UNUSUAL ACTIVITY EMAIL SCAM

PART 1

Stephan is in his early 70s. He was working at a local college for many years, but retired six months ago. Some of his former students are still in touch with him through email and he helps them out from time to time.

CHALLENGE 1

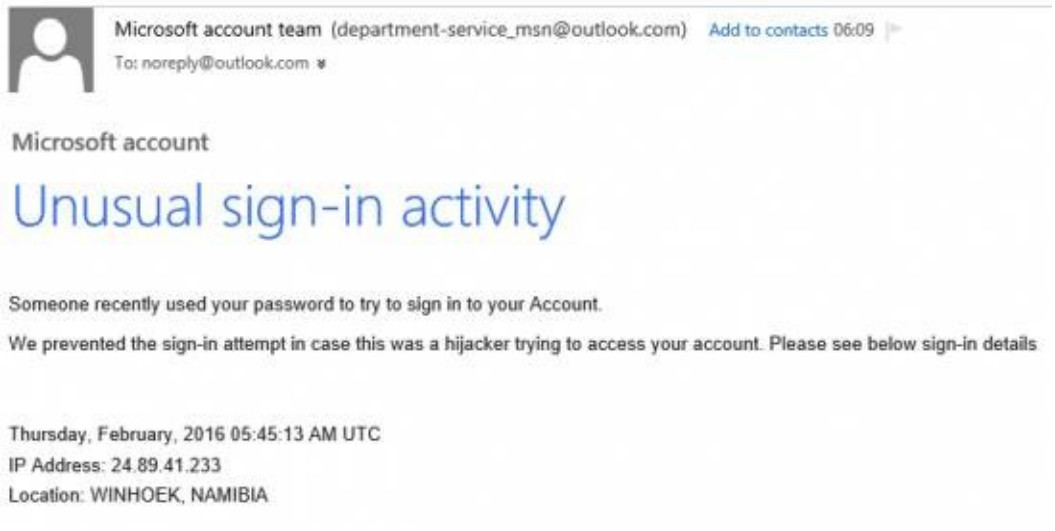
What is the best kind of password for your email account?

a) a password that you can easily remember like date of birth
b) a password that is a combination of your name and date of birth
c) a password with uppercase and lowercase letters and special characters.
d) none of the above

ANSWER: c - a password with uppercase and lowercase letters and special characters

PART 2

He recently received an email informing him of unusual activity from his account.



Challenge 2

How can you protect against someone else hacking your account?

Fill in the blanks with the words in the box

software	wifi	authentication	reputable	strong

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission under the Erasmus+ Programme. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein. [Project Number: 2021-1-ER01-KA220-ADU-000023422]

1. Use a _____ password.
2. Enable two-factor _____
3. Keep your _____ updated.
4. Avoid using public _____
5. Use a _____ email service provider

ANSWER: 1 - strong, 2 - authentication, 3 - software, 4-wifi, 5-reputable

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission under the Erasmus+ Programme. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein. [Project Number: 2021-1-ES01-KA220-ADU-000023422]

1. ONLINE BANKING

1.1. Introduction

Our characters are two seniors, one male and one female. They are in the living room in front of their computer (together if it is easier) and they are connecting to their online banking account (we can see it on the screen).

Introduction: Meet Martin & Maria, they have just come back from their bank where they received explanations on how to create and activate their online banking profile. They are very excited and curious; today is the first time they connect. Can you help Martin & Maria to use their online banking account safely and appropriately?

https://www.freepik.com/free-vector/online-banking-concept-illustration_33530845.htm#query=bank%20online&position=13&from_view=search&track=sph

Step 1

Maria receives an email from her bank asking for the validation of her credit card number and code. She receives it the same day when Martin and her connect to their online banking account for the first time.

The e-mail reads:

From: National bank: nationalbank @ mhswt.com

To: Maria: maria @ yahoo.com

Dear Maria,

We are happy that you are our client. We had a problem with our system, you are obliged to confirm your credit card number and code.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission under the Erasmus+ Programme. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein. [Project Number: 2021-1-ES01-KA220-ADU-000034423]

Step 2

Question: What should Maria do?

- Answer to the email and give the required information
- Ignore the email and not give the required information

Answer: The second answer is correct. Your bank will never ask for your personal information and especially not your credit card codes, especially not by email or phone. These information are confidential, you shouldn't give them to anyone. This email is spam. The date it was sent (the same date as the first online banking connection) is just a coincidence. You can recognize it is a spam as the email it comes from is "mhswt", an unknown server and not "national bank", the official email server. Be careful, you can recognize the server after the character @ and not before it. Also note that the language is very informal.

Step 3

In order to connect to their online banking account, Maria & Martin need two things: their user number (assigned to them by the bank) and generally a token that will give them an individual password each time they connect. Alternatively, banks can decide the token will be the users' smartphones and they need to install an application from the bank. The third option is that the bank will ask users to set several passwords and security questions.

Step 4

Question: What is the most appropriate password that Martin and Maria can set for their account?

- QsgtUpnbV69!!Tgh
- HowisTheweather2day?

Answer: Both answers are appropriate and safe passwords. Indeed, they contain at least one capital letter, a mix of letters and numbers and a special character. Nevertheless, the second password is more appropriate as it is constructed as a sentence and it is easy to remember while the first password is a combination of random numbers and letters which is safe but impossible to remember.

Step 5

Now Maria & Martin are connected to their personal online banking account where they can perform several actions such as consult their account statement, transfer money, consult their credit card statement and eventually cancel their credit card, invest money or send their bank a message *[Instructions: show a screen that looks like an online banking account homepage where you can see the following sections: "your accounts", "investments", "transfer", "your credit card", "messages".]*

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission under the Erasmus+ Programme. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein. [Project Number: 2021-1-ES01-KA220-ADU-000023423]

Co-funded by the European Union

Step 6

Question: Martin and Maria would like to transfer money to their son who is renovating his house. What do they need to do in order to do the operation online?

- They need to give the transfer order (with the recipient bank account number, name, address, amount and reason). The bank will eventually send them a code and confirmation sms or email
- They need to give the transfer order (with the recipient bank account number, name, address, amount and reason) and send a message to their bank adviser to confirm it

Answer: The first answer is right. You don't need the authorization or confirmation of your bank adviser for a transfer online. Everything is done on your computer or smartphone. As a security measure, the bank can ask you for a code or send you a confirmation by email or sms.

Step 7

Question: Taking into account the previous situation: Martin & Maria transfer money to help their son renovate his house. Various types of payments are possible. Which one should they choose?

- Recurrent payment
- One time payment
- Future payment

Answer: The second answer is correct. It is a punctual payment that they are making at the occasion of their son's house renewal.

Step 8

Let's recall the different types of payments that are possible online. A **one time payment** has a fixed amount and is executed immediately after the order is given. A **recurrent payment** is made to the same person, scheduled with a certain frequency and with the same amount each time. A **future payment** is a payment that is scheduled for later : the order is only executed at a later date decided by the user. Note that a recurrent payment or a future payment can be cancelled at any time before the payment is executed.

Step 9

Finally, after making the payment to their son, the couple wishes to transfer some money from their savings account to their current account.

Question: Is it possible to do this operation online?

- Yes. They need to check if there are enough funds in their savings account. As long as there is, there is no problem making the transfer online.
- No. Transfers from your savings account is very specific and you need the signed authorization of the account holder(s) and of the bank adviser.

Answer: The first answer is correct. Transferring money from your savings account to your current account is one of the operations that is available online. No extra signature is needed.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission under the Erasmus+ Programme. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein. [Project Number: 2021-1-FR01-KA220-ADU-000023422]

3: Conclusion & Image

Both seniors wave enthusiastically, the computer is in the background with the phrase: “Operation completed!”. Congratulations, thanks to your help Martin and Maria were able to connect safely to their online bank account and perform several banking operations. Don’t forget to log-out from your online banking account once you are done using it! [Instruction: show the logout button]

https://www.freepik.com/premium-vector/bullseye-business-conpept-arrow-center-target-make-money-vector-design-element_37707542.htm#query=mission%20completed&position=31&from_view=search&track=sph

3.1: Final Reflection

Using online banking is safe and practical!

It is a convenient way to manage your current account and savings. There is a strong authentication process to connect to your online banking profile. You can pay bills and transfer funds rapidly. It also allows you to stay informed while consulting your account statements.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission under the Erasmus+ Programme. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein. [Project Number: 2021-1-ES01-KA220-ADU-000034423]

Do you feel like using online banking? Do you feel safe with the possibilities it offers you? For you, does the advantage overweigh the disadvantages?

Co-funded by the
Erasmus+ Programme
of the European Union

This project has been funded with support from the European Commission under the Erasmus+ Programme. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein. [Project Number: 2021-1-FR01-KA220-ADU-000034423]

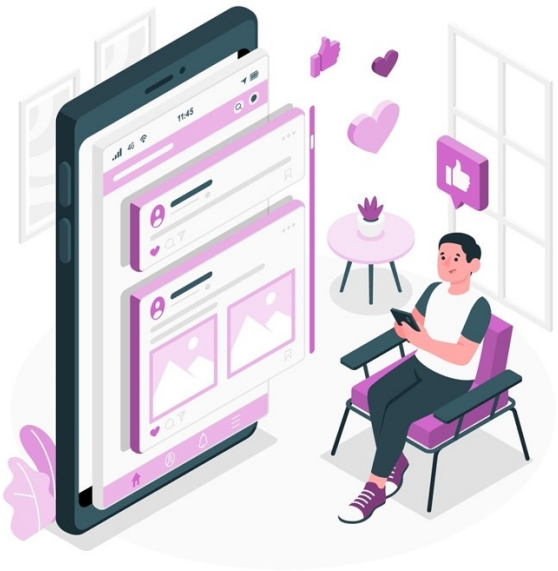
1. SOCIAL MEDIA FAKE PROFILE

1.1. Introduction

Our characters is an older man. He has been lonely for many years and has seen on the internet that it is possible to look for people like him who are lonely.

The man is in front of his computer.

Introduction: Meet Juan, a man who has been a widower for more than 15 years, who wants to find other people to communicate with or to go out with. Can you help Pedro to connect with other people?



https://www.freepik.com/free-vector/mobile-feed-concept-illustration_12445721.htm#query=Online%20concept%20illustration&position=29&from_view=search&track=ais

Step 1

Juan receives a message on his social networks asking him to accept in order to continue talking.

Good morning Juan. My name is Lucia, I have been a widow for 3 years, I work as a doctor during the week, but I am interested in meeting other people with the same interests as me. I am Catholic and go to church every weekend. For that reason, I have seen that we could hit it off.

Please accept me so we can continue to talk and get to know each other.

Step 2

Question: What should do Juan?

- Accept the invitation

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission under the Erasmus+ Programme. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein. [Project Number: 2021-1-FR01-KA220-ADU-000033422]

- Don't dismiss the profile immediately, but do some more research.

Answer: The second answer is the correct. Key words you will find in most fake online profiles include the words Catholic, widower, female, PhD, Nigeria, engineer, self-employed and royalty. People who create fake profiles want to get your attention. If you see any of the above words heavily accentuated in a profile, there is a chance that it belongs to a scammer and is fake. While there are certainly genuine profiles that will have these keywords, consider this a red flag. Instead of dismissing the profile outright, do some research and check for other classic signs of a fake profile.

Step 3

Before accepting the invitation, Juan decides to investigate Lucia's profile a little, so he goes to her profile and looks at her photos.
He discovers that she only has 2 profile photos, in which she looks very attractive, but she has no more photos.
What should Juan do?

Step 4

Question: What is the next step that Juan needs to take?

- To ask for more pictures and double check other information in the profile
- To send some photo of himself.

Answer: The first answer is the best option, to check all the information related to the person is a good idea and can give you more realistic overview if the person that you are talking in a fake profile or real person.

Step 5

Juan has found some information in Lucia's profile, so he decides to accept Lucia's invitation to be friends and talk to her.
Once the invitation is accepted, Juan asks Lucia to send him a picture of her that is different from the one in her profile.
Lucia sends him a photo but it is the same as the one in her profile.

Step 6

Question: What Juan need to do??

- Take the picture that Lucia sent and do a reverse image search in google
- Ask Lucia for a more pictures another time.

Answer: If you're really unsure if it's fake or not, save the image to your computer and do a reverse image search on Google. If you can find the image in a Google search, there's a good chance that it's a fake profile.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission under the Erasmus+ Programme. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein. [Project Number: 2021-1-FR01-KA220-ADU-000033422]

Step 7

At the same time Lucia ask for some personal information about Juan and Juan is a bit confused because the information Lucia is asking for is very personal (name surname, family,etc)

Step 8

What should he do?

- He needs to avoid giving out personal information.
- He needs to give the information and ask the same to her.

Answer: The first answer is right. Avoid identifying yourself and hesitate to give your address, telephone number, email address or any other personal information requested.

Step 9

After seeing all the information sent by Lucia and the personal questions, she has asked him, Juan decides to cancel the invitation to continue talking to Lucia, as he believes she is a Robot or a fake profile who wants to take advantage of him.

Question: How can he unfollow and report Lucia as fake profile from his social network??

- Juan need to go to his account, check the account of Lucia, click unfollow and later in the 2 three dots beside the account name and click report fake account and explain the reason.
- Close Juan profile

Answer: The first answer is correct. Is very important to unfollow the account that cannot send more information and you are not receiving more info from that account, but also is important to report to the social network the fake profile that they can delete from the system.

3: Conclusion & Image

Juan looks happy, after having cancelled the friendship with LUCIA, Juan has been able to learn and recognise a fake profile on social networks.

Now he has to look for new real friendships on social networks.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission under the Erasmus+ Programme. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein. [Project Number: 2021-1-FR01-KA220-ADU-000033422]

https://www.freepik.com/premium-vector/user-deleting-social-account-waste-bin-conceptual-design-premium-vector_23903849.htm#page=2&query=cancel%20account&position=18&from_view=search&track=ais

- THERE IS THIS IMAGE BUT NEED TO BE BUY WITH PREMIUM ACCOUNT (WE CAN ASK THE GREEK IF THEY CAN FIND SOMETHING SIMILAR)

3.1: Final Reflection

There's no surefire way to get fakes to stop contacting you, but if you learn to spot them you lose the risk of contacting one first and you're able to remove the threat at first contact. You will still get fakes contacting you, but you will be better able to recognize them and end the conversation quickly or not engage in a conversation at all.

If you have been in contact with them and you only realize afterward that they seem phony, don't be afraid to block them or report them to the platform that you're communicating on. They are trying to trick you and they have bad intentions. Blocking and reporting them will not only protect you, but it may prevent them from being able to trick anyone else too.

Lastly, never underestimate the power of a good first impression for yourself and the profiles you browse through. Trust your gut instinct. If you're not sure whether a profile seems legit, play it safe. Look for the profiles that have completed information and a lot of pictures.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission under the Erasmus+ Programme. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein. [Project Number: 2021-1-FR01-KA220-ADU-000033422]

1. Internet platforms: Going on vacation

1.1. Introduction

Our characters are two female seniors. They are together sitting in the living room couch and discussing what they will do in the summer vacations.

Introduction: Meet Maria and Eleni, they are discussing what will they do in the summer vacation and they want to book a girls trip. They have been friends for other 30 years and they said it was time to arrange a trip. They are very excited about that, but they are anxious on who to book their vacations safe. Can you help Maria and Eleni to book their vacations safely?

https://www.covermore.com.au/blog/travel-tips/seniors-best-destinations

Step 1

Maria and Eleni start discussing where they can go so they can relax and enjoy their summer vacations. They want to travel somewhere close in order to avoid any potential stressful scenarios or being too much tired.

While they were searching they found a page online for an upcoming cruise in the Caribbean. They page said “Are you a senior citizen? Do you want to travel safely with us and enjoy your summer vacation? Just click here and you are almost there”

Step 2

Question: What should Maria and Eleni do?

- Click on the page and continue
- Ignore the page and continue with their search

Answer: The second answer is correct. When you search on the internet about a trip you need to be aware that your computer reads this information and some sites will pop up with no safe sites and try to trick you by taking your information. You always need to stay alert and proceed with your booking in a safe site.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission under the Erasmus+ Programme. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein. [Project Number: 2021-1-FR01-KA220-ADU-000033422]

Step 3

Being conscious that we disclose personal data with search engines, social media, and websites every time we use the internet for shopping, hobbies, or other purposes. Realizing the effects of these exchanges and the fact that some goods and services in the digital market can be obtained for "free" in return for our personal information.

In order to keep oneself and others safe from online threats, it is crucial to understand how to disclose identifiably personal information in the digital marketplace.

Step 4

Having that in mind, Maria and Eleni decided to visit an official cruises website to book their vacations. Now, it is time for the two senior friends to organize more in detail their vacations. They discussed that they want to book some senior friendly activities. They agree that Maria's niece will help them search and they stop the search.

Step 5

The next morning Eleni, received a phone call in WhatsApp. She didn't recognized the number but she answer it anyways. A young man was on the other side promoting some organize group activities that are very friendly to seniors and that they only thing she has to do is to give him a credit card number and he will handle everything.

What are the risks / options with that?

A: The young man probably is a scammer who wants to steel her money

B: The young man really works at a company and he provide vacations services.

Step 6

The correct answer is A: "The young man probably is a scammer who wants to steel her money" Avoid giving your personal information to strangers.

Data protection is very important. The process of preventing critical information from being corrupted, compromised, or lost is known as data protection.

3: Conclusion & Image

Maria and Eleni are very excited! Now they can go on their trip felling safe and happy and can enjoy their friendship.

Congratulations, thanks to your help Maria and Eleni were able to book their summer vacation. Don't forget to always be aware of the risks!

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission under the Erasmus+ Programme. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein. [Project Number: 2021-1-FR01-KA220-ADU-000033422]

https://companionsforseniors.com/2020/08/safe-day-trips-and-outings-elderly/

3.1: Final Reflection

No matter your age, travellers should constantly plan their trips to guarantee a secure and enjoyable trip. Age shouldn't be a barrier to travel. In truth, taking a trip can be quite helpful for seniors, but careful planning is even more crucial for them.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission under the Erasmus+ Programme. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein. [Project Number: 2021-1-FR01-KA220-ADU-000033422]

1. Title: The Truth Detective

1.1. Introduction

Enter a brief introduction to the challenge. Describe the scenario that you will address. Who are the characters? Where is it located? What is the background? Make sure to engage the learner.

The learner needs to be presented with challenges for them to overcome. Here you can introduce the scenario that will lead into the challenges.

Introduction:

You are an expert in spotting fake news and disinformation. As a trusted member of your community, your friends and family come to you for information about what's going on in the world. But with so much information available online, it can be hard to separate fact from fiction. It's up to you to be the truth detective and help your community stay informed!

Step 1

Setting the Scene You receive a message from a friend on social media claiming that a new law has been passed that will require everyone over the age of 65 to pay a special tax. Your friend is outraged and wants you to spread the word. But something about the message seems off to you. You decide to investigate further.

Image: An elderly person reading a newspaper or watching TV, with a thought bubble or caption questioning the authenticity of the news they are consuming.

Step 2

Checking the Source

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission under the Erasmus+ Programme. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein. [Project Number: 2021-1-FR01-KA220-ADU-000033422]

You decide to do some research to see if the information is true. You learn that the message came from a website that you've never heard of before. You do some digging and find out that the website is not reputable and has a history of spreading false information. You share this information with your friend and encourage them to be cautious about where they get their news.

A split-screen image, with one side showing a legitimate news article and the other showing a fake news article about the same topic, highlighting the differences between the two.

Step 3

Understanding Bias

You receive an email from a family member claiming that a popular news network is biased and cannot be trusted. They ask you to share a story from an alternative news source. You decide to do some research to understand the difference between bias and outright lies. You find out that all news sources have some degree of bias, but some are more reliable than others. You share this information with your family member and encourage them to seek out multiple sources before making up their mind about a story.

An image of a computer or smartphone screen, with a pop-up warning about a potentially fake news article or website.

Step 4

Evaluating the Evidence

You receive a message on your phone claiming that a new study has found that a popular food is toxic and should be avoided at all costs. You are skeptical and decide to look into the study. You find that the study is not peer-reviewed and that the researchers have ties to a company that produces a competing product. You share this information with your friends and encourage them to be cautious about sensational headlines.

A cartoon or graphic showing how fake news spreads on social media, with a chain reaction of shares and likes leading to widespread misinformation.

Step 5

Spotting Deepfakes

You receive a video on social media showing a politician making a controversial statement. The video looks convincing, but something seems off. You decide to investigate further and discover that the video has been manipulated using

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission under the Erasmus+ Programme. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein. [Project Number: 2021-1-FR01-KA220-ADU-000033422]

deepfake technology. You share this information with your friends and encourage them to be wary of videos that seem too good to be true.

An image of a group of seniors engaged in a discussion about a news topic, with some expressing skepticism and others accepting the information at face value.

Step 6

The Consequences of Sharing Fake News

You receive a message from a friend claiming that a new study has found a link between a popular medication and a serious health condition. You are concerned and decide to share the information with your community. But after some digging, you discover that the study has been debunked and that sharing false information can have serious consequences. You share this information with your friend and encourage them to be careful about what they share online.

A collage of news headlines, with some real and some fake, demonstrating the difficulty in distinguishing between the two.

Other images:

- *An image of a library or a bookshelf, with a focus on books about media literacy or critical thinking skills, emphasizing the importance of staying informed and vigilant in the face of fake news.*
- *A picture of a senior citizen interacting with a fact-checking website or tool, such as Snopes or FactCheck.org, to verify the accuracy of a news story.*
- *An illustration of a news outlet or social media platform, with a magnifying glass highlighting areas of concern or suspicion regarding the accuracy of the information being presented.*
- *A picture of an elderly person engaging in a group discussion or workshop focused on identifying and combatting fake news, highlighting the importance of community and education in combating this issue.*

Conclusion

You have successfully completed the challenge and helped your community stay informed about the dangers of fake news and disinformation. Remember to always check your sources, evaluate the evidence, and be cautious about what you share online.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission under the Erasmus+ Programme. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein. [Project Number: 2021-1-FR01-KA220-ADU-000033422]

3: Conclusion & Image

How does your initial story end? Make sure the learners have been brought on a journey and they know that there is an ending to this section of the story.

3.1: Final Reflection

Use this section as an opportunity to engage the learner even further and reinforce the material that they have just seen.

Pose a self-reflection style question to make them think about this information in further details.

This is the final opportunity for the learner to use the knowledge that they have learned in the scenario. Do not present new information, make them aware of all of the information that they have learned.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission under the Erasmus+ Programme. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein. [Project Number: 2021-1-FR01-KA220-ADU-000033422]

This is the Story of Josephine

PART 1

Josephine's children signed her up to Facebook and gave her some basic lessons on how to use it.

Josephine said: 'They told me everyone was using it and that it would help us keep in touch and see photos of my grandchildren.'

One day Josephine received a friend request from a man who told her he was a retired accountant who was currently stationed in Cameroon as a volunteer for a humanitarian project.

Challenge 1 : What should Josephine do? (more than one answer can be correct)

Take measures to spot a Fake Profile

a) Check his about section and accept
b) Go through his timeline and photos CORRECT
c) If he is a friend of a friend she is safe to accept the friend request
d) She should google him CORRECT

Information that can personally identify someone, such as addresses, birthdays, phone numbers, workplace/school, login details.

Answer: Fake profiles don't have a lot of things to say about their day-to-day life because, well, they aren't living it. Josephine needs to look closer at the timeline of the account, observing photos, dates of posting, to spot an inconsistent timeline with large gaps in activity and then huge bursts of activity.

PART 2

She decided to accept the request and allowed 'Jim' to be her Facebook friend.
Jim told her that he was lonely and looking for friends his age. Soon after befriending her, Jim told Josephine he had lost his wife to cancer. Jim's story of how he looked after his wife during her illness, was similar to Josephine's own experience when her husband had died of cancer.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission under the Erasmus+ Programme. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein. [Project Number: 2021-1-FR01-KA220-ADU-000033422]

Challenge 2
How should Josephine react to this information? Fill in the Blanks with the words from the options below:

gaps **attached** **timeline**

Josephine should not get emotionally 1)_____ at this early stage of her friendship. She should go over Jim's 2) _____and see if there are any big 3)_____ or inconsistencies in his story.

ANSWER: 1- attached, 2-timeline, 3-gaps

PART 3
'He then said his volunteer team was moving to Chad after which he was planning to come back home. He sent her pictures of where he was and Josephine found him to be very interesting and adventurous. He then asked for her email saying it was easier to stay in touch than using Facebook.

Challenge 3: Sharing your email with someone can expose you to online…?
Unscramble to find the answers.

a) Onlien Mascs
b) Phihsing Attakcs

ANSWER: a) Online Scams, b) Phishing Attacks.
Here are a few things to consider before sharing your email with a new friend on Facebook:

Evaluate your level of trust: How well do you know this person? Have you only recently connected with them on Facebook or have you had multiple interactions and conversations with them?

Consider the context of your interactions: What types of conversations have you had with this person on Facebook? Have they asked for personal information in the past?

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission under the Erasmus+ Programme. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein. [Project Number: 2021-1-FR01-KA220-ADU-000033422]

Understand the risks: Sharing your email with someone on Facebook can potentially expose you to spam, phishing attacks, or other security risks. Make sure you're aware of these risks and take necessary precautions to protect yourself.

PART 4

Jim later told Josephine that his volunteer group had left Chad but he was staying for a few more days to get a chance to explore the place. But then the next day he sent her a desperate email telling her that his bag with his wallet and passport was stolen.

He said he was stuck with no cash and no papers and asked her to send him some money.

Challenge 4 - What should you do if a new Facebook friend asks you for financial help?

1) Try to help them since you are friends
2) Cease contact with him immediately and inform a family member.
3) Ask for their bank details and send the money immediately
4) Get a ticket for Chad to go there and help him

ANSWER: Cease contact with him immediately and inform a family member

PART 5

Josephine transferred some money to him to help him out of the situation. It was not a lot of money to send, and she thought he was a good and honest person and would return it to her.

Challenge 5: MATCH THE FOLLOWING

1. Online scammers	a)find out about your likes, dislikes and past experiences
2. Scammers use “foot in the door” technique	b)on several social media sites like Facebook
3. They use your personal information to	c)prefer victims who lack social support or are lonely
4. There are many fake accounts	d)to get you to commit to small

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission under the Erasmus+ Programme. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein. [Project Number: 2021-1-FR01-KA220-ADU-000033422]

	payments first, so that later when they ask for bigger amounts it is harder to say no.

ANSWER: 1 -c, 2-d, 3-a, 4-b

An important note: In April 2020, Google alone saw more than 18 million daily email scams related to COVID-19 in a single week. Hackers are taking advantage of psychological factors such as stress, social relationships, and uncertainty that affect people's decision-making.

https://www.scamwatch.gov.au/get-help/real-life-stories/dating-romance-scam-georginas-facebook-fianc%C3%A9-leaves-her-flat-broke

https://www.fraudsmart.ie/personal/fraud-stories/

https://www.dbs.com/livemore/money/understanding-the-psychology-behind-scams.html

More scams: https://www.dbs.com/livemore/money/top-3-scams-in-singapore.html

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission under the Erasmus+ Programme. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein. [Project Number: 2021-1-FR01-KA220-ADU-000033422]

FAKE INVOICE PHISHING SCAM

PART 1

George is 68 years old. He lives with his wife Sabina in Madrid, Spain. George is retired and enjoys doing some DIY carpentering work around the house. He sometimes goes online to order certain materials for this.

Challenge 1: When George goes online to buy things what should he be careful about:

Match the following:

1. Shop from reputable websites	a) This indicates that your information will be transmitted securely.
2. Look for the padlock icon	b) these should be hard to guess and unique for each online shopping account.
3. Avoid public Wi-Fi	c) never share your payment information with anyone
4. Use strong passwords	d)These networks are less secure and hackers can intercept your data.
5. Protect your debit/credit card information	e) only shop from websites that you trust or that have a good reputation.

ANSWER:

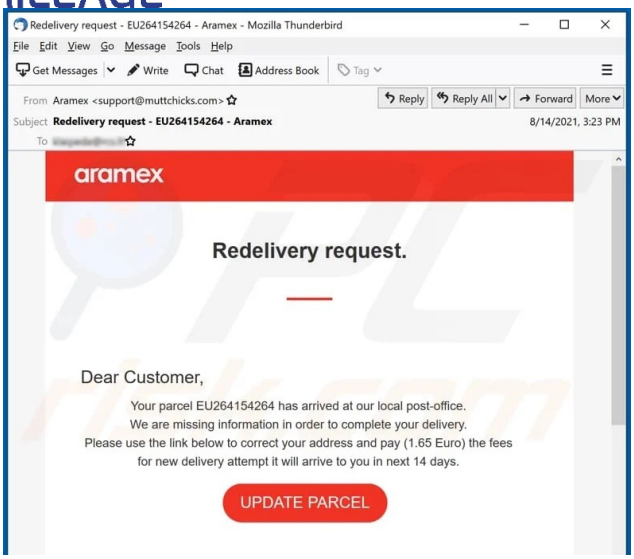
1e, 2a, 3d, 4b, 5c

PART 2

One day George receives an email from a courier service informing him that a parcel has arrived at their logistics centre but some information is missing and they cannot release the item to him. They ask him to click on a link to update his information. (Illustration below)

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission under the Erasmus+ Programme. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein. [Project Number: 2021-1-ES01-KA220-ADU-000023422]



CHALLENGE 2

TRUE OR FALSE
The email address of the sender looks to be authentic and safe.

ANSWER: FALSE - the email of the sender is support@muttchicks.com and not support@aramex.com as should be the case.

What should George do? Select One

- Immediately pay the invoice so that his parcel gets released
- Call up Aramex with the parcel number and confirm if indeed such a parcel has been sent to him

PART 3
George checks in his records to see if he has ordered anything recently. He then calls Aramex to confirm if there is a parcel there waiting for him. He uses the parcel number given in the email. Aramex informs him that no such parcel in his name can be found in their records.

CHALLENGE 3
George almost became a victim of a scam. What kind of scam was it and why do victims fall for it? **Choose one option**

a) Identity theft scam
b) Online banking scam
c) Phishing scam
d) None of the above

ANSWER
Phishing scam: Phishing is a type of online scam where criminals impersonate legitimate organizations via email, text message, advertisement or other means in order to steal sensitive information.

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission under the Erasmus+ Programme. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein. [Project Number: 2021-1-ER01-KA220-ADU-000032422]

Fill in the Blanks from the words in the box

bank	ordered	urgency	phishing	legitimate

1. _____ emails are used to trick recipients into providing personal information.

2. Most scammers pretend to be _____ organisations.

3.Scammers ask to provide credit card details, _____account numbers, and so on.

4.This scam relies on fear and _____

5.They pressure the end user to pay for goods and services they never even _____.

ANSWER: 1)Phishing, 2)legitimate, 3)bank, 4) urgency, 5)ordered

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission under the Erasmus+ Programme. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein. [Project Number: 2021-1-ES01-KA220-ADU-000023422]