CURRICULUM

Module 4: Online Security

Please, list the individual topics of the module.

- Security of devices – the risks
- Security of devices – the instruments
- Security on online banking

GENERAL DESCRIPTION OF THE MODULE

Please, make a general description of the module and refer to the importance of the module in the whole curriculum. Describe also whether the knowledge of the module is the basis for another module (for example: module 1 is the basis for module 2).

This module is an indispensable part of the training. It cannot be divided into basic and advanced requirements, as security is fully required for every activity on online banking. Money and finance are very sensitive topics, especially for senior citizens. Even in the analogic world, there are threats related to money management and banking for example con artists who pretend to rob other's people savings. On the Internet, the risks seem even more threatening, incomprehensible and difficult to avoid. For seniors to use online banking, it is, therefore, essential that they can act safely, feel safe and know where to get advice in case of doubt. This includes knowing and understanding the central concepts related to security, the risks, the security instruments and the rules for dealing with money on the internet.

Senior citizens are often very trusting, they seek contact with others and are used to seeking help. For them, it is particularly important to learn that in online banking you cannot trust anyone, but must act on your own. In this module it is important to acquire knowledge, but also to try things out for themselves. The first two topics of this module should be placed before the Module "Online banking environment" and the third topic should be placed after seniors get the general information about online banking environment. Therefore, basically trainings of this Module and Module Online banking environment should be done together.

LEARNING OBJECTIVES AND DESIRED COMPETENCES OF THE MODULE

Please describe the learning objectives and desired competences of the module. Try to integrate the results of the Skill Card and upgrade them.

At the end of this module, learners

should know

- what risks online banking entails
- what to look out for when using PCs and mobile devices to operate safely on the Internet
- what to look out for especially on online banking
- know the security procedures on online banking
- know the most important terms of online security

be able to

- check the PC and WLAN for security
- recognize the security of Internet addresses
- enter the online banking account safely
- securely create, store and use passwords, access data, PIN and TAN
- avoid phishing attempts
- recognise the importance of not entrusting their access data to anyone
- respond in the event of unauthorised access to the account
- secure the bank statements and credit card statements

LENGTH OF THE MODULE

Please, write, how many hours has the module
8

TEACHING AND LEARNING CONCEPT OF THE MODULE

Possibilities are face-to-face, E-learning or a webinar. If necessary, it would be possible to describe why you use a certain method. Also, think on possibilities to include learning games in the module and discuss about it with VITECO.
This module includes face- to-face learning which could be replaced by webinar and online sessions under special circumstances (e.g. seniors who are not able to participate). However, face-to-face learning would be preferable as the trainer has better possibilities to respond to the seniors' learning needs and to make sure that, especially, this important topic has been understood correctly. It is accompanied by online and printed materials for general information and later use.

DETAILED INFORMATION ON THE TOPICS

TOPIC	LENGTH OF THE TOPIC	LEARNING CONTENTS	AIM	LEARNING TASKS/ACTIVITIES	OUTCOME	TEACHING METHODS
Security of devices – the risks	1	SAFETY RISKS - Viruses, worms and Trojans as a threat - Malware access routes	Participants will know security risks when using the PC	Participants watch a presentation in which they learn that viruses, worms and Trojans can be used to carry out unauthorised activities on their computers and that passwords can be spied out. Seniors collect ideas on how malware gets into the computer and learn about the access routes of this malware (emails from unknown senders with email attachments or links, unsecured downloads, missing encryption, fake websites) through corrections and additions by the teacher.	Participants are aware of the risks of the Internet and answer questions on the topic correctly.	Face to face: Presentation Brainstorming with trainer-controlled result assurance
Security of devices – the instruments	2	INSTRUMENTS FOR SAFETY -WLAN configuration (backup) -Firewall -Antivirus software -regular update -Password protection for	Participants will know and will be able to use the most important instruments of PC security.	The participants see a video of the introduction (Germany: https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Mediathek/Videos/videos_node.html) The trainer picks up the most important instruments mentioned and explains them in simple language. Using a worksheet, the participants check their training computer and mobile device under the trainer's guidance. The participants note in their own words the meaning of the hedging instruments and where they are tested.	The participants know the tools for security and can use them independently.	Short Video Editing a working sheet and Working on the PC under guidance

		mobile devices Choice of Browser Browser Settings				
Security in online banking	5	AVOIDING AND AVERTING RISKS - Phishing - what is that -use the private computer only -Do not use an open WLAN network, rather use the mobile network - regularly check account activities -create secure passwords -Do not save passwords	Participants will know the risks involved in online banking. Participants will know and be able to apply patterns of action for safe online banking. Participants will be able to react in case of irregularities.	Senior citizens search the Internet for "Risks in online banking", find familiar general risks from the first unit and come across "phishing" again. They explain what this is. Exchange of experience in the group: Seniors -report if they have received unknown emails before and how they have reacted -report how they handle passwords. Participants receive information on the topic (presentation and information sheet "tips for security" for now and later use).	Participants are aware of the risks involved in online banking, behave in a risk-conscious manner and apply security strategies. They regularly save their bank statements and credit card statements.	Internet research Face-to-face: exchange of experience Face-to-face or online: Trainer lecture with presentation and information sheet Internet research

		and user names on the computer -Securing PIN and TAN procedures -Never open unknown emails -detect and fend off fake calls and emails -never disclose access data - Enter the address line of the bank yourself or use bookmarks DATA SECURITY: Download and save bank statements, credit card statements		Irregularities should be clarified by the seniors with the customer service: The seniors look for contact possibilities on various bank websites. The participants try out safe behaviour in a gaming situation. Input of the trainer: Bank statements and credit card statements are only 12 months on the online account! The participants create a sample folder for bank statements and credit card bills. Save what the participants have learned with a worksheet (gap text, checkbox questions, open questions on the topic).		Scenario Game Fake Email demands reaction, wrong debit, call customer service Face-to-face or online: Trainer input, individual work on the PC Face-to-Face, worksheet

FURTHER METHODOLOGICAL RECOMMENDATIONS

Please indicate methodological recommendations for the whole module.

This module includes face-to-face learning which could be replaced by webinar and online sessions under special circumstances (e.g. seniors are not able to participate). However, face-to-face learning would be preferable as the trainer has better possibilities to respond to the learning needs of the seniors and to make sure that especially this important topic has been understood correctly. It is accompanied by online and printed materials for general information and later use. It is very important to provide materials which the seniors can use at home for their practical daily online-banking. They need clear material to look up (e.g. "tips on security issues"). Practical sessions on the PC are important for training the seniors analysing the security of devices and accounts and dealing in a correct way. A scenario game could train seniors to try out safe behaviour.

REFERENCE LIST FOR THE WHOLE MODULE

Please indicate the most important literature which is used for the whole module. Examples are books, journals, internet links, videos, games etc.

https://www.bsi-fuer-buerger.de/BSIFB/DE/; last call 08.05.2020

Polizeipräsidium Hessen, Senioren auf Zack to find under: www.auf-zack.de, last call 08.05.2020

https://www.postbank.de/geschaeftskunden/gk_hilfe_sicherheit.html, last call 18.05.2020

https://www.sparkasse.de/service/sicherheit-im-internet/sicheres-online-banking.html, last call 18.05.2020

Markus Krimm, ECDL IT-Sicherheit, Herdt Verlag Bodenheim, 2015

REFERENCE LIST FOR FURTHER READING

Please indicate the suggested literature for further reading. Examples are books, journals, internet links, videos, games etc.

Markus Krimm, ECDL IT-Sicherheit, Herdt Verlag Bodenheim, 2015 (probably similar publications are available in other languages)