Programa del curso

Título: **Evitar las amenazas derivadas del uso de las TIC en la vida cotidiana**

Modo de enseñanza:

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.

Información de contacto

STAWIL es responsable de este curso. Si tiene alguna pregunta, si necesita más información o si quiere hacernos llegar sus comentarios, no dude en ponerse en contacto con nosotros. Póngase en contacto con nosotros a través de nuestro correo electrónico: biuro@stawil.pl

Pre-requisitos:

El curso está especialmente indicado para los principiantes que conocen los pasos básicos con un ordenador. Los pasos básicos pueden definirse de la siguiente manera:

- conocimiento básico del uso del teclado del ordenador,
- conocimiento básico del uso del ratón del ordenador,
- conocimientos básicos sobre el uso del panel táctil,
- saber encender el ordenador y saber apagarlo,
- trabajar con un navegador de Internet,
- conocer el uso básico del dispositivo.

Duración:

16 horas en total (960 minutos)

Descripción del curso:

El tema principal del curso es:

- **aclaración de los términos básicos relativos a los delitos de protección de la información**

El desarrollo de tecnologías para la recogida, el tratamiento y la transmisión automáticos de información conlleva amenazas hasta ahora desconocidas. Esto hace necesaria la introducción de nuevas medidas de protección contra las injerencias ilícitas en la esfera de la vida privada y social, así como la regulación de los métodos de obtención y utilización de la información relacionada con estas esferas.
Los participantes aprenderán más sobre las amenazas del phishing, relacionadas con el uso de las tecnologías de la información y la comunicación, sus efectos y métodos de prevención.

- **explicar los términos básicos relacionados con los delitos en las redes sociales y las formas de utilizar las TIC en este tipo de delitos**

Los participantes aprenderán más sobre las amenazas que plantean Internet y las TIC en relación con el ciberacoso, los contenidos nocivos en línea, los contactos inseguros y la seducción y el sexting, los efectos y los métodos de prevención, así como los aspectos legales de estos delitos.

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

- **introducción y aclaración de los términos básicos relacionados con las amenazas informativas (enfermedades) de los usuarios de las TIC**

Los participantes aprenderán más sobre los métodos de búsqueda, la verificación de la información, las campañas de desinformación y propaganda, el odio, las noticias falsas, el smog informativo.

- **introducción y explicación de términos básicos relacionados con la salud física y mental de los usuarios de las TIC**

Los participantes conocerán los peligros físicos y mentales asociados al uso prolongado y frecuente de los dispositivos electrónicos, los efectos, las dolencias y la forma de prevenir estas amenazas. Aprenderán a preparar un espacio seguro para el uso de dispositivos electrónicos y conocerán las normas de uso seguro de las TIC.

Objetivos del curso:

- aprender los conceptos básicos de los ciberataques, incluido el concepto de phishing
- aprender a detectar y combatir las amenazas del ciberespacio,
- conocer los hábitos que protegerán contra las amenazas que acechan en la red (contraseñas seguras, autenticación de dos factores, análisis del contenido del correo electrónico),
- conocer las formas de prevenir el phishing,
- conocer las amenazas del phishing en la banca electrónica,
- de los dispositivos electrónicos,
- aprender a detectar, prevenir y combatir las amenazas del ciberespacio,
- aprender hábitos que le protejan de las amenazas que acechan en Internet,
- conocer las actividades de lucha contra los contenidos ilícitos y el spam en Internet y presentar cuestiones relacionadas con las amenazas derivadas del uso de los teléfonos móviles, los juegos en línea, el intercambio de archivos P2P y otras formas de comunicación en línea (chats, mensajería instantánea, etc.)
- conocer las formas de prevenir la delincuencia en línea mediante el uso de nuevos y mejores programas informáticos,
- aprender los conceptos básicos de las amenazas a la información,
- conocer las causas y los efectos de las amenazas a la información,
- conocer los métodos de búsqueda de información valiosa,
- conocer los métodos de verificación de la información, navegar entre la niebla informativa,
- aprender los conceptos básicos de los tratamientos físicos y mentales,
- conocer las causas y los efectos relacionados con el tema,
- conocer los riesgos psicológicos, incluyendo los tipos de adicción, los síntomas y la prevención,
- desarrollar hábitos de uso seguro de los dispositivos electrónicos.

Resultados de aprendizaje del alumno/a:

El participante en el curso:

- demostrar el conocimiento de los conceptos básicos relacionados con las ciberamenazas,
- conocer las normas de uso de inicios de sesión y contraseñas seguras, el uso seguro de la banca por Internet y las normas de uso seguro de equipos informáticos y sitios web del grupo de "alto riesgo",

- fue capaz de reconocer un intento de phishing y también de almacenar los datos informáticos de forma segura,
- podrá demostrar que conoce los términos especializados en este campo, estará familiarizado con las disposiciones legales básicas relacionadas con los ciberdelitos,
- podrá identificar los tipos de ciberacoso, los tipos de contenidos nocivos en línea, podrá conocer los procedimientos de reacción ante el ciberacoso y reconocer los contactos peligrosos en línea,
- podrá demostrar que conoce los conceptos relacionados con las amenazas de la información, entre ellos: la frustración informativa, la soledad informativa, el estrés informativo, las amenazas de la aceptación acrítica de las noticias, las noticias falsas, el caos informativo, la niebla informativa, el odio, las campañas de desinformación,
- sabía utilizar diversos métodos de verificación/búsqueda de información y cómo verificar la información y comprobar sus fuentes,
- podría demostrar que conoce las amenazas físicas y mentales básicas derivadas del uso prolongado y frecuente de dispositivos electrónicos,
- conocer los conceptos relacionados con estas amenazas, saber qué medidas tomar para contrarrestarlas, aprender las normas de uso seguro de los dispositivos electrónicos,
- fue capaz de reconocer las dolencias relacionadas con el uso prolongado y frecuente de dispositivos y herramientas TIC, evaluar eficazmente las causas y efectos de estas amenazas y preparar un espacio seguro para su uso.

Texto, materiales y suministros:

Enlaces relacionados con el tema que se está tratando:

- Correo electrónico y ataques de phishing, „OUCH!”, Boletín de seguridad informática de 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
- Banca por Internet: nuevas amenazas, artículo de http://www.chip.pl/artykuly/porady
- Actualizando el 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)
- Algunos consejos sencillos del correo electrónico, „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
- Evaluación de la credibilidad de la información en los sitios web, las revistas científicas de la 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
- „Ecología de la información y recursos de información en las bibliotecas y el ciberespacio”, edited by Katarzyny Materskiej, Beaty Taraszkiewicz, ISBN 978-83-88783-24-1

- " Enfermedades de los medios de comunicación " of the 21st century in the Polish media, Dariusz Baran
- Estrés informativo -¿vemos un riesgo para la salud? 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.

Forma básica de las clases: las clases fijas se imparten en una sala de ordenadores conectada a Internet con un proyector multimedia conectado, que incluye

- materiales de formación preparados por el formador,
- ordenadores / tabletas / teléfonos inteligentes, conexiones a Internet, proyector,
- presentación con información clave y gráficos.
-

Política de calificaciones:

El participante es clasificado al final del curso. Consiste en sumar el compromiso y determinar la nota final. La nota final se determina en función del test. Se considera que el test de aprobación es el 50% de las respuestas correctas.

Estructura del curso:

Delitos contra la protección de la información - 240 minutos.
Delitos en las redes sociales - 240 minutos.
Amenazas a la información (enfermedades) - 240 minutos.
Amenazas y salud - 240 minutos.