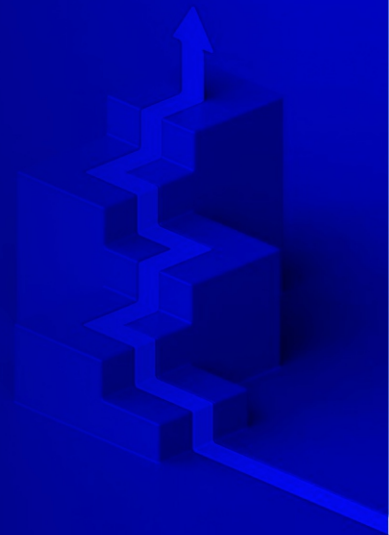


Digital Democracy Initiative

DIGITAL CIVIC PROTECTION TOOLKIT

A bilingual (English and Hausa) practical resource for strengthening digital safety, cyber incident response, and digital rights awareness among civic actors.



Prepared by:
Open Knowledge Development Initiative

Nigeria
2026



DIGITAL CIVIC PROTECTION TOOLKIT

**A Simple, Practical Guide to Digital
Safety for Civil Society Organizations**

WHO THIS IS FOR:

CSO directors, youth activists, community
journalists, and human rights defenders
who want to keep their organization,
data, and people safe online.

Prepared by:

Open Knowledge Development Initiative

KAYAN AIKIN KARIYAR JAMA'A TA HANYOYIN SADARWA NA ZAMANI

**Jagora Mai Sauki da Aiki Kan Tsaron
Hanyoyin sadarwa na Zamani ga Kungiyoyin Farar Hula**

WANDA AKA SHIRYA DOMIN:

Shugabannin kungiyoyin farar hula (CSOs), matasa masu
fafutuka, yān jarida na al'umma, da masu kare haƙƙin ɗan
Adam waɗanda ke son kare kungiyoyinsu, bayanansu, da
mutanensu daga barazanar yanar gizo.

Shiryawa:

Open Knowledge Development Initiative

2026 | ENGLISH & HAUSA

About this Toolkit

This Digital Civic Protection Toolkit was developed by the Open Knowledge Development Initiative (OKDI) through a participatory co-creation process involving civil society organizations, youth activists, Cyber-security experts, translators, and media practitioners, it reflects real risks that CSOs in Gombe State and Northeastern Nigeria face every day.

It is designed to be practical, locally relevant, and accessible. It is written in plain language and translated into Hausa so that organizations with varying levels of digital literacy can use it. Whether you are a CSO director, a youth activist, a community journalist, or a frontline human rights defender, this toolkit is for you.

What this Toolkit Covers

This toolkit is organised into nine sections:

1. Digital Security Basics
2. Threats You Should Know
3. Protecting Your Accounts
4. Securing Devices, Data & Your Work
5. Communicating Safely
6. Protecting Your Online Presence
7. When Something Goes Wrong
8. Know Your Digital Rights
9. Quick Reference Card
10. Build Your Own Security Policy

How to Use This Toolkit

- Read it once as a full team, then keep it as a reference.
- Use the checklist at the end of every section to track your progress.
- Print Section 9 (Quick Reference Card) and pin it in your office.
- Share it freely with staff, partners, and community members.

GAME DA WANNAN KAYAN AIKI

Wannan Kayan Aikin Kariyar Jama'a Na Hanyoyin Sadarwa na Zamani (Digital Civic Protection Toolkit) Open Knowledge Development Initiative (OKDI) ce ta samar da shi, ta hanyar tsarin haɗin gwiwa da ya haɗa da kungiyoyin farar hula, matasa masu fafutuka, kwararru a fannin tsaron yanar gizo, masu fassara, da kuma ma'aikatan watsa labarai. Ya kunshi haƙiƙanin haɗurran da kungiyoyin farar hula a Jihar Gombe da sauran sassan Arewa maso Gabashin Najeriya ke fuskanta a kullum.

An tsara shi domin ya zama mai sauƙin amfani, ya dace da yanayin gida, kuma kowa ya iya amfani da shi. An rubuta shi cikin sauƙaƙaƙken harshe, an kuma fassara shi zuwa Hausa domin kungiyoyi masu matakan fahimtar fasaha daban-daban su iya amfani da shi. Ko kai shugaban kungiyar farar hula ne, ko ɗan fafutuka, ko ɗan jarida na al'umma, ko mai kare haƙƙin ɗan Adam, wannan jagora naka ne.

01

Digital Security Basics (Why It Matters for Civil Society)

1.1 What Is Digital Security?

Digital security refers to the practices, tools, and habits that protect your organization's online presence, data, communications, and devices from unauthorized access, surveillance, and attack. It is not just a technical issue, it is a fundamental part of keeping your people, your work, and your communities safe.

1.2 Why CSOs Get Targeted

Your work, holding power to account, defending rights, organizing communities and speaking truth, makes you visible and sometimes inconvenient to powerful actors. That visibility can attract attackers.

Common reasons CSOs are targeted include:

- Advocacy work challenges powerful people or institutions
- Foreign funding is sometimes wrongly seen as suspicious
- Staffs are outspoken and visible online
- You hold sensitive data about communities and beneficiaries
- You work in areas where surveillance is common

Why It
Matters
for
Civil
Society

1.3 What Poor Security Can Cost You

Risk	What Can Happen	Impact on Your Work
Account compromise	Email/WhatsApp hacked	Lost trust and data
Data breach	Beneficiary data exposed	Legal risk, harm to communities
Phishing	Malware installed	Devices and files compromised
Harassment	Staff doxxed, or threatened	Burnout, self-censorship
Surveillance	Communications monitored	Compromised operations and partner safety

CHECKLIST 1

- ☐ Our leaders understand why digital security matters
- ☐ We have discussed the threats specific to our work
- ☐ One person is responsible for digital security oversight
- ☐ This toolkit has been shared with all staff

HAUSA TRANSLATION**SASHE NA 1:****TUSHEN TSARON
HANYOYIN SADARWA
NA ZAMANI**

Wannan sashe ya bayyana cewa tsaron hanyoyin sadarwa na zamani na nufin matakan kariya da ake amfani da su wajen kare bayananku kungiya, na'urori, hanyoyin sadarwa, da asusun yanar gizo daga kutse, sata, sa ido ba tare da izini ba, da sauran hare-haren yanar gizo. Ya jaddada cewa tsaron hanyoyin sadarwa na zamani ba alhakin masu fasahar kwamfuta kadai ba ne, illa dai alhakin kowane ma'aikaci ne. Haka kuma, ya bayyana cewa kungiyoyin farar hula (CSOs) kan zama abin hari saboda ayyukansu na kare hakkin jama'a, wayar da kai, da kuma riƙe bayanai masu muhimmanci. An ba da misali na wata kungiya a Gombe da ta karɓi sakon imel na bogi domin a yaudare ta ta shigar da bairos a cikin na'urorinta.

Har ila yau, sashen ya nuna irin illolin da rashin tsaron hanyoyin sadarwa na zamani zai iya haifarwa, kamar sace asusun imel ko WhatsApp, fallasa bayananku masu cin gajiyar ayyukan kungiya, shigar bairos cikin na'urori, cin zarafi ga ma'aikata ta yanar gizo, da kuma sa ido kan hanyoyin sadarwa. Don rage waɗannan haɗurra, shugabannin kungiya su fahimci muhimmancin tsaron hanyoyin sadarwa na zamani, su tattauna barazanar da ta shafi ayyukansu, su naɗa mutum mai kula da tsaron hanyoyin sadarwa na zamani, sannan su tabbatar cewa dukkan ma'aikatansu sun karanta kuma sun fahimci wannan jagora.

02

Understanding the Threats (What CSOs Face Online)

2.1 Overview of Digital Threats

Before you can protect yourself, you need to understand what you are protecting against. This section explains in plain language the most common digital threats facing CSOs in Northeastern Nigeria.

2.2 Phishing and Social Engineering

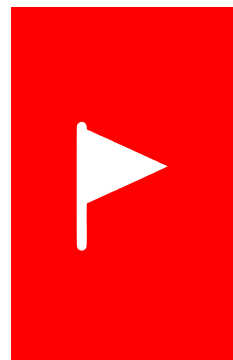
SIMPLE TERM: Phishing = a fake message trying to trick you into clicking a bad link or giving away your password. Like a fisherman casting bait, hoping you bite.

Social Engineering: Psychological, instead of exploiting technical software vulnerabilities, it targets human error and exploits natural tendencies like trust, fear, and urgency.

What CSOs Face Online

Watch for these red flags:

- Urgency: 'Act now or lose Access'
- Generic greeting: 'Dear User' instead of your name
- A link that doesn't match the real sender's website
- Unexpected attachments (.exe, .zip, .docm)
- A wrong email address, e.g. funders@gmail.com instead of the real organization domain
- Any request for your password or payment by message



2.3 Account Hacking and Takeover

Account takeover happens when someone gains access to your email, social media, or other accounts without your permission.

Signs your account may have been compromised:

Warning signs: password-reset emails you didn't request; contacts receiving strange messages 'from you'; you're locked out; your profile details changed without your action.

2.4 Surveillance

Type	What It Looks Like
Network	Your provider or an agency monitors your internet or SMS traffic
Device	Spyware secretly records calls, messages, location
Social Media	Someone tracks your posts and contacts to map your network
Physical	Someone watches or photographs your office and staff

2.5 Harassment

Online harassment targeting CSOs often comes in organized waves. Common forms include:

1. Doxxing:- Publishing staff's private details to endanger them
2. Impersonation:- Fake accounts pretending to be your organization
3. Pile-ons:- Mass reporting to get your account suspended

What
CSOs
Face
Online

2.6 Malware

Malware is malicious software that damages or takes control of your device.

Ransomware is a type of malware that locks your files and demands payment to restore access.

CHECKLIST 2

- | |
|--|
| ☐ All staff can name 3 red flags of phishing |
| ☐ We know the signs of a hacked account |
| ☐ We have discussed surveillance risks specific to our work |

SASHE NA 2:

FAHIMTAR BARAZANA — ABIN DA KUNGIYOYIN FARAR HULA KE FUSKANTA A YANAR GIZO

Wannan sashe ya bayyana manyan barazanan tsaron hanyoyin sadarwa na zamani da kungiyoyin farar hula (CSOs) ke fuskanta a yanar gizo, tare da nuna cewa fahimtar waɗannan barazana shi ne mataki na farko wajen kare kai. Ya yi bayani kan phishing, wato sakonnin bogi da ake amfani da su wajen yaudarar mutane su danna hanyar haɗi mara aminci ko su bayyana kalmar sirrinsu, da kuma zamba cikin aminci (social engineering), wato amfani da yaudara, tsoro ko gaggawa domin sa mutum ya aikata abin da zai jefa shi cikin haɗari. Haka kuma, sashen ya bayyana alamomin da ke nuna an kutsa cikin asusu, hanyoyin sa ido ta yanar gizo, da dabarun cin zarafi kamar kirƙirar asusun bogi ko fallasa bayanan sirri na ma'aikata.

Bugu da ƙari, sashen ya yi bayani kan malware, wato kwayoyin cuta da ke lalata ko sarrafa na'urori ba tare da izini ba, da kuma ransomware, wanda ke kulle fayiloli tare da neman kuɗi kafin a sake buɗe su. An nuna cewa irin waɗannan hare-haren na iya zuwa ta sakonnin imel masu ɗauke da fayilolin cutarwa ko kuma ta na'urorin USB. A ƙarshe, sashen ya ƙarfafa ma'aikata su iya gane alamomin sakonnin bogi (phishing), su san yadda za su gano idan an kutsa cikin asusunsu, sannan su tattauna irin haɗarin sa ido da ke iya shafar ayyukan ƙungiyarsu domin su ɗauki matakan kariya da wuri.

03

Protecting Your Accounts

3.1 Account Security- The First Line of Defense

Most digital security incidents begin with a compromised account, a hacked email, a stolen password, or an account accessed on a lost device. Strengthening your account security is the single most powerful thing you can do to protect your organization.

3.2 Strong Passwords

What makes a strong password:

- At least 12 characters, mixing upper/lower case, numbers, symbols
- Never use your name, organization name, or '123456'
- A different password for every account
- Try a passphrase: 4+ random words, e.g. 'purple-engine-river-dance'

Example of a good Password:- Cherry\$47916#

3.3 Use a Password Manager

A password manager stores every password safely behind one master password.

Recommended: Bitwarden (bitwarden.com, free).

Set it up:

- create an account with your work email
- install the app and browser extension
- add your passwords
- let it auto-fill logins
- every staff member gets their own account.

Protecting
Your
Accounts
and
Access

3.4 Turn On Two-Factor Authentication (2FA)

SIMPLE TERM: 2FA = a second lock on top of your password, like needing both a key AND a fingerprint to open a door.

- Best: Authenticator app (Google Authenticator, Authy)
- Most secure: Hardware key (YubiKey), for high-risk users
- Better than nothing: SMS code

To enable on Gmail: myaccount.google.com

- Security
- 2-Step Verification
- follow the prompts and save your backup codes.

Repeat for Facebook, WhatsApp, and X.

3.5 Access Management

- Every staff member gets their own login — never share passwords
- Remove access immediately when someone leaves
- Review who has access every 3 months
- Give people only the access their role needs

CHECKLIST 3	
☐	All staff use a password manager
☐	2FA is enabled on all key accounts
☐	We have a process to remove access when staff leave

SASHE NA 3:

KARE ASUSUNKU

Wannan sashe ya bayyana cewa kare asusun yanar gizo shi ne mataki na farko kuma mafi muhimmanci wajen kare kungiya daga hare-haren yanar gizo. Ya ba da shawarar amfani da kalmomin sirri masu karfi, waɗanda suka kunshi haruffa, lambobi da alamomi, tare da amfani da kalmar sirri daban ga kowane asusu. Haka kuma, ya karfafa amfani da Password Manager domin adanawa da sarrafa kalmomin sirri cikin tsaro, da kuma kunna 2FA (Two-Factor Authentication), wato karin matakin kariya da ke buƙatar tabbatar da shiga ta hanya ta biyu bayan amfani da kalmar sirri. Misalin da aka bayar ya nuna yadda 2FA ya hana masu kutse shiga asusun Gmail na wani shugaban kungiya.

Bugu da kari, sashen ya jaddada muhimmancin kula da damar shiga asusun kungiya. Ya nuna cewa kowane ma'aikaci ya kamata ya kasance da nashi asusun shigar, ba tare da raba kalmar sirri da wani ba. Haka kuma, idan ma'aikaci ya bar aiki, ya zama dole a cire masa damar shiga nan take, sannan a rika duba waɗanda ke da damar shiga asusun kungiya akai-akai. Yin amfani da waɗannan mataakai zai taimaka wajen rage haɗarin kutse da kuma kare bayanai da dukiyyoyin hanyoyin sadarwa na zamani na kungiya.

04

Securing Devices, Data & Your Work

4.1 Device Security

Action	How
Screen lock	PIN/biometric, auto-lock after 1–2 minutes
Update	Turn on automatic software updates
Antivirus	Free tools: SmadAV, Malwarebytes, Avast — scan monthly
Encryption	Android/iPhone: on by default; Laptop: BitLocker or FileVault
Shared Computers	Never log into work accounts on cybercafe PCs

4.2 Backup With the 3-2-1 Rule

Losing your data whether through a cyber-attack, a stolen device, or hardware failure, can be devastating.

Thus the need to follow the 3-2-1 Backup Rule:

- 3 copies of your data (original + 2 backups)
- 2 different storage types (e.g. cloud + external drive)
- 1 copy stored off-site

4.3 Handling Sensitive Data

CSOs hold sensitive information including beneficiary names and contacts, programme data, financial records, donor communications, and partner details.

Rules for handling sensitive data:

- Only collect the data you truly need
- Store sensitive files in a restricted Google Drive folder, not personal phones
- Never share beneficiary data in WhatsApp groups
- Share view-only links, not editable files

Securing
Devices,
Data &
Your
Work

4.4 Protecting Intellectual Property & Personal Information

Civil society organizations create valuable intellectual property (IP), reports, research, training materials, toolkits, videos, logos, and brand identity that can be stolen, misused, or misrepresented online. Protecting your organization's IP and digital assets is an essential part of digital security.

- Add a copyright notice or Creative Commons license to published materials
- Keep master files (logos, templates, original reports) in a restricted admin-only folder
- Get written consent before using beneficiary names, photos, or stories
- Watch for organizations or people copying your work without credit, and use platform reporting tools or a take-down request if this happens
- Remove personal staff details (phone numbers, home addresses) from public websites and documents

CHECKLIST 4	
☐	All devices have screen lock and encryption on
☐	We follow the 3-2-1 backup rule
☐	Sensitive data is stored in a restricted folder, not on phones
☐	Our published materials carry a copyright/license notice

SASHE NA 4:**KARE NA'URORI,
BAYANAI DA AYYUKANKU**

Wannan sashe ya bayyana yadda kungiyoyi za su kare na'urorinsu da bayanansu daga kutse, sata ko lalacewa. An ba da shawarar amfani da makullin kariya (PIN ko hoton yatsa), da kunna sabunta manhajoji ta kai tsaye, da amfani da manhajar kariya daga kwayoyin cuta (antivirus), da kuma boye bayanai (encryption). Haka kuma, an gargadi ma'aikata da kada su shiga asusun kungiya ta amfani da kwamfutocin jama'a. Don kare bayanai daga facewa, sashen ya ba da shawarar bin ka'idar 3-2-1, wato a rika adana kwafi uku na bayanai, a wurare biyu daban-daban, sannan a ajiye kwafi daya a wani wuri daban.

Haka kuma, sashen ya jaddada muhimmancin kula da bayanan sirri kamar bayanan masu cin gajiyyar ayyuka, bayanan kudi da na abokan hulda. Ya nuna cewa a tattara bayanan da ake bukata kawai, a adana su a wurare masu kariya, kuma kada a raba su ta WhatsApp. Haka kuma, ya yi bayani kan kare haƙƙin mallakar kungiya ta hanyar sanya sanarwar haƙƙin mallaka, neman izini kafin amfani da sunaye ko hotunan masu cin gajiyyar ayyuka, da kuma kare bayanan sirri na ma'aikata daga bayyana a fili.

05

Safe Communication Tools and Practices

5.1 Choose the Right Tool

Not all communication tools offer the same level of security. The right choice of tool depends on the sensitivity of what you are discussing.

Sensitivity Level	Examples	Recommended Tool
Low	Public announcements	Facebook, email
Medium	Team coordination	WhatsApp (disappearing messages)
High	Beneficiary/incident data	Signal, ProtonMail
Very High	Whistle-blowers, at-risk sources	Signal + in-person where possible

5.2 Signal: The Gold Standard for Secure Messaging

Signal is a free, open-source messaging app that uses end-to-end encryption for all messages, calls, and video calls. Signal encrypts every message so only you and the receiver can read it.

Setup tips:

Download from the official app store

- register your number
- turn on disappearing messages for sensitive chats
- enable Screen Security and Registration Lock
- never back up Signal chats to Google Drive/iCloud, this removes the encryption protection.

5.3 Email & WhatsApp Rule

- For sensitive work, use ProtonMail (free, encrypted, based in Switzerland) instead of Gmail/Yahoo
- Never post beneficiary or financial details in WhatsApp groups
- Turn on disappearing messages in internal groups
- Restrict who can change group settings to admins only
- Enable WhatsApp two-step verification (Settings > Account)

CHECKLIST 5

- ☐ Staff know which tool to use for which sensitivity level
- ☐ Signal is set up for sensitive conversations
- ☐ WhatsApp groups have disappearing messages and two-step verification on

SASHE NA 5:**SADARWA CIKIN AMINCI**

Wannan sashen ya bayyana cewa ya kamata a zaɓi hanyar sadarwa gwargwadon muhimmancin bayanar da ake son aikawa. Don tura bayanar da ba su da matuƙar muhimmanci ana iya amfani da Facebook ko imel, yayin da WhatsApp ya dace da sadarwar cikin kungiya. Amma idan ana musayar bayanai masu muhimmanci ko sirri, ya fi dacewa a yi amfani da Signal ko ProtonMail, domin suna ba da kariya mai karfi ga sakonni da bayanai.

Sashen ya kuma bayyana yadda ake amfani da Signal cikin aminci ta hanyar kunna sakonnin da suke gogewa da kansu. Haka kuma, ya ba da fa'idojin amfani da WhatsApp da imel, ciki har da kada a raba bayanar masu cin gajiyar ayyuka ko na kuɗi a guruf din WhatsApp, a kunna Two-Step Verification, a takaita masu canza saitunan kungiya ga masu gudanarwa kawai, da kuma amfani da ProtonMail wajen aika bayanai masu muhimmanci.

06

Protecting Your Online Presence

6.1 Manage What's Public

Your organization's digital footprint, that is what appears when someone searches for you online, can be a resource or a risk. The goal is not to disappear online, but to be intentional about what you share and with whom.

- Audit your website: remove staff phone numbers, home addresses, meeting locations
- Ask staff to review what's public on their personal profiles
- Check haveibeenpwned.com for your organizational emails
- Search your organization's name to spot impersonation accounts

6.2 Quick Privacy Settings

Platform	Key Privacy
Facebook Page	Enable 2FA, review admins, check for fake pages
Facebook Personal	Past posts 'Friends only', location off
X (Twitter)	Protect tweets if discussing sensitive topics
Instagram	Switch to professional account, enable 2FA
WhatsApp	Profile photo 'My Contacts', two-step verification on

6.3 Developing a Social Media Security Policy

Every organization should have a simple, written social media policy that guides how staff behave online in connection with their work. It does not need to be long.

Cover:

- what staff may post about the organization
- How to handle hostile messages
- who to report incidents to
- whether staff identify as employees online
- who can post on official accounts.

CHECKLIST 6

- ☐ We've audited our website and social profiles for exposed personal data
- ☐ Key social accounts have 2FA and updated privacy settings
- ☐ We have a one-page social media policy

SASHE NA 6:**KARE KASANCEWARKU
A YANAR GIZO**

Wannan sashe ya yi bayani kan yadda kungiya za ta kare bayanana da take bayyanawa a yanar gizo da kuma martabarta. Ya karfafa cewa a rika duba shafin yanar gizon kungiya da shafukan sada zumunta domin cire bayanana sirri kamar lambobin waya, adireshin gida da wuraren taro. Haka kuma, ma'aikata su duba abin da suke bayyanawa a shafukansu, a bincika ko adireshin imel na kungiya ya taba fallasa, sannan a gano ko akwai wasu asusun bogi da ke amfani da sunan kungiya.

Bugu da kari, sashen ya ba da shawarar sabunta saitunan sirri na Facebook, X(Twitter), Instagram da WhatsApp tare da kunna 2FA. Ya kuma karfafa kowace kungiya ta samar da gajeriyar ka'ida kan amfani da kafafen sada zumunta, wacce za ta fayyace abin da ma'aikata za su iya wallafawa, da yadda za su magance sakonnin cin zarafi, da wanda za a kai wa rahoton matsaloli, da kuma waɗanda ke da izinin amfani da asusun kungiya.

07

When Something Goes Wrong

A Cyber incident is any event that compromises or threatens your organization's digital systems, data, or communications. This includes account hacks, phishing attacks, malware infections, data breaches, online harassment, and device loss or theft.

Golden rule: Do not panic, and do not delay.

7.1 5-step incident Response Framework

STEP	TO DO
1. Contain	Immediately disconnect the affected device from the internet. Do not turn it off, just disable Wi-Fi and mobile data. This stops malware spreading to other devices or data being ex-filtrated.
2. Assess	What happened? Which account or device is affected? How long ago? Who might have been exposed? Write it down. Do not rely on memory.
3. Respond	Change passwords on all affected accounts from a different unaffected device. Log out from all active sessions. Alert other staff if their data may be at risk.
4. Report	Contact OKDI Support Desk, Report hacked accounts to the platform (Facebook, Google, etc.). File a report with ngCERT at ngcert.gov.ng .
5. Recover	Restore data from your most recent backup. Document what happened, what data was affected, and what steps were taken. Learn from the incident and update your practices.

7.2 Fast Actions by Scenario

Email hacked:

- Recover from another device,
- Change password,
- Enable 2FA,
- Check for forwarding rules the attacker set, warn your contacts

Social account hacked:

- Report to the platform,
- Change password if you still have access,
- Post a warning on other channels,
- Screenshot the attacker's posts as evidence

Device lost/stolen:

- Change all passwords used on it,
- Remotely lock/wipe with Find My Device,
- Revoke its access,
- File a police report

CHECKLIST 7

- | |
|--|
| ☐ All staff know the 5-step framework |
| ☐ We know how to contact ngCERT and OKDI Support Desk |
| ☐ We have practiced the 'contain and report' steps once |

HAUSA TRANSLATION

SASHE NA 7:

IDAN WATA MATSALA TA FARU

Wannan sashen ya bayyana abin da ya kamata a yi idan aka fuskanci wata matsalar tsaro ta yanar gizo, kamar kutse cikin asusu, sakonnin yaudara, kwayoyin cuta, satar bayanai ko facewar na'ura. Ya jaddada cewa kada a firgita ko a yi jinkiri, sannan ya gabatar da tsarin mata kai biyar na OKDI, wanda ya haɗa da dakatar da yaɗuwar matsalar, tantance abin da ya faru, daukar matakan gyara, kai rahoto ga hukumomin da suka dace, da kuma dawo da bayanai tare da koyon darasi daga abin da ya faru.

Haka kuma, sashen ya ba da matakan gaggawa da za a bi idan an kutsa cikin imel ko kafafen sada zumunta, ko kuma idan waya ko kwamfuta ta face. Waɗannan sun haɗa da canza kalmomin sirri, kunna 2FA, kai rahoto ga dandalin da abin ya shafa, amfani da Find My Device domin kulle ko goge bayanai daga nesa, da kuma sanar da sauran ma'aikata idan akwai yiwuwar bayanansu sun shiga haɗari.

08

Know Your Digital Rights: Nigerian Law and Your Rights Online

Digital rights are human rights. Your right to freedom of expression, privacy, assembly, and access to information all extend to the online environment. Understanding the legal framework in Nigeria helps you know what protections you have, where the gaps are, and what to do if your rights are violated.

**What
to Do
When
Some-
thing
Goes
Wrong**

Law	What It Means for You
Cybercrimes (Prohibition, Prevention, Etc) Act. 2015 (As Amended) 2024	Criminalizes hacking, identity theft, phishing, and cyberstalking. CSOs can use this to report attacks. However, Section 24 has been used against journalists and activists for online expression (narrowed in 2024, but still vague), and Section 38 allows data requests/interception without a court order in "urgent" cases. Be aware of this risk.
Nigeria Data Protection Act (NDPA) 2023	Establishes data protection rights for individuals. CSOs that collect personal data must handle it responsibly and have a data protection policy. The Nigeria Data Protection Commission (NDPC) enforces this.
National Information Technology Development Agency (NITDA) Act 2007	Establishes NITDA as the regulatory body for IT in Nigeria. NITDA also issues Cyber security guidelines.
Freedom of Information Act 2011	Grants citizens the right to request information from public institutions. CSOs can use this to obtain government records relevant to their advocacy.
Constitution, Ss. 37 & 39	Section 37 guarantees the right to privacy. Section 39 guarantees freedom of expression. These rights extend to online activities.

If Your Rights Are Violated

- Document everything: screenshots, timestamps, URLs, witnesses
- Report Cybercrime to ngCERT (<https://cert.gov.ng/incident-report>) or the Police Cyber Crime Unit
- Report data violations to Nigeria Data Protection Commission (NDPC) (<https://services.ndpc.gov.ng/breach/>)
- Seek legal help from SERAP or Media Rights Agenda
- Contact the OKDI Support Desk for referrals

CHECKLIST 8

- ☐ Staff know their basic digital rights under Nigerian law
- ☐ We know where to report a rights violation

SASHE NA 8:

SANIN HAKKOKINKU NA HANYOYIN SADARWA NA ZAMANI

Wannan sashe ya bayyana cewa hakƙoƙin hanyoyin sadarwa na zamani suna daga cikin hakƙoƙin ɗan Adam, kuma dokokin Najeriya suna kare yancin sirri, faɗin albarkacin baki da kuma samun bayanai a yanar gizo. Ya yi bayani kan muhimman dokoki kamar Dokar Hana Laifukan Yanar Gizo (Cybercrime Act), Dokar Kare Bayanan Sirri ta Najeriya (NDPA), Dokar Hukumar Haɓaka Fasahar Sadarwa ta Kasa (NITDA Act), Dokar Yancin Samun Bayanai (FOIA), da kuma Kundin Tsarin Mulki, tare da bayyana yadda suke kare mutane da ƙungiyoyi da kuma nauyin da yake kansu wajen kare bayanan sirri.

Idan aka tauye hakƙin mutum a yanar gizo, sashen ya ba da shawarar a tattara hujjoji kamar hotunan allo da sauran bayanai, sannan a kai rahoto ga ngCERT, ko Hukumar Kare Bayanan Sirri ta Najeriya (NDPC) ko sashen yaƙi da laifukan yanar gizo na yān sanda. Haka kuma, ya nuna cewa ana iya neman taimakon doka daga ƙungiyoyi irin su SERAP da Media Rights Agenda, ko kuma a tuntubi OKDI Support Desk domin samun shawarwari da tallafi.

09

Quick Reference Card

Print this page and pin it in your office, share with all staff

Essential Free Tools

Tool	Use	Where
Signal	Secure messaging	signal.org
Bitwarden	Password manage	bitwarden.com
Google Authenticator	2FA codes	App/Play Store
ProtonMail	Encrypted email	proton.me
HaveIBeenPwned	Check leaked email	haveibeenpwned.com
Malwarebytes	Antivirus	malwarebytes.com

Emergency Contacts

Contact	Details
OKDI Support Desk	supportdesk@okdinitiative.org WhatsApp +234 7044354546 24–48hr response
ngCERT	ngcert.gov.ng info@ngcert.gov.ng
Nigeria Data Protection	ndpc.gov.ng
Access Now Helpline	accessnow.org/help
Front Line Defenders	frontlinedefenders.org

SASHE NA 9:

KATIN BAYANI MAI SAUIN FAHIMTA

Wannan sashe ya tattara muhimman kayan aikin tsaron hanyoyin sadarwa na zamani da ma'aikata za su iya amfani da su wajen kare bayanai da asusun kungiya. An bayyana manhajoji kamar Signal domin sadarwa mai tsaro, Bitwarden domin adana kalmomin sirri, Google Authenticator domin 2FA, ProtonMail domin imel mai kariya, HaveIBeenPwned domin bincika ko an fallasa adireshin imel, da kuma Malwarebytes domin gano da cire kwayoyin cuta.

Bugu da kari, sashen ya kunshi jerin muhimman wuraren neman taimako idan aka fuskanci matsalar tsaro ta dijital. Ya haɗa da bayanan tuntuɓar OKDI Support Desk, ngCERT, da Hukumar Kare Bayanan Sirri ta Najeriya (NDPC), da Access Now Helpline, da kuma Front Line Defenders. An ba da shawarar a buga wannan shafi kuma a rataye shi a ofis domin dukkan ma'aikata su samu sauƙin amfani da shi a duk lokacin da buƙata ta taso.

10

Build Your Own Security Policy

A digital security policy is a written document that sets out how your organization will protect its digital systems, data, devices, and communications. It tells staff what is expected of them, what tools to use, how to respond to incidents, and who is responsible for what.

Without a policy, digital security depends entirely on individual habits, some staff may be careful, others may not. A policy creates a shared standard that everyone in the organization follows, reducing risk and building collective resilience.

[ORGANIZATION NAME] — DIGITAL SECURITY POLICY

Effective Date: [Insert Date] | Reviewed by: [Name, Role] | Next Review: [Date]

PURPOSE

This policy sets out [Organization Name]'s standards for digital security. It applies to all staff, volunteers, and consultants who use organizational devices, accounts, or data.

CHECKLIST — Passwords & Access

- ☐ Every account password: 12+ characters, unique
- ☐ All staff use a password manager
- ☐ Every staff member has their own login — no shared passwords
- ☐ Access removed within 24 hours of a staff member leaving

CHECKLIST — Devices & 2FA

- ☐ 2FA enabled on all key accounts
- ☐ Screen lock and encryption on all work devices
- ☐ Antivirus installed and updated

CHECKLIST — Data, IP & Communication

- ☐ Sensitive data stored in restricted folders, never on personal phones
- ☐ Beneficiary data never shared in WhatsApp groups
- ☐ 3-2-1 backup rule followed
- ☐ Published materials carry copyright/licence notice; consent obtained for beneficiary photos/stories
- ☐ Sensitive conversations use Signal or ProtonMail only

CHECKLIST — Incident Response

- ☐ Incidents reported immediately using the 5-step framework
- ☐ All incidents logged in a case register

REVIEW

This policy will be reviewed annually or following a significant digital security incident, whichever comes first. All staff must sign and acknowledge receipt of this policy.

SIGNED: _____ NAME: _____ DATE: _____

Note: This Digital Security Policy should serve as a template that should be adopted and tailored to your specific organization.

HAUSA TRANSLATION

SASHE NA 10:**KIRKIRI MANUFAR
TSARONKU**

Wannan sashen ya bayyana muhimmancin samar da rubutacciyar manufar tsaron hanyoyin sadarwa na zamani da za ta jagoranci yadda kungiya za ta kare bayananta, da na'urorinta, da asusunta da kafafen sadarwa. Ya nuna cewa irin wannan tsari yana tabbatar da cewa dukkan ma'aikata suna bin ka'ida dāya, maimakon dogaro da yadda kowane mutum yake gudanar da kansa. Haka kuma, ya gabatar da samfurin manufa da kowace kungiya za ta iya daidaitawa gwargwadon bukatarta.

Sashen ya kuma lissafo muhimman abubuwan da ya kamata manufar ta kunsu, kamar amfani da kalmomin sirri masu karfi, Password Manager, 2FA, kare na'urori da bayanai, bin ka'idar 3-2-1 wajen ajiyar bayanai, amfani da Signal ko ProtonMail wajen sadarwa mai muhimmanci, da kuma bin tsarin mataakai biyar na magance matsalolin tsaro. Haka kuma, ya nuna cewa ya kamata a riƙa duba da sabunta manufar tsaron hanyoyin sadarwa na zamanin akai-akai domin ta ci gaba da dacewa da bukatun kungiya.

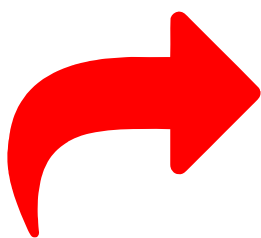
Acknowledgments & Next Steps

This Digital Civic Protection Toolkit was developed by the Open Knowledge Development Initiative (OKDI) as part of the Digital Resilience & Protection for Civic Actors in Northeast Nigeria project, 2026.

This final version, which follows a series of versions, incorporates recommendations adopted at the Co-Creation Workshop held on 27 June 2026 in Gombe State, attended by 27 participants from civil society organisations, youth activist groups, cybersecurity experts, translators, and media practitioners.

We are grateful to all participants who contributed their time, experience, and expertise to the creation and refinement of this resource.

How to Share and Adapt This Toolkit



This toolkit is free to share, adapt, and translate under a Creative Commons Attribution-noncommercial 4.0 International License (CC BY-NC 4.0). If you adapt it, please credit the Open Knowledge Development Initiative (OKDI) and share any improved versions with us so we can incorporate learning for future editions.

Contact	Details
Organisation	Open Knowledge Development Initiative (OKDI)
Address	No. 2, Gurama Plaza, Opposite Mazadu House Chamber, Buba Shongo, Gombe, Gombe State, Nigeria
Email	info@okdinitiative.org supportdesk@okdinitiative.org
WhatsApp / Support	+234 704 435 4546

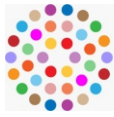
GODIYA DA MATAKAI NA GABA

Wannan Kayan Aikin Kariyar Jama'a ta hanyoyin sadarwa na zamani an kirkire shi ne daga Open Knowledge Development Initiative (OKDI) a matsayin wani bangare na aikin "Digital Resilience & Protection for Civic Actors in Northeast Nigeria" na shekarar 2026.

Wannan sigar karshe, wadda ta biyo bayan wasu sigogi da aka samar a baya, ta kunshi shawarwarin da aka amince da su a Taron Kirkira da Hadin Gwiwa (Co-Creation Workshop) da aka gudanar a ranar 27 ga Yuni, 2026, a Jihar Gombe. Mahalarta 27 daga kungiyoyin farar hula, kungiyoyin matasa masu fafutuka, kwararrun tsaron yanar gizo, masu fassara, da masu aikin kafafen yadda labarai ne suka halarci taron.

Muna godiya ga dukkan mahalarta da suka ba da lokacinsu, gogewarsu, da kwarewarsu wajen kirkira da inganta wannan kayan aiki.

Yadda Ake Rabawa Da Daidaita Wannan Kayan Aiki: Wannan kayan aiki kyauta ne domin a raba, a daidaita, kuma a fassara shi karkashin lasisin Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0). Idan an daidaita shi, a nemi a ba OKDI (Open Knowledge Development Initiative) yabo, kuma a raba sabbin fasalulluka da OKDI domin taimakawa fitowar da za a yi nan gaba.



Digital Democracy Initiative

DIGITAL CIVIC PROTECTION TOOLKIT

This bilingual (English and Hausa) toolkit provides practical guidance for improving digital safety, responding to cyber threats, and promoting secure digital practices among civil society organisations, youth activists, and grassroots civic actors in Northeast Nigeria.

Under the project:

**Digital Resilience and Protection for
Civic Actors in Northeast Nigeria**

Prepared by:

Open Knowledge Development Initiative

With support from:

CIVICUS under the Digital Democracy Initiative

