Programa detallado del curso

Título de la actividad de aprendizaje	**Evitar las amenazas derivadas del uso de las TIC en la vida cotidiana**
Tema	**Delitos contra la protección de la información**
Resumen	La delincuencia informática es un fenómeno relativamente nuevo y su aparición está claramente vinculada al desarrollo de Internet. El desarrollo de tecnologías para la recogida, el tratamiento y la transmisión automáticos de información conlleva amenazas hasta ahora desconocidas. Esto plantea la necesidad de introducir nuevos medios de protección contra las injerencias ilícitas en la esfera de la vida privada y social, así como de regular los métodos de obtención y utilización de la información relacionada con estas esferas. Esta formación explicará el significado básico de los términos de los delitos de protección de la información. Los participantes aprenderán más sobre los riesgos asociados al uso de las TIC, los efectos y los métodos de prevención. Los participantes aprenderán más sobre las amenazas del phishing, facilitadas por las TIC, sobre sus efectos y métodos de uso.
Duración	240 min
Grupo de edad	30+
Objetivos de la actividad	- Aprender los conceptos básicos de los ciberataques, incluyendo el concepto de *phishing* - Aprender a detectar y combatir amenazas del ciberespacio - Conocer los hábitos que protegerán contra las amenazas que acechan en la red (contraseñas seguras, autenticación de dos pasos, análisis del contenido del correo electrónico)) - Aprender sobre formas para prevenir el *phishing* - Conocer las amenazas del *phishing* en la banca electrónica
Orientación para una correcta realización de las actividades	
Metodología para la realización de la actividad	Forma básica de las clases: las clases fijas se imparten en una sala de ordenadores conectada a Internet con un proyector multimedia conectado. Otras formas de clases aceptadas: aprendizaje en línea o semipresencial. Tipo de técnica de aprendizaje: aprendizaje entre iguales. Tipo de técnica de aprendizaje: aprendizaje en acción. Se aceptan todas las ayudas visuales (presentaciones, fotos, vídeos...). Un máximo de 12 personas deben participar en el proceso de aprendizaje y todos deben ser apoyados por un segundo formador que proporcionará apoyo individual al alumnado.
Métodos	Conferencia, ejercicios, lluvia de ideas, concurso, espectáculo multimedia Trabajo en parejas, trabajo en grupo, debate

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

	Método de resolución de problemas
Herramientas y materiales	- Materiales formativos preparados por el professor - Ordenadores/ tabletas/ smartphones, conexiones a internet, proyector - Presentación con información clave y gráficos - aplicaciones informáticas
Conocimientos adquiridos durante las clases	La persona participante sabe: - conceptos básicos relacionados con las ciberameanzas: ciberataques, *phishing,* softwares maliciosos (*malware)*, *phishing*, - normas para el uso seguro de contraseñas y registros, - principios del uso seguro de la banca por internet, - normas para el uso seguro de los equipos y sitios informáticos del grupo de "alto riesgo«.
Habilidades	La persona participante es capaz de: - configurar un ordenador para incrementar su seguridad, - crear y almacenar de forma segura contraseñas de apliacaciones, - reconocer los intentos de *phishing*, - almacenar de forma segura los datos informáticos.
Proceso	La tarea del formador es destacar el tema y combinarlo con ejemplos prácticos de la vida cotidiana. El proceso se apoya en una presentación interactiva y fomenta el debate y la participación de los participantes. En la medida de lo posible, la transmisión de conocimientos se combina con la acción práctica.
Sesión 1 **Sesión de apertura** *30 min*	El formador se presenta y da la bienvenida a los participantes. Informa a los participantes sobre los principios, los objetivos de la formación y su relación con los temas anteriores y futuros (si procede). El formador puede establecer objetivos adicionales y el programa del módulo. Otros elementos de motivación son bienvenidos.
Sesión 2 Tipos de ciberamenazas *60 min*	El objetivo principal de la sesión es identificar, en un ejemplo sencillo, las ciberamenazas como el malware, y en particular el concepto de *phishing*. Introducción al tema mediante la presentación de una historia que contenga los principales hilos conductores del tema tratado, por ejemplo.: *la historia de un amigo que recibió por casualidad un correo electrónico con un enlace peligroso. El correo electrónico se enviaba desde la institución DHL e informaba sobre el envío del artículo, el correo contenía un enlace al formulario de datos de corrección de los gastos de envío. El mensaje contenía todos los síntomas de veracidad: logotipos de la institución, firmas, dirección de correo electrónico, sólo el contenido carecía de caracteres polacos, el enlace dirigía al formulario de pago, el pago de una tasa adicional por el envío.* *El formador mostrará el correo electrónico en el proyector.* *El formador llevará a cabo un debate sobre el aspecto visual del mensaje y destacará los puntos básicos que deben comprobarse en una situación de este tipo.* Un mensaje apoyado por imágenes / puede ser una presentación / para crear una atmósfera auténtica.

	<u>Desarrollo de la sesión</u> Contenido didáctico: - el fenómeno del *phishing*, - correo electrónico - visualización y descarga segura de archivos adjuntos, enlaces. Al principio, los temas individuales deben ir precedidos de ejemplos de amenazas, incluir informes y descripciones de casos "de la vida real". Presente y practique ejemplos de cómo prevenir las amenazas utilizando programas informáticos y el sentido común. Un resumen de la información más importante al final de la sesión.
Sesión 3 Ciberamenazas – causas y efectos *60 min*	Plantear una cuestión introduciendo el tema de la sesión: - *¿Sabes cómo reconocer una amenaza de phishing?* - *¿Has sufrido un ataque de malware?* - *¿Da ejemplos de ciberataques con los que te has enfrentado?* - *¿Cómo se crean las contraseñas para acceder a los servicios de Internet?* *Facilita el debate con/entre los participantes.* *Da a los participantes espacio suficiente para que compartan sus experiencias y pensamientos. Apoye el debate en sus grupos y anime a los participantes a ser activos y comprometidos.* Con la ayuda de los participantes y los formadores, se responderá a la pregunta: - *¿Cómo protegerse contra el phishing?* - *¿Cómo comportarse en caso de detectar un ciberataque?* - *¿Cómo crear contraseñas de acceso seguras?* Introducción de conceptos y normas sobre el uso seguro de las TIC*:* - *formas de crear y almacenar inicios de sesión y contraseñas seguras,* - *seguridad de los sitios web (certificado SSL),* - *uso de software antispam.* Resumen de las cuestiones más importantes relativas a las causas y los efectos de las amenazas de ciberataques*.*
Sesión 4 Ciberamenaza -retos y banca electrónica *90 min*	Plantear una pregunta que introduzca el tema de la sesión: - *¿Utilizas la banca electrónica? ¿En qué medida?* - *¿Recibes información del banco? ¿Por qué vía?* - *¿Con qué frecuencia realizas transferencias por Internet?* - *¿Compruebas/comparas los números de cuenta antes de enviar la transferencia?* *Conduce a un intercambio constructivo de opiniones. Anota las declaraciones de todos los participantes en la pizarra o en notas adhesivas.* *Deja a los participantes espacio suficiente para que compartan sus ideas y pensamientos. Apoya el debate en tus grupos y anima a los participantes a ser activos y a participar.* **En la siguiente parte, puedes utilizar un ejemplo**, *la historia de una persona que hizo una transferencia a una cuenta equivocada, porque no comprobó que el número de cuenta era correcto antes de aceptar la transferencia (comprobación cuidadosa de los mensajes de texto).* *Pregunta a los participantes si se han encontrado con estos casos.* *Apoya el debate en sus grupos y anima a los participantes a mostrarse activos y comprometidos*.

	El tema principal de la sesión es la banca electrónica en cuanto a la suplantación de identidad: la ejecución segura de las transferencias. Por último, haz un análisis conjunto de los problemas de phishing que has aprendido. Prepara un mapa mental de las mejores prácticas para detectar estas amenazas. El mapa mental debe contener min.: - el análisis de los mensajes de correo electrónico para comprobar su corrección y veracidad - comprobación de la exactitud de la dirección del sitio web (certificado SSL), enlaces enviados en el correo electrónico, - comprobación de la corrección gramatical y ortográfica del contenido del correo electrónico, - comprobar la hora y el día de envío del correo electrónico, - el sentido común en las operaciones financieras en línea, - comprobación de la corrección del número de cuenta / mensaje de texto durante la transferencia en línea, - uso de inicios de sesión y contraseñas seguras, - utilizar la autenticación de cuenta de dos factores (cuando sea posible), - utilizar la dirección del sitio web verificado del banco, no entrar a través del enlace del correo electrónico. El formador al final de esta sección resume la información más importante en el tema de los Delitos de Protección de la Información.
Evaluación/valoración	La evaluación del módulo en forma de cuestionario (por ejemplo, en papel o en versión electrónica en Kahoot) incluye al formador (cuestionario1) y a los participantes (cuestionario2). Las herramientas de evaluación y el proceso de evaluación son preparados y realizados por el organizador de la formación.
Bibliografía, enlaces o recursos	Enlaces que se asocian con el tema que se está tratando. Debe ser actual para el país y la época actual. - Correo electrónico y ataques de phishing, "¡OUCH!", Boletín de seguridad informática del Instituto SANS y CERT Polonia, 2/2013 (http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201302_po.pdf) - Laskowski P., Seguridad de las operaciones bancarias electrónicas, "Boletín científico de la Sección de Matemáticas e Informática de Chełm", 1/2008 - Internet banking - new threats, artículo de http://www.chip.pl/artykuly/porady - Actualización del software, "OUCH!", Boletín de seguridad informática del Instituto SANS y CERT Polonia - 8/2011 (http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201108_po.pdf) - Contraseñas seguras y fuertes, "¡OUCH!", Boletín de seguridad informática del Instituto SANS y CERT Polonia - 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., Guía de seguridad del correo electrónico - Visión general de las amenazas más populares, "Haking" 1/2011 - Liderman K., Seguridad de la información, editorial científica polaca PWN, Varsovia 2013.

Actividades adicionales	Ejemplos presentados en forma de minipresentación, realización de un debate temático, basado en una cuestión seleccionada, prueba de grupo, elaboración conjunta de un mapa mental que consolide la cuestión. Realización de un test de prueba: enlace al test "¿Reconoces un phishing?". Google: https://phishingquiz.withgoogle.com
¿Tutoría para los oyentes?	Sí; el objetivo de la tutoría es desarrollar competencias y actitudes para estar atentos a la necesidad de proteger la información, ser conscientes de las consecuencias de los delitos contra la protección de la información y cumplir con los principios de uso seguro de las herramientas TIC en el día a día.
Validación del proceso de enseñanza	La validación del proceso de aprendizaje es bienvenida siempre que se centre en algunos puntos clave. El método de validación debe estar relacionado con la forma de impartir las clases y debe motivar a los participantes a actuar.
Requisitos especiales para el formador	Además del conocimiento de los temas de seguridad, el formador debe tener cualificaciones en TI y tener un buen conocimiento de las aplicaciones/herramientas que se enseñan/utilizan durante la formación. El formador también debe tener experiencia en el trabajo con adultos, especialmente con adultos poco cualificados.
Elementos innovadores	Cómo se documenta el programa. Vinculación de la teoría con la práctica. Evaluación electrónica de las actividades.

Diccionario de términos:

Aprendizaje entre iguales - *trabajo en grupo de los participantes en la formación, durante el cual tienen la oportunidad de intercambiar información y habilidades, basándose en su propio análisis, sin la forma de libro de texto.*

Aprendizaje en acción *- el trabajo de un grupo de participantes en la formación con diferentes competencias y experiencia, que trabajan en la resolución de un problema real y complejo y al mismo tiempo desarrollan sus habilidades de liderazgo, convirtiéndose al mismo tiempo en un equipo altamente eficaz.*

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