Seguridad de la Información |

Seguridad y Peligros en Internet

Detalles del curso:

Duración: 5 h.

Modalidad: e-Learning

Información e inscripción:

685 457 610 - 615 844 193

formacion@laberit.com

LÃBERIT | CENTRO DE FORMACIÓN TIC.

Introducción

En la actualidad, vivimos conectados a Internet, ya sea para acceder a nuestro correo electrónico, redes sociales, sistemas o sitios laborales, entre otros. Pero también existen riesgos.

Al navegar por Internet nos exponemos a diversas amenazas y encontrarnos con muchas direcciones de sitios web, o URLs, maliciosas, que nos pueden traer problemas si accedemos a ellas. Entre otras cosas, los ciberdelincuentes intentarán: engañarnos para poder borrar o secuestrar nuestros archivos y hacerse con nuestros datos personales y/o nuestras contraseñas. Por ello, es muy importante aprender una serie de buenas prácticas que nos ayudarán a navegar tranquilos por Internet y no caer en los constantes engaños de los que podemos ser víctimas.

Almacenar nuestra información en Internet, en la nube, tiene grandes ventajas, pero también veremos los peligros que ello puede conllevar y cómo prevenirlos.

Las redes sociales ya son parte de nuestras vidas. Generar contenido y compartirlo con otras personas es el objetivo principal. Sin embargo, debemos ser conscientes de que toda la información que voluntariamente publicamos puede ser utilizada de manera incorrecta por personas con malas intenciones. Cualquier información relativa a nuestra identidad, ocupaciones y preferencias debe ser considerada sensible y privada. Un tercero malintencionado con dicha información podría causar daño e nuestra reputación, difamándonos e incluso acosándonos.

Nuestros menores pueden llegar a ser víctimas de chantajes y abusos sexuales a través de Internet. Existen adultos que se hacen pasar por menores en Internet y buscan establecer un contacto con niños/as y adolescentes. Establecen una relación de confianza pasando después al control emocional y, finalmente, al chantaje con fines sexuales. Esto es el grooming. Esta práctica tiene diferentes niveles de interacción y peligro: el acosador puede hablar de sexo con la víctima, conseguir material íntimo y hasta llegar a mantener un encuentro sexual.

Las fake news, también llamadas bulos, son noticias falsas que se propagan por Internet con el objetivo de desinformarnos, engañarnos y manipularnos. Gracias a las redes sociales y a las aplicaciones de mensajería instantánea, como WhatsApp, se publican y se difunden a gran velocidad. Las noticias falsas pueden tratar sobre cualquier temática o noticia de actualidad y gestarse en distintos ámbitos, como dentro de un colegio, una ciudad, o incluso a nivel mundial.

En la actualidad, la compras en tiendas online son cada vez más frecuentes. En la actualidad, más del el 50% de los ingresos producidos por ventas online se producen en redes sociales, y una gran cantidad de usuarios de Internet han comprado o comprarán a través de ellas. Este

auge, conocido como “Comercio social” hace que las publicidades en las redes sociales se incrementen, convirtiéndolas en el cebo perfecto para los ciberdelincuentes, especialmente en fechas como el Black Friday, Cyber Monday y Navidad.

¿Por qué hacer este curso?

Para empezar, es un curso divertido y se hace fácil; conocerás los riesgos más comunes que se dan cuando usas Internet y aprenderás una serie de buenas prácticas y costumbres que será importante seguir para evitarlos.

Una de las mayores preocupaciones hoy en día si trabajas en entornos digitales e informáticos es estar prevenido ante los constantes peligros a los que te enfrentas cuando usas Internet. Este curso te ayudará a conocerlos, detectarlos y a saber cómo actuar frente a ellos para tener protegidos tus equipos informáticos.

¿Para qué sirve o qué es la formación en seguridad y peligros en Internet?

Con este curso conocerás los riesgos y peligros que podemos encontrarnos en el uso de Internet. No sólo existen peligros cuando navegamos o hacemos búsquedas en Internet, también los podemos encontrar con los archivos que subimos a la nube, cuando usamos nuestro correo electrónico, las redes sociales hacemos compras en tiendas online. Otros de los peligros más habituales hoy en día son el grooming y las fake news. En este curso no sólo conocerás todas estas amenazas, sino que aprenderás a combatirlas.

En definitiva, el objetivo de este curso es facilitar la adopción de nuevos hábitos de seguridad, concienciar de la responsabilidad de cada persona al utilizar Internet y saber cómo actuar antes las constantes amenazas y peligros de los que podeos ser víctimas.

El conocimiento que aporta es un valor añadido que, sin duda, se convierte en una ventaja competitiva definitiva.

¿A quién va dirigido?

Este curso está dirigido a todas aquellas personas que usan Internet y quieran aprender a proteger de la mejor forma posible su entorno digital e información privada.

De esta forma, cualquier persona habituada al uso de medios informáticos y digitales en su entorno laboral o personal puede sacar provecho de esta formación.

Objetivos didácticos

Los principales objetivos didácticos de esta acción formativa son:

- Conocer los riesgos y seguridad en la navegación web.
- Conocer los riesgos y seguridad de la utilización y compartición de datos en la nube.
- Conocer los riesgos y seguridad de las direcciones de Internet maliciosas.
- Conocer los riesgos y seguridad del uso del correo electrónico.
- Conocer los peligros que podemos encontrar en el uso de las redes sociales y las medidas a adoptar para combatirlos.
- Conocer los peligros del Grooming (abuso sexual a través de Internet) y las medidas a adoptar para evitarlos.
- Conocer los peligros de la fake news (noticias falsas) y saber cómo evitarlos).
- Conocer los riesgos y seguridad de las compras en tiendas online y su relación con las redes sociales.

Metodología

Se van a aplicar varias metodologías didácticas.

- **Deductiva**. Se expone la teoría de tal forma que el alumno va accediendo a los contenidos de manera secuencial, de menor a mayor importancia, complejidad, etc.
- **Inductiva**. Se plantean preguntas a modo de ejercicios para explicar la teoría. El alumno aprende sobre la acción que va realizando, con ejemplos y contraejemplos, y de las consecuencias de dicha práctica (negativa y positiva).

La idea es generar actividad entre las alumnas y los alumnos, haciendo que se sientan involucrados en el proceso de aprendizaje.

El curso está desarrollado siguiendo los estándares técnicos y funcionales que tiene la plataforma de teleformación Moodle de Lãberit.

Una vez se accede al curso, podrás acceder a los siguientes recursos didácticos:

- **Guía del alumno**

  Se trata de una guía donde se exponen los objetivos, contenidos, organización e instrucciones de manejo del curso.

- **Unidad didáctica**

  Son los contenidos propiamente dichos del curso. Están estructurados en Capítulos y/o Temas y éstos, a su vez, en páginas y ejercicios prácticos relacionados con el contenido aprendido. Para la navegación por la unidad de aprendizaje dispondrás de una serie de botones tanto en el margen superior como inferior de la pantalla.

A través del curso, podrás trabajar de dos maneras:

- **FORMACIÓN:** El curso tiene una navegación **secuencial** si es la primera vez que accedes a él; es decir, es obligatorio ver los contenidos de cada página en el orden que se muestran en el índice de contenidos y dentro de cada tema. Además, será obligatorio realizar las acciones que se piden en cada página.

- **CONSULTA:** Una vez hayas visto todo el contenido de una página, tema o el curso completo, la navegación por esa página, tema o curso quedará abierta y ya podrás navegar libremente por sus contenidos, sin necesidad de volver a verlos de forma secuencial.

Programa

El curso “Seguridad y peligros en Internet” consta de 2 unidades de aprendizaje. Los títulos y contenidos son los siguientes:

UNIDAD DE APENDIZAJE 1: SEGURIDAD EN INTERNET Y EN LA NAVEGACIÓN WEB

Capítulo 1. Seguridad en la navegación web

Tema 1.1.: Introducción. Importancia de la navegación segura.
Tema 1.2.: Escenario 1: Complementos y extensiones maliciosos.
Tema 1.3.: Escenario 2: Instalación de aplicaciones maliciosas.
Tema 1.4.: Escenario 3: Enlaces, botones y ventanas emergentes peligrosos.
Tema 1.5.: Conclusiones.

Capítulo 2. Seguridad en la nube

Tema 2.1.: Introducción. Ventajas de usar un servicio en la nube.
Tema 2.2.: Escenario 1: Compartir carpetas de forma insegura.
Tema 2.3.: Escenario 2: Notificaciones y enlaces inseguros de acceso a la nube.
Tema 2.4.: Escenario 3: Cifrar nuestros archivos para prevenir riesgos.
Tema 2.5.: Prevenir el acceso no autorizado a nuestros archivos.
Conclusión.

Capítulo 3. Direcciones de Internet maliciosas

Tema 3.1.: Introducción. Las URLs.
Tema 3.2.: Escenario 1: Sitios Web que no son seguros.
Tema 3.3.: Escenario 2: URLs similares.
Tema 3.4.: Escenario 3: URLs engañosas. Subdominios.
Tema 3.5.: Conclusiones.

Capítulo 4. Internet y correo electrónico

Tema 4.1.: Introducción. Conceptos básicos.
Tema 4.2.: Escenario 1: Petición de datos personales en sitios web.
Tema 4.3.: Escenario 2: Descarga de archivos maliciosos.
Tema 4.4.: Escenario 3: Recepción de correos basura (SPAM).
Tema 4.5.: Conclusiones.

UNIDAD DE APENDIZAJE 2: SEGURIDAD EN LAS REDES SOCIALES, GROOMING, FAKE NEWS, Y COMPRAS SEGURAS

Capítulo 1. Redes sociales seguras

Tema 1.1.: Introducción: Datos sensibles y privados.
Tema 1.2.: Escenario 1: Peligro de compartir información y fotos personales.
Tema 1.3.: Escenario 2: Peligro de aceptar solicitudes de amistad de desconocidos.
Tema 1.4.: Escenario 3: Tener cuidado con las opiniones vertidas en las redes sociales
Tema 1.5.: Conclusiones.

Capítulo 2. Grooming: Abuso sexual a través de Internet

Tema 2.1.: Introducción: Qué es y objetivos del grooming.
Tema 2.2.: Escenario 1: Juegos en línea con menores.
Tema 2.3.: Escenario 2: Amigos en línea.
Tema 2.4.: Escenario 3: Conocidos cercanos.
Tema 2.5.: Cómo debemos actuar. Conclusión.

Capítulo 3. Fake News

Tema 3.1.: Introducción. Noticias falsas y engaños deliberados.
Tema 3.2.: Escenario 1: Estafas económicas.
Tema 3.3.: Escenario 2: Comentarios falsos y difamatorios.
Tema 3.4.: Escenario 3: Tratamientos y curas milagrosas.
Tema 3.5.: Conclusiones.

Capítulo 4. Compras seguras en tiendas online y redes sociales

Tema 4.1.: Introducción. E-commerce y Marketplace.
Tema 4.2.: Escenario 1: Una publicidad demasiado atractiva.
Tema 4.3.: Escenario 2: Una App engañosa y maliciosa.
Tema 4.4.: Escenario 3: Peligro de insertar nuestras credenciales en sitios web maliciosos.
Tema 4.5.: Reducir las publicidades en nuestras redes sociales.
Conclusiones.

LÃBERIT | CENTRO DE FORMACIÓN TIC.

Acreditado:

Microsoft Imagine Academy
Program Member

Fundación Estatal
PARA LA FORMACIÓN EN EL EMPLEO

LABORA
Servei Valencià d'Ocupació i Formació

CertiProf® | Partner

Pearson VUE
Authorised
Test Centre

CERTIPORT
A PEARSON VUE BUSINESS
AUTHORIZED TESTING CENTER

Avenida Cataluña, 11, bajo derecha. 46020 -Valencia
960 075 817 (Ext. 257) (Ext. 276) | formacion@laberit.com
formacion.laberit.com