



Digital Literacy 101

Staying safe, smart, and kind online

SECTION 1
Online Scams

SECTION 2
Privacy & Footprints

SECTION 3
Cyberbullying

About this guide

Why we made this

We use phones, WhatsApp, TikTok and Facebook every day. The same tools that help us learn and stay connected can also be used to cheat us, bully us, or steal from us. This is the stuff we wish someone had explained to us earlier – written by students, for students.

How to use it

Read it once. Keep it. Share it with a friend or a younger sibling. There are three sections – Scams, Privacy, and Cyberbullying. Each one follows the same simple path:

1. Understand

What the danger actually is, in plain words.

2. Spot

The warning signs and red flags to watch for.

3. Act

Exactly what to do, step by step.



Made by

The Giiyo STEM Club at Olive Bilingual School, Bonaberi
– students from Form 4 to Upper Sixth.

WHAT'S INSIDE

Contents



1

Online Scams

What a scam is · How to spot one · What to do if you're targeted

p.4

2

Privacy & Digital Footprints

Your digital footprint · Who can see it · How to protect yourself

p.8

3

Cyberbullying

What it is · What to do if it happens · How to help a friend

p.12

★ Stay safe online — three things to remember

p.16

SECTION ONE

Online Scams

How to recognise them
and what to do

AUTHORS

Adrian German — 1ère
Christy Helloise — 2nde
Princesse Marie — 2nde
Ebolo Ethan — Tle
Fonkeu Darelle — 1ère
Keumejeu Alvine — 2nde



1

What is a scam?

A scam is a trick used to steal your money, your information, or your trust. The scammer pretends to be someone they are not, lies, or makes a promise that is too good to be true.



A scammer might...

- Tell you that you won a prize or a lottery
- Offer a job that pays a lot for almost no work
- Pretend to be your bank, MTN, or Orange
- Pretend to be a friend or relative in trouble

In short: a scam is when someone cheats you on purpose, for their own benefit.

COMMON IN CAMEROON

- Fake Mobile Money alerts — “You received 50,000 FCFA, confirm with this code...”
- Fake scholarships, job offers, or visa assistance
- “You won a phone!” texts that ask for a small fee to claim it
- WhatsApp messages from “a relative abroad” asking for urgent money

How to spot a scam

- 1 You were contacted out of the blue.** Unexpected calls, SMS or WhatsApp messages asking for personal details or money should always raise suspicion. A real bank will never ask for your PIN, password, or OTP code.
- 2 The contact details are vague.** Real companies have a real office, phone number and email. Scammers often use a WhatsApp number with no photo, no website, and no address.
- 3 You are being rushed.** “Confirm in 5 minutes or lose your account!” Urgency is a scammer’s favourite weapon. A real company gives you time to think.
- 4 They ask for secrets or strange payments.** Never share your password, Mobile Money PIN, or verification code — not even with someone claiming to be from MTN, Orange, or your bank.

THE GOLDEN RULE

If a message creates fear or excitement and then asks you to **act fast** or **share a code** — stop. Slow down. Ask someone you trust before doing anything.



Red flags & what to do

Red flags

- **Too good to be true:** “Double your 10,000 FCFA in 24 hours!” No real investment works like that.
- **Bad grammar & spelling:** strange capital letters, typos, awkward phrasing.
- **Strange links:** *mtn-cameroun-promo.net* is not mtn.cm. Check addresses carefully.
- **Empty profiles:** new account, no photo, no posts, few friends.

If you are targeted

1. Don't reply. Don't send money, airtime, or any code.
2. Screenshot everything: message, number, date, time.
3. Block the number or account.
4. Report it: on WhatsApp: open the chat → Report. Same on Facebook, Instagram, TikTok.
5. Tell someone. If money was lost, tell your parents and the nearest police station.



Being scammed is not your fault. Scammers are professionals.
Speaking up protects the next person.

SECTION TWO

Digital Footprints

2

What you leave behind online
and how to protect it

AUTHORS

Nembu Maxwell — Form 4 Science Kammogne

George — Form 4 Science

Foahom Ethan — Form 4 Science Kotta

Caroline — Form 4 Science



What is a digital footprint?

Your digital footprint is the trail of information you leave on the internet through everything you do online — posts, likes, photos, searches, app downloads, and comments.

Two Types

Active: what you post on purpose: a photo, a comment, a video.

Passive: what is collected without you noticing: your location, your browsing history, the ads you click.

Why it matters

Your footprint can be seen by apps and websites, future employers and universities, and complete strangers — including people with bad intentions. Once something is online, it is very hard to fully remove. A photo posted today can resurface in a job interview in ten years.

Controlling your footprint protects you from identity theft, harassment, scams, and embarrassment.

Who can see it & how to take control



Who can see it

- Apps build a profile of you — age, interests, location, friends — and sell it to advertisers.
- Websites track your activity through cookies.
- Public posts can be seen by anyone, forever. Even a deleted post may already be screenshotted.
- Bad actors use public information to scam, blackmail, or impersonate people.

How to take control

- One **strong, different password** for each account. A password manager helps you remember them.
- Turn on **two-factor authentication (2FA)**, the single most effective step you can take.
- Check app permissions. Does that flashlight app really need your contacts?
- Be careful on public Wi-Fi. Don't log into your bank or Mobile Money on open networks.
- Keep your phone and apps updated, updates fix security holes.



Five things you can do this week

- 1 Turn on 2FA. On WhatsApp: Settings → Account → Two-step verification. Do the same for Facebook, Instagram, Gmail and TikTok.
- 2 Do a privacy checkup. Set your Instagram, TikTok and Facebook profiles to private. Review who can see your posts, stories and friend list.
- 3 Clean up your passwords. If you use the same password everywhere, change it — especially for email. Your email is the key to everything else.
- 4 Check your app permissions. Phone Settings → Apps → Permissions. Remove access for apps that don't need your location, contacts, microphone or camera.
- 5 Think before you post. Would you want your parent, your teacher, or a future employer to see this? If not, don't post it.



Your information is yours. Protect it.

SECTION THREE

Cyber Bullying

What it is, how to respond,
and how to help a friend

AUTHORS

Moh Joshua — Form 4 Science

Clyde Che — Form 4 Science

Ndipnu Yannick — Upper Sixth Science



What is cyberbullying?

Cyberbullying is the repeated and deliberate harm done to another person through phones, computers, or any digital device. It is not a one-time argument or a joke between friends, it is repeated behaviour meant to hurt, shame, or isolate someone.

Common forms

- **Trolling:** insults or cruel comments to provoke a reaction
- **Rumours:** spreading false information in group chats
- **Exposure:** posting embarrassing photos without permission
- **Harassment:** repeated threatening or hateful messages
- **Exclusion:** deliberately leaving someone out
Impersonation – fake accounts to mock or shame someone

Why it matters

Cyberbullying hurts just as much as face-to-face bullying – often more – because it follows you home on your phone. There is no escape from it at the end of the school day.

It can cause anxiety, depression, and in serious cases much worse. That is why it has to be taken seriously, every single time.

If you are being bullied

- 1** Don't retaliate. Answering back usually makes things worse, and can get you in trouble too.
- 2** Disengage. Log off. Change your privacy settings. Block the person on every platform.
- 3** Save the evidence. Screenshot the messages before they're deleted. Keep the date, time and username — this is your proof if you need to report.
- 4** Don't forward the messages. Sharing bullying content — even to complain about it — spreads the harm further.
- 5** Tell someone you trust. A parent, a teacher, an older sibling, or the STEM Club coordinator. You do not have to handle this alone.



You are not the problem. Bullies try to make you feel small so they can feel bigger.

If you see someone else being bullied



Being a bystander has power. What you do — or don't do — matters.

- 1 Document. Screenshot the harmful posts before they get deleted. Note the date, time and username of the bully.
- 2 Support the victim. Reach out privately. A simple “I saw what happened. Are you okay? It’s not your fault.” can change someone’s day. Victims often feel alone.
- 3 Don’t engage the bully. Don’t comment, argue or retaliate, that only gives the bully attention.
- 4 Report the content. Use the Report button on the platform — Facebook, Instagram, TikTok, WhatsApp. Every platform has one.
- 5 Tell a trusted adult. A teacher, a parent, or the STEM Club coordinator. If there are real threats, the school and parents must be told.



Silence protects the bully. Your action protects your friend.

REMEMBER THIS

Stay safe online

1

If it feels wrong, it probably is. **Trust that feeling.**

2

You are never alone. Tell **someone you trust.**

3

Your actions online matter, **for you, and for everyone around you.**



WHO TO TELL

A parent · A teacher · The STEM Club coordinator

