



VITAL VOICES
GLOBAL PARTNERSHIP

DIGITAL SAFETY TOOLKIT FOR WOMEN LEADERS





This toolkit was developed by Vital Voices Global Partnership in collaboration with Safe Sisters, Internews.

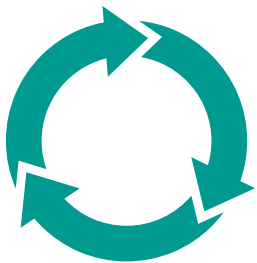
Please do not distribute without written permission from the Vital Voices Crisis Response Team, crisis@vitalvoices.org.

MEET JULIE!

“Hi there! I am here to guide you in achieving our goals in digital safety and security so that you can pursue your goals online using technology in full confidence.”



“Your journey to digital safety requires some time and effort but it is possible! The first step is realizing that there exists potential risks and consequences from your online presence.”



“Although some terms and technologies may seem unfair or confusing, do not give up! You probably know more than you think. Work through this toolkit and the resources and you will get there. Remember, practice makes perfect!”

“Start small: Set regular reminders to update your software or change your password. Take lessons: Today you have the opportunity to learn digital safety skills in your own time and at your own pace so that you prioritize protecting yourself and the things you value most.”

START

CYBER HARASSMENT

“Online gender-based violence is a common form of discrimination that exists on social media platforms world-wide. It can be identified as body shaming, revenge porn, hate speech, doxxing and trolling. Victims of online gender-based violence often face stigma, isolation and suffer severe depression. Let’s find a solution!”



Do you have a trusted circle?



You should speak up about the abuse to family members and friends that you trust and take a tactical break from the face of harassment. Let them handle your social media accounts and help you report the perpetrator to authorities.

Are you considering reporting the abuser?



Do you have an office or cybercrimes unit through which victims can report online harassment directly to the police in your community? Do you know about the reporting mechanism available on the platform where the abuse has occurred?

Are you documenting the abuse?



Use a ledger to record all the communications sent by the perpetrator. Take photos or screenshots, collect IP addresses, save text messages, call logs and Call ID. Be ready to show this data as evidence for the legal authorities.

Are you including self-care?



Eat fresh and healthy foods and stay hydrated. Try simple and regular exercise and keep strict hours of sleep at least 7 hours in a quiet and dimly lit space. Seek professional care if your mental health is affected. Consider finding a support group for women going through similar experiences.



ACCOUNT SECURITY



“Get to know the Settings page for your most important accounts. This is where the most configurations can be made for account security and recovery.”

First brainstorm what are the **most important 3-5 accounts** for your online work and online identity, and list them below. Some examples are WhatsApp, Facebook and Signal Chat. These are accounts you use daily for communication, advocacy and connection.

Next find and visit the **Settings Section** for each of them and **review** the account security, login, and recovery settings to make sure everything has been set up (e.g with **2-factor authentication**, up-to-date **account recovery** information, and any other security or privacy settings you would like to change). Check off each account when done.

Some platforms include an ‘**account check-up**’ or ‘**privacy check-up**’ feature that combines multiple checks at once. Following this section, use the checklists below to secure your devices. After listing your accounts, follow the checklists below to secure your devices.

ACCOUNT/PLATFORM NAME	FOUND THE SETTINGS	CHANGES MADE
Example: Signal Chat	<input checked="" type="checkbox"/>	Added 2 Factor Authorization, Added Disappearing Messages, Changed who can see my phone #
	<input type="checkbox"/>	
	<input type="checkbox"/>	
	<input type="checkbox"/>	
	<input type="checkbox"/>	



“Don’t forget that instant messengers like WhatsApp, Telegram, and Signal are all accounts too. Have you included them?”

DEVICE SECURITY CHECKLIST – LAPTOP/DESKTOP DEVICE

“Your device is the home for your digital life. Let’s regularly check and tidy up and fix problems if they are there.”



Device Name: _____

MEASURE	COMPLETE	NOTES
Screen Lock enabled on device (e.g. password, biometric lock)	<input type="checkbox"/>	
Create non-administrative user for anyone else who uses the device	<input type="checkbox"/>	
Utilize cloud backup for your work files, ensure files are backed up to an account whose security you have already checked	<input type="checkbox"/>	
Enable full disk encryption (e.g. BitLocker, FileVault)	<input type="checkbox"/>	
Install available updates, and check automatic update settings	<input type="checkbox"/>	
Install available updates on your other software (e.g. Browsers, Adobe)	<input type="checkbox"/>	
Check Windows Security/Security Settings for status and enable features as recommended	<input type="checkbox"/>	
Run a full anti-virus scan	<input type="checkbox"/>	
Check for startup items and installed programs and remove those which aren't needed or which you can't confirm	<input type="checkbox"/>	

DEVICE SECURITY CHECKLIST – PHONE/TABLET

“Your device is the home for your digital life. Let’s regularly check and tidy up and fix problems if they are there.”



Device Name: _____

MEASURE	COMPLETE	NOTES
Screen Lock enabled on device (e.g. password, biometric lock)	<input type="checkbox"/>	
Check how to give someone else access to the phone if needed: see if your device supports additional users, otherwise see how to use App Pinning (Android) or Guided Access (iOS)	<input type="checkbox"/>	
Utilize cloud backup for your work files, ensure files are backed up to an account whose security you have already checked	<input type="checkbox"/>	
Check security settings to see if device is encrypted	<input type="checkbox"/>	
Install available system and app updates, and check automatic update settings	<input type="checkbox"/>	
Check for apps granted ‘Install Unknown Sources’ permission and remove the permission	<input type="checkbox"/>	
Check for Device Admin Apps in settings and ensure they are correct/legitimate	<input type="checkbox"/>	
Run a full anti-virus scan	<input type="checkbox"/>	
Install and use a VPN	<input type="checkbox"/>	
Remove apps which are unnecessary or you do not trust	<input type="checkbox"/>	

DEVICE SECURITY CHECKLIST – PHONE/TABLET 2



“For your second phone, if you have one.”

Device Name: _____

MEASURE	COMPLETE	NOTES
Screen Lock enabled on device (e.g. password, biometric lock)	<input type="checkbox"/>	
Check how to give someone else access to the phone if needed: see if your device supports additional users, otherwise see how to use App Pinning (Android) or Guided Access (iOS)	<input type="checkbox"/>	
Utilize cloud backup for your work files, ensure files are backed up to an account whose security you have already checked	<input type="checkbox"/>	
Check security settings to see if device is encrypted	<input type="checkbox"/>	
Install available system and app updates, and check automatic update settings	<input type="checkbox"/>	
Check for apps granted ‘Install Unknown Sources’ permission and remove the permission	<input type="checkbox"/>	
Check for Device Admin Apps in settings and ensure they are correct/legitimate	<input type="checkbox"/>	
Scan with Play Protect	<input type="checkbox"/>	
Install and use a VPN	<input type="checkbox"/>	
Remove apps which are unnecessary or you do not trust	<input type="checkbox"/>	

RESOURCES

Cyber Harassment

[Online Harassment Field Manual \(PEN\)](#)

[Online Violence Response Hub](#)

[Coalition against Stalkerware](#)

[Cyber Civil Rights - Image Removal requests](#)

[iheartmob- Self-care for people facing harassment](#)

[Totem Project - Know Your Trolls Course \(see their other courses as well\)](#)

[Online SOS](#)

[FeedShield - Tools for harassment on Twitter \(Africa only\)](#)

[Disconnecting from your ex-partner checklists \(and others\)](#)

[Harassment and Doxxing Slides](#) - Digital Defense Fund

Digital Security Guides and Checklists

[Digital Defence Online Checklists](#)

[Safe Sisters - Toolkit on Digital Safety](#)

[Security in a Box](#)

[Digital First Aid Kit](#)

[Access Now - Digital Security Emergency Helpline](#)

[Internews - SaferJourno](#)

[Open Briefing - Digital Security Protocol](#)

[Surveillance Self Defense](#)

[Frontline Defenders - Women Human Rights Defenders Toolkit](#)