Secure Voices

A Community Manual for Digital Safety, Privacy and Care

HER Internet

Citation

HER Internet (2025). Secure Voices: A Community Manual for Digital Safety, Privacy and Care

Inside this manual...

Who is HER Internet?

HER Internet is a feminist organization based in Uganda, working at the intersection of technology, gender, and feminism. We champion the digital rights and safety of structurally silenced communities by building spaces of care, learning, and resilience online.

Our Vision

An equal and just Internet for all womxn restoring their agency as their own agents of social change.

Our Mission

Equipping womxn with digital literacy and cyber security information and skills for increased and safer online engagement.

Our Core Values

- Inclusivity and Fairness to celebrate our diversity as womxn;
- Innovation and Creativity to adapt to, and leverage the opportunities presented by the ever-changing environment in which we operate;
- Collaboration and Teamwork to leverage the power of partnerships to achieve our goals;
- Transparency and Accountability with those that we work for and with, and to our values and principles so we can build and maintain trust.

Who is HER Internet?

Strategic Priorities

- Through **community building and engagement**, HER Internet seeks to create engaged communities that are knowledgeable about the internet, digital technologies, their rights and advocate for themselves and others. This remains crucial to the safer and increased online engagement for structurally silenced communities.
- Through **knowledge sharing**, HER Internet seeks to build awareness and knowledge amongst womxn on the safe and effective use of digital technologies. We recognise that the first step to the full utilisation of any technology is the awareness and knowledge of how it works, and how to use it to achieve one's intended goal.
- Through **advocacy and policy influence**, HER Internet seeks to advocate and lobby for the protection of digital rights for womxn while supporting their agency as they navigate digital technologies. A safe environment must be created for all womxn to freely and maximally utilise digital technologies.

Since our founding in 2018, HER Internet has become a regional thought leader in feminist tech practice, grounding our work in the lived realities of those most affected by digital exclusion and online harm. Through community-led research, digital safety trainings, advocacy and knowledge production, we have shaped new narratives around feminist digital resilience, and influenced both local and global conversations on inclusive, rights-based internet governance.

Our interventions are driven by a feminist belief that technology must serve liberation, not oppression. From developing safety manuals, co-creatings spaces for dialogue, to establishing Uganda's first community-led digital resilience fellowship and rapid response mechanisms for activists, HER Internet continues to model how feminist principles can transform digital spaces into places of care, safety, and power.

About this manual

As Uganda approaches the 2026 general elections, the online environment is becoming increasingly volatile, particularly for structurally silenced communities such as queer and sex worker communities. Individuals are experiencing a surge in online harassment, hate speech, digital surveillance, as well as coordinated disinformation campaigns and public outings. For many, the internet remains both a lifeline and a battleground. On the one hand, it is a space for connection, expression, and organizing, but also one where violence, silencing and fear take root.

HER Internet recognizes that digital spaces are political spaces. This Securing Voices manual is therefore designed to respond to an urgent reality: the need for communities to protect themselves, support one another and sustain digital engagement safely in a climate of repression and uncertainty.

Purpose of the Manual

This manual serves as a practical companion for communities navigating Uganda's digital terrain during the election season and beyond. It brings together context-specific guidance, easy-to-use safety tools, and community-centered strategies for secure communication, safe browsing, account protection, and crisis response. Written in accessible language and illustrated for engagement, it aims to transform complex digital security concepts into everyday practices that anyone can use.

Securing Voices developed through HER Internet's feminist digital resilience initiative, responds directly to this gap. It forms part of a broader effort that includes in-person digital security trainings, interactive webinars, and a 24/7 encrypted crisis hotline. Together, these interventions aim to build a culture of digital care and collective safety, where communities not only survive online but thrive with confidence and autonomy.

Common digital threats

Phishing

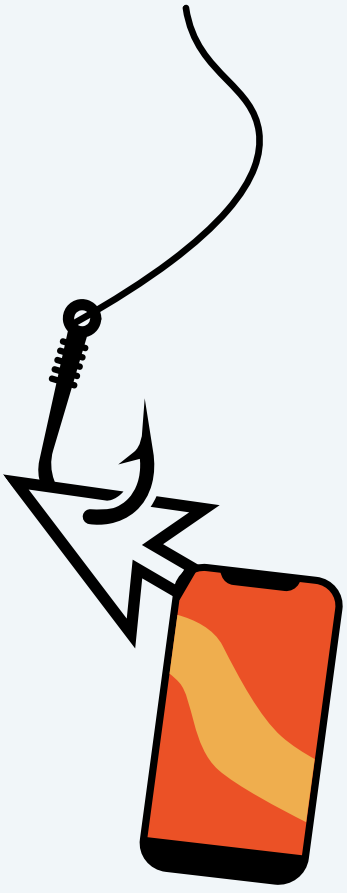
Phishing is a cyber-attack where someone tricks you into giving away personal information (like passwords or account access) by pretending to be a trusted person or company. The hacker can also manipulate you into clicking links or downloading attachments that could inadvertently install malware onto your device.

Common signs of phishing

- Requests for sensitive info: Passwords, bank PINs, OTP codes
- Attachments from unknown senders: Malware may be hidden in PDFs, Word docs, etc.
- Too good to be true offers: **“You’ve won!”** or **“Claim free data bundles”**
- Urgent “***click here now***” messages

Safety tips against phishing

- Always verify sender identity before clicking links. It’s good to call the person directly when you receive a strange or unexpected email or message from them and check.
- Enable 2-Factor Authentication (2FA)
- Never share passwords or verification codes.
- Visit official websites instead of clicking links in messages.
- Always update your software and apps with the latest version.
- Drag your cursor over the email sender as well as any links in the email. Malicious links will likely not match up with the email or link description.
- Avoiding over sharing personal information on social networking platforms, this can potentially be used for social engineering purposes.



Common digital threats

Malware

Malware or malicious software is any software code or computer program intentionally written to harm computer systems and/or their users.

Types of Malware

1. **Computer viruses**; Viruses are usually designed to delete important data, disrupt normal operations, and spread copies of themselves to other programs on the infected computer.
2. **Trojans** disguise themselves as useful programs or hide within legitimate software to trick users into installing them.
3. **Scareware** frightens users into downloading malware or passing sensitive information to a fraudster. Scareware often appears as a sudden pop-up with an urgent message, usually warning the user that they have broken the law or their device has a virus. The pop- up directs the user to pay a "fine" or download fake security software that turns out to be actual malware.
4. **Spyware** hides on an infected computer, secretly gathering sensitive information and transmitting it back to an attacker usually through the device camera and microphone. One common type of spyware, called a keylogger, records all of a user's keystrokes, allowing hackers to harvest usernames, passwords, bank account and credit card numbers and other sensitive data.
5. **Adware** spams a device with unwanted pop-up ads. Adware is often included with free software, unbeknownst to the user. When the user installs the program, they unwittingly install the adware, too. Most adware is little more than an annoyance. However, some adware harvest personal data, redirect web browsers to malicious websites or even download more malware onto the user's device if they click one of the pop-ups.
6. **Ransomware** locks up a victim's devices or data and demands a ransom payment, financial or otherwise, to unlock them.

Common digital threats

Surveillance

Surveillance is the act of monitoring, tracking, collecting, or analyzing information about people, often without their knowledge or consent. It happens through digital tools, devices, systems and relationships.

Common signs of surveillance include:

- Sudden password reset emails,
- Strange followers,
- Someone referencing private chats in public,
- Unexpected login alerts
- Unusual battery/data usage on phone (spyware)
- Social media account logins from strange locations
- Being asked for your phone during protests
- Sudden targeting after posting political or feminist content

Safety tips against Surveillance

- Use encrypted apps (Signal, Proton mail)
- Turn off GPS/location when not needed
- Regularly update device software and apps
- Use VPNs and secure browsers (like Tor, Brave)
- Create “decoy” or “public” accounts for risky spaces

Common digital threats

Misinformation and Disinformation

Misinformation and disinformation have become powerful tools in the hands of anti-rights and anti-gender actors to undermine social justice movements and feminist causes. These tactics are used to distort facts, incite moral panic, discredit activists, and justify repressive policies

How false narratives are spread

- Narrative Framing: They create simple, emotionally charged stories that frame feminist and queer movements as existential threats. These narratives are deliberately designed to provoke fear, disgust, or rage.
- Weaponizing Culture and Religion: Local customs are co-opted to suggest that gender equality is “Western” or “colonial,” despite long local histories of feminist and queer resistance. This strategy works by making hate look like heritage, which makes it harder for communities to question it.
- Digital Media Amplification: False narratives are spread widely using: Coordinated social media campaigns with bots, fake accounts, and influencers; Disguised misinformation that looks like legitimate news, research, or community content; Hashtag hijacking to infiltrate feminist or human rights conversations with harmful messaging.
- Anti-rights actors often create fake grassroots movements, a process called astroturfing, to make their views look widely supported e.g “Parents groups” opposing gender education. These groups are often well-funded, scripted, and connected to powerful interests but they are branded to look like spontaneous, concerned citizens.

Misinformation and disinformation are not just obstacles, they are weapons. They fracture communities, exhaust organizers, and block policy change.

Common digital threats

Non-Consensual Sharing of Intimate Images & Information (NCII)

NCII refers to the distribution of sexual or intimate photos/videos without the consent of the person depicted. NCII is a form of technology-facilitated gender-based violence (TFGBV) that disproportionately affects women. It is often misleadingly called “revenge porn” but this term is harmful because it not only implies blame on the victim for creating the content, it also suggests the motivation is always “revenge,” while in reality it can be for shaming, extortion, control, or profit.

NCII is worse for womxn with intersecting identities such as queer folk, gender-diverse folk, sex workers, women living with disability, etc because they face intersecting layers of stigma and criminalization that make them especially vulnerable to NCII abuse. For queer womxn, NCII is often used as a weapon to out, shame and/or expose them to violence, arrest, or family rejection, as their intimacy is framed as both “immoral” and “illegal.” Similarly, for sex workers whose livelihoods often depend on digital platforms and private exchanges, NCII can result in loss of income, public humiliation, and physical harm. Deep-rooted stigma means that both communities are often disbelieved, blamed or denied support, forcing many to suffer in silence rather than report abuse.

What can survivors do?

- **Document:** Take screenshots, save URLs, record dates/times.
- **Report to platforms:** Facebook, Instagram, TikTok, and X have NCII reporting processes.
- Seek support: HER Internet, feminist collectives, or community helplines.
- **Legal caution:** Reporting to police may be unsafe for queer or sex worker communities. It is important to assess risk before engaging them.
- **Collective care:** Have a trusted friend/ally to help monitor, report, and provide emotional support.

NCII is not about “poor choices,” it is about abuse, power, and control.

Passwords: Our Digital Locks!

1 Why do I even need a strong password? It's just my account!

Because your password is the key to your digital house. Weak passwords make it easy for strangers to sneak in. Make it at least 12 characters long, mixing letters (Aa-Zz), numbers (0–9), and symbols (@#$%) — skip birthdays and pet names!

2 Can't I just use the same password for everything? Easier to remember!

Big mistake! If one door gets kicked open, all your rooms are exposed. Use different passwords for each app. Try a password manager (like Bitwarden, Google Password Manager, Apple Passwords) to remember them all for you.

3 What is this 2FA thing people keep talking about?

Think of it as a second lock on your digital door. Even if someone guesses your password, they still can't get in.
Use authenticator apps like Google Authenticator instead of SMS codes because those can be intercepted.

4 How do I know if my password has been hacked?

If you notice strange logins, password reset emails, or messages you didn't send, act fast! Change your password immediately and check your account's login history (Google, Facebook, and X all let you do this).

Safe browsing

How do I browse safely without leaving digital breadcrumbs everywhere?

Start by using browsers like Firefox or Brave — they respect your privacy. Add browser extensions like HTTPS Everywhere and uBlock Origin to block trackers and ads. If you face censorship, use a trusted VPN to keep your traffic private. Also, make it a habit to clear your history and cookies often, especially on shared devices.

Should I let my browser remember my passwords?

Not at all, that is risky! Instead, use a password manager (like Google Password Manager, Apple passwords, Bitwarden).

And what about those strange emails and links?

If it looks weird, sounds strange or urgent — DO NOT click it! Phishing attacks thrive on curiosity. Always double-check the sender and URLs.

Okay, what about my phone and laptop? They are full of stuff!

Time for a little digital cleaning!

- Delete apps you don't use because they often collect unnecessary data.
- Review permissions: If an app does not need your camera or microphone, turn that access off.
- Empty your trash/recycle bin — "deleted" does not always mean gone.
- Back up important files to an encrypted drive or secure cloud.
- And if you are letting go of an old device, wipe it clean completely before you pass it on.

Secure Communications

1. Why does secure communication even matter?

Because every message, call, or post leaves a trace — and for folks from structurally silenced communities in Uganda, those traces can expose your identity, networks, or even your location. Staying secure is not paranoia — it is protection for yourself and your community.

2. Is my phone number really that risky?

Yes, your phone number is like your digital fingerprint!
It is tied to your name, location, and SIM card registration. Avoid sharing it publicly, and if possible, use a separate SIM for activism and community work.

3. Which messaging apps are safer?

Use Signal, it allows you to hide your number and control who can find you.
On WhatsApp, stick to trusted contacts and avoid adding strangers to groups.
Both Signal and WhatsApp support end-to-end encryption.

4. What is this "end-to-end encryption" everyone talks about?

It means only you and the person you are chatting with can read or hear your messages — not hackers, not the app, not even your internet service provider. Signal is the gold standard, although WhatsApp also supports it by default.

5. Even with encryption, can people still see my activity?

Encrypted apps still reveal metadata — like who you talk to and when. To reduce this:

- Keep groups small and temporary.
- Avoid obvious posting or texting patterns.
- Use a VPN or Tor when you are on public Wi-Fi.

Privacy is not secrecy, it is safety!

Secure Communications

Handling Files & Documents

- Redact first: Blur names, faces, and other identifiers before sharing.
- Password-protect sensitive files (pdf, doc, excel). Share the password in a different app or by different means.
- Use expiring links with access control (view-only, disable download if possible).

If you are doxed or threatened:

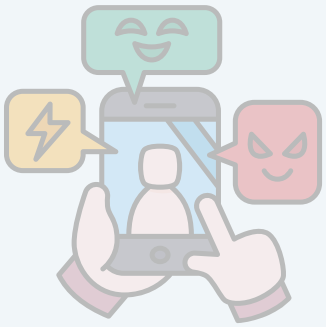
1. Preserve evidence: Screenshots, links, timestamps.
2. Lock down accounts: Change passwords; enable 2FA; check sessions/logged-in devices.
3. Tighten privacy: Make profiles private; limit who can find you; remove location from recent posts.
4. Alert your network: Share a short “what to ignore/what is real” note.
5. Contact support: HER Internet or any other emergency contacts on page 18.
6. Safety check: If threats include physical harm, update a trusted person with location and plan.

Travel & High-Risk Moments

- Travel phone with minimal apps and contacts. Log out of high-risk accounts.
- Disable biometrics just in case you are compelled by the authorities to unlock your device; use a strong password/PIN.
- Turn off the device or use lockdown mode (iOS/Android) when approaching risky checkpoints.

Navigating Online Harassment and Crisis Response

For individuals from structurally silenced communities in Uganda, online harassment can escalate quickly from harmful comments to coordinated campaigns, doxing, or threats of physical violence. Knowing how to recognize, respond, and recover from these incidents is critical for protecting your well-being and continuing to engage online safely.



Recognizing Online Harassment

Harassment takes many forms. Common tactics include:

- Targeted abuse: hateful slurs, insults, or bullying.
- Doxing: publishing private details such as your phone number, address, or workplace.
- Impersonation: fake accounts created to misrepresent you or spread harmful content.
- Mass reporting: coordinated efforts to get your accounts suspended.
- Threats of violence: messages suggesting physical harm, rape threats and even death threats.

Recognizing these patterns helps you act quickly before the harassment escalates.

If you are being targeted:

- Document evidence: Take screenshots or screen recordings of abusive messages, comments, or posts (including timestamps, usernames, and URLs). These may be useful for legal, advocacy, or platform reporting.
- Strengthen account security: Immediately update your passwords, enable two-factor authentication, and review connected apps or sessions for suspicious activity.
- Block and mute: Use platform tools to block harassers, mute harmful conversations, and limit who can comment or message you.
- Adjust privacy settings: Temporarily restrict who can view your posts, tag you, or send friend requests.
- Do not engage: Arguing with abusers often escalates the harassment and can make you more visible to trolls.

When threats escalate:

- Contact HER Internet's trusted digital safety support team for immediate help or referrals to any other emergency contacts on page 18.
- Legal support: Consider consulting a lawyer or human rights organization if doxing or threats of physical harm occur.
- Report to platforms: Use the official reporting channels for harassment, hate speech, and impersonation. Although platforms may be slow, filing a report creates a record.
- Seek psychosocial support: Online harassment can cause trauma, anxiety, and isolation. Reach out to trained mental health professionals or peer support groups for care.
- Physical safety: If harassment includes threats of physical harm, assess your personal safety (change routines, avoid disclosing location, and if necessary, temporarily relocate to a safer space with community support).

Preventive Practices

To reduce your risk:

- Limit personal information shared online: Avoid posting addresses, workplaces, or identifiable daily routines.
- Review audience controls: Share sensitive updates only with trusted circles.
- Diversify communication channels: Use encrypted apps (Signal, WhatsApp with disappearing messages) for sensitive conversations.
- Prepare a digital crisis plan: Know in advance who you would call for legal advice, psychosocial support, and technical help.

Community & collective care

No one should face harassment alone. Collective safety is key:

- Buddy system: Have trusted friends who can help monitor your accounts, flag abuse, or take over communication if you need a break.
- Amplify safely: When someone in your community is harassed, offer support by reporting abusive accounts rather than directly engaging with harassers.
- Healing spaces: Create safe offline and online spaces where community members can process harassment, share coping strategies, and rebuild confidence.

Online harassment is not a personal failure—it is a structural issue targeting structurally silenced communities, especially during politically tense periods. Crisis response is not just about surviving attacks but reclaiming safety, dignity, and collective power.

Emergency Contacts

If you or someone you know is facing an urgent digital threat such as account hacking, doxing, online harassment or surveillance, please reach out immediately using the contacts below. HER Internet's digital support team and trusted referral partners are available to offer confidential assistance, whether technical, legal or psychosocial.
Remember: You are not alone, and reaching out early can help prevent further harm.

Description	Phone	Email
HER Internet ***Digital Security support***	+256 707057393	info@herinternet.org
Access Now ***Digital Security support***		help@accessnow.org
Stop NCII reporting tool ***Support with NCII cases***		https://stopncii.org
Revenge Porn Helpline ***Support with NCII cases***	+44 345 6000 459	https://revengepornhelpline.org.uk
Feminist Helplines Index ***Digital Security support***		feministhelplines.org
DefendDefenders ***Emergency support for HRDs***	+256 707020086	protection@defenddefenders.org
Human Rights and Awareness Promotion Forum (HRAPF) ***Legal support***	+256 800130683	info@hrapf.org
Defenders Protection Initiative (DPI) ***Emergency support for HRDs***	+256 392201102	https://www.defendersprotection.org/report/
Ubuntu Justice and Law Centre ***Legal support***	+256 782683824 / +256 414480143 / +256 414580144	

Contact Us

+256 707057393

www.herinternet.org

info@herinternet.org

123 Anywhere St., Any City