

Digital Safety Guide for Persons with Disabilities (PWDs)

Inclusive Cybersecurity Awareness | Kenyan Edition 2025

Introduction

Persons with disabilities (PWDs) in Kenya whether living in urban areas like **Nairobi, Kisumu, Mombasa**, or in rural counties such as **Busia, Kakamega, and Isiolo** are increasingly using the internet for communication, business, education, and social interaction.

However, PWDs also face unique digital safety risks due to:

- Reliance on assistive technologies or shared devices.
- Limited access to digital literacy training.
- Higher vulnerability to scams targeting their needs (e.g., “donation fraud” or fake disability grants).
- Social stigma and cyberbullying on public platforms.

This guide is tailored for persons with **physical, visual, hearing, and intellectual disabilities**, and for organizations or caregivers supporting them.

1. Use Strong Passwords with Assistive Tools

- Use password managers like **Bitwarden** (works well with screen readers).
- Avoid reusing one password across multiple sites like **MPESA apps, NHIF portals, or eCitizen**.
- Combine **capital letters, numbers, and symbols** (e.g., *Wanjiru@2025!*).

- Turn on **auto-lock** features in shared devices or phones used by multiple caregivers.

✓ If you struggle with typing, use **voice input** or **biometric login (fingerprint/face ID)** for apps like WhatsApp and banking platforms.

2. Prioritize Accessible, Safe Platforms

For Visually Impaired:

- Use platforms with **screen reader compatibility** like TalkBack on Android or VoiceOver on iPhone.
- Avoid apps/websites that do not support **labelled buttons** or **alt-text for images**.

For Hearing Impaired:

- Enable **automatic captioning** on YouTube, Zoom, or TikTok.
- For video calls, use apps that allow **text chat** as backup (e.g., WhatsApp or Telegram).

📱 Organizations like *InAble Kenya* and *Sightsavers* advocate for accessibility standards. Use their materials when choosing apps.

3. Watch Out for Common Scams Targeting PWDs in Kenya

Scam	Example
Fake grant offers	"NCPWD is giving 10K to all registered PWDs. Send 200 via MPESA to apply."
Romance scams	Scammers pretending to be interested in you then asking for help, airtime, or money.
Job scams	Fake NGOs offering jobs for disabled persons demanding a "registration fee."

Tech support fraud	Callers claiming your phone or app has a virus and asking for remote access.
---------------------------	--

✓ How to stay safe:

- Verify all opportunities via **official websites or verified social media pages** (e.g., @ncpwd_ke).
 - Never send money to unknown individuals via MPESA or WhatsApp.
 - Call **100 (Safaricom)** or **456 (Airtel)** to confirm sender authenticity.
 - Report to **333** (Safaricom fraud line) if you receive a scam SMS.
-

4. Adjust Privacy & Security Settings for Inclusion

- On **Facebook**: Set profile visibility to "Friends" only. Disable "Face Recognition".
- On **WhatsApp**: Go to **Settings** → **Privacy** → Set "Profile Photo" and "Status" to "My Contacts".
- Use **Google Voice Typing** for easier text input (helpful for people with limited mobility).

For public computers (e.g., in a **community centre or cyber café**), ensure you always **log out fully**, and **never save passwords**.

5. Children with Disabilities & Online Safety

Children and youth with disabilities are especially at risk of:

- **Online grooming or exploitation.**
- **Cyberbullying due to speech or physical impairments.**
- **Being excluded from digital safety lessons in school.**

What to do:

- Use **parental controls** on YouTube, TikTok, and browsers.
 - Join **child-friendly platforms** like “YouTube Kids” with accessible content.
 - Talk openly about unsafe online behaviors and how to seek help.
 - Work with special needs schools or organizations like **Little Rock Kenya** to include digital safety in learning.
-

6. Mental Health and Online Harassment

PWDs, especially those with psychosocial or intellectual disabilities, may face:

- Insults or discrimination in comment sections.
- Emotional harm from trolls or fake relationships.

Don't suffer in silence. You can:

- Block and report the bully.
 - Talk to a trusted caregiver, teacher, or community leader.
 - Call mental health support like **254 Mental Health** or **Chiromo Hospital Group**.
 - Reach out to NGOs like **Basic Needs Basic Rights Kenya**.
-

7. How to Report Online Abuse

If you experience **harassment, fraud, impersonation, or threats**:

Step-by-step:

1. Take **screenshots** of messages, profiles, or MPESA transactions.

2. Save **phone numbers or profile URLs** of the offender.
3. Report to:
 - **Safaricom fraud line (333) or call 100**
 - **Facebook/Instagram Report button**
 - **Nearest Police Station or DCI Office**
 - **Email: cybercrime@dci.go.ke**
4. Get an **OB number** and follow up every week.

Organizations that can help:

- **NCPWD Legal Aid** – www.ncpwd.go.ke
- **HEDSO**
- **Kenya Union of the Blind**
- **Sense International Kenya**

8. Resources Available in Kenya

Resource	Contact
National Council for Persons with Disabilities (NCPWD)	Call: 020 260 5076 / SMS: 21514
Safaricom Fraud Report	SMS “fraud” to 333
Kenya DCI Cyber Unit	cybercrime@dci.go.ke
InAble Kenya	www.inable.org
Article 19 East Africa (Digital Rights)	www.article19.org

Final Thoughts

“Disability is not inability even online.”

With the right tools, information, and support, persons with disabilities in Kenya can use digital platforms safely, confidently, and with dignity.

 **Speak out. Stay safe. Report abuse. Share this guide.**