WHO ARE YOU REALLY?

SAFETY > 4.2 PROTECTING PERSONAL DATA AND PRIVACY

TARGET GROUP	AGE GROUP	PROFICIENCY LEVEL	FORMAT	COPYRIGHT	LANGUAGE
School drop outs, Students (primary school), Students (secondary school)	Children, Teenagers	Level 1	Activity sheet	Creative Commons (BY-SA)	English, French

This workshop focusses on being able to spot online impersonators who want to steal one's information. Participants practice their anti-phishing skills by acting out – and discussing possible responses to – suspicious online texts, posts, friend requests, pictures, and emails. This resource forms part of the "Cyber Heros" learning programme designed for 8 to 14 year olds.

General Objective	Skillset building
Preparation time for facilitator	less than 1 hour
Competence area	4 - Safety
Time needed to complete activity (for learner)	0 - 1 hour
Support material needed for training	• A copy of the worksheet cut into strips, with one scenario on each strip - A bowl or container to hold the strips (each group of students will pick one) - Phishing cheat sheet
Resource originally created in	French

WORKSHOP DIRECTIONS

1 Goals for students

- Recognize that their online audience might be bigger than they think.
- Confirm that they really know the identity of the people they talk with online.
- Stop and think before they “friend” or connect with someone online.
- Be careful about whom they give personal information to and what kinds of things they share.
- Ask questions and/or seek help from an adult if theyaren’t sure.
- Tell an adult if someone tries to discuss something online that makes them uncomfortable.
- Act with honesty in all their online interactions

2 Let's talk

How do you know it’s really them?

When you’re on the phone with your friend, you can tell it’s them by the sound of their voice, even though you can’t see them. The online world is a little different, though. Sometimes it’s harder to be sure someone is who they say they are. In apps and games, people sometimes pretend to be someone else as a joke, or to mess with them in a mean way. Other times, they impersonate people to steal personal information. When you’re on the Internet, people you don’t know could ask to connect with you. The safest thing to do is not to respond or to tell a parent or adult you trust that you don’t know the person trying to connect with you. But if you decide it’s okay to respond, it’s a really good idea to see what you can find out about them first. Check their profile, see who their friends are, or search for other information that confirms they’re who they say they are. There are multiple ways to verify someone’s identity online. Here are a few examples to get us started.

Note to facilitator:

You might consider leading a class brainstorm on the question “How do we verify a person’s identity online?” first; then continue the conversation with these thought starters.

• Is their profile photo suspicious?

Is their profile photo blurry or hard to see? Or is there no photo at all, like a bitmoji or cartoon

character's face? Bad photos, bitmojis, photos of pets, etc., make it easy for a person to hide their identity in social media. It's also common for scammers to steal photos from a real person in order to set up a fake profile and pretend to be them. Can you find more photos of the person with the same name associated?

• Does their username contain their real name?

On social media, for instance, does their screen name match a real name? (For example, Jane Doe's profile has a URL like SocialMedia. com/jane_doe.)

• Do they have a profile bio?

If so, does it sound like it was written by a real person? Fake accounts might not have much "About Me" information or might have a bunch of information copied or pulled together randomly to create a fake profile. Is there anything in their bio that you can confirm by searching for it?

• How long has the account been active?

Does the activity you see line up with your expectations? Is the profile new or does it show a lot of activity? Does the person have mutual friends with you like you would expect? Fake accounts usually don't have much content or signs of people posting, commenting, and socializing in them.

3 Activity

1. Groups review **scenarios**

Okay, now we're going to separate into groups. Each group will pick a scenario from this container and talk about how you should respond to this situation.

2. Groups act out scenarios

Now each group acts out its scenario: one student narrating, a second performing the "message," a third responding, maybe a fourth explaining the reasoning.

3. Class discusses groups' choices

Finally, let's use this cheat sheet to discuss each group's choices. Feel free to write more messages that you think would be even trickier. If you do, each group should share the messages they create with the

other groups.

4 Takeaway

You control whom you talk to online. Make sure the people you connect with are who they say they are!