IO3: Financial Literacy Training for Parents

Handout 3.7 – Making a secure online payment.

Part A- Michael's online payment

Michael receives an email from his bank asking him to immediately make a payment of 85 euros/pounds which has been suspended and which could increase further if not paid immediately.

In the email there is also the payment link.

Michael, alarmed, immediately clicks on the link and makes the payment using his card details.

A few days later, his bank calls him to tell him that they have noticed repeated suspicious payments of 600 euros/ pounds at a time.

At that point Michael realizes that he has been scammed and asks the bank to immediately block his card, also asking the bank to get back the money lost with the scam.

The bank replies that it will try to recover the money but is not at all sure that it can return it.

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein. [Project Number: 2020-1-UK01-KA204-079048

Handout 3.7 – Making a secure online payment.

PART B

Reflective questions. Discuss in small groups and then share with the facilitator:

Have you, or someone you know, ever received emails like Michael's one?

Do you think this is something that might rarely happen?

What would you do if it happened to you or a close friend?

What would you do if Michael was your son?

What should Michael have done to avoid the scam?

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein. [Project Number: 2020-1-UK01-KA204-079048]

Handout 3.7 – Making a secure online payment.

PART C

What should Michael have done to avoid the scam?

- Not open the email (Yes, it might be a good idea not to open any suspicious emails, especially if they have a strange phrase in the subject bar)

- Open the email but don't click on the link provided (Absolutely yes! Never open a payment link received from a bank email without calling the bank first for confirmation)

- Open the link but do not write the card credentials (While it is not recommended to open any suspicious link, it is essential to at least not write the details of the card)

- Call the bank immediately (Yes, if you have any doubts, better call your bank)