

Comprehensive Guide to Staying Safe Online

Audience: General Public | **Context:** Kenya | **Version:** June 2025

Introduction

The digital world offers powerful tools for communication, learning, and business. But it also comes with risks of fraud, **misinformation**, **scams**, **cyberbullying**, and more. In Kenya, with the widespread use of **M-PESA**, **WhatsApp**, and **social media platforms**, it's important to understand how to protect yourself, your data, and your money.

This guide is for individuals, youth, businesses, and families across Kenya who want to stay safe and informed online.

1. Password Safety

- Use **strong passwords**: Combine uppercase, lowercase, numbers, and symbols.
Example: M@toke2025!
 - **Do not reuse** passwords across platforms.
 - **Use 2FA (Two-Factor Authentication)**: Always activate this on platforms like Gmail, Facebook, M-PESA apps, and online banking.
 - Avoid saving passwords in browsers on shared devices (e.g. in cyber cafés).
-

2. Mobile Money Safety (M-PESA & Others)

- Never share your **M-PESA PIN**, not even with Safaricom staff.
- Use **official apps** like M-PESA App or banking apps downloaded from the **Google Play Store** or **Apple App Store**.
- Confirm the number before sending any money.

- Do not accept help from strangers at M-PESA agents.
 - **Report fraud immediately** to Safaricom by dialing 100 or sending “fraud” via SMS to 333.
-

3. Device & App Security

- Install a **trusted antivirus** for your PC or Android phone (e.g., Avast, Kaspersky, Bitdefender).
 - Keep your software, apps, and operating system **updated**.
 - Avoid installing APKs from unknown sources.
 - Regularly **review app permissions** does a calculator really need access to your contacts?
-

4. Social Media Safety

- Avoid oversharing: Don't post your ID number, school details, home address, or travel plans.
 - Review privacy settings for **Facebook**, **Instagram**, and **TikTok**.
 - Don't click on suspicious links sent via DM or WhatsApp.
 - Report abusive users and block trolls or impersonators.
 - Watch out for **fake giveaways** no legit brand asks you to send money to “win” something.
-

5. Avoiding Phishing & Scams

- Don't click on links that look suspicious or contain errors like mpesa-supporte.com.

- Phishing often mimics official logos and language look closely at URLs and grammar.
 - Never submit personal info via unknown online forms.
 - Banks and mobile operators will never ask for your PIN or passwords via email or SMS.
-

6. Cyberbullying & Harassment

- Harassment on WhatsApp, TikTok, or Facebook can be **reported** and **blocked**.
 - Take screenshots and report the behavior to:
 - **DCI Kenya**: <https://www.dci.go.ke>
 - **KICTANet or Usiku Games** (organizations promoting digital rights in Kenya)
 - If it gets serious, report at a **Huduma Centre** or the nearest police station.
-

7. Children & Teen Online Safety

- Talk to your children about **safe online behavior**.
 - Install parental control apps like **Google Family Link**.
 - Teach them not to talk to strangers online or share photos/videos.
 - Encourage them to report if they are bullied or harassed.
-

8. Fake News, Hate Speech & Misinformation

- Always verify headlines and forwards via **trusted sources** like Nation, Citizen TV, or PesaCheck.
- Avoid forwarding unverified news or hate messages on WhatsApp.

- Misinformation can lead to arrests under Kenya's **Computer Misuse and Cybercrimes Act**.
-

9. Useful Resources

Service	Contact
Safaricom Fraud Hotline	100 or SMS "fraud" to 333
DCI Kenya – Cybercrime Unit	https://www.dci.go.ke
CA Kenya (Reporting Digital Harms)	https://www.ca.go.ke
Facebook/Instagram Reporting	Use in-app tools

10. Summary: Stay Safe, Stay Smart

- **Think Before You Click**
 - **Keep Your Info Private**
 - **Verify Before You Trust**
 - **Secure Your Devices**
 - **Report & Educate Others**
-

Proudly Made for Kenya

This guide was created for everyday Kenyans students, parents, businesses, and changemakers who use the internet to thrive. Help your community by **sharing this guide** and staying alert.