Defense Mode: teacher's guide

For teaching the "Defense Mode" class (24 slides, 40–45 minutes) with students aged 12 to 15. It covers sensitive topics (intimate images, fake profiles): read section 05 before teaching and coordinate with administration or the counseling office.

01 The tone that makes it work

This age group detects a lecture instantly and tunes out. The class is written in an **"insider" information tone, peer to peer**: how attackers think and how to shut the door on them. It works if the teacher delivers it as someone sharing valuable knowledge, not as someone handing down a rule. The closing flips the role: they go from protected to protectors of their family.

THE TEACHER'S GOLDEN RULE

On sensitive topics, never ask for personal experiences out loud, and always keep the no-blame path to help visible. The goal is for anyone already in trouble to know they can get out — not to sink deeper into silence.

02 What's in the package

FILE	WHAT IT IS	USE
Slide deck 12–15 (.pptx)	24 slides with teacher notes on each one ("Presenter" view).	Project
This guide	Agenda, handling sensitive topics and frequently asked questions.	Read beforehand
Activity sheet 12–15	2 pages: the suspicious DM, the red flags and the 7-Day Challenge.	Print 1 per student
Online resources	"Real or scam?" simulator, quiz and Hacker Academy at guiadeunhacker.com/en/.	Share / homework

03 Preparation

- Go through the 24 slides reading the notes (the ones on slides 13 and 15 are mandatory).
- **Coordinate beforehand with administration or the counseling office:** make sure they know intimate images and fake profiles will be discussed, and confirm the referral path if a student discloses a situation.
- Check your local law on the distribution of intimate images of minors so you can answer precisely if asked (slide 13 mentions that forwarding can be a crime).
- Print one activity sheet per student.

04 Class agenda (40–45 minutes)

TIME	SLIDES	BLOCK	TEACHING KEY
0–6 min	1–4	**Opening.** Your life on your phone; "nobody would attack me"; hackers vs. criminals; the map of the 5 fronts.	The NYC traffic-lights anecdote (slide 3) hooks them: tell it as a story. The map on slide 4 is the promise of the class.
6–14 min	5–8	**Front 1: accounts.** The old-game domino effect, the faceb00k test, MFA, and phone theft.	On slide 6, have them vote before revealing. The challenge of turning on MFA that afternoon (slide 7) can be verifiable homework.
14–20 min	9–10	**Front 2: messages.** The 3 baits (prize, rush, story) and the link's disguises (shortened, QR).	Ask who received any of the 3 baits this month: the hands make the point on their own.
20–28 min	11–13	**Front 3: footprint and images.** The past gets indexed; a sent photo is no longer yours; the rule of three.	SENSITIVE. Deliver slide 13 in a calm tone, no anecdotes, and the light-blue closing (help without blame) is ALWAYS read out loud. Don't open a debate about cases.
28–34 min	14–15	**Front 4: fake people.** A profile can lie about its age; the 4 red flags.	SENSITIVE. Flags as observable behaviors, without describing scripts. Repeat: any one of the 4 = cut off and tell, and it is never the fault of the person it happened to.
34–40 min	16–19	**Front 5 + plan B.** Whoever forwards is part of it; the one who stops it; deepfakes; the protocol if it already happened.	"Gasoline or fire extinguisher?" gives the bystander an active identity. The family anti-deepfake codeword is homework.
40–45 min	20–24	**Closing.** 7-day challenge, review of the fronts, resources, "the one who protects", habit.	Review with the screen covered. End by asking "what will your day 1 be?" and listen to three answers.

SHORT VERSION (25 MINUTES)

Slides 1–2, 4, 5–7, 9, 12–13, 15, 19 and 24: opening, accounts, baits, images with the rule of three, red flags, protocol and closing.

05 Handling the sensitive topics (slides 13 and 15)

- **Do not ask for personal experiences** or allow the group to point to classmates' cases. If someone alludes to a real case, cut it off respectfully and return to the general level.
- **Pattern language:** behaviors are named (asks for secrets, asks for images, rushes, suggests meeting alone); manipulation scripts or harm scenarios are never described.
- **The no-blame path to help is always said in full:** it's not your fault, don't delete anything, tell a trusted adult today. It's the sentence that can change the outcome for someone already in trouble.
- **If a student discloses a situation** (in class or afterwards): validate in one sentence, don't probe in public, talk in private, refer according to protocol, and never promise secrecy — do promise support.
- **If a situation involves intimate images of minors**, do not request or review them: evidence preservation is directed by administration and the competent authorities.

06 Frequently asked questions from students

"IS IT WRONG TO BE ON SOCIAL MEDIA / PLAY ONLINE?"

No. The class doesn't demonize the tool: it teaches how to use it with the doors closed. The useful comparison: driving isn't wrong; driving without a seatbelt is.

"WHAT IF I ALREADY SENT A PHOTO?" (OUT LOUD OR IN PRIVATE)

Don't work through it in public. General answer: "if this already happened to someone, it's not their fault and there is a way out: a trusted adult, today". In private: listen, don't judge, refer according to protocol.

"WHY IS FORWARDING A CRIME IF I DIDN'T TAKE THE PICTURE?"

Because distribution is what does the damage, and every forward is a new act of distribution. The practical rule: another person's intimate image is never touched — not even to "show what's going on".

"CAN HACKERS BREAK INTO ANYTHING?"

In the movies. In real life, the vast majority of attacks exploit simple mistakes: reused passwords, hurried clicks, data given away. That's why the defenses in this class work.

07 Checklist

- [ ] I read the notes on all 24 slides (13 and 15 with special attention).
- [ ] I coordinated with administration/counseling and I know the referral path.
- [ ] I checked the local law on the distribution of intimate images of minors.
- [ ] I printed the activity sheets and I have the links to the online resources.