Protecting Your Privacy on Social Media Platforms

Kenyan Digital Safety Guide | June 2025 Edition

Why Social Media Privacy Matters in Kenya

From Facebook groups for *"Buy and Sell Busia"* to TikTok influencers, Kenyans are increasingly using social platforms to connect, do business, and express themselves. But with every post, like, or share, you leave a **digital footprint** one that fraudsters, hackers, and stalkers can misuse.

This guide helps you control what others can see, protect your personal information, and stay safe on social media platforms like **Facebook**, **Instagram**, **TikTok**, **X (formerly Twitter)**, **WhatsApp**, and **LinkedIn** especially in the **Kenyan context**.

---

1. Limit What You Share Publicly

Avoid posting:

- Full names of children or relatives.
- Photos of your national ID, passport, KCSE/KCPE certificate.
- MPESA screenshots with balances or PayBill details.
- Your **location in real time** (e.g., "Huko Gikambura sahi!").
- Phone numbers, exact addresses, or places of work unless it's a business profile.

> ✋🏾 Remember: Even if you're just showing off your plot or car in Syokimau, someone could be planning a scam, robbery, or identity theft.

---

2. Lock Down Your Privacy Settings

Facebook

- Go to **Settings** → **Privacy** → Limit who sees your posts to “Friends” only.
- Set your **friends list to private**.
- Turn off **face recognition**.
- **Review tagged posts** before they appear on your timeline.
- Disable location access in your phone’s Facebook app.

Instagram

- Set account to **Private** if it’s not for business.
- **Approve followers manually**.
- Don’t allow reposts of your stories unless you trust the audience.

X / Twitter

- Make your account private or **limit replies** to followers.
- Be cautious with viral threads. Scammers target public commentators.

WhatsApp

- Go to **Settings** → **Privacy**
    - Set **Last Seen**, **Profile Photo**, **About**, and **Status** to “My Contacts” or “Nobody”.
    - Turn on **2-Step Verification**.
- Be wary of WhatsApp groups with unknown members (like alumni or political groups).
- **Leave group chats** where fraud, chain messages, or adult content is shared.

---

3. Enable Two-Factor Authentication (2FA)

This adds a **second layer of security** to your account beyond your password.

- Use it on **Facebook, Instagram, Gmail, and TikTok**.
- Prefer **app-based codes** like Google Authenticator over SMS if possible.
- For Gmail: go to myaccount.google.com/security

---

4. Watch Out for Fake Accounts and Catfishing

Kenya has seen rising cases of:

- Fake Facebook pages posing as NGOs, job companies, or celebrities.
- “Sugar Mummy/Daddy” scams via Facebook, TikTok, or Telegram.
- Romance scammers targeting single women and men via Instagram or LinkedIn.

Protect Yourself:

- Reverse-search profile pictures using Google Images.
- Don’t share intimate photos/videos with strangers online.
- Block and report suspicious accounts.
- Never send money, air time, or PINs to strangers you’ve never met.

---

5. Protect Your Photos and Videos

Your photos can be:

- **Cloned to create fake profiles**.
- Used in **blackmail scams or sextortion**.
- Taken out of context for **defamation** or **misinformation**.

Best Practices:

- Avoid posting kids in school uniforms (can reveal location).
- Watermark sensitive images.
- Avoid uploading every family or property detail online.

In Kenya, even TikTok or IG videos filmed outside your gate can help criminals plan.

---

6. Be Cautious With Check-ins and Location Sharing

- Turn off **automatic location tagging** in apps.
- Avoid posting **“Now at Java Garden City”** while still there.
- Don’t post your travel plans (e.g. “Kwisha, Nairobi till Monday!”) this tells robbers you're away.

---

7. Don’t Overshare in Facebook/Telegram Groups

- Avoid giving out phone numbers or IDs when applying for job ads in groups.
- Scammers often impersonate brands or employers and ask you to **“inbox your details”** this is how identity theft begins.
- Confirm the legitimacy of a group or post before engaging.

✅ Quick Do's and Don'ts for Social Media Privacy

DO:
✔️ Use strong, unique passwords
✔️ Enable 2FA (Two-Factor Authentication)
✔️ Limit who sees your content
✔️ Report and block suspicious activity
✔️ Educate friends and family about digital privacy

DON'T:
❌ Share personal information publicly
❌ Accept friend requests from strangers
❌ Post real-time locations
❌ Store passwords or ID photos in gallery/cloud
❌ Engage in viral challenges that ask for personal info (e.g., "What's your first car, favorite school, nickname?")

Useful Resources

Issue	Contact
Report fake accounts (Meta/Facebook)	facebook.com/help
WhatsApp impersonation	Report via the app or support.whatsapp.com
Online fraud in Kenya	SMS "fraud" to 333 (Safaricom)
Kenya Police Cybercrime Unit	www.dci.go.ke
Communications Authority	www.ca.go.ke

🇰🇪 A Safer Social Media Experience Starts With You

> "Ukipost, fikiria kwanza."
> Before you share, think about who might see it and how it could be misused.

Stay smart, stay secure, and help others around you do the same. Let's make Kenya's digital streets as safe as our homes.