Detailed course program

Title of the Learning Activity	**Avoiding threats resulting from the use of ICT in everyday life**
Topic	**Offenses against the protection of information**
Summary of the activity	Computer crime is a relatively new phenomenon and its emergence is clearly linked to the development of the Internet. Developing technologies for the automatic collection, processing and transmission of information carry previously unknown threats. This raises the need to introduce new means of protection against unlawful interference in the sphere of private and social life, as well as to regulate the methods of obtaining and using information relating to these spheres. This training will explain the basic meaning of information protection crime terms. Participants will learn more about the risks associated with the use of ICT, the effects and methods of prevention. Participants will learn more about the threats of phishing, facilitated by ICT, about their effects and methods of use.
Duration	240 min
Age Group	30+
Aims of the Activity	- to learn the basic concepts of cyber attacks, including the concept of phishing - to learn how to detect and combat threats from cyberspace - to learn about habits that will protect against threats lurking in the network (secure passwords, two-factor authentication, e-mail content analysis) - to learn about ways to prevent phishing - to learn about threats of phishing in electronic banking
Guidance for a proper performance of the activities	
Methodology to implement the Activity	Basic form of classes: stationary classes are conducted in a computer room connected to the Internet with a connected multimedia projector. Other accepted forms of classes: e-learning or blended learning. Learning technique type: peer learning. Learning technique type: action learning. All visual aids (presentations, photos, videos ...) are welcome. A maximum of 12 people should participate in the learning process and all should be supported by a second trainer who will provide individual support to the learners.
Methods	Lecture, exercises, brainstorming, quiz, multimedia show Working in pairs, working in a group, discussion Problem solving method

Erasmus+

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

is better life

Tools and materials	- training materials prepared by the trainer - computers / tablets / smartphones, internet connections, projector - presentation with key information and graphics - computer applications
Knowledge acquired during the classes	The participant knows: - basic concepts related to cyber threats: cyberattack, phishing, malicious software (maleware), phishing, - rules for using safe logins and passwords, - principles of safe use of internet banking, - rules for the safe use of computer equipment and sites from the "high-risk" group.
Skills	The participant is able to: - configure the computer to increase its security, - create and securely store application passwords, - recognize a phishing attempt, - securely store computer data.
Process	The trainer's task is to highlight the topic and combine it with practical examples of everyday life. Process supported by interactive presentation and encouraging discussion and participation by participants. Where possible, the transfer of knowledge is combined with practical action.
Session 1 **Opening session** *30 min*	The trainer introduces himself and welcomes the participants. Informs participants about the principles, objectives of the training and its relationship to previous and future topics (if applicable). The trainer can set additional goals and the program of the module. Other motivational elements are welcome.
Session 2 Types of cyber threats *60 min*	The main purpose of the session is to identify, on a simple example, cyber threats such as malware, and in particular the concept of phishing. Introduction to the subject by presenting a story containing the main threads of the discussed issue, e.g.: *the story of a friend who happened to receive an e-mail with a dangerous link. The e-mail was sent from the DHL institution and informed about the shipment of the item, the e-mail contained a link to the data form correcting the shipping fee. The message contained all the symptoms of truthfulness: logos of the institution, signatures, email address, only the content was devoid of Polish characters, the link directed to the payment form, payment of an additional fee for the shipment.* *The trainer will display the e-mail on the projector.* *The trainer will lead to a discussion about the visual appearance of the message and highlight basic points to check in such a situation.* A message supported by images / it can be a presentation / in order to create an authentic atmosphere. Session development Teaching content: - the phenomenon of phishing, - e-mail - safe display and download of attachments, links.

	At the outset, individual issues should be preceded by examples of threats, include reports and descriptions of "real-life" cases. Present and practice examples of how to prevent threats using computer software and common sense. A summary of the most important information at the end of the session.
Session 3 Cyber threats – causes and effects *60 min*	Posing a question introducing the topic of the session: - *Do you know how to recognize a phishing threat?* - *Have you experienced a malware attack?* - *Give examples of cyberattacks that you have encountered?* - *How do you create passwords to access Internet services?* *Bring discussions with / between participants.* *Give participants enough space to share their experiences and thoughts. Support the debate in your groups and encourage participants to be active and engaged.* With the help of training participants and trainers, the question will be answered: - *How to protect yourself against phishing?* - *How to behave in case of detection of a cyberattack?* - *How to create secure access passwords?* Introduction of concepts and rules regarding the safe use of ICT: - ways to create and store secure logins and passwords, - securing websites (SSL certificate), - use of anti-spam software. Summary of the most important issues regarding the causes and effects of cyberattack threats.
Session 4 Cyber threats – challenges and electronic banking *90 min*	Posing a question introducing the topic of the session: - *Do you use electronic banking? To what extent?* - *Do you receive information from the bank? Which road?* - *How often do you make transfers via the Internet?* - *Do you check / compare account numbers before sending the transfer?* *Lead to a constructive exchange of views. Write down all participants' statements on the board or on post-it notes.* *Give the participants enough space to share their ideas and thoughts. Support the debate in your groups and encourage participants to be active and engaged.* **In the following part, you can use an example***, a life story of a person who made a transfer to the wrong account, because she/he did not check the correctness of the account number before accepting the transfer (careful text message check).* *Ask the participants if they have encountered such cases.* *Support the debate in your groups and encourage participants to be active and engaged.* The main issue of the session is electronic banking in terms of phishing - safe execution of transfers. Finally, do a joint analysis of the phishing issues that you learned. Prepare a mind map of the best practices for detecting such threats. The mind map should contain min.: - analysis of e-mail messages for correctness and truthfulness,

	- checking the correctness of the website address (SSL certificate), links sent in the e-mail, - checking the grammatical and spelling correctness of the e-mail content, - checking the time and day of sending the e-mail, - common sense in on-line financial operations, - checking the correctness of the account number / text message during the online transfer, - use of secure logins and passwords, - using two-factor account authentication (where possible), - using the bank's verified website address, not entering via the link from the e-mail. The trainer at the end of this section summarizes the most important information in the topic Information Protection Offenses.
Evaluation/Assessment	Evaluation of the module in the form of a questionnaire (e.g. paper or electronic version in Kahoot) includes the trainer (questionnaire1) and participants (questionnaire2). The evaluation tools and the evaluation process are prepared and carried out by the training organizer.
Bibliography, links or resources	Links that are associated with the topic being discussed. It must be current for the country and the current time. - E-mail and phishing attacks, „OUCH!", Computer security bulletin from SANS Institute and CERT Poland, 2/2013 (http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201302_po.pdf) - Laskowski P., Security of electronic banking operations, „Scientific Bulletin of Chełm Section of Mathematics and Computer Science", 1/2008 - Internet banking - new threats, article from http://www.chip.pl/artykuly/porady - Updating the software, „OUCH!", Computer security bulletin from SANS Institute and CERT Poland – 8/2011 (http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201108_po.pdf) - Safe and strong passwords, „OUCH!", Computer security bulletin from SANS Institute and CERT Poland – 5/2011 (http://www.securingthehuman.org/ newsletters/ouch/issues/OUCH-201105_po.pdf) - Email some simple tips, „OUCH!", 3/2012, http://www.securingthehuman.org - Stecko K., Email Security Guide - Overview of Popular Threats, „Haking" 1/2011 - Liderman K., Information security, Polish Scientific Publishers PWN, Warsaw 2013.
Additional activities	Examples presented in the form of a mini-presentation, conducting a thematic discussion, based on a selected issue, group quiz, joint preparation of a mind map consolidating the issue. Performing a proof test: link to the test "Do you recognize a phishing?" Google: https://phishingquiz.withgoogle.com
Mentoring for listeners?	Yes; the purpose of mentoring is to develop competences and attitudes to be alert to the need to protect information, to be aware of the consequences of crimes against information protection, and to comply with the principles of safe use of ICT tools on a daily basis.
Validation of teaching process	Validation of the learning process is welcomed as long as it focuses on a few key points. The method of validation should relate to the way classes are conducted and should motivate participants to act.

Special requirements for the trainer	In addition to the knowledge of security issues, the trainer should have IT qualifications and have good knowledge of the applications / tools taught / used during the training. The trainer should also have experience working with adults, especially low-skilled adults.
Innovative elements	How the program is documented. Linking theory with practice. Electronic conducted evaluation of activities.

Dictionary of terms:

peer learning *- group work of training participants, during which they have the opportunity to exchange information and skills, based on their own analysis, without the textbook form.*

action learning *- the work of a group of training participants with different competences and experience, who work on solving a real, complex problem and at the same time develop their leadership skills, at the same time becoming a highly effective team.*