Syllabus

Course Title: **Avoiding threats resulting from the use of ICT in everyday life**

Mode of delivery:

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.

Contact Information:

STAWIL is responsible for this course. If you have any questions, if you need to know more information or would like to provide us with your feedback, please do not hesitate to contact us. Please contact us via our email: biuro@stawil.pl

Prerequisites:

The course is especially suitable for beginners who know the basic steps with a computer. The basic steps can be defined as follows:

- basic knowledge of using the computer keyboard,
- basic knowledge of using the computer mouse,
- basic knowledge of using touchpad,
- being able to turn on the computer and being able to turn off the computer,
- work with an Internet browser,
- know the basic use of device.

Course Duration:

A total of 16 clock hours (960 minutes)

Course Description:

The main topic of the course is:

- **clarification of basic terms relating to information protection offenses**
  Developing technologies for the automatic collection, processing and transmission of information carry previously unknown threats. This makes it necessary to introduce new measures 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.
  Participants will learn more about the threats of phishing, related to the use of ICT technologies, their effects and methods of prevention.
- **explaining basic terms related to crimes in social media and the ways of using ICT in this type of crime**
  Participants will learn more about the threats posed by the Internet and ICT related to cyberbullying, harmful online content, unsafe contacts and seduction and sexting, the effects and methods of prevention, as well as the legal aspects of these crimes.
- **introduction and clarification of basic terms related to the information threats (diseases) of ICT users**
  Participants will learn more about the methods of searching, verifying information, disinformation and propaganda campaigns, hate, fake news, information smog.

Erasmus+

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

is better life

- **introduction and explanation basic terms related to the physical and mental health of ICT users**
  Participants will learn about the physical and mental dangers associated with the long and frequent use of electronic devices, about the effects, ailments and how to prevent these threats. They will learn how to prepare a safe space for the use of electronic devices and learn the rules of safe use of ICT.

Course Goals:

- 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,
- of electronic devices,
- to learn how to detect, prevent and combat threats from cyberspace,
- to learn habits that will protect you from threats lurking in the Internet,
- to learn about activities to combat illegal content and spam on the Internet and presenting issues related to the threats resulting from the use of mobile phones, online games, P2P file sharing and other forms of online communication (chats, instant messaging, etc.),
- to learn about ways to prevent on-line crime using new and better software,
- to learn the basic concepts of information threats,
- to learn about the causes and effects of information threats,
- to learn about ways of searching for valuable information,
- to learn about the methods of verifying information, navigating among information smog,
- to learn the basic concepts of physical and mental treats,
- to learn about the causes and effects related to the topic,
- to learn about the psychological risks, including types of addiction, symptoms and prevention,
- developing habits of safe use of electronic devices.

Learner Learning Outcomes:

The course participant will:

- could demonstrate knowledge of the basic concepts related to cyber threats,
- know the rules of using safe logins and passwords, safe use of internet banking and the rules of safe use of computer equipment and websites from the "high-risk" group,
- was able to recognize a phishing attempt and also store computer data in a safe manner,
- could demonstrate knowledge of specialist terms in this field, will be familiar with the basic legal provisions related to cybercrimes,
- be able to identify types of cyberbullying, types of harmful online content, will be able to know the procedures for reacting to cyberbullying and recognize dangerous online contacts,
- could demonstrate knowledge of the concepts related to information threats, including: information frustration, information loneliness, information stress, threats of uncritical news acceptance, fake news, information chaos, information smog, hate, disinformation campaigns,
- knew how to use various methods of verification / searching for information and how to verify information and check its sources,
- could demonstrate knowledge of the basic physical and mental threats resulting from long and frequent use of electronic devices,
- know the concepts related to these threats, will know what steps to take to counteract these threats, learn the rules of safe use of electronic devices,

Erasmus+

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

is better life

- was able to recognize ailments related to long hours of frequent use of ICT devices and tools, efficiently assess the causes and effects of these threats and prepare a safe space for their use.

Text, Materials, and Supplies:

Links that are associated with the topic being discussed:

- 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
- „Secure Internet step by step", Wojciech Wrzos
- https://www.saferinternet.pl/materialy-edukacyjne/poradniki-i-broszury.html
- https://www.saferinternet.pl/materialy-edukacyjne/kursy-e-learning.html
- https://www.saferinternet.pl/materialy-edukacyjne/podcasty-i-audiobooki.html
- https://www.edukacja.fdds.pl/?option=com_szkolenia&optrs=4
- https://www.edukacja.fdds.pl/kursy-e-learning
- https://akademia.nask.pl/baza-wiedzy.html
- Assessment of the credibility of information on websites, scientific journals of the University of Szczecin, NR 863 http://www.wneiz.pl/nauka_wneiz/studia_inf/36-2015/si-36-103.pdf
- https://ocena-informacji.weebly.com/wiarygodno347263.html
- „Information ecology and information resources in libraries and cyberspace ", edited by Katarzyny Materskiej, Beaty Taraszkiewicz, ISBN 978-83-88783-24-1
- "Media diseases" of the 21st century in the Polish media, Dariusz Baran
- Information stress - do we see a health risk? Wioletta Jachym, Health Promotion & Physical Activity, 2017, 1 (1), 23-30
- Ledzińska M., Contemporary man in the face of information stress, Warsaw, 2009
- https://www.uzaleznieniabehawioralne.pl/
- https://www.medicover.pl/o-zdrowiu/zespol-ciesni-nadgarstka-przyczyny-objawy-i-leczenie,173,n,192
- https://digitalreport.wearesocial.com/ - Global Digital Report 2018
- http://www.psychologia.net.pl/artykul.php?level=52
- Caught in the web [online], reż. Artur Sochan i Michalina Taczanowska, cz. 1, available on the Internet: http://www.youtube.com/watch?v=cZVE2uOtTcw
- Caught in the web [online], reż. Artur Sochan i Michalina Taczanowska, cz. 2, available on the Internet: http://www.youtube.com/watch?v=zHWerpLQsU0
- Phone addiction: https://www.youtube.com/watch?v=aqwljSIImHU
- Internet addiction as an expression of social pathology, Piotr Zawada
- Computer and Internet addiction - selected problems, Panasiuk Katarzyna , Panasiuk Bazyli, ttp://yadda.icm.edu.pl/yadda/element/bwmeta1.element.desklight-fb7cdc89-3972-4de0-ac3b-3ebc3e524116/c/Katarzyna_Panasiuk__Bazyli_Panasiuk.pdf.

Basic form of classes: stationary classes are conducted in a computer room connected to the Internet with a connected multimedia projector, including:

- training materials prepared by the trainer,
- computers / tablets / smartphones, internet connections, projector,
- presentation with key information and graphics.

Grading Policy:

The participant is classified at the end of the course. It consists in summing up the commitment and determining the final grade. The final grade is determined on the basis of the test. The pass test is considered to be 50% of correct answers.

Course Schedule:

Offenses against the protection of information – 240 minutes.
Crimes in social media – 240 minutes.
Information threats (diseases) – 240 minutes.
Threat and health – 240 minutes.