

PROJECT "DIGITAL RIGHTS FOR ALL" — LOMÉ, TOGO

PRACTICAL GUIDE TO ONLINE SAFETY

Using the Internet and social
media safely



NAFASI

magamba★

**DEFEND
DEFENDERS**



This guide was created as part of the "Digital Rights for All" project, led by JAIE in Lomé. It is aimed at young people and women who use the Internet, WhatsApp, Facebook or TikTok every day, and offers simple tips to protect themselves from scams, online harassment and the loss of their personal data.

It can be read alone, used during training workshops, or shared with family and friends. Key sections end with a "What to do?" box to remember.

1. Choosing and protecting your passwords

Your password is the first door protecting your accounts (WhatsApp, Facebook, e-mail, Mobile Money). If it is weak or shared, anyone can get in.

- Use a password of at least 8 characters, with letters, numbers and a symbol.
- Never use your date of birth, your name or "123456".
- Use a different password for each important account.
- Turn on two-step verification when it is offered (a code sent by SMS in addition to your password).
- Never share your password or the code you receive by SMS, not even with a relative or someone claiming to be an official agent.

What to do if my account is hacked?

- Change the password immediately, from another device if possible.
- Use the "hacked account" feature of the social network concerned.
- Warn your contacts that your account has been hacked, so they do not answer suspicious messages sent in your name.

2. Protecting your privacy on social media

What you post can be seen, copied and shared by people you do not know, even after it has been deleted.

- Set your accounts to "private" and regularly check who can see your posts.
- Think before posting a photo, a location or personal information (address, daily schedule).
- Do not accept friend or contact requests from strangers.
- Check the privacy settings of the apps you install.

3. Recognizing online scams

In Togo, fake announcements (auctions, job offers, contest prizes) regularly circulate on WhatsApp, Facebook and TikTok to steal money or personal information.

- Be wary of messages promising easy money, a job that pays too well or a surprise gift.
- No serious administration or company will ask for your PIN code, your password or an ID document by simple message.
- Always check the information on the official website of the organization concerned before believing it or paying "file fees".
- Do not click on links sent by strangers, even if they look urgent or official.
- If a message pressures you to act "immediately", it is often a sign of a scam.

What to do when facing a scam?

- Do not reply, do not pay, do not share the message.
- Report the message on the cert.tg website, under "Report an incident".
- If you have already paid or shared information, immediately contact the police (117) and your Mobile Money operator.

4. Dealing with cyberbullying

Cyberbullying means repeated messages, mockery, threats or insults online. It particularly affects girls and women. It is never the victim's fault.

- Keep evidence: take screenshots of the messages before blocking the person.
- Block and report the person or the account on the app concerned.
- Talk to someone you trust (parent, teacher, JAIE facilitator) rather than facing the situation alone.
- Do not respond to provocations: this generally does not stop the harasser.

What to do in case of harassment or serious threats?

- Keep the evidence (screenshots, dates, account names).
- Report the account to the platform and block it.
- In case of threats, blackmail or sharing of intimate images, contact the police (117) and JAIE to receive support.

8. Need help? Who to contact

Situation	Who to contact	How
Scam, hacking or cybersecurity incident	CERT.tg — National Cybersecurity Incident Response Centre	Website cert.tg, "Report an incident" section, or incidents@cert.tg
Emergency, threat, theft, assault, serious harassment	Police / Gendarmerie	Free call to 117 (24/7)
Content targeting you (harassment, photo shared without consent, fake account)	The platform concerned (Facebook, WhatsApp, TikTok...)	Use the "Report" button on the post or profile
Need someone to listen, advice or support	JAIE — Active Youth for Integration and Education	Focal point of the "Digital Rights for All" project, Lomé



Sources: CERT.tg
(Togo National Cybersecurity Incident
Response Center, cert.tg); official
emergency numbers in Togo (Police or
Gendarmerie: 117).

This guide was developed by JAIE as
part of the “Digital Rights for All”
project, Lomé, 2026.

