CYBER

CONSCIOUS YOUTH BEHAVIOURS IN EMERGING REALITIES

Non-formal education practices:

Phishing

R2 CYBER TOOLKIT

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

#9	**Something Is Phishy**
Threat(s)	Phishing
	Phishing attacks often involve fraudulent e-mails, messages, or websites designed to impersonate legitimate organisations, such as banks, social media platforms, or government agencies. These deceptive communications typically prompt recipients to disclose confidential information, such as login credentials or financial account numbers, under false pretences. Cybercriminals use this stolen information to commit identity theft, financial fraud, or other malicious activities, posing significant risks to individuals' privacy (Identity Theft and Fraud), finances, and online security.
Typology	*Simulation exercises*
Duration	In minutes 2x40
Modality	*In-presence [classroom setting]*
Aim	This lesson shares how scammers can attempt to obtain personal information through phishing. Many times, electronic communication, such as emails and text messages, can appear to be coming from a trustworthy source, but they are actually fraudulent.
Learning Objectives	After participating in this lesson, adult learners will be able to: • Identify the characteristics of trustworthy electronic communication • Explain the importance of knowing how to avoid phishing attempts • Distinguish between legitimate and fraudulent messages and phishing attempts
Trainee profile	13-17 years
n° participants	Ideally up to 20 participants, or students of a maximum of one class.
Materials	The following materials and supplies are needed for this lesson: • Phishing examples (see in annex, or you can print the next examples here - source: https://blog.usecure.io/the-most-common-examples-of-a-phishing-email#Email-account-upgrade-scam)
Preparation	In preparation for this lesson, facilitators should: • Review lesson plan • Print phishing examples
Implementation	**Terminology:** The following terms will be discussed during the lesson: • **Password**: a combination of keyboard letters, numbers, and characteristics that must be entered to gain admission into many online services (e-mail, social media accounts, online shopping accounts, etc.)

- **Phishing**: the fraudulent attempt to obtain sensitive information such as usernames, passwords, and credit card details by disguising as a trustworthy entity in an electronic communication

Background Information:

Implementation: (10 minutes)

Phishing is a fraudulent attempt to obtain sensitive information such as usernames, passwords, and credit card details by disguising as a trustworthy entity in an electronic communication. Many times, these emails or text messages appear if they are coming from a legitimate source and usually have a sense of urgency. Links in phishing emails typically take the user to an untrusted website to enter sensitive information. Risks associated with phishing attempts include people obtaining your passwords, impersonating you to access your bank account and other financial services, purchasing items online, people impersonating you in social media networking sites, and accessing private information on your computer.

Activity 1: What is Phishing?
Distribute examples of phishing.

Work in groups (20 minutes) - divide the students into small groups of 4 students and give them phishing examples (see attachment). The students have the task of describing individual examples, whether it is a fraud or not. If so, why?

Presentation of students' results - (20 minutes)

Clarifying and explaining - (10 minutes)

Activity 2: Dealing with Phishing Attempts
Why is it important to avoid phishing attempts? For example one city employee sent over the city's banking information, and the cybercriminal was able to transfer nearly 800,000 Eur from the account before someone realised the mistake. While the city does have insurance and the scam was reported to the authorities, it is unlikely that all of the money can be recovered. While this example applies to a city, anyone can be a victim of a phishing attempt.
Use the flip chart and markers to collectively brainstorm actions to take if you experience a phishing attempt. (10 minutes)

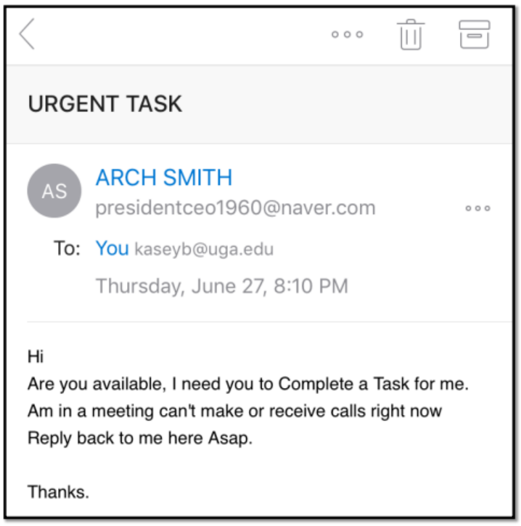
Examples include:

- Not clicking on any links or downloading any attachments. They might contain viruses or spyware.
- Don't reply to the e-mail or text message.
- Mark/categorise the email as "junk" or "spam".

	• If the email references an account and you are concerned about that account, call the company. However, do not use any of the contact information in the email or text. Many times, these criminals create fake phone numbers. Verify the company's contact information elsewhere first. • Report the phishing e-mail to officials. **Activity 3: Spot the Phishing Attempts** Quiz to verify knowledge - (10 minutes) you can run it for everyone, each student can do it individually and then we share the results together. While the intent is for the activity to build privacy and security skills related to technology, it is important for the facilitator to lead a debrief discussion at the end of the lesson. Potential debrief questions could include: • What are some characteristics of trustworthy electronic communications? • What are some characteristics of fraudulent electronic communications? • Why is it important to know how to avoid phishing attempts? • What should you do if you receive an email or text that you think is fraudulent?
Tips and hints	We recommend doing phishing tests with the students at the end of the lesson. The link is here: https://phishingquiz.withgoogle.com/. https://phishingquiz.withgoogle.com/?hl=en https://www.proprofs.com/quiz-school/topic/phishing It is a very good reflection on the acquired knowledge.
Safety measures	-
External reference and Resources	• https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams •https://www.commonsense.org/education/digital-citizenship/lesson/dont-feed-the-phish • https://georgia4h.org/wp-content/uploads/Something-is-Phishy.pdf
Partner/ Author	CPM- Centrum Prevencie Mladeze Slovakia

Annex.

Distribute examples of a phishing email and a phishing text.



URGENT TASK

ARCH SMITH
presidentceo1960@naver.com

To: You kaseyb@uga.edu

Thursday, June 27, 8:10 PM

Hi
Are you available, I need you to Complete a Task for me.
Am in a meeting can't make or receive calls right now
Reply back to me here Asap.

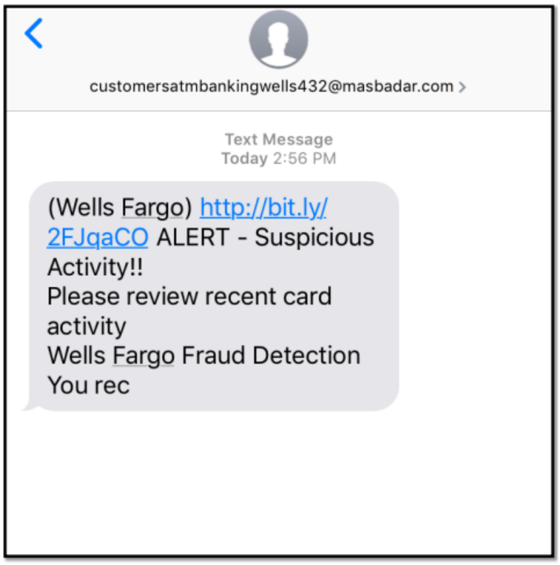
Thanks.

Explain the following for the e-mail message:

The employee (who works for the University of Georgia) received this e-mail message. Her supervisor is Arch Smith, so she regularly receives emails from him. However, after further investigation, there are some suspicious things about this message:

- While the email is from "Arch Smith," the sent e-mail address does not indicate that Arch sent the message. Since the correspondence is related to work, it's also suspicious that it did not come from an email account associated with the University of Georgia.
- The spelling, grammar, and mechanics of the email raise concerns. Words are capitalised that should not be. Punctuation and grammar are incorrect in some instances.
- The email isn't actually signed from Arch Smith. Most emails end with some sort of closing and signature.
- The email seems very urgent and does not specifically cite why things are urgent. The sender also is not able to take phone calls (which would be considered a 'normal' practice in an emergency situation).

Explain the following for the text message:



customersatmbankingwells432@masbadar.com >

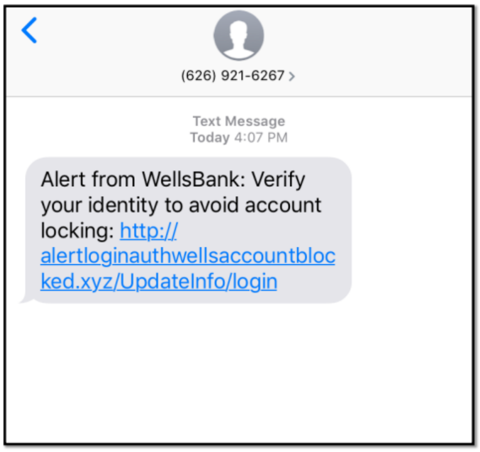
Text Message
Today 2:56 PM

(Wells Fargo) http://bit.ly/2FJqaCO ALERT - Suspicious Activity!!
Please review recent card activity
Wells Fargo Fraud Detection
You rec

Explain the following for the text message:

The person banks with Wells Fargo and sometimes gets email updates from the bank. However, after further investigation, there are some suspicious things about this message:

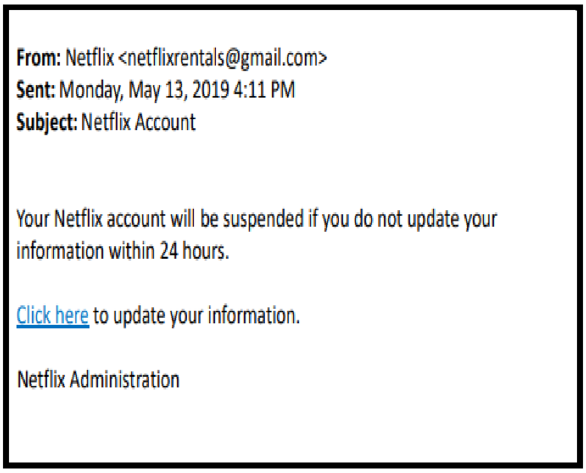
- The sender of this message uses the email address customersatmbankingwells432@masbadar.com. It does not appear to be a legitimate e-mail address associated with Wells Fargo.
- The link embedded in the message is a bigly url. Bigly is a service that shortens urls – not showing the complete website url. While many groups use these services, you should only click on the shortened url when you know the sender.
- The spelling, grammar, and mechanics of the text raise concerns. The message is not complete.



(626) 921-6267 >

Text Message
Today 4:07 PM

Alert from WellsBank: Verify your identity to avoid account locking: http://alertloginauthwellsaccountblocked.xyz/UpdateInfo/login



From: Netflix <netflixrentals@gmail.com>
Sent: Monday, May 13, 2019 4:11 PM
Subject: Netflix Account

Your Netflix account will be suspended if you do not update your information within 24 hours.

Click here to update your information.

Netflix Administration

A typical cases for obtaining your online banking data - Phishing is a fraudulent attempt to obtain sensitive information such as usernames, passwords, and credit card details by disguising as a trustworthy entity in an electronic communication. Many times, people who reply to these types of emails are asked to do something that does not keep them safe online. They may also be asked to click on a link and share information. For example, they may be asked to share their password, financial information, pin codes, or asked to send money or buy items (such as gift cards). Many times, timing is urgent because "suspicious activity has been detected" or "your account is locked" until further actions.

Some features of a phishing email include:

- Needing to verify account information (ex. e-mail account, banking account, money transfer account, etc.). Many times, the email says your personal information has expired or needs to be verified.
- Link in the e-mail/text or attachment. Usually, the link does not provide you with the URL, so it's hard to determine what website it will redirect you to. Regardless, only click on links from reputable senders.
- Sense of urgency. Many times, phishing emails give you a limited amount of time (ex. 24 hours) to resolve a "problem" that doesn't exist.
- Too good to be true. Phishing emails could promise some sort of "return" such as cash or gift cards if you do something first (usually giving them personal/sensitive information).
- Spelling, grammar, and/or mechanics errors. An occasional typo sometimes happens in a legitimate e-mail, but an excessive amount of errors includes a phishing email.
- Length. Some phishing emails can tend to be short. Others may be very long, explaining a circumstance (ex. why this person can't do something and why they need your help).
- Generic greeting. Many phishing emails don't have a greeting or simply start with 'hello.'

Conscious Youth Behaviours in Emerging Realities

Erasmus+ KA2 Cooperation Partnerships in School Education

[Reference n. 2023-1-EL01-KA220-SCH-000156982]

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.