needing support. Everyone deserves help that feels respectful and safe. In this chapter, we will discuss **how to identify a safe support person.**

Learning Objectives

- Learn to identify real, safe support people, and people who are not safe.

A support person is someone you choose. This might be a friend, family member, caregiver, partner, or community worker. A safe support person listens to you, respects your choices, and does not take over your device or accounts without your permission.

Choosing Safe Support

You have the right to decide who helps you with your technology. You also have the right to change your mind at any time.

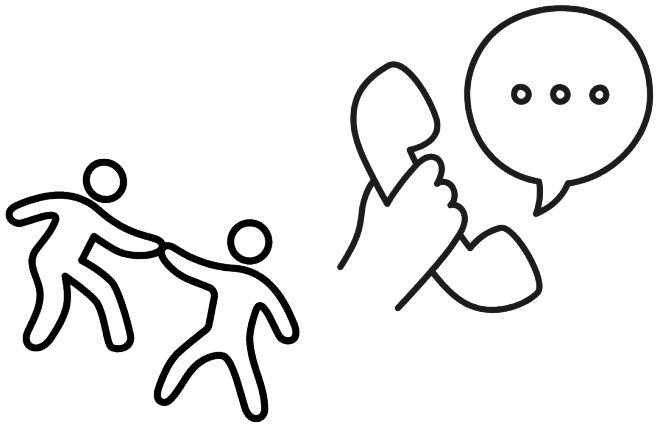
It is important to know that not all people you think are safe, actually are safe. Just because someone is a family member, a caregiver, or a friend, it **doesn't mean that they are safe.** You should be careful to choose a support person thoughtfully.

A safe support person should:

- Ask before touching your device.
- Explain what they are doing in a way you understand.
- Respect your privacy.

- Follow your choices.
- Stop if you say no.

If someone becomes angry, controlling, or secretive when helping you with technology, this is **not** safe support.



Where to Find Support

You may have people around you who can be a support person or community. If not, there are lots of places you can look for one.

You can go to:

- A trusted friend or family member
- A disability support worker
- A community organization
- A crisis or GBV support centre.
- Online support communities.

If someone who is supposed to support you is harming you or controlling your technology, you are allowed to reach out for help. You **do not** need permission from the person causing harm.

To see a list of resources for South African residents, please go to the Support and Resources Page. These services can help you understand what is happening, make a plan, and stay safe.

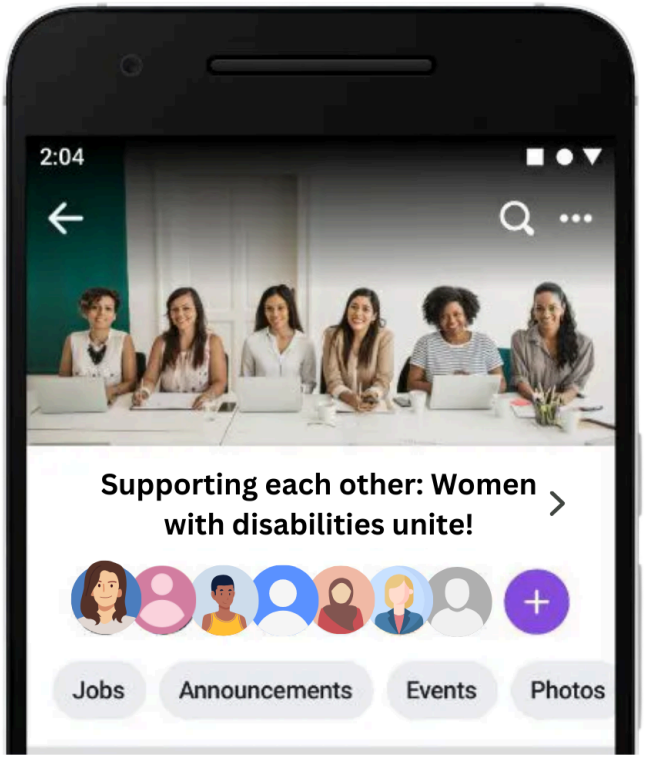
Finding Support in *Online* Communities

Many people find **comfort, friendship, and understanding in online spaces**. Online communities can be helpful when you feel alone, when you want to talk to people with similar experiences, or when you need advice from others who understand disability, technology, or safety.

Things to consider when choosing safe online communities:

- Look for groups that have clear rules about respect, privacy, and safety.
- Choose spaces where moderators or admins are active and respond to harmful behaviour.
- Notice how people talk to each other. Supportive communities use kind, patient, and non-judgmental language.
- Trust your feelings. If a group makes you feel nervous, confused, or pressured, it may not be the right place for you.

An interactive H5P element has been excluded from this version of the text. You can view it online here: https://pressbooks.library.torontomu.ca/tfgbvsafetytraining/?p=646#h5p-9



An example of an online community, through Facebook Groups. This one is called "Supporting each other: Women with disabilities unite!" Even though this group seems safe, make sure to remain vigilant.

When Support Becomes *Unsafe*

Sometimes the people we trust can also be the people who harm us. This can be confusing and upsetting. Abuse can happen in families, friendships, romantic relationships, and caregiving relationships. It can happen slowly over time or suddenly.

Signs of unsafe support include:

- Taking your device away forcefully
- Forcing you to share passwords

- Checking your messages or your devices without asking
- Telling you that you “cannot understand technology”
- Making you feel scared, guilty, or like you’re not allowed to use your own technology
- Using your disability as a reason to tell you what to do.

If this is happening, it is **not your fault**. You deserve safety and respect.

Recognizing Red Flags

Some online spaces or people may seem supportive at first but become unsafe over time.

Warning signs include:

- Someone asking for private information.
- Someone trying to move conversations to private texts or messages too quickly.
- Someone telling you not to trust your friends, family, or support workers.
- Someone making you feel guilty for not replying fast enough.

- Someone asking for money or gifts.
- Someone trying to control your choices or your technology.

If you notice any of these signs, it is okay to leave the conversation or group, or block the person who is doing these things.

Activity

An interactive H5P element has been excluded from this version of the text. You can view it online here:
https://pressbooks.library.torontomu.ca/tfgbvsafetytraining/?p=646#h5p-8

Chapter 9: Responding Safely to TFGBV

In this chapter, we will walk you through **how to document and collect evidence of TFGBV and respond safely.** It can be very overwhelming to do this, so we will provide additional resources for you that helped us to come up with this toolkit. This can come before or after you have found safe support, as we talked about in Chapter 8.

Learning Objectives

- Practice safe documentation and evidence collection.
- Identify at least two formal or community-based reporting options.
- Apply emotional regulation and self-care strategies after online harm.

Documenting and Collecting Evidence Safely

Why documentation and evidence matters:

If you experience TFGBV, keeping evidence can help you get support, report to platforms, or take legal action. Documentation can also help you understand what is happening and can be useful if you decide to report the abuse.

You do not need to collect everything. Only do what feels safe. In fact, you may wish to have someone else with you to help you document evidence. Make sure that this person is a safe support person, and is respectful of your wishes.

How to preserve digital evidence:

- Take screenshots of messages, posts, images, and profiles.
- Write down profile usernames.
- Save URLs, dates, and times.
- Keep original emails or messages (they contain metadata). Do not delete them.
- Store evidence in a safe place (not on a device the abuser can access).
- Make both digital and printed copies. Store data on external hard drives that are not connected to the Cloud (such as USB sticks) if possible.

If you think **someone is monitoring your device, it may be safer to document on paper** or on a **different device** that the person cannot access.

(Taken from Prime Legal Team, 2023.)

You do not need to organize everything perfectly. Even small pieces of information can help later. We have developed a short form that will give you ideas of how to document TFGBV events.

Checklist: Evidence Preservation

Task	Done?
Take screenshots of messages, posts, images, and profiles.	Yes/No
Write down profile names or usernames.	Yes/No
Save URLs, dates, and times.	Yes/No
Keep original emails or messages.	Yes/No
Store evidence in a safe place (not on a device the abuser can access).	Yes/No
Make both digital and printed copies.	Yes/No

While this document is imperfect, we hope it provides insight into how you can record a TFGBV event, which will in turn help law enforcement, applications, and crisis support workers to address your needs and wants. You can access and download the TFGBV Reporting Template to use here.

You can view a built-in version of the template in the activity below.

Activity

An interactive H5P element has been excluded from this version of the text. You can view it online here:
https://pressbooks.library.torontomu.ca/tfgbvsafetytraining/?p=309#h5p-4

If you want a bigger picture of digital evidence, you can learn more with Tech Safety Canada's Preserving Digital Evidence Toolkit, which has been linked here.

TFGBV Reporting Options

You have choices about whether and how to report TFGBV. You do not need to report right away. You do not need to report at all if it does not feel safe. Reporting is one option, but not the only option. However, please know that you are not alone, and there is support and help for you. You do not have to experience this by yourself.

Formal reporting options

These options are important to know if you are in danger, if someone is threatening you, or if someone has taken control of your accounts or devices. These options are more "formal" or, **traditional pathways of accessing law enforcement and crisis supports.**

- Police or law enforcement.
- A protection order through the court.
- Reporting to a gender-based violence or crisis centre.
- Reporting to a disability rights organization.
- Reporting to a professional such as a doctor, therapist, or nurse.

We have made a list of several formal reporting options that are available in South Africa for residents of South Africa. To view this list, you can view our list of options on the **Support and Resources Page, at this link.**

If someone is threatening to hurt you, or you feel in danger right now, you need to get help immediately. **This is an emergency.**

Community-based reporting options

Community-based options can feel safer and more accessible, especially if you are not ready to involve formal systems.

- Reporting harmful posts on social media platforms.
- Blocking or muting the person causing harm.
- Asking a trusted support person to help you report.
- Reaching out to an online support group for guidance. Please ensure that you engage in safe digital practices as you are reaching out to online communities, as detailed in Chapter 9.

Emotional Regulation and Self-Care

TFGBV affects your body and emotions. You may feel scared, angry, confused, or exhausted.... and these feelings are normal. Know that you did nothing wrong. Ways to care for yourself can include:

- Taking breaks from your devices.

- Doing something grounding, like deep breathing or stretching.
- Talking to someone who helps you feel calm.
- Spending time on activities that bring comfort.
- Using sensory tools, such as weighted blankets or calming music.
- Moving your body with light exercise, like taking a walk or doing yoga.
- Eating a meal that makes you happy.
- Spending time with a loved one who can support you.

If you feel overwhelmed, it can help to pause and return to the situation later with support and a calmer body. You can visit the Patient Voices Network blog post which is linked here, which lists 45 unique self-care ideas.

Self-care is vital to ensuring that you are able to heal from experiences of TFGBV. It is also an important part of empowering yourself to protect against future abuse.

Reflect

Have you made your digital safety plan? If so, how have you incorporated emotional regulation and self-care?

Putting It All Together

Responding to TFGBV is not about doing everything perfectly. It is about staying as safe as possible, choosing support that feels right for you, and taking small steps that help you regain control. You deserve safety, respect, and care in every part of your digital life.

Resources

Looking for Self-Care Ideas? Here Are 45! (2021, July 20). *Patient Voices Network*. https://patientvoicesbc.ca/2019/04/26/looking-for-self-care-ideas-here-are-45/
Prime Legal Team. (2023, July 16). DIGITAL EVIDENCE & It's Complexities. *Prime Legal Law Firm Blogs*. https://blog.primelegal.in/digital-evidence-its-complexities/
Tech Safety Canada. (2026). *Preserving and Storing Evidence Toolkit*. Women's Shelters Canada. https://techsafety.ca/resources/toolkits/preserving-and-storing-evidence-of-tfgbv-best-practices

Chapter 10: Building a Safety Plan

Staying safe online is an important part of protecting yourself from future harm. Digital safety is not about being perfect. It is about learning small habits that help you feel more confident, more in control, and more aware of risks.

In this chapter we talk about how to **protect against future online harm** by strengthening digital safety and awareness. We have created a **digital safety plan template** for your personal use, which is available for **download** at the link here, which was modelled after this chapter.

Safety Note:

Share your safety plan *only* with a small group of designated, safe people (see Chapter 8: Finding Safe Support). Do not include any of your personal *usernames* or *passwords* on your safety plan. The safety plan should be a guide for you to know what to do in case of TFGBV. In case of emergencies, call 112 (if you are in South Africa), or your local emergency number.

Learning Objectives

- Understand protective digital practices, including privacy, consent, and safe data storage
- Identify common risks and prevention strategies for image-based abuse
- Recognize how survivor-led advocacy builds long-term safety

Building Protective Digital Habits

Protective digital habits help you stay safer online. These habits are simple steps you can take to protect your information, your privacy, and your devices. For more about how to engage in specific protective behaviours, you can view Chapter 6: Online Safety How-To's.

Key protective practices include:

- Keeping your passwords private (see Chapter 6).
- Using strong passwords that are hard to guess (see Chapter 6).
- Turning on two-factor authentication (see Chapter 6).
- Checking your privacy settings on apps and social media (see Chapter 6).
- Being careful about what you share and with whom.
- Storing sensitive information in safe places.
- Asking for help from someone you trust when you need it (see Chapter 8: Finding Safe Support).

These habits help you stay in control of your digital life.

Creating a Technology Safety Plan: Step-by-Step

A technology safety plan helps you think ahead and take steps to protect yourself. Here is an idea of what a technology safety plan might look like:

Step 1: List Your Devices and Accounts

- Write down all the devices you use (phone, laptop, tablet, smart home devices).
- List all your online accounts (email, social media, banking, shopping, cloud

storage, etc.). Do not include usernames or passwords.

Step 2: Identify What Might Be at Risk

- Does anyone else know your passwords?
- Are you sharing devices or accounts with someone you don't trust?
- Are there apps or devices you don't recognize?

Step 3: Change Passwords and Security Settings

- Change passwords to strong, unique ones.
- Turn on two-factor authentication where possible.
- Remove any shared access or unknown devices from your accounts.

Step 4: Check App Permissions and Location Settings

- Review which apps have access to your location, camera, microphone, and contacts.
- Turn off permissions for apps that don't need them.

Step 5: Plan for Emergencies

- Know how to quickly log out or lock your accounts.
- Have a list of emergency contacts. Who will you call? Where will you find support?
- Keep evidence (screenshots, messages) in a safe place.

Step 6: Get Support & Change Habits

- Plan how you will reach out to local services, shelters, or emergency contacts. Phone call? Email? In-person visit?
- Use a safer device (like a library computer) if you think yours is being monitored.

Step 7: Self-Care

- Engage in self-care and regulating activities (See Chapter 9: Responding Safely to TFGBV).

Reflect

Everyone is different, and different disabilities or identities or contexts might require different supports and steps.

Thinking about your own experiences, what steps might you add to customize this plan for yourself?

EXIT SITE

Content Warning: The following story contains strong language, and depicts cyberbullying and sexual harassment. Reader discretion is advised.

Case Study #1: Is Thandi being cyberbullied?

Thandi is a Deaf woman in her 20s. She enjoys posting signed Instagram Reels about accessibility. Lately, she's noticed cruel comments mocking her signing and editing her videos with hateful captions. She's unsure if this is "real" abuse.

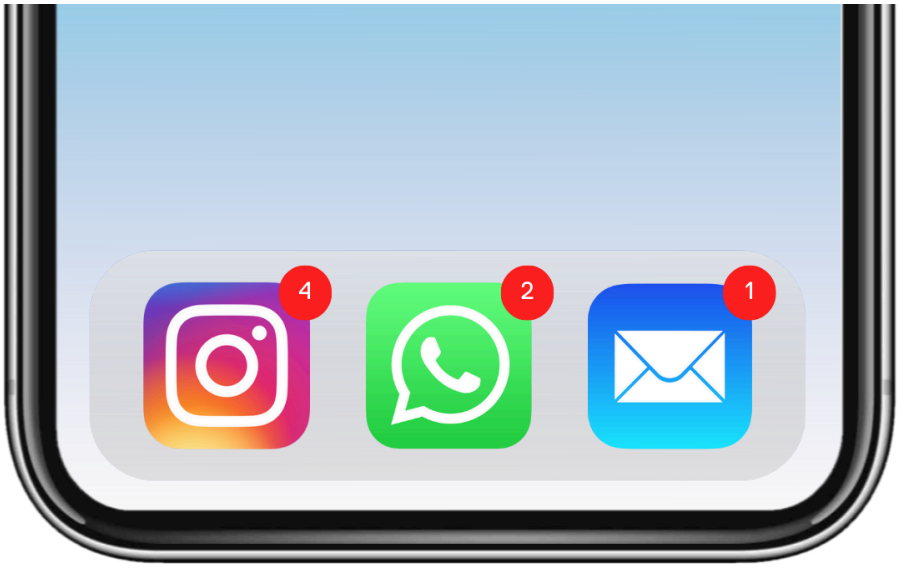
Let's hear a little more about Thandi's experience...

Thandi's Story

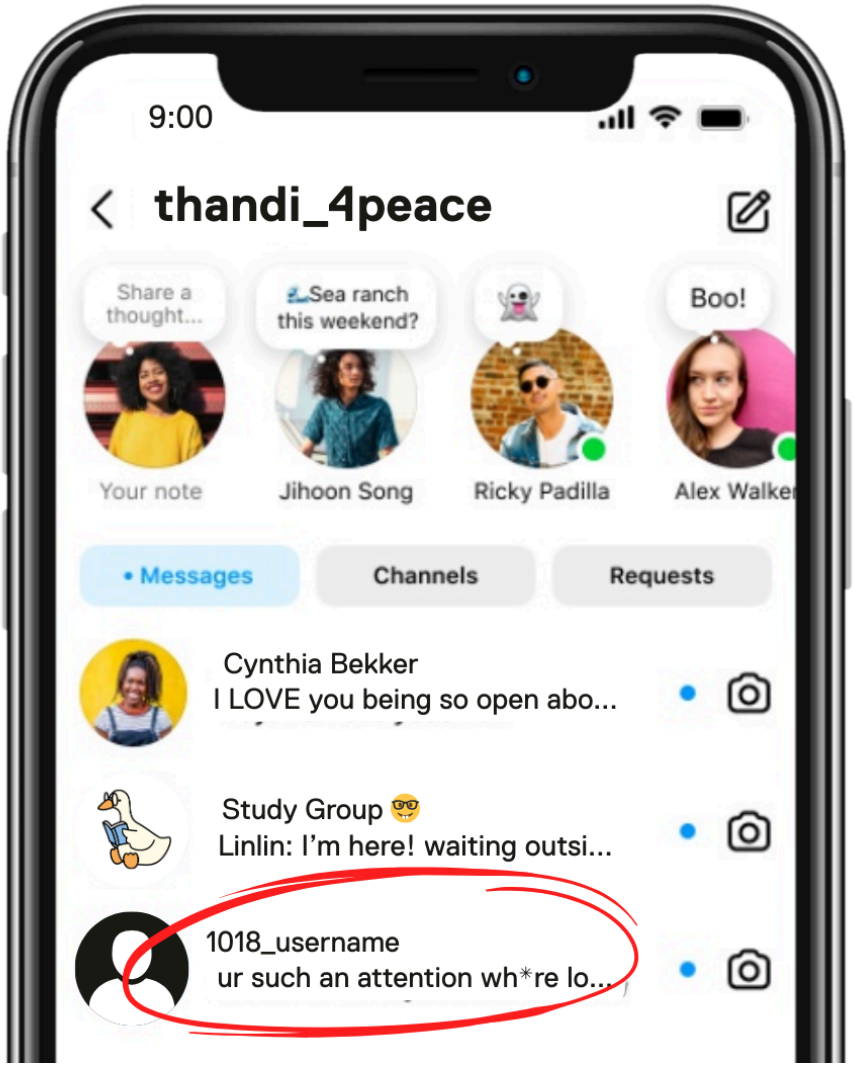
Good morning sleepyhead! Thandi wakes up to check her Instagram, then

WhatsApp, and then email messages. Her mornings always begin with scrolling on your phone, and today is no different.

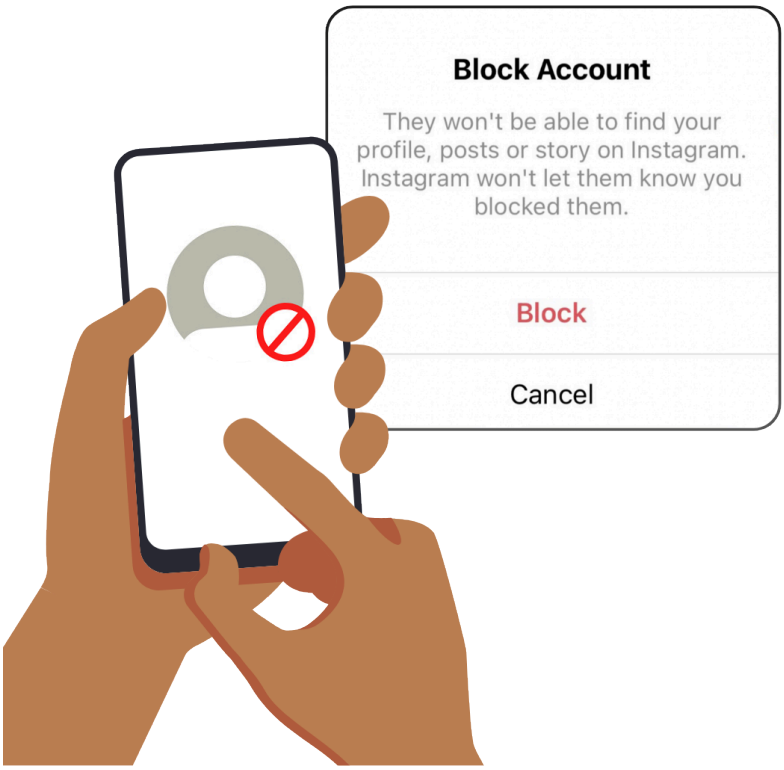
Oh! Thandi has a few new messages in her Instagram inbox. Yesterday, she posted a new video on her Instagram. Thandi likes filming herself using sign language to connect with her d/Deaf and hard-of-hearing community, and posting these videos to Instagram and TikTok. Maybe people responded to it! Let's open Instagram and see.



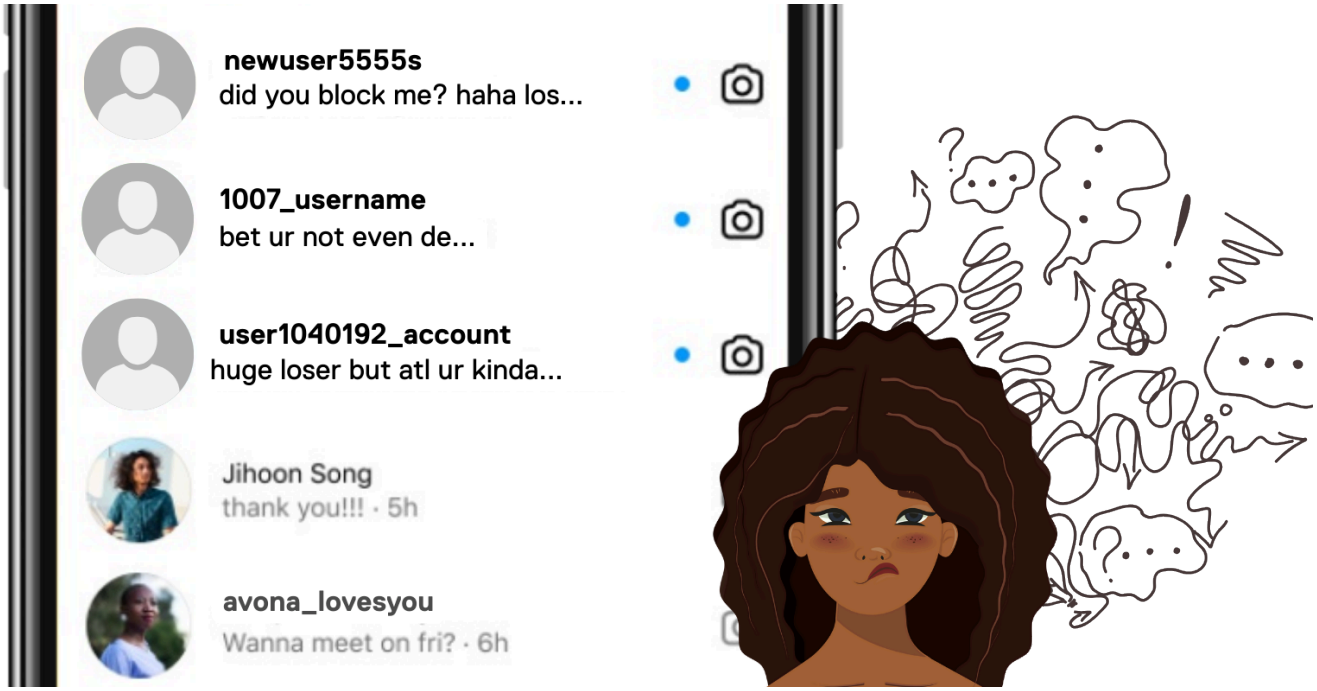
One of the messages is really mean. An unknown user saw Thandi's video and is being very hateful, accusing her of being attention-seeking, and even saying, "I bet you're not even deaf."



Thandi decides to block the person, so they can't contact her again. Afterwards, she heads off to work and continues with her day.

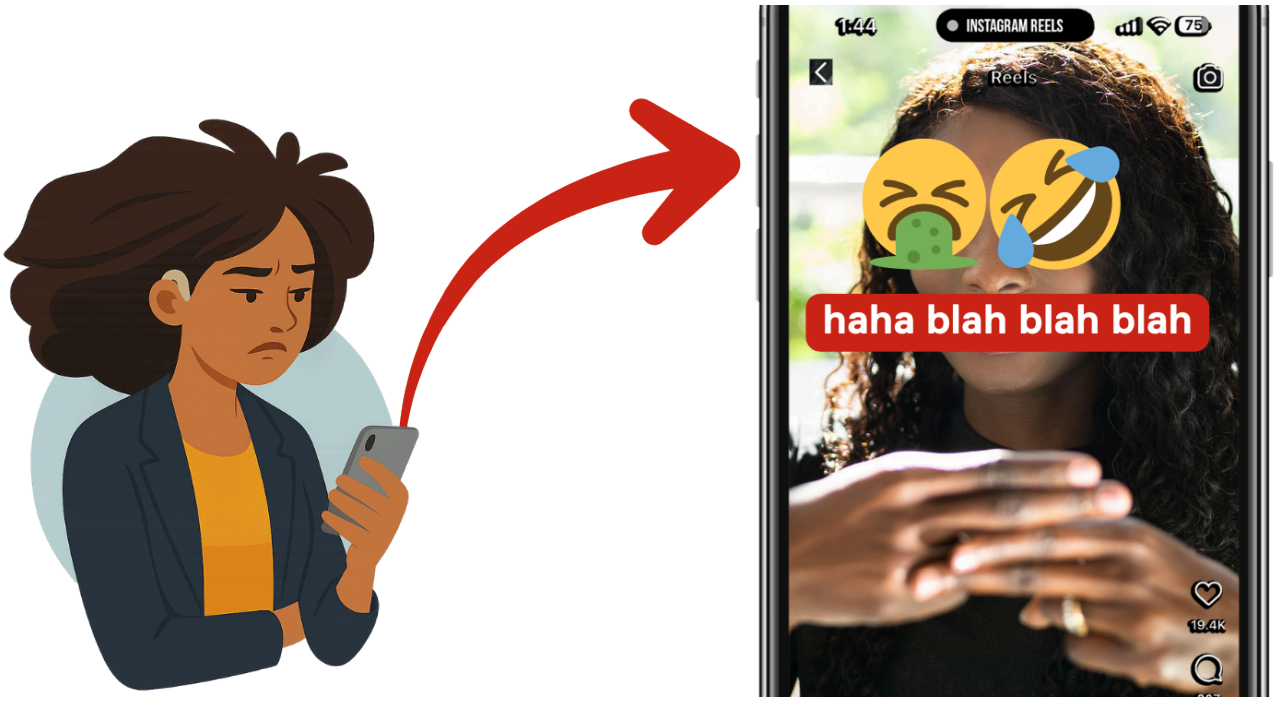


When Thandi checks her Instagram inbox that night, she has several more messages and comments from unknown accounts. Maybe her video went viral! Oh no... It seems like the person that Thandi blocked made another account and is continuing to send messages.



There are also new people sending mean messages. She tries to delete all the hurtful comments and messages, but they keep coming in and she can't keep up. She feels extremely sad, and doesn't know how to proceed.

Someone even edits her video with offensive captions and reposts it. Thandi hesitates to post again, unsure if this is “just trolling” or something more serious. In any case, she decides not to post the video she had planned for today because she is afraid of more backlash.



Reflection Prompts...

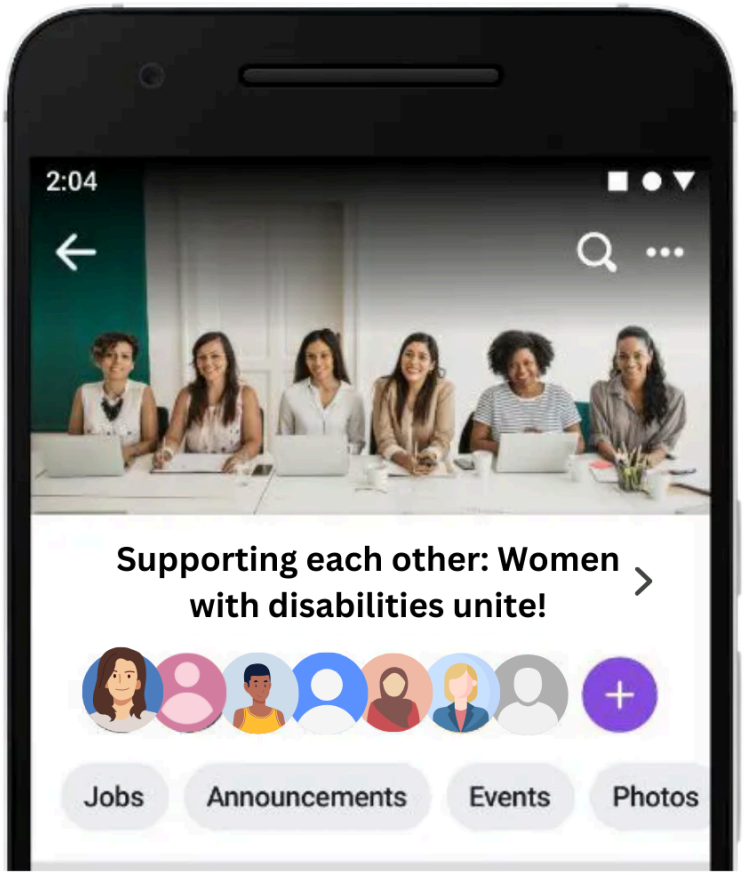
1. What are the red flags (or signs of danger) in Thandi’s experience?
2. Have you or someone you know experienced something similar?
3. How can you tell when online “teasing” becomes abuse?
4. What do you think that Thandi should do about these Instagram messages and reposts?

Content Warning: The following story contains mentions of online and sexual harassment. Reader discretion is advised.

Case Study #1B: Thandi's Journey to Online Empowerment

After a stressful and overwhelming night of negative spam messages, Thandi is not sure what to do. She reaches out to her best friend, who mentions an online Facebook group that she knows and trusts.

After reading through other posts and seeing how much support this group has provided, Thandi decides to join the Facebook group. Maybe someone else will understand and have some advice?



Thandi reads through other women's posts and sees how much support this group has provided for others. Finally, she decides to post about her situation.

A few hours later, Thandi sees a huge outpouring of support with other women with disabilities relating to her. It's a huge relief to her, but also very troubling. So many women experience this, but she had no idea about these experiences or how to protect herself until it had already happened to her!

Thandi S P

New Member Today at 7:00 PM

Hello everyone... I'm new to this but here goes. People have been making horrendous comments and messages about my social media posts about deafness and I don't know if this is a normal experience or if there is something to do to make them stop or learn to manage my emotions about it? I am doing social media for the first time and really enjoy most of it, but this is so hard. Any deaf sisters have advice? Based in South Africa BTW in case that changes the advice.

23 11 Comments

One of the commenters is a woman named Rachel, who lives in Gauteng, and is a Deaf advocate. Rachel extends an invitation to Thandi to chat online, and even to call her. Thandi is hesitant at first. After all, online spaces have not been kind to her lately.

23 11 Comments

Like Comment

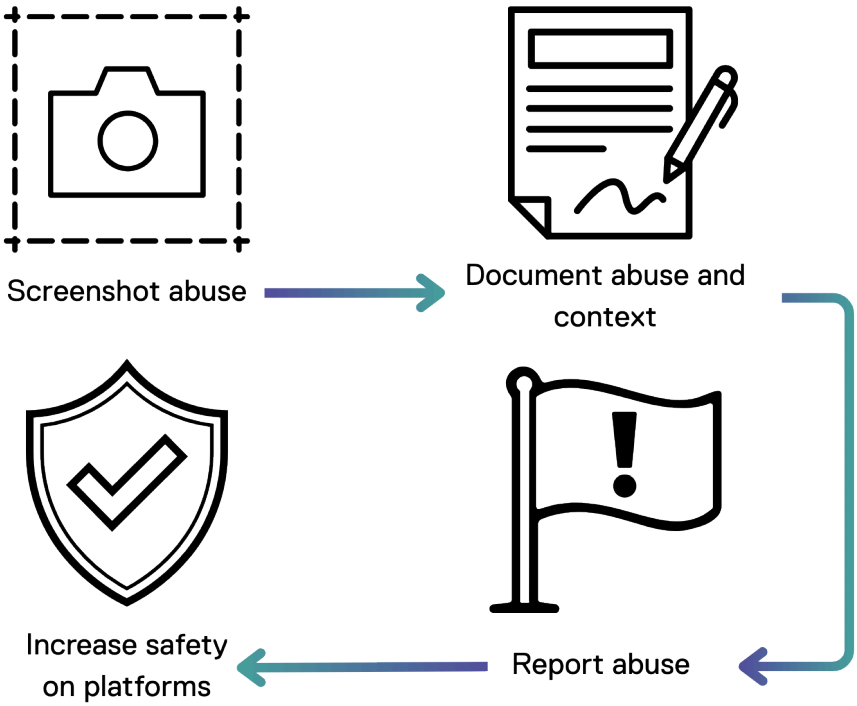
Hi Thandi my name is Rachel! I'm in Gauteng and work as a disability advocate for women at [redacted] I'm also Deaf! Message me if you want, we can chat on video call using SASL or in English if you're comfortable!! I understand that the internet can be an overwhelming place so maybe we can be friends ❤️❤️

But Rachel doesn't pressure her. In fact, she suggests that Thandi bring her best friend along to their video chat, to ensure that Thandi feels safe and secure. Eventually, Rachel and Thandi and Thandi's best friend schedule a video call to introduce themselves and to talk about Thandi's situation.

Thandi shares all the things that have been happening to her. As Rachel listens, she explains that this is targeted harassment and not "just trolling." The ongoing, direct and repeated abuse is not okay, and not something to just brush off.

Collaboratively, they start by taking screenshots of the messages and comments, as well as writing down all the usernames of the fake accounts and dates the spam took place at. Rachel helps Thandi to write out reports for all the abusive accounts to Instagram and review the privacy settings to limit who can comment or direct

message Thandi. This gives Thandi some relief and control returning to her account and wellbeing.



Rachel invites Thandi to join a Deaf peer support group that meets online. During the first meeting, Thandi is able to listen to other peers who share a similar experience of online harassment and discrimination. She realizes she is not alone and her feelings are valid.

Now, Thandi meets with this online group regularly... It becomes a safe place to rebuild confidence, talk about experiences and learn about digital safety strategies to find her passion to post again.

Even though this was a painful experience, Thandi slowly builds up the confidence to start posting again... but this time she has community support, knowledge and tools to protect herself.

Thandi now recognizes the dual role of technology, as both a dangerous and vulnerable place, but also a place where she can find friends, share her story, and be a part of a wonderful community. She just needed to learn how to use it and make it safe for her.

Reflection Prompts

- What helped Thandi respond safely?
- Are there any steps of responding to TFGBV might be risky or difficult without support? If so, what are they, and why?
- How can communities empower survivors to respond collectively?

Content Warning: The following story depicts domestic violence, including online sexual and image-based abuse. Reader discretion is advised.

Case Study #2A: Maya's experience of image-based abuse

Maya, a woman who uses a wheelchair for a physical disability, meets someone on a dating app. They exchange private photos. After she ends the relationship, the ex-partner threatens to share her pictures online unless she reconnects.

Maya feels trapped and ashamed, unsure if she can report it because she voluntarily sent the images.

Maya’s Dating Life

As a big introvert, and a woman with a mobility-related disability, Maya often finds it difficult to meet potential romantic partners in-person. She decides to make a Tinder account, which is a mobile dating app.

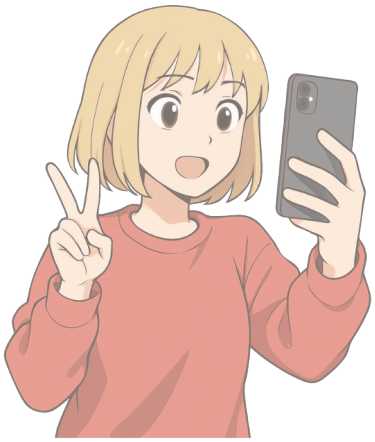
Maya always discloses her disability in her dating profiles, because she’s had bad experiences in the past of being “ghosted” by people once they find out she has a disability. And look... A new match! This guy, Alec, seems really nice.

Over the next few days, Maya and Alec exchange mobile phone numbers, and are constantly messaging. Maya is very excited about this relationship. By the third day of chatting, Alec asks her to be his girlfriend, and tells Maya that he is in love with her.

An Uncomfortable New Dynamic

They date online for about a month. During this time, Alec asks Maya to send

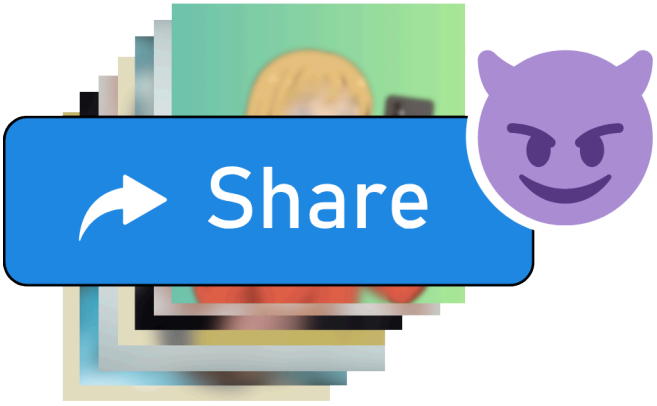
several intimate photos and videos of herself as they maintain a long-distance relationship. She obliges, but Alec asks for more photos, with more of her body being shown each time.

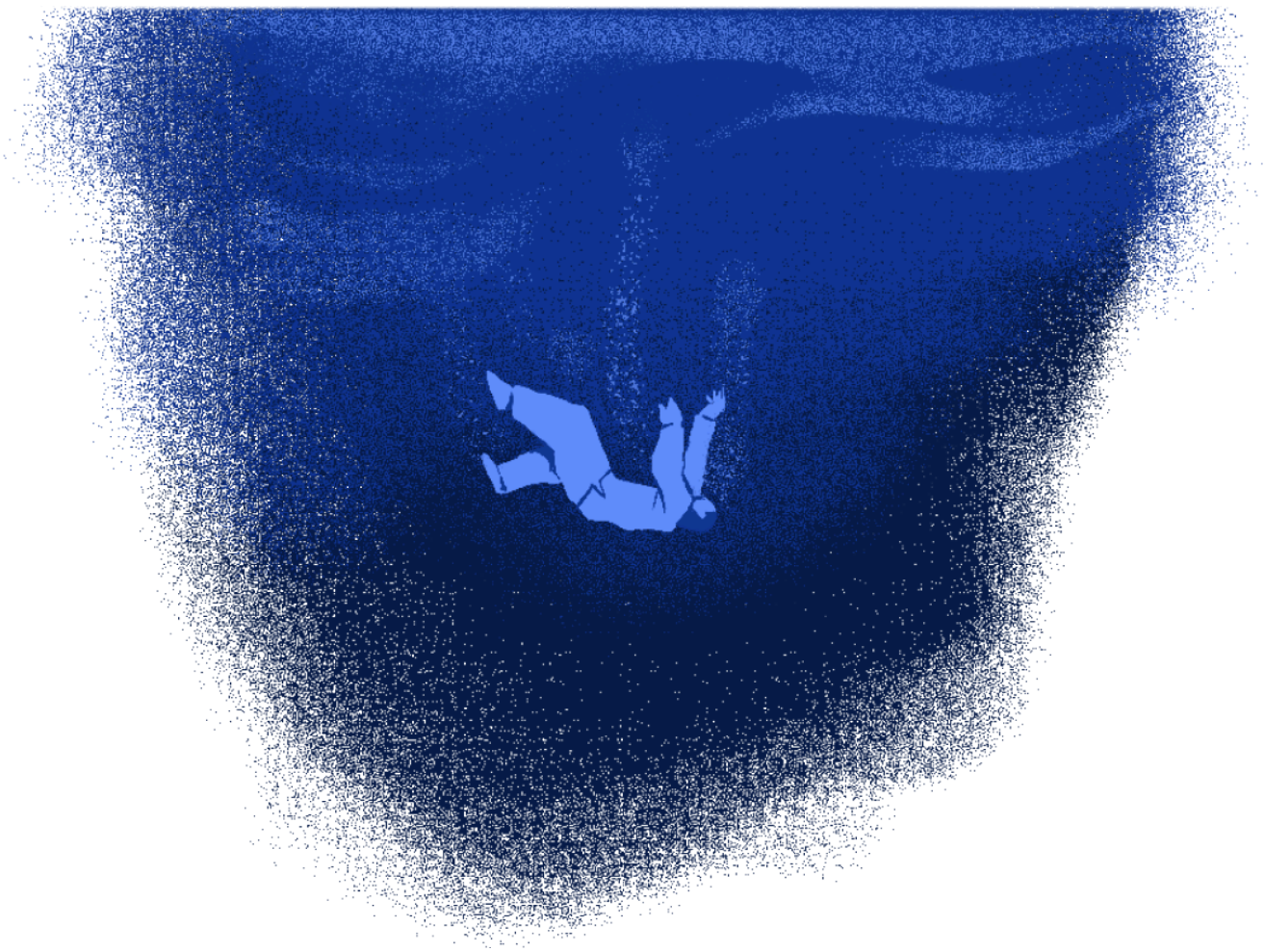


Even though Maya doesn't feel totally comfortable sending photos that show so much of her body, Alec says he "needs it", or else he may begin looking at other women. Eventually, their text conversations become mainly about sex and sexting.

After two months, Maya has had enough. She tells Alec that she wants to break up. Alec is very angry about this, saying: "No one else will want you because you're disabled... You should be grateful that I even looked at you!"

Alec then threatens to share all of her intimate photos and videos on social media if she breaks up with him. He says that because Maya shared the pictures and videos with him willingly, they are now his personal property, and he can do whatever he wants with them.





Maya is terrified that Alec is right. Now she feels trapped and ashamed, unsure if she can report the threats because she voluntarily sent the images. Her world feels like it's falling apart, bit by bit. She feels so alone.

Reflection prompts...

- Can you identify any red flags or warning signs in this situation, that came up *before* Maya experienced abuse?
- What would you tell Maya to do in this situation, to respond to these forms of TFGBV?
- What steps could you take today to feel safer online?

EXIT SITE

Content Warning: The following story depicts domestic violence, including online sexual and image-based abuse. Reader discretion is advised.

Case Study #2B: Maya's Journey to Digital Safety

You can read about the beginning of Maya's experience in Case Study #2A which is linked here.

What Maya does next

When Maya first learns that Alec has distributed her images, she feels shock, shame, and fear. Alec sends her threatening WhatsApp messages, implying he will "expose her further" if she doesn't comply with his demands. The messages escalate into harassment, including:

- Threats to send the images to her employer
- Screenshots showing he has already shared them with strangers
- Attempts to contact her through new numbers when she blocks him

Maya initially freezes, unsure of her rights or what steps to take. She deletes some messages out of panic, then realises she needs support.

Support From a Disability Advocate and Legal Clinic

After a quick search, she finds gender-based violence resources (you can too, by navigating to our Support and Resources Page). She connects with a local disability rights organisation in Cape Town. A disability legal advocate meets with her and explains that **image-based abuse is a crime under South African law**, and she has the right to report it.

The advocate helps Maya understand her options and encourages her to document everything. With guidance and support, Maya begins to:

- **Save all threatening messages** from Alec; she does not delete them before reporting Alec.
- **Take screenshots** of the shared images and timestamps.
- **Record voice notes** describing what happened, since typing is difficult for her.
- **Store evidence securely** in a password-protected folder

The advocate also refers her to a community legal clinic that specialises in gender-based violence and digital abuse.

Reporting Alec

With the legal advocate's support, Maya takes several steps to report Alec's actions:

- She reviews her rights under the **Cybercrimes Act in South Africa** by visiting accessible resources, such as the accessible website, https://cybercrimesact.co.za/.
- She files a **case at her local SAPS station**, providing the evidence she collected (see more about evidence collection in Chapter 8: Responding Safely to TFGBV).
- The legal clinic helps her submit a **Protection Order application** under the Domestic Violence Act (see more about this in Chapter 5: What Are Your Rights Online?).
- She reports Alec's accounts to **Facebook, Instagram, and WhatsApp**, using their reporting tools (see more about this in Chapter 9: Staying Safe Online).
- She blocks all known numbers and accounts linked to him.

The process is emotionally difficult, but each step helps her regain a sense of control.

Strengthening Her Digital Safety

The disability advocate teaches Maya practical digital safety skills tailored to her needs:

- Using **encrypted messaging apps** for private communications, and avoiding sending very private images over the internet.
- Setting up **two-factor authentication** on all accounts
- Adjusting privacy settings on social media
- Learning how to recognise coercive digital behaviour
- Creating a **safety plan** for future online interactions

As she becomes more confident, Maya notices her anxiety easing. She begins to feel safer using her phone again.

Healing Through Counselling and Peer Support

Maya attends counselling sessions offered through a local women's centre. Through individual therapy and peer support groups, she learns:

- That **consent must be informed, enthusiastic, and freely given.**
- That coercion, pressure, or manipulation invalidate consent.
- That she is not to blame for Alec's actions.
- How to rebuild trust in herself and set personal boundaries.

Hearing other women's stories helps her feel less alone and reduces the shame she carried.

Outcome

Maya now feels more confident in her digital presence. She understands her rights, knows how to protect herself, and has built a strong support network through peer support and therapy.

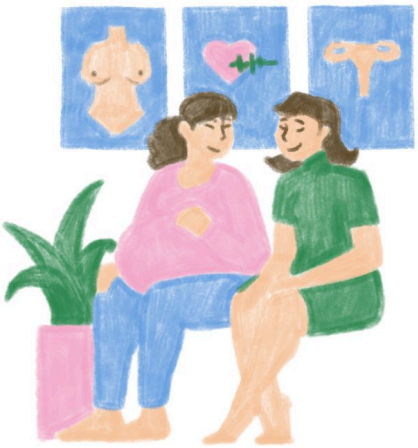
Reflection Questions

- How can sharing stories like Maya's reduce stigma?
- What steps could you take today to feel safer online?
- Were any of the steps that Maya took surprising to you? Why or why not?

FAMILY AND CAREGIVERS

EXIT SITE

Family and caregivers include loved ones (family members, friends, romantic partners) or daily care providers (such as parents, hired caregiving staff) of women with disabilities, who are part of their immediate support system.



In this section, we will be referring to the person who has experienced TFGBV as a "**survivor**": someone who has survived violence.

Chapter 11: Recognizing that TFGBV is Happening to a Loved One

As a **caregiver, family member, or partner**, you play an important role in noticing early signs that something is wrong. This chapter helps you understand **what TFGBV can look like in a loved one's behaviour, emotions, and daily life**. These signs do not prove that abuse is happening, but they can help you recognize when someone may need support, safety, or a gentle conversation.

Learning Objectives

- Recognize emotional, psychological, and behavioural signs that may show a loved one is experiencing online harassment or digital control
- Learn how to notice changes that signal discomfort, fear, or loss of digital independence
- Understand how TFGBV can affect a person's wellbeing, routines, and relationships

Tech-facilitated gender-based violence can be difficult to see from the outside. Many people who experience digital abuse do not talk about it right away. They may feel confused, ashamed, or unsure if what is happening "counts" as violence.

They may also rely on the person causing harm for support, care, or daily needs, which can make it even harder to speak up.

How Do You Know If Someone You Care About Might Be Experiencing TFGBV?

Survivors often show signs in their feelings or behaviour long before they name the situation as abuse. You may notice changes in how they act, how they use technology, or how they talk about their online experiences.

These signs are not proof on their own, but they are **signals that something deserves attention.** They likely warrant a bigger conversation, where you ask about their safety.

Recognizing the warning signs of TFGBV in your loved one is important to being able to act quickly and support them.

Emotional and Psychological Signs

Think about how your loved one has been feeling lately. Have you noticed shifts in their mood, confidence, or comfort with technology? These changes may be connected to TFGBV. **Possible signs might include:**

- Sudden anxiety when messages or notifications appear
- Nervousness about posting online or checking accounts
- Embarrassment or shame about something happening online
- Blaming themselves for someone else's harmful behaviour
- Feeling watched or monitored, even when alone
- Confusion because the person harming them also claims to be "helping"

These emotional shifts often appear before a survivor is ready to talk about what is happening.

Behavioural and Daily Life Signs

People sometimes change their routines to protect themselves. These changes can be subtle or sudden. **You may notice the following signs:**

- Avoiding certain apps, platforms, or devices
- Deleting posts or changing how they communicate
- Trouble sleeping, concentrating, or enjoying activities

- Withdrawing from friends, family, or online communities
- Repeatedly changing passwords or checking devices for tampering
- Feeling pressure to respond immediately to messages

These behaviours can be signs that someone feels unsafe or is being harassed or abused online. **TFGBV affects a survivor's sense of safety, privacy, and control.**

These feelings often show up in the body and in daily habits long before someone names the situation as abuse. Recognising these early signs can help you offer support in a gentle and non-judgmental way.

Reflection

- Which of these signs have you witnessed before, if any?
- How would you approach a survivor after witnessing some of these warning signs? If you're not sure, then don't worry! **We'll discuss this in the next chapter.**

Chapter 12: Providing Support for TFGBV Survivors

Sometimes, a survivor who is experiencing TFGBV will not bring it up to you at first. Instead, you may have to do your own check-in, if you suspect TFGBV.

In these cases, you may feel something is "off" with a person, but you may also worry about saying the wrong thing or making the person feel judged or pressured. In this chapter we will discuss having **conversations about TFGBV and then how to provide support to survivors.**

Learning Objectives

- Learn how to approach conversations about TFGBV while prioritizing safety, curiosity, and autonomy of survivors.
- Learn how to provide support for survivors of TFGBV.

How to ask about TFGBV

Asking about TFGBV requires gentleness, respect, and a focus on the person's feelings rather than the technology itself. The goal is to open a door to a conversation, rather than to force them to tell you everything. A supportive approach works best when it combines three elements: **safety, curiosity, and autonomy.**

Safety: Creating the Conditions for a Safe Conversation

A person is more likely to talk if they feel calm, respected, and in control. Before asking anything, caregivers can pay attention to:

- Privacy, so the person is not overheard
- Tone of voice that is soft and non-urgent
- Body language that is open and relaxed
- Timing, choosing a moment when the person is not stressed or distracted

These small choices help the person feel safe enough to share.

You may also want to consider if you are the best person to have this conversation with. For example, if you have triggers or have experienced traumatic events related to GBV or something similar, you need to consider whether you are able to engage in this conversation safely.

Your safety and ability to engage in this conversation appropriately will have a **big impact on how the survivor will feel and respond.**

Reflect

In **Leila and Aisha's** story in **Case Study #3A**, how should Aisha approach a conversation with her daughter about TFGBV?

What did she do well? What would you add to her approach?

Gentle: Gentle Ways to Start the Conversation

Openers that focus on **feelings rather than accusations** help reduce fear and shame. You might be able to try:

- “I have noticed you seem stressed when your phone goes off. How are you feeling about things online lately?”
- “Sometimes online spaces can feel overwhelming. Has anything been bothering you?”
- “You deserve to feel safe when you use your phone. Is anything making you uncomfortable?”
- “I care about you and want to check in. How have things been going with your apps or messages?”

These questions first reaffirm a truth and feeling of care, which grounds the conversation. Then, they ask a general question around their technology use and experiences. Hopefully, this invites conversation without assuming anything is wrong or creating unnecessary fear.

Being gentle in your line of questioning and approach to conversations around TFGBV is vital to ensuring that survivors feel safe, and avoid being retraumatized.

Sometimes your instinct or hunch is wrong, and no TFGBV is actually occurring.

However, if you see the signs of TFGBV, it's better to ask to make sure that there is nothing wrong, than to assume all is well.

Autonomy: Questions That Respect Autonomy

People experiencing TFGBV often feel watched or controlled. Questions should give them space to choose what to share, and with whom. **Supportive examples include:**

- "Would you like to talk about anything that has been happening online?"
- "Do you want help with anything on your device, or would you prefer to handle it yourself?"
- "Is there anything online that feels confusing or upsetting?"
- "Do you feel safe with the people you talk to online?"
- "If something is going on that you don't want to tell me, do you have someone you can talk to for support?"

These questions show care without taking over the conversation or forcing disclosures or reporting.

People with disabilities are often subject to excessive surveillance and limited privacy. They are also subject to [pb_glossary id="729"]infantilization[/pb_glossary]. These factors mean that people with disabilities often have their choices and autonomy taken away from them, and are forced to be dependent on others (Robey et al., 2006).

Below, we have provided further examples of how questions about different forms of violence, which do not directly accuse or pressure someone.

Examples of asking gentle and curious questions

Questions that can help assess if someone is experiencing digital coercive control:

If you suspect that someone is being monitored or pressured, you can ask in a way that avoids blame, instead of: *"Have you experienced coercive control?"*, **try:**

- "Has anyone been asking for your passwords or checking your phone without

asking?"
- "Has anyone been telling you what you can or cannot do online?"
- "Has anyone made you feel scared to post or message people?"
- "Has anyone changed things on your device without explaining why?"

These questions focus on behaviour, not the person's choices.

Questions to check if someone is experiencing TFGBV from a caregiver or service provider:

For people who need help with technology, it is important to separate support from control. **Ask questions like:**

- "Do you feel comfortable with the way people help you with your technology?"
- "Is there anyone helping you with your device who makes you feel nervous or unsure?"
- "Do you want to choose someone else to help you with your phone or apps?"

These questions reinforce that support should feel safe, not forced.

Reflect

Can you think of other specific questions you can ask about different forms of violence? For example, **try to reword the following questions:**

1. Has someone been cyberstalking you?
2. Why did you stop posting on Instagram? Are you being harassed?
3. Why would you keep texting him? I told you he would keep threatening you!

What should you avoid when asking about TFGBV?

Certain approaches can shut down conversation or increase fear for the person who may be experiencing TFGBV. As a caregiver, family member, or other loved one, you have a responsibility to try to avoid re-traumatizing or assigning blame to the survivor. To do this, **keep the following rules in mind:**

Do not ask: "Why did you let this happen?" or saying things like, "I told you they were bad news!" As it places blame on the survivor.

Do not demand or confiscate the survivor's phone or devices. This strips them of autonomy in an already vulnerable situation.

Do not threaten to hurt or seek revenge about the person you suspect is causing harm. This does not help and can make the survivor feel responsible for your own negative reaction, and may even cause them to hold back information.

Do not minimize the survivor's feelings, for example, saying, "It's not that bad." Or, "Don't be silly, they can't hurt you."

Do not make promises you cannot keep. For example: saying "I will never let them hurt you again," may disempower them, and create dependence on you. Instead, say, "I will help you as much as I can, and you will find a way for you to feel safe again."

Activity

An interactive H5P element has been excluded from this

✍ version of the text. You can view it online here: https://pressbooks.library.torontomu.ca/tfgbvsafetytraining/?p=688#h5p-27

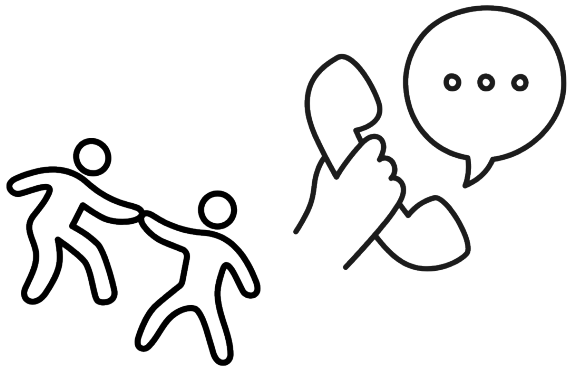
“What do I do if a survivor does not want to talk to me?”

Not everyone is ready to share. Caregivers and family members can keep the door to communication open by keeping calm and using very open language. You can say things like:

- “That is okay. You can talk to me anytime.”
- “You do not have to explain anything right now.”
- “I am here for you whenever you feel ready.”

This helps the person feel respected rather than pressured.

Safety note: If there are obvious signs of immediate physical danger to this person, either due to their own mental health, due to the severity of the TFGBV, or if the survivor is an underage (under the age of 18) victim of sexual violence, you need to speak up. **Immediate safety should come first. Access supports listed in our linked Support and Resources Page.**



Supporting a Survivor's Next Steps

After beginning the conversation about TFGBV, **what do you do next?** Next steps should be **survivor-directed,** but also **appropriate** according to the situation. In some cases, the survivor will not wish to do anything beyond receiving support from yourself or other loved ones, and engaging in online protection behaviors. While this can be a fine response in some cases, in others, there needs to be an escalation to outside supports.

Again, if there are obvious signs of immediate physical danger to this person, **immediate safety should come first. Call 112 to contact the SAPS for emergencies. Access additional supports listed in our linked Support and Resources Page.**

If not, but you still know that they need additional help, consider accessing outside supports.

Encouraging outside supports

If the person is in danger, it is important to help them connect with someone trained to support people experiencing violence. This may include a trusted friend or family member, a disability support worker, a community-based organization, a doctor or therapist, or a crisis or gender-based violence center. **You can use phrases like:**

- "There are people who can help you stay safe. Would you like me to help you connect with them?"
- "You do not have to handle this alone. There are services that understand situations like this."

The goal is to offer options, not instructions. Another way to help is by taking on the task of managing accessibility for them. Many times, people with disabilities are forced to do the work of locating accessible and inclusive resources, on their own. This can create fatigue and labour that makes it more difficult to seek help (read more about this in an article by Annika Konrad).

Consider the suggestions we have provided, but also look into your own **local**

resources. By doing so, you can check for their accessibility and appropriateness for your loved one, giving them a simpler route to finding support.

Resources

- Konrad, A. M. (2021). Access Fatigue: The Rhetorical Work of Disability in Everyday Life. *College English*, *83*(3), 179–199. https://doi.org/10.58680/ce202131093.
- Robey, K. L., Beckley, L., & Kirschner, M. (2006). Implicit Infantilizing Attitudes About Disability. *Journal of Developmental and Physical Disabilities*, *18*(4), 441–453. https://doi.org/10.1007/s10882-006-9027-3

Chapter 13: Helping Prevent and Protect Against TFGBV

Preventing TFGBV requires that caregivers and family members help survivors gain skills, confidence, and options, rather than taking control away from them. Supporters should aim to **teach, enable, and empower**. This means explaining risks clearly, offering practical help when asked, and respecting the person's choices even when those choices carry risk.

This chapter will go over **how to support women with disabilities in protecting against and preventing TFGBV** from occurring. Not all women with disabilities will require this level of guidance or support.

Learning Objectives

- Explore how to build long-term digital literacy and safety habits.
- Learn how friends and allies can support safety and autonomy without control.

Prevention work sits at three levels: the individual (skills and habits), the relationship (boundaries and trust), and the environment (policies, community resources, and accessible technology). Effective prevention combines small daily practices with longer-term learning and community supports.

Teach, and Avoid Control

Teaching focuses on showing how tools work and why certain steps help. It avoids doing everything for the person and stripping autonomy.

Explain privacy and security simply. If needed, show how privacy settings, two-factor authentication (2FA), and strong passwords protect accounts.

Practice scam identification. Review a few common scam messages together and point out red flags (requests for money, urgent demands, requests for codes). We have included a few examples below:

- "You're the only one I trust. I lost access to my bank after an emergency... can you send $500 now? Don't tell anyone, it's private."
- "We detected suspicious activity. Click this link and enter the 6-digit code we just sent you to secure your account."
- "This is the billing department. You owe $1,200. Pay via gift card or we will disconnect service today."
- "Your computer is infected. Install this remote-access tool so we can fix it now."

Help set up safety features with consent. For example, offer to set up 2FA or change passwords... But only if the person agrees and understands what you are doing.

Provide resources. Share accessible guides, local workshops, or helplines the person can use later. We have provided several throughout this book, if you wish to use them.

When you are teaching, use accessible language, repeat steps, and check understanding. If your role as a supporter is to teach a someone with a disability who uses assistive technology, aim to do a check of whether the different tools and methods work alongside these technologies.

Helping your loved ones find accessible technology and safety tools for their own autonomy is an important part of support.

Supporting autonomy without taking over

Friends and family must balance safety with respect for independence.

Ask before acting. Offer help, but do not seize devices or change settings without consent unless there is immediate danger.

Offer choices. For example: "I can set up 2FA for you now, or I can show you how and we can do it together."

Model healthy digital behaviour yourself. Show how you set boundaries online and how you respond to suspicious messages.

Practice boundary language. Help the person rehearse short phrases: "I don't share passwords," "I will check with a friend before sending money," or "I don't have to respond right away."

These practices build trust and reduce the chance that support becomes control.

Encourage safe exploration and digital confidence

People learn best by doing. Encourage safe, supported exploration of apps and services so the person can use technology without fear.

- Introduce **disability-friendly apps** and settings that improve accessibility (screen readers, voice commands, simplified interfaces).
- Point to **safe online communities** where people with similar experiences share tips.
- Support practice of everyday tasks: sending messages, checking account notifications, and recognizing suspicious links.
- Frame mistakes as learning opportunities to reduce shame and build resilience.

Encouraging exploration helps the person feel powerful online rather than afraid.

Creating safer digital habits

Small, regular habits reduce risk over time. These routines should be collaborative and respectful. If your loved one is able to do these actions on their own or without support and wishes to do so, please respect that.

- **Regular device checkups (with permission).** This is dependent on the needs of your loved one. In cases where it would be best for a support person to help navigate devices, you can **ask permission from the device owner** to review installed apps, recent logins, and unfamiliar settings together.
- **Use strong, memorable passwords** and a simple password manager if appropriate (see Chapter 6).
- **Enable 2FA** on important accounts and explain how codes work (see Chapter 6).
- **Keep software updated** to reduce vulnerabilities.
- **Limit sharing of sensitive information** and practice saying “no” to requests for photos, codes, or money.
- Make a short routine: a consensual, weekly check of device settings and account activity that is lead by the survivor.

Disability-inclusive considerations

Prevention must be accessible. For people with disabilities, tailor all approaches to their needs.

- Use **assistive tech-compatible** security tools (e.g., 2FA via voice call if SMS is inaccessible).
- Provide **audio or large-print guides**, or demonstrate steps verbally while the person follows on their device.
- Ensure any password manager or security app works with screen readers or other assistive tools.
- Address **dependency risks**: if a caregiver manages devices, create a plan that preserves the person’s privacy and control where possible.

Design safety routines that the person can maintain independently or with trusted, trained support. We recommend that you co-design a safety plan alongside them, which we provide in Chapter 10: Staying Safe Online, and in our online resources folder.

Community and systemic actions

Friends and families are important, but prevention also needs community supports.

- Encourage participation in **local digital literacy workshops** and peer support groups.
- Advocate for **accessible banking practices** and fraud protections for people with disabilities.
- Support organizations that provide **specialized help** for TFGBV survivors, including legal and psychosocial services.
- Share knowledge in community spaces so more people can spot scams and support one another.

Collective action reduces isolation and strengthens safety nets. It's also important for you and other support people to share the task of improving technology-based safety and protection.

One person cannot hold the entire responsibility of online safety; **engaging in community and publicly available support** and resources is a great way to redistribute this burden.

Reflection

- **What immediate step can you take today** to improve a loved one's account security?
- **What simple digital safety routine** can you build with your loved one and who will lead it?

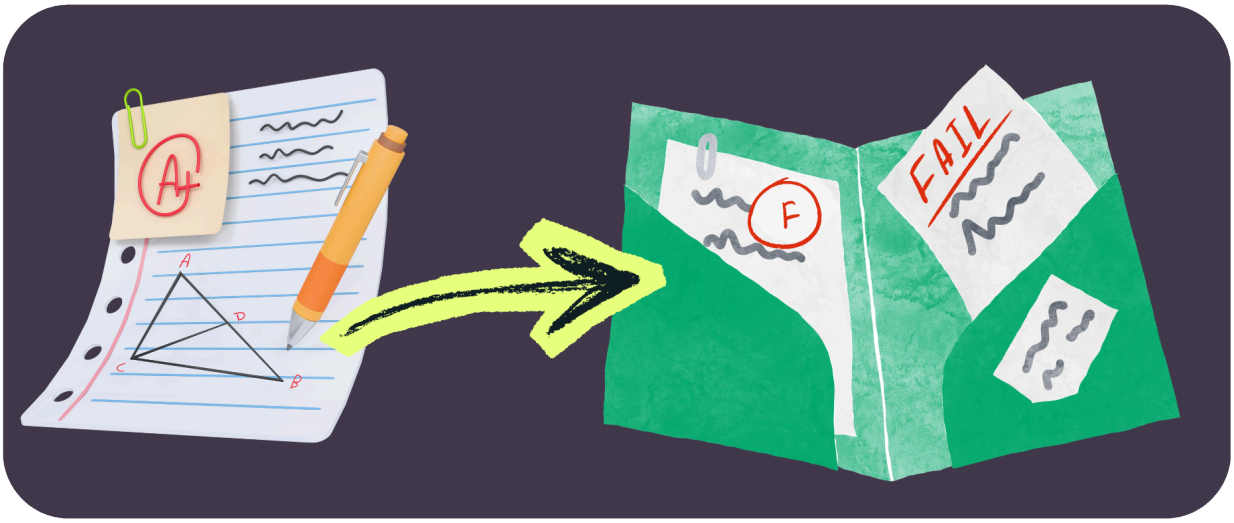
Content Warning: The following story depicts cyberbullying and disability-related online harassment. Reader discretion is advised.

Case Study #3A: What's going on with Leila?

Background

Leila is a 16-year-old learner in Johannesburg who has dyslexia and receives exam accommodations at school. She is usually social, creative, and active online, but over several weeks her behaviour changes noticeably.

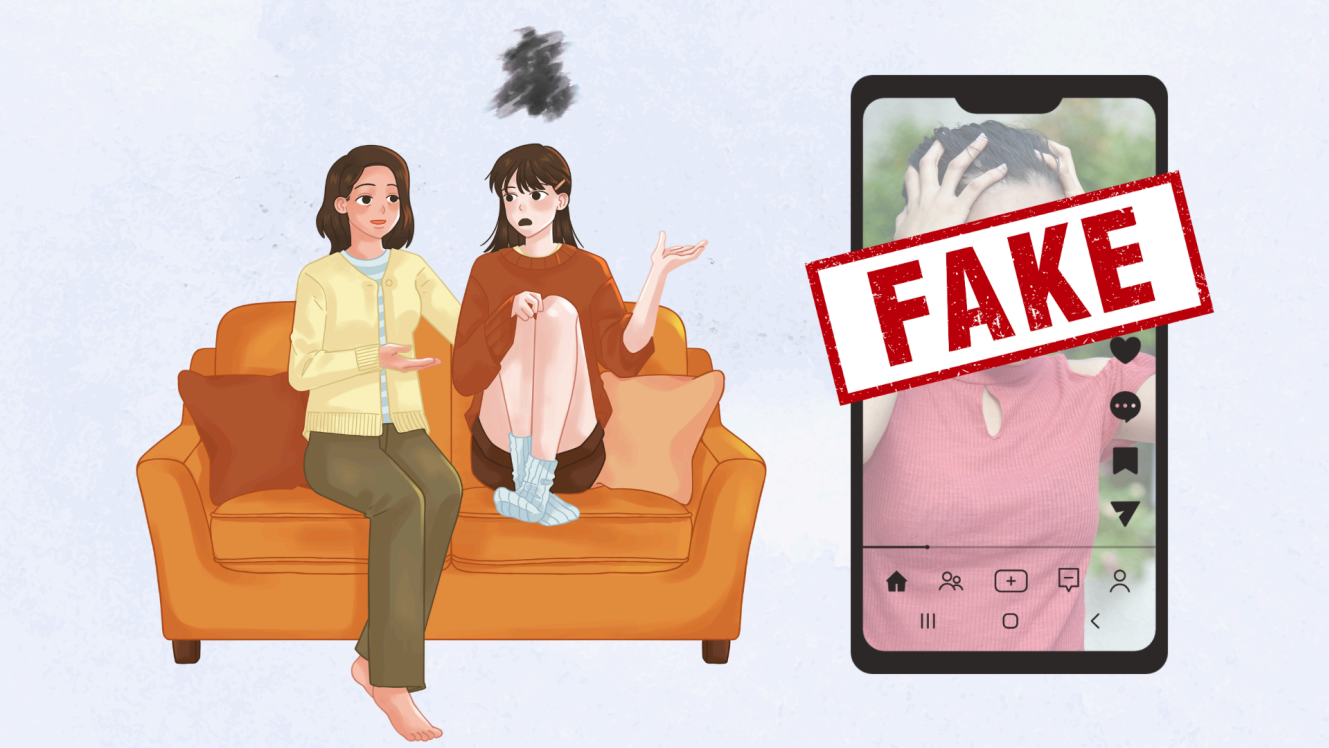
Aisha notices it first in small ways. Leila stops humming while getting ready for school. She keeps her phone face-down on the table. She no longer rushes to show Aisha her latest drawing or TikTok draft. At first, Aisha wonders if it's just normal teenage moodiness. But then Leila's teachers mention her grades slipping, and Aisha's worry grows.



Leila seems to be struggling with school more than she has before. Aisha notices this small change.

One evening, Aisha sees Leila looking upset while reading her phone. Leila says she is “just tired.” However, the next morning she hesitates before unlocking her phone and looks distressed by the notifications she receives

When Aisha checks in again, Leila explains what is happening. A group of classmates have been sending her cruel messages, accusing her of faking her dyslexia to get extra exam time. They mock her spelling and call her names. The messages arrive throughout the day and night.



Leila then shows Aisha a video circulating at school. It looks like Leila, but it is an AI-generated deepfake of someone who resembles her making vulgar gestures. Leila explains that it’s an AI-generated deepfake. The video was posted on TikTok with a caption implying she threatened another student. It has been shared widely.

Leila says she has considered giving up her exam accommodations to stop the bullying. Aisha reassures her that dyslexia is nothing to be ashamed of and that none of this is her fault.

Dyslexia is a brain difference that makes reading, spelling, and writing harder. This is not because of intelligence, but because the brain processes letters and sounds differently.

Aisha knows they will need to take action, but she focuses first on making sure Leila feels supported and not alone.

Reflection Questions

- What signs did Aisha notice that something was wrong?
- How can a caregiver tell when online behaviour crosses the line into harassment?
- What impact might the deepfake video have on Leila's sense of safety and identity?
- What steps could Aisha take next to support Leila and address the situation?

Content Warning: The following story depicts cyberbullying and disability-related online harassment. Reader discretion is advised.

Case Study #3B: Parental Support for Leila

Aisha knew something was wrong the moment Leila finally showed her the WhatsApp messages and the TikTok deepfake. Seeing the cruel comments and the way the video twisted her daughter's image made her heart sink, but she stayed calm for Leila's sake. She sat beside her, helped her take screenshots, saved the videos, and documented everything so they would have a clear record of what was happening.

The next day, Aisha arranged a meeting with the school principal, the guidance counsellor, and key staff. Together, they reviewed the evidence and created a safety plan for Leila to regain a sense of safety.

To support Leila's learning needs, they discussed the possibility of the school developing some digital safety and protection training videos to overcome any barriers around reading. The school committed to addressing online violence, ableism and disability misinformation, as well as promoting online and digital safety and privacy measures in accessible formats.

A high school assembly on online integrity and safety.

One of the first measures was a school-wide assembly, on online integrity, the dangers of technology-facilitated violence, and how to protect yourself against it.

At home, Aisha focused on making Leila feel safe and secure again, by reaffirming her and providing a listening ear. Over time, Leila began to feel more grounded. Knowing her learning difference is valid, that she deserves her accommodations, and that she has a right to feel safe while she learns, all help her to exceed in her studies.

Content Warning: The following story depicts financial abuse and disability-related victimisation. Reader discretion is advised.

Case Study #4: Bank Scammers and Financial Abuse

Rosa is a 32-year-old woman living in Durban. She is blind and uses screen-reader software to navigate social media and manage her personal finances. She recently joined a popular South African Facebook group focused on budgeting and debt management. Daniel is her long-time friend. They speak weekly and have a close, trusting relationship.

Early Warning Signs

During a routine phone call, Daniel notices Rosa sounds unusually anxious. When he gently asks how she's doing, she mentions that someone from a Facebook finance group has been "helping" her create a debt repayment plan.

Daniel becomes concerned when Rosa describes the interaction:

- The man contacted her privately after she commented on a post about debt relief.
- He claimed he could "fast-track" her debt clearance through "special industry contacts."
- He asked for her ID number and banking details to "check her credit score."
- He insisted she not involve her bank because "they make things complicated."
- He pressured her to respond quickly and keep their conversations secret.

Daniel recognises these as common tactics used in online scams.

Daniel's Approach

Instead of criticising or alarming her, Daniel invites Rosa to explain everything at her own pace. Rosa admits she feels embarrassed and confused. She worries she has been naïve. However, Daniel reassures Rosa that scammers deliberately target people who are seeking help, and that her trust was exploited. This is not a matter of her intelligence.

Together, they review the messages. Daniel reads them aloud, and Rosa listens closely. She begins to notice:

- The shift from friendly tone to urgency
- The manipulation through guilt ("I'm trying to help you, why aren't you cooperating?")
- The requests for personal information
- The promises of unrealistic financial outcomes

This helps Rosa recognise the manipulation herself, which becomes a turning point in her confidence.

Taking Action

Once Rosa feels ready, Daniel helps her take practical steps to secure her safety. To protect Rosa's financial and social media accounts, here are the **actions** which Daniel and Rosa did together:

- They report the scammer's profile and messages to Facebook.
- Rosa contacts her bank's fraud department by calling them on the phone, who help her secure her accounts (freezing her cards) and checking for suspicious activity.
- She changes all her banking account passwords and sets up two-factor authentication.

Privacy Adjustments

- Daniel helps her adjust Facebook settings to limit who can message her.
- They review her email and banking app security settings.

Rosa begins to feel more in control and less overwhelmed.

Rebuilding Confidence

Daniel encourages Rosa to join a digital safety workshop run by a Johannesburg-based disability rights organisation. The workshop covers:

- Recognising common South African scams
- Understanding manipulative online behaviour
- Protecting personal information
- Safe use of social media and messaging apps
- How to ask for help without shame

Rosa meets others with similar experiences, which reduces her sense of isolation and guilt.

Outcome

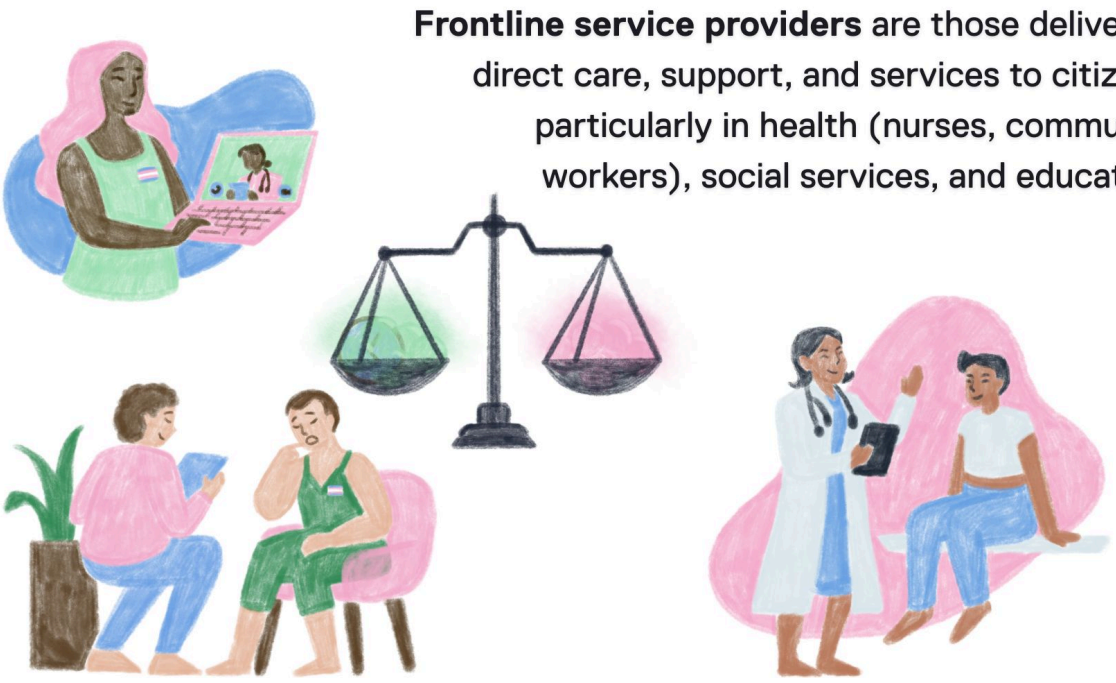
By the end of the process:

- Rosa feels safer and more confident online.
- She understands how to identify fraud and protect her information.
- She feels supported rather than ashamed.
- She has built new connections with others who share her experiences.
- She recognises the importance of a trusted support system.

Daniel's calm, non-judgmental approach played a key role in helping her regain her sense of agency.

FRONTLINE SERVICE PROVIDERS

EXIT SITE



Chapter 14: Identifying TFGBV in Client Care

Technology-facilitated gender-based violence (TFGBV) can be difficult to detect in service settings. Clients may not recognize digital abuse, may feel ashamed, or may fear losing support. Staff may overlook digital harm because it leaves no visible injuries. Identifying TFGBV requires noticing behavioural changes, shifts in communication, and inconsistencies in how clients describe their digital lives.

In this chapter we will review ways to identify TFGBV in care contexts. For more information on how to reocgnise subtle signs that someone may be experiencing TFGBV, you can read more in Chapter 11: Recognizing that TFGBV is Happening.

Learning Objectives

- Understand your role as a service provider in facing TFGBV cases.
- Second

Why Health and Frontline Care Staff Need This Training

Staff benefit from reflecting on their own assumptions about “digital abuse” in clinical or support environments. This helps them notice signs that might otherwise be dismissed.

Frontline workers (such as healthcare providers, disability-support staff, GBV workers, and law enforcement) are often the first people clients trust. Clients may disclose indirectly or show distress through behaviour rather than words. Because TFGBV is often hidden, staff must create safe, nonjudgmental spaces where clients feel comfortable sharing concerns.

Early intervention matters. Sensitive documentation, careful listening, and timely referral can prevent further harm and preserve evidence. Staff do not need to

be technology experts; they need awareness, gentle inquiry, and clear referral pathways.

Reflection

A useful starting point is to reflect on your own assumptions.

What comes to mind when you hear the term digital abuse in a clinical or supportive environment? This reflection might help prepare staff to notice signs that might otherwise be dismissed

How TFGBV Appears in Service Environments

TFGBV can occur across many service settings, including healthcare facilities, disability services, shelters, home-care agencies, and community programs. Technology is embedded in daily operations, such as appointment booking systems, caregiver apps, telehealth, communication platforms, digital records, and assistive devices. These tools can support care but can also be misused for surveillance or coercion. **Common indicators include:**

- Repeated loss of device access
- Unexplained gaps in communication
- Sudden changes in online activity
- Anxiety around device use
- Inconsistencies in caregiver app logs
- Unusual device behaviour
- A caregiver or partner managing all digital communication

Example: A support worker notices that a client suddenly avoids using her phone and becomes tense whenever messages arrive. Her caregiver insists on answering questions for her and manages all her digital communication.

Digital tools within the service can also be misused:

- Falsified entries in caregiver or support apps
- Photos taken without consent
- Monitoring through clinic Wi-Fi or waiting areas

Observing relational dynamics around technology is essential. Staff should ***consider the following questions:***

- Who holds or controls the device?
- Who answers questions?
- Who insists on being present during digital interactions?
- How might digital abuse be occurring within the systems and **tools we use every day?**

These questions may reveal power imbalances that place clients at risk.

Example: A staff member uses his personal phone to contact a client and secretly edits her caregiver-app logs to make her appear non-compliant. He restricts her access to shared devices and stores photos of her without consent.

Organizational Factors Can Increase Risk of TFGBV

Service environments can unintentionally create conditions that allow TFGBV to go unnoticed. Contributing factors include limited privacy, shared devices, rushed appointments, and unclear policies on device use or harassment.

Women with disabilities may face additional risks due to reduced privacy, lower digital literacy, and greater reliance on caregivers. Staff may also blur boundaries by using personal phones for client communication or storing client information on unsecured devices.

Power imbalances matter. Clients who depend on staff or caregivers for mobility,

communication, or daily living may feel unable to question digital decisions or raise concerns.

Recognizing TFGBV Across the Service Journey

TFGBV can appear at any stage of service interaction.

At **client intake**, it may resemble a client hesitating to share contact information, or requests for unusual communication arrangements.

> **Example:** During intake, a client named Rina asks the clinic to only contact her through her partner's email address and says she "isn't allowed" to receive texts directly. When staff try to confirm her phone number, her partner answers every question and insists all follow-up messages should go through him.

During **appointments or meetings with clients**, it may look like avoidance around discussing home life, relationships, or even technology use, or anxiety when devices ring or vibrate.

In can show up in **follow-up calls and communication** (often through phone calls or email) as messages going unanswered or being answer by someone else, or as sudden changes in communication patterns.

During **home care visits or community care settings**, you might see that devices are frequently missing broken, or "being fixed", that family or caregivers are monitoring all digital interactions, or that there are high levels of restriction of device use.

Recognizing TFGBV requires looking beyond isolated incidents and considering how systems, routines, or technologies might enable harm.

The Importance of Trauma-Informed, Nonjudgmental Inquiry

Clients may not have the language to describe digital abuse. They may feel ashamed, confused, or afraid of retaliation. Staff should use open-ended questions, avoid assumptions, and ask privately about device safety and account control.
Trust is essential. Clients are more likely to share concerns when they feel respected and believed. Confidentiality should be emphasized, and next steps explained clearly

---

Building a Culture of Awareness

Recognizing TFGBV is an organizational responsibility. Services need clear digital-conduct policies, regular staff training, and safe reporting systems. When staff share a common understanding of TFGBV, they are better equipped to identify risks and respond appropriately.

Reflect

What **changes** in your service environment would **make it easier to recognize and respond to digital abuse**?

Chapter 15: Responding to TFGBV as Frontline Service Providers

In this chapter, we want to **equip frontline service providers** with a **trauma- and disability-informed approach** to TFGBV, using a survivor centered approach. It centers an applied case, practical frameworks, and ready-to-use tools for assessment, documentation, immediate safety, and referral.

Learning Objectives

- Learn foundational principles of GBV responses and survivor-centered care.
- Apply the **Ask–Validate–Document–Refer** framework in digital abuse disclosures, centering survivors throughout.
- Identify local and organizational referral pathways for survivors of digital abuse.
- Integrate emotional support while preserving survivor autonomy and safety.

Foundational Principles for Safe Responses

In your approaches to client disclosures of TFGBV there are several general considerations that you need to make regarding how to proceed in ways which are empowering to the survivor.

In general, following **Gender-Based Violence (GBV) guiding principles** (keeping standards of safety, confidentiality, respect, and non-discrimination) and a **survivor-centered approach** (ensuring that survivors' experiences and wishes are central and essential to guiding decisions and actions) are vital to best practices.

Gender-Based Violence (GBV) guiding principles are as follows:

- **Safety-based approach.** Attending to both immediate, short-term, and long-term physical, emotional, mental, and digital risks.
- **Confidentiality.** Give the survivor control over what is shared and when. Women with disabilities are frequently stripped of autonomy due to societal and structural barriers, and it is essential that service providers do not continue to do this. However, there are some limits to confidentiality, and service providers should inform survivors of this.
- **Respect.** Respect the choices and dignity of all people who you serve, by including them, respecting their identity and experiences, and approaching with openness.
- **Non-discrimination.** All actions should be informed with approaches that acknowledge the many parts of a person and survivor. Gender, race, disability, sexual orientation, religious affiliation and any other identifiers should be respected and approached without bias.

To **learn more about GBV Principles**, you can go to the resource from the UNFPA, which is **linked here.**

Core parts of a survivor-centered approach to GBV also include:

- **Trustworthiness.** Be transparent about limits of confidentiality and next steps. Disability and gender-based stigma experienced in many societal spheres can create atmospheres of distrust and fear.
- **Collaboration**. Aim to co-create safety plans and referrals with your clients. Nothing should occur without survivors' consultation and involvement, except in extreme circumstances.
- **Empowerment**. Support digital autonomy and reduce shame around experiences. You can do this by providing resources around digital literacy and digital safety that are accessible, and facilitating teaching digital safety in ways that support self-sufficiency.

Reflect

1. **What barriers in your context** (healthcare, GBV support, advocacy, disability rights, et cetera) can you foresee in applying these principles?
2. How might you plan to overcome or circumvent these barriers?

Using an Ask–Validate–Document–Refer framework

This framework provides a simple, structured way to respond to TFGBV disclosures.

Ask (permission first): *Ask about TFGBV.*

Ask permission to discuss, and then about the TFGBV. Ask about frequency, content, sender identity, platforms used, whether images were shared, and whether the perpetrator has offline access to locations or contacts.

- **Try phrases like:** "May I ask some questions about what happened and how it's affecting you? You can stop at any time."

Validate: *Validate the experience.*

- Avoid blame or minimising language; do not pressure immediate reporting unless there is an emergency situation.
- **Try phrases like:** "That sounds frightening"; or, "You did the right thing telling me."

Document (with consent): *Record evidence.*

- Record **verbatim** statements, dates, times, platforms, and witnesses. Note whether the client consents to evidence collection and sharing. Use the documentation template below.

Refer: *Refer to services.*

- Offer options that you are able to directly refer them to, such as legal advice, digital forensics, police follow-up, psychosocial counselling, medical appointments, shelter services, and peer support. Let the survivor choose which referrals to accept and when.

The AVDR framework ensures that responses remain structured, supportive, and aligned with the survivor's needs.

Developing an AVDR framework requires an organisation or institution has a base of **knowledge around locally available facilities and services**. If this is not yet in place, we deeply encourage a review of your internal policies and services. For reference, we have compiled a list of resources and services in South Africa, which may be useful to you, which is linked on our Support and Resources Page.

Communication with Clients Around TFGBV

Clear, respectful language supports safety and trust during difficult conversations. Example of possible scripts to use through the service delivery and reporting or response process include:

- "I'd like to write down what you've shared so we can support you appropriately. Is that okay?"
- "If there is an immediate risk to your safety, I may need to involve others. I will tell you before I do that."
- "I can connect you with legal support, a forensic specialist, or a counsellor. What would you prefer at this stage?"

Incident Report Flow Charts

An incident-report flow chart helps frontline workers know exactly what to do when TFGBV is suspected or disclosed, and to progress through the AVDR stages. Because digital abuse can escalate quickly and survivors may share information gradually or under pressure, staff need a clear sequence of steps that guides their actions from first concern to final follow-up.

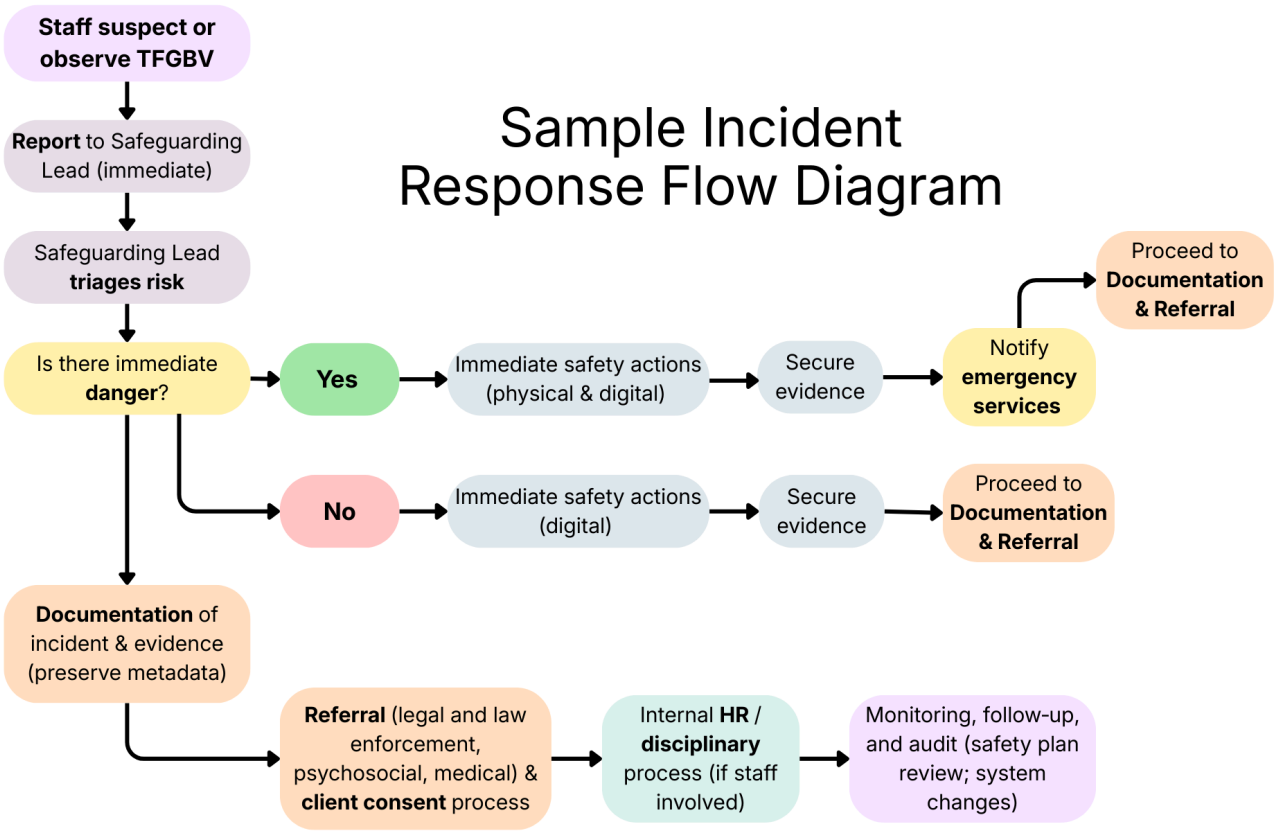
The flow chart provides this structure by outlining who to notify, what safety checks to complete, how to document the incident, and when emergency procedures must be activated.

These types of incidence reporting flow structures are common for many organizations, but they do not always follow survivor-led or GBV principles

Each organisation should adapt the details to its own staffing and legal requirements to support a safe, coordinated, and trauma-informed response to TFGBV.

We have provided a sample incident report flow chart, which should be updated to include roles, responsibilities, and organisation-specific practices to accompany each step.

The typical **sample incident report flow chart** is as follows:



This is a typical flow diagram of incident responses to GBV. In this case, we can see that a lot occurs outside of the control of the survivor. Decisions are predetermined based on a care provider's perception of a situation, without discussing them with the survivor.

What should we do instead?

To help guide the development of your own responses, we have added survivor-centered processes to the sample flowchart. You can view these changes in the diagram below:

An interactive H5P element has been excluded from this version of the text. You can view it online here:
https://pressbooks.library.torontomu.ca/tfgbvsafetytraining/?p=325#h5p-30

Practical risk assessment and intake checklists

After initial disclosure, providers must assess risk across both clinical and digital domains. This assessment guides immediate safety actions and determines which referrals are most urgent.

- **Clinical risks** may include threats of physical harm, suicidal ideation, lack of safe housing, or limited social support.
- **Digital risks** may include device or account access by the perpetrator, spyware, image-based abuse, doxxing, location tracking, online harassment, or other forms of TFGBV.

According to your service or institutional scope, you may also want to develop a combined intake checklist that flags:

- Immediate danger (requires emergency services)
- High digital risk (requires digital-forensics referral)
- Psychosocial needs (requires counselling or support services)

Immediate danger that require calls for emergency or immediate reporting can include the following…

- **Threats of physical or sexual violence** delivered through digital means, especially when they include location details, stalking patterns, or timelines.
- **Real-time stalking or tracking**, such as live GPS monitoring, forced location sharing, or evidence that someone is on their way to the victim's physical location.
- **Compromised safety-critical accounts**, like access to home security systems, medical devices, financial accounts, or communication channels the person relies on for safety.
- **Non-consensual intimate image release** that is happening now or is being used to coerce immediate compliance.
- **Escalating harassment** that shows clear intent to harm or that coincides with in-person threats or breaches of physical boundaries.
- **Digital abuse** that prevents someone from calling for help, accessing medication, contacting support, or finding a safe shelter.

As a service provider, you must be transparent about your role's mandatory reporting obligations and any limits to confidentiality at the beginning of conversations.

Immediate Digital Safety Strategies

Once risks are identified, providers may support immediate digital safety steps. These actions must be taken carefully, especially when device monitoring is suspected. **Immediate safety strategies** (with informed consent) include:

- Change passwords from a trusted device not accessible to the perpetrator.
- Enable two-factor authentication on critical accounts.
- Turn off location sharing and make social accounts private.
- Preserve evidence (screenshots, message headers, timestamps).
- Use a temporary "safe device" if monitoring is suspected.
- Avoid deleting messages until a forensic specialist advises.

Safety Note:

Changing any typical digital behaviour (changing passwords, logging out of or deleting accounts, turning off location, uninstalling apps) may alert an abuser. Ensure that the survivor has a safe shelter before making changes, and opt to use different devices and accounts other than the accounts which are accessible to the abuser.

Reflect

Consider the risks of altering device settings when a client's device may be monitored, and **identify strategies** to reduce those risks.

Documentation Standards

Accurate, secure documentation is essential for safety planning, continuity of care, organisational accountability, and potential legal supports. **Documentation should include:**

- Date, time, and setting of the disclosure
- all individuals present
- Client's statements (verbatim)
- Observed behaviour and communication needs
- Evidence collected and consent status
- Referrals made and agreed next steps

Records must be stored securely with restricted access and clear data retention and deletion policies.

Accessibility and power dynamics

When TFGBV intersects with disability, its experience and safe response may be impacted by factors such as caregiving relationships, and communication barriers. Providers must ensure that their approach does not reinforce existing power imbalances. **Service providers should:**

- Use the client's preferred communication mode (sign language, text, pictorial aids, assistive tech).
- Recognise that caregivers or staff may monitor devices; plan private, safe ways to communicate.
- Adapt phrasing and pacing for cognitive or sensory needs.

Legal, ethical, and data-protection considerations

Legal and ethical obligations shape how information is collected, stored, and shared. Providers should:

- Explain confidentiality limits and mandatory reporting obligations clearly.
- Obtain informed consent before sharing evidence; use plain-language consent forms.
- Store sensitive records securely and follow relevant data-protection laws and organisational policies.

Reflect

How might your documentation practices need to change to better protect TFGBV-related data?

Ongoing safety planning

Safety planning is not a one-time event; it is an evolving process that adapts to the survivor's changing circumstances.

- **Develop a physical safety plan.** Identify important safe contacts, emergency numbers, safe locations.
- **Develop a digital safety plan.** Consider safe devices, password rotation, trusted backups, and a plan for social media privacy.
- **Follow-up.** Schedule check-ins, update risk assessment, and revise the plan as needed.

A well-structured safety plan supports both immediate protection and long-term sustainability.

Building partnerships and referral networks

No single service can address all aspects of TFGBV. Effective response depends on strong partnerships across sectors. Organisations and service staff should:

- Map local forensic, legal, psychosocial, and shelter services. You can see some examples of organisations in this textbook in on the following pages:
  - South African Support and Resources Page
  - Global Support and Resources Page
- Establish referral agreements and rapid-response pathways with local resources to create an accessible network of support for survivors.
- Train staff in digital-evidence preservation and trauma-informed, survivor-directed care.

Partnerships can strengthen the organisation's capacity to respond comprehensively and consistently.

Reflect

Which local partners could strengthen your organisation's TFGBV response?

Responding to TFGBV requires a structured, trauma-informed, and disability-inclusive approach. By applying the AVDR framework, conducting thorough risk assessments, documenting safely, and maintaining strong referral networks, frontline providers can offer survivors meaningful protection and support.

When these practices are consistently applied, organisations strengthen their overall readiness and ensure that survivors receive responses that are safe, respectful, and empowering.

Resources

- UNFPA. (2019). *The Inter-Agency Minimum Standards for Gender-Based Violence in Emergencies Programming*. United Nations Population Fund. https://gbvaor.net/sites/default/files/2019-11/19-200%20Minimun%20Standards%20Report%20ENGLISH-Nov%201.FINAL_.pdf

- Women's Shelters Canada. (2026). *Toolkits*. Women and Gender Equality (WAGE) Canada. Tech Safety Canada. https://techsafety.ca/resources/toolkits

Chapter 16: Protecting Against TFGBV and Changing Policies

Technology-facilitated gender-based violence (TFGBV) affects how clients access care, communicate with services, and feel safe in support environments. Protecting clients requires trained staff, clear digital-conduct policies, and systems that respond quickly when harm is suspected.

This chapter outlines **practical steps for building safer digital practices** across healthcare, social services, disability support, and community programs.

Learning Objectives

- Understand how to build digital safety and TFGBV responses into healthcare and frontline services.
- Strengthen organisational accountability and respectful digital conduct.
- Design prevention-focused policies that protect clients and workers.

Training and Resources for Frontline Workers and Caregivers

Frontline workers and caregivers are often the first to notice digital harm. They need training, tools, and clear guidance to respond safely.

Workers should learn:

- The basics of technology safety and how TFGBV appears in client care (see Chapter 5, and Chapter 14).
- Trauma-informed and disability-inclusive communication (see Chapter 12 to

learn about how to talk about TFGBV)
- How to help clients preserve digital evidence without increasing risk
- How to support reporting, referrals, and safety planning (see Chapter 15: Responding to TFGBV With Clients)
- How to use plain language and accessible explanations for clients with diverse communication needs.

Training should be refreshed regularly so staff stay confident and prepared

Staying Informed About New Threats

Technology evolves quickly. New features, scams, forms of online violence, and platform changes can create new risks for clients. Staying informed helps organizations anticipate harm rather than reacting after it occurs.

Care leads and organizational leaders should **prioritize:**

- Regular reviews of privacy and security settings on eHealth platforms and communication tools.
- Staying aware of new scams, phishing attempts, and app policy changes.
- Keeping all service devices, apps, and internal care-flow structures updated.

These practices reduce vulnerabilities, strengthen organizational readiness, and support early recognition of TFGBV.

Staff Conduct and Digital Boundaries

Clear digital-conduct policies protect both clients and workers. They set expectations, reduce risk, and create accountability. **Key policy practices include:**

- Obtain consent before taking photos before or using a client's device.
- Never share client images or personal data outside approved processes.
- Establish rules for using facility devices during work hours for client response

and care (phones, tablets, wearables).
- Review caregiver, clinician, and other staff digital logs and app entries for inconsistencies.
- Treat TFGBV as a form of violence requiring appropriate referrals.
- Make TFGBV and digital-safety training *mandatory* and regularly *renewed*.

Strong boundaries help prevent misuse and build trust.

Digital Incident Reporting and Response

A clear process helps staff respond quickly and safely when TFGBV is suspected. We previously provided an example incident response flowchart and chain of response (see Chapter 15: Responding to TFGBV With Clients), which can be adapted and should be regularly reviewed and updated to include essential institution-specific details.

Prevention Through Policy and Training

Prevention is stronger when safety and prevention strategies are built into everyday practice. **Prevention strategies** within frontline service settings include:

- Regular TFGBV, digital-safety, and online integrity and ethics training.
- **Privacy Impact Assessments** before adopting new caregiver apps or digital tools.
- Client education through workshops, fact sheets, and diverse formats of accessible materials.
- Data minimization, where only data that is necessary is collected.
- Develop clear data-*retention* and *deletion* policies.

These measures can reduce levels of misuse and strengthen organizational safety culture.

However, ultimately, online spaces can only be made as safe as the platforms

allow them to be. As such, advocating with your organisation for safety by design, and using your influence and voice to promote causes which hold digital platforms accountable for allowing TFGBV to persist, is a big way that you can support safety for all.

Reflect

1. What policy gaps exist in your organization?
2. What changes could be implemented immediately?

Monitoring, Evaluation, and Sustainability

Ongoing evaluation helps organisations understand what is working and where improvements are needed. TFGBV prevention requires continuous monitoring and adaptation. **What to measure:**

- Proportion (%) of all GBV cases which were committed, facilitated or amplified through the use of technology.
- Proportion (%) of survivors who were referred for external supports.
- Proportion (%) of survivors who were satisfied with their referrals and subsequent supports (if consenting to provide the information).
- Implementation of training and staff confidence level in identifying, responding to, and educating about TFGBV, before and after training.
- Collect anonymous feedback from service users, survivors, staff, partner organisations, and the community.

Sustainability practices strengthen safety practices in the long-term. They help organisations maintain momentum, adapt to new risks, and ensure that TFGBV prevention and response strategies do not go out-of-date, or fade over time. These practices include:

- **Offering annual or bi-annual TFGBV refresher training for staff, partner**

organisations, and communities.
Regular refreshers help communities stay confident as technology, platforms, and forms of digital harm evolve. They also reinforce shared language, expectations, and trauma-informed approaches across the organisation.

- **Quarterly case reviews.**
  Reviewing cases or service uses every few months may help teams to identify patterns, gaps in services and safety, and new or emerging risks. These reviews can highlight where policies/training are working, where staff need more support, and where new procedures may be required.
- **Regular updates to referral lists and policies.**
  Keeping referral lists current, and actively engaging with referral partners on a regular basis helps ensure that clients receive timely, appropriate support. Policies should also be updated to reflect new technologies, legal requirements, and organisational learning.
- **Adjustments based on new technology trends.**
  Organisations should build in a routine for monitoring these changes and adjusting safety plans, training materials, and internal procedures accordingly. The **Safety Net Project** website, which is linked here, provides regular global technology abuse and safety updates.

Together, these sustainability practices help organisations remain responsive, accountable, and prepared. They ensure that TFGBV prevention is not a static policy but an ongoing commitment woven into everyday care.

Reflect

1. What is one thing I can do differently in my role after this training?
2. What barriers might prevent us from implementing safety planning or documentation?
3. Who else in the organization needs to be involved in policy change?
4. How can we include women with disabilities in designing safe digital-space policies?

Resources

UN Women and SVRI's TFGBV Community of Practice TFGBV Policy Dialogues Series.

- Includes extensive talks on TFGBV from multidisciplinary and multisector lenses, tackling TFGBV collaboratively.
    - De Fillippo, A., Magwaza, K., & De Silva, A. (2025, July 1). *Staying aligned with global standards & commitments in the TFGBV*. Sexual Violence Research Initiative [Linked here].
    - De Silva, A., Airoldi, G., & Rafin, R. (2025, August 4). *Actioning global standards on technology-facilitated gender-based violence: From commitments to implementation*. Sexual Violence Research Initiative [Linked here].

SVRI's Global Library on TFGBV is linked here.

- Includes an expansive list of peer-reviewed and non-reviewed articles and added resources on TFGBV research and policy.

- A ***shared research agenda*** from SVRI, UN Women, The Global Partnership, & APC, which islinked here.
- A tip sheet from UNFPA about responding to and reporting TFGBV made for journalists and reporters, linked here.
- A ***fact sheet*** **about responding** to TFGBV from LEAF, which is linked here.
- Accessible full-text of the Cybercrimes Act in South Africa, available at cybercrimesact.co.za.

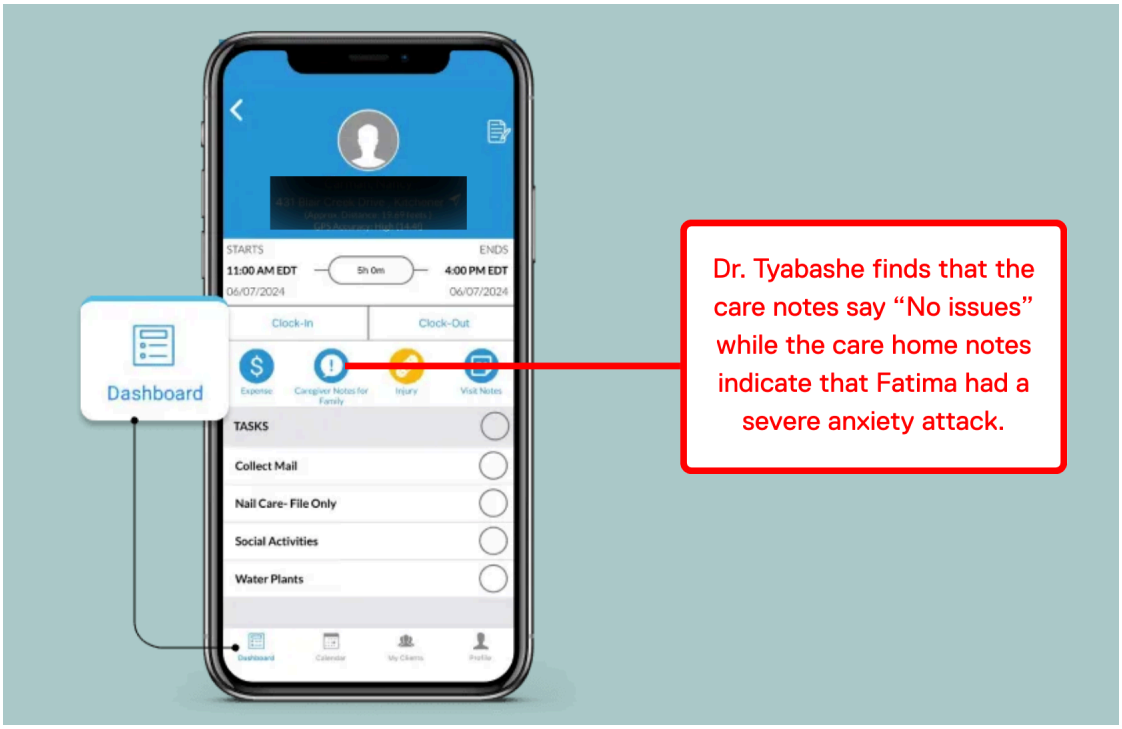
The Safety Net Project is provided by the National Network to End Domestic Violence. The website is linked here.

EXIT SITE

Content Warning: The following story depicts caregiver-directed violence, including sexual and image-based abuse. Reader discretion is advised.

When Dr. Tyabashe reviews Amahle's home care records during a routine check, she notices that something is not right. Amahle is a woman with high-support-needs autism who is nonverbal, who resides in a care home. **Entries in the caregiver app do not match the clinical notes she is reviewing.**

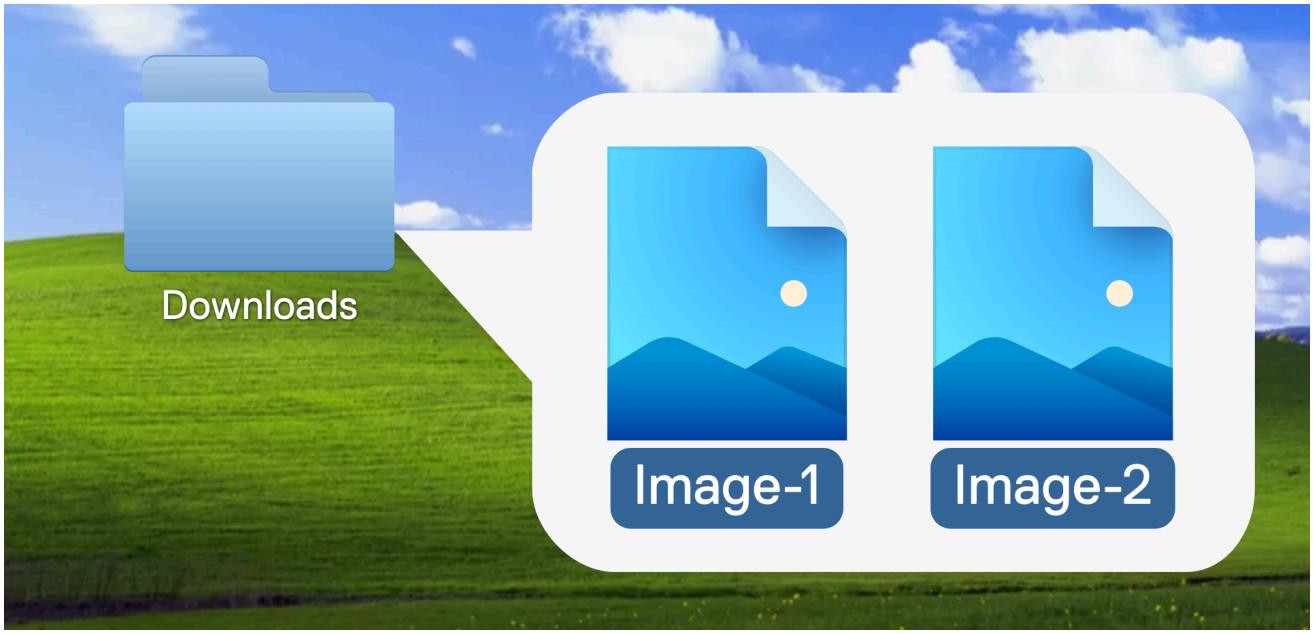
The physicians' notes indicated that last week, Amahle had been feeling extremely distressed. However, when reviewing caregiver app notes provided by the agency, her main caregiver logged that Amahle was in good spirits, no issues. Dr. Tyabashe decides to investigate this discrepancy.



A routine check of the agency's shared folder reveals uploads from a caregiver's device during the same week. The IT lead flags unfamiliar filenames and thumbnail previews that do not match authorised documentation. Family members confirm

Amahle had a difficult week and report the caregiver insisting on being alone during personal care.

A caregiver's private device had been used to download a file from the agency's shared folder in the same week that Amahle's clinical notes recorded severe distress. When Dr. Tyabashe asked the agency IT lead for a routine folder review, the lead flagged several **unfamiliar filenames** and thumbnail previews that did not match any authorised documentation.



Several unfamiliar filenames and that do not match any authorised documentation within the app.

A cautious preview (without opening intimate content) shows images saved under innocuous names in a personal downloads folder. Message threads in the app include an intimate, sexualised tone inconsistent with professional care, and some app entries appear edited after clinical visits.

Alarmed, Dr Tyabashe preserves exports and screenshots, documents the timeline, removes the caregiver from Amahle's roster, arranges alternative care, and reports the matter to the agency and authorities. She meets Amahle and her family, and apologises for the breach of trust, and outlines immediate supports and longer-term safeguards.

Once the immediate crisis is addressed, Dr. Tyabashe turns her attention to the bigger picture. She raises the issue with agency leadership and **advocates for systemic improvements.** She recommends **mandatory digital safety training for all caregivers**, stronger **documentation** policies, regular **supervision**, and routine **audits** of the caregiver app to detect misuse early. She emphasises that technology can support care, but only when staff are trained and systems are monitored.

A new vetted caregiver replaces the previous, after a thorough criminal records check and onboarding with new anti-violence, anti-TFGBV, and safe documentation training.

Content Warning: The following story depicts threats, sexual harassment and stalking violence. Reader discretion is advised.

Case Study #6: Nasha and Evie Make a Safety Plan

Nasha is finishing up her day at the community centre when she notices a new message request. It is from Evie, a young wheelchair user she met during an outreach workshop a few months earlier. Evie rarely reaches out, so the sudden message catches Nasha's attention.

Evie writes that a man has been texting her nonstop. At first the messages seemed like unwanted flirting, but they quickly turned into threats of violence or assault.

He even writes that because she uses a wheelchair, she would never be able to "outrun" him. Evie blocked him, but he keeps creating new numbers. She went to the police through the My SAPS app, but there has been no movement on their end.

Nasha feels a knot in her stomach. She asks Evie if she feels comfortable talking more and waits for her reply. When Evie agrees, they set up a call. Evie's voice shakes as she explains how the messages have escalated. She has stopped going out alone, and can barely sleep. She says she feels silly for being scared, but the fear is real. Nasha listens closely. .

She tells Evie that her fear makes sense and that digital threats are serious, even if they have not turned physical. She asks if she can help document the messages, and Evie gives her permission. Together they go through the screenshots, save everything as physical and digital copies, noting important dates and times.

Evie then chooses to go to their local police station; Nasha accompanies Evie as a support figure. Once they are able to speak to a police officer, they are able to at least document the incident with the evidence they collected.

Once they finish, Nasha gently asks if Evie would like support exploring her options. Evie says yes. Nasha explains that there are legal services that can help her apply for a protection order and escalate the case beyond the initial police

response. She also offers to connect her with a counsellor who understands trauma and disability, and a peer support group where other disabled women share their experiences with online harassment.

They talk about safety next. Evie admits she has not changed her passwords in years and that her social media accounts are still public. Nasha helps her think through small steps she can take, like adjusting privacy settings, turning off location sharing, and using a trusted device to update her passwords. They also identify people Evie can contact quickly if she feels unsafe. Nasha reminds her that she has choices and that she deserves to feel safe both online and offline.

Evie thanks her, because for the first time in weeks, she feels like she can breathe again

Content Warning: The following story depicts domestic violence, and coercive control. Reader discretion is advised.

Case Study #7: Naomi Experiences Digital Monitoring

Noticing Naomi does not have her mobile phone which she uses to keep in touch with family and friends, Carmen checks in with her. Naomi explains that her boyfriend took her phone for “safekeeping,” which raises red flags for Carmen about Naomi’s safety.

Carmen responds calmly and reassures Naomi that she is not in trouble but that her access to her phone and communication is important. She documents what Naomi’s perspective is and brings the concerns to the care team at the supportive living community.

All together, they have a conversation with Naomi about why keeping her phone matters for her independence, privacy and wellbeing. They also have another conversation about boundaries and healthy relationships along with digital rights.

Naomi gave her consent to get her phone back and to set up a safe plan so she can use it without pressure. Carmen still checks in with Naomi making sure she is supported and empowered to make her own decisions about her relationship and mobile phone.