Sylabus

Název kurzu: **Předcházení hrozeb vyplývajících z používání ICT v každodenním životě**

Forma kurzu:

Základní forma výuky: stacionární výuka probíhá v počítačové učebně, připojené k internetu a vybavené multimediálním projektorem.
Další akceptované formy výuky: e-learning nebo blended learning.
Typ techniky učení: peer learning
Typ techniky učení: action learning

Kontaktní informace:

Za tento kurz odpovídá STAWIL. Máte-li jakékoli dotazy, potřebujete-li vědět více informací nebo byste nám chtěli poskytnout zpětnou vazbu, neváhejte nás kontaktovat. Kontaktujte nás prosím prostřednictvím našeho e-mailu: biuro@stawil.pl

Předpoklady:

Kurz je vhodný zejména pro začátečníky, kteří znají základní počítačové dovednosti. Základní dovednosti lze definovat následovně:

- základní znalost práce s klávesnicí počítače,
- základní znalost práce s myší,
- základní znalost používání touchpadu,
- schopnost zapnout/vypnout počítač,
- práce s internetovým prohlížečem,
- základní použití zařízení.

Délka kurzu:

16 hodin (960 minut)

Popis kurzu:

Hlavním tématem kurzu je:

- **objasnění základních pojmů souvisejících s trestnými činy ochrany informací**
  Vývoj technologií pro automatický sběr, zpracování a přenos informací přináší dříve neznámé hrozby. Z toho vyplývá nutnost zavést nová opatření na ochranu před neoprávněným zasahováním do sféry soukromého a společenského života a upravit způsoby získávání a využívání informací týkajících se těchto oblastí.
  Účastníci se dozvědí více o hrozbách phishingu, souvisejících s využíváním ICT technologií, jejich účincích a způsobech prevence.

Erasmus+
Co-funded by the Erasmus+ Programme of the European Union
is better life

- **vysvětlení základních pojmů souvisejících s kriminalitou na sociálních sítích a způsoby využití ICT u tohoto typu kriminality**
  Účastníci se dozvědí více o hrozbách, které představuje internet a ICT v souvislosti s kyberšikanou, škodlivým online obsahem, nebezpečnými kontakty a sváděním a sextingem, o účincích a metodách prevence a také o právních aspektech těchto trestných činů.
- **představení a objasnění základních pojmů souvisejících s informačními hrozbami uživatelů ICT**
  Účastníci se dozvědí více o metodách vyhledávání, ověřování informací, dezinformačních a propagandistických kampaních, nenávisti, fake news, informačním smogu.
- **úvod a vysvětlení základních pojmů souvisejících s tělesným a duševním zdravím uživatelů ICT**
  Účastníci se dozvědí o fyzických a psychických nebezpečích spojených s dlouhým a častým používáním elektronických zařízení, o účincích, neduzích a jak těmto hrozbám předcházet. Naučí se připravit bezpečný prostor pro používání elektronických zařízení a osvojí si pravidla bezpečného používání ICT.

Cíle kurzu:

- naučit se základní koncepty kybernetických útoků, včetně konceptu phishingu,
- naučit se odhalovat hrozby z kybernetického prostoru a bojovat s nimi,
- dozvědět se o návycích, které ochrání před hrozbami číhajícími v síti (bezpečná hesla, dvou faktorová autentizace, analýza obsahu e-mailů),
- dozvědět se o způsobech, jak zabránit phishingu,
- dozvědět se o hrozbách phishingu v elektronickém bankovnictví, elektronických zařízení,
- naučit se odhalovat, předcházet a bojovat proti hrozbám z kyberprostoru,
- naučit se návykům, které vás ochrání před hrozbami číhajícími na internetu,
- dozvědět se o aktivitách v boji proti nelegálnímu obsahu a spamu na internetu a prezentovat problémy související s hrozbami vyplývajícími z používání mobilních telefonů, online her, sdílení P2P souborů a dalších forem online komunikace (chaty, instant messaging atd.),
- dozvědět se o způsobech prevence online kriminality pomocí nového a lepšího softwaru,
- naučit se základní pojmy informačních hrozeb,
- dozvědět se o příčinách a dopadech informačních hrozeb,
- dozvědět se o způsobech vyhledávání cenných informací,
- seznámit se s metodami ověřování informací, orientací v informačním smogu,
- osvojit si základní pojmy fyzických a duševních požitků,
- dozvědět se o příčinách a následcích souvisejících s tématem,
- seznámit se s psychologickými riziky, včetně typů závislosti, symptomů a prevence,
- rozvoj návyků bezpečného používání elektronických zařízení.

Vzdělávací výsledky:

Účastník kurzu bude:

- moci prokázat znalost základních pojmů souvisejících s kybernetickými hrozbami,
- znát pravidla používání bezpečných přihlašovacích údajů a hesel, bezpečné používání internetového bankovnictví a pravidla bezpečného používání výpočetní techniky a webových stránek ze skupiny „vysoce rizikové“,
- schopen rozpoznat pokus o phishing a také uložit počítačová data bezpečným způsobem,
- umět prokázat znalost odborných pojmů v této oblasti, bude znát základní právní ustanovení týkající se kybernetické kriminality,

- umět identifikovat druhy kyberšikany, typy škodlivého online obsahu, bude schopen znát postupy reakce na kyberšikanu a rozpoznat nebezpečné online kontakty,
- umět prokázat znalost pojmů souvisejících s informačními hrozbami, včetně: informační frustrace, informační osamělosti, informačního stresu, hrozeb přijímání nekritických zpráv, fake news, informačního chaosu, informačního smogu, nenávisti, dezinformačních kampaní,
- umět používat různé způsoby ověřování / vyhledávání informací a jak ověřovat informace a kontrolovat jejich zdroje,
- umět prokázat znalost základních fyzických a duševních hrozeb vyplývajících z dlouhého a častého používání elektronických zařízení,
- znát pojmy související s těmito hrozbami, bude vědět, jaké kroky podniknout, abychom těmto hrozbám čelili, osvojili si pravidla bezpečného používání elektronických zařízení,
- umět rozpoznat neduhy spojené s dlouhým častým používáním ICT zařízení a nástrojů, efektivně vyhodnotit příčiny a dopady těchto hrozeb a připravit bezpečný prostor pro jejich použití.

Texty, Materiály, Pomůcky:

Odkazy, které jsou spojeny s probíraným tématem:

- 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

Erasmus+

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

is better life

- 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.

Zásady hodnocení:

Na konci kurzu je účastník klasifikován. Vše je spojeno s docházkou, aktivním přístupem. Výsledná známka je určena na základě testu. Za úspěšné složení testu se považuje 50 % správných odpovědí.

Harmonogram kurzu:

Přestupky proti ochraně informací – 240 minut.
Zločiny na sociálních sítích – 240 minut.
Informační hrozby – 240 minut.
Ohrožení a zdraví – 240 minut.