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

‘Personal Finance Programme’

(project reference 2017-1-UK01-KA201-036799)

Personal finance curricula and training programme – Internet Security Banking Case Study

May 2019

Produced by Emphasys Centre.

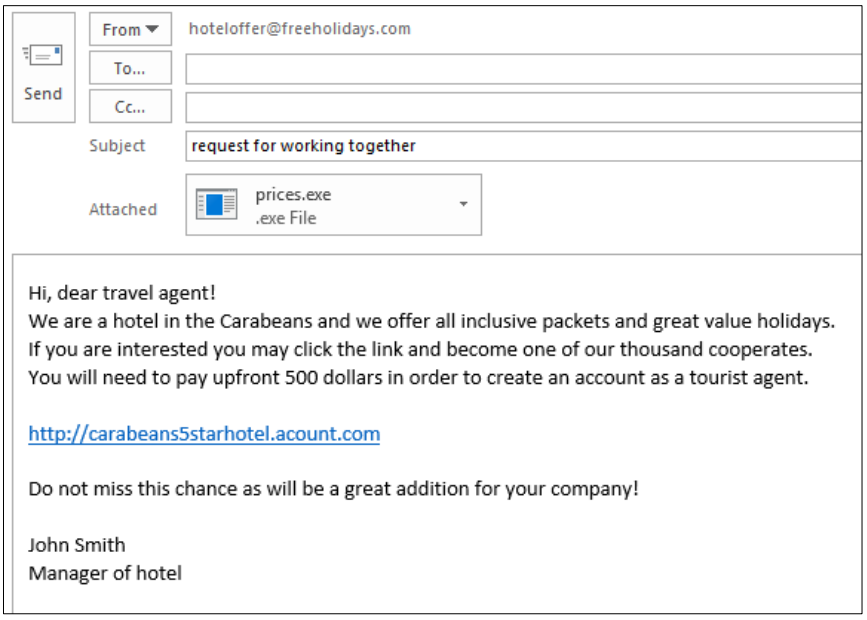
Erasmus + Personal Finance Programme Module 2: Internet Security Banking

Case Study 2

Part A:

Irene works as a tourist agent. Her daily tasks involve making payments to hotels and airplane companies, as well as booking hotels and flights and organizing trips for her clientele. A large portion of her working time is devoted in her physically going to her clients' premises, usually companies which send their personnel on business trips, in order to receive payments.

Irene usually receives emails from various hotels around the world which wish to cooperate with her agency. She received the following email this morning:



Erasmus + Personal Finance Programme Module 1: Savings

Case Study 2

Part A:

Questions

1) How can Irene save time and receive payments without her physically going to her clients' premises?
2) Identify the issues of the email she received.
3) How can she confirm the authenticity of the email?
4) Identify the category of scam which the email falls in.
5) The website indicated by the email is not a secure website. Identify two properties that a website should have in order to be considered secure.

Erasmus + Personal Finance Programme Module 1: Savings

Case Study 2

Part A:

Answers

1) How can Irene save time and receive payments without her physically going to her clients' premises?

She can direct her clients to make payments using an online banking system.

2) Identify the issues of the email she received.

- The email address is not one she knows.
- There is an attachment which is an executable file and most probably not what it claims to be.
- There are apparent spelling and grammatical errors in the text.
- The email requires a payment upfront just for creating an account.
- The website link also has spelling errors and does not have a secure connection – https.
- The name of the manager is a very common name.

3) How can she confirm the authenticity of the email?

She can try contacting by phone the hotel and also check if there are other tourist agencies, she is affiliated with, know or conduct business with the hotel.

4) Identify the category of scam which the email falls in.

The email is an example of Social engineering - phishing scam.

5) The website indicated by the email is not a secure website. Identify two properties that a website should have in order to be considered secure.

A secure website must have:

- Secure connection – https.
- A valid Digital Certificate.

Case Study 2:

Part B:

During the summer months Irene may also escort a group of usually seniors in an organized tour in a European country.

Last summer she escorted a group travelling in a Mediterranean country. During the second day of the trip she received an SMS on her mobile phone coming from her bank containing an OTP number for purchasing goods from an online shop which she clearly had not try to purchase from. The debit card Irene uses for her online purchases is connected with her personal banking account where her salary is credited at the end of every month.

The day before Irene used the same card and made payments in a café and also in a souvenir shop. She recollects that when she was about to pay, the waiter and also the sales person took, in their hands, her credit card and inserted it in the POS machine in order to complete the payment. She also believes that one of them was also holding a mobile phone.

Case Study 2:

Part B:

Questions:

1) Upon receiving the SMS from the bank identify what actions Irene has to perform.
2) Identify the type of security used in OTP SMS messaging.
3) Identify the type of card Irene should use for her online purchases.
4) Identify the extra safety measure Irene could use in order to make more secure payments during her trip.

Case Study 2:

Part B:

Answers:

1) Upon receiving the SMS from the bank identify what actions Irene has to perform.

Irene needs to immediately contact her bank and inform them of the situation.

2) Identify the type of security used in OTP SMS messaging.

In OTP messaging is used in 3d Secure Credit card payments.

3) Identify the type of card Irene should use for her online purchases.

For online purchases an Internet Credit Card is advisable to be used where the exact amount to be spend is credited just before the transaction.

4) Identify the extra safety measure Irene could use in order to make more secure payments during her trip.

Irene could have used her card using the Contactless card option without having other persons physically touching her card and memorizing or taking a picture of her cards number and security code.

www.personalfinanceprogramme.eu

www.facebook.com/Personal-Finance-Programme-PFP

@PFPproject

YouTube Personal Finance Programme

Lancaster Royal Grammar School

IESS IL LICEO EUROPEO

Emphasys CENTRE

TAMPEREEN YLIOPISTO

DHE Solutions Ltd

Erasmus+

This project has been funded with support from the European Commission. This communication 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.
Submission Number: 2017-1-UK01-KA201-036799

ERASMUS+ KA2 STRATEGIC PARTNERSHIP IN SCHOOL EDUCATION