DON'T BITE THE PHISHING HOOK!

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 safety on the internet. During the activity part, participants play a game where they study various emails and texts and try to decide which messages are legitimate and which are phishing scams. 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
Resource originally created in	French

WORKSHOP DIRECTIONS

1 Goals for students

- Learn techniques people use to steal identities
- Review ways to prevent identity theft.
- Know to talk to a trusted adult if they think they're a victim of identity theft.
- Recognize the signs of phishing attempts.
- Be careful about how and with whom they share personal info.

2 Let's talk

What is this phishing thing, anyway?

Phishing is when someone tries to steal information like your login or account details by pretending to be someone you trust in an email, text, or other online communication. Phishing emails – and the unsafe sites they try to send you to or the attachments they try to get you to open – can also put viruses on your computer. Some viruses use your contacts list to target your friends and family with the same, or a more personalized, phishing attack. Other types of scams might try to trick you into downloading malware or unwanted software by telling you that there's something wrong with your device.

Remember: A website or ad can't tell if there's anything wrong with your machine! Some phishing attacks are obviously fake. Others can be sneaky and really convincing – like when a scammer sends you a message that includes some of your personal information. That's called spearphishing, and it can be very difficult to spot because using your info can make it seem like they know you. Before you click on a link or enter your password in a site you haven't been to before, it's a good idea to ask yourself some questions about that email or webpage.

Here are some questions you could ask:

• Does it look professional like other websites you know and trust, with the product's or company's usual logo and with text that is free of spelling errors?

• Does the site's URL match the product's or company's name and information you're looking for? Are there misspellings?

• Are there any spammy pop-ups?

• Does the URL start with https://with a little green padlock to the left of it? (That means the connection is secure.

• What's in the fine print? (That's often where they put sneaky stuff.)

• Is the email or site offering something that sounds too good to be true, like a chance to make a lot of money? (It's almost always too good to be true.)

• Does the message sound just a little bit weird? Like they might know you, but you're not completely sure? And what if you do fall for a scam?

Start with this: Don't panic!

• Tell your parent, teacher, or other trusted adult right away. The longer you wait, the worse things could get.

• Change your passwords for online accounts.

• If you do get tricked by a scam, let your friends and people in your contacts know right away, because they could be targeted next.

• Use settings to report the message as spam, if possible.

3 Activity

1. Groups study examples

Let's divide into groups, and each group studies these examples of messages and websites from the **worksheet**

2. Individuals indicate choices

Decide “real” or “fake” for each example, and list reasons why below it.

3. Groups discuss choices

Which examples seemed trustworthy and which seemed suspicious? Did any answers surprise you? If so, why?

4. Further discussion

Here are some more questions to ask yourself when assessing messages and sites you find online:

• Does this message look right? What’s your first instinct? Do you notice any untrustworthy parts? Does it offer to fix something you didn’t know was a problem?

• Is the email offering you something for free? Free offers usually aren’t really free.

• Is it asking for your personal information? Some websites ask for personal info so they can send you more scams. For example, quizzes or “personality tests” could be gathering facts to make it easy to guess your password or other secret information. Most real businesses won’t ask for personal information over email.

• Is it a chain email or social post? Emails and posts that ask you to forward them to everyone you know can put you and others at risk. Don’t do it unless you’re sure of the source and sure the message is safe to pass on.

• Does it have fine print?
At the bottom of most documents you’ll find the “fine print.” This text is tiny and often contains the stuff you’re supposed to miss. For example, a headline at the top might say you’ve won a free phone, but in the fine print you’ll read that you actually have to pay that company $200 per month. No fine print at all can be just as bad, so pay attention to that too.

Note: *For the purposes of this exercise, assume that Internaut mail is a real, trusted service.*

4 Answers to worksheet

1. Real. The email asks the user to go to the company’s website and sign into their account on their own, rather than providing a link in the email or asking them to email their password (links can send users to malicious websites).

2. Fake. Suspicious and not secure URL

3. Real. Note the https:// in the URL

4. Fake. Suspicious offer in exchange for bank details

5. Fake. Not secure and suspicious URL

5 Takeaway

When you’re online, always be on the lookout for phishing attacks in emails, texts, and posted messages—and make sure you tell the right
people about it if you do get fooled.