

CIBERSEGURIDAD PARA USUARIOS: PROTECCIÓN Y PREVENCIÓN



Presentación

La ciberseguridad es un concepto que todos, las personas profesionales del mundo de las tecnologías de la información y, sobre todo, los usuarios de estos servicios, debemos conocer a fondo. Vivimos en un mundo cada vez más conectado, mejor dicho, "hiper-conectado". Móvil, tabletas, ordenador, relojes, coches, pulseras de salud... todo está conectado y generando multitud de datos en muchos sitios distintos.

Prácticamente no hay ningún ámbito de información de nuestras vidas que no esté almacenado en algún lugar: datos personales, médicos, ubicación, profesionales, circuitos de ejercicios ("running"), bancarios...

En este curso trataremos la seguridad en los principales ámbitos de las tecnologías que nos rodean. Veremos casos reales de cómo, de una forma sencilla, pueden obtener acceso a nuestra información privada. Y otros casos más complejos, pero habituales, que nos darán una idea de lo vulnerable que es el mundo digital en el que estamos inmersos.

Objetivos

El principal objetivo de este curso es conocer las amenazas del mundo de las tecnologías de la información: los virus, el "malware", los intentos de intrusión y el robo de información confidencial, entre otros.

Veremos cuáles son las principales amenazas y cómo funcionan. A partir de este conocimiento, aprenderemos cómo protegernos ante ellas, adquiriendo técnicas preventivas que harán que nuestra documentación y privacidad estén a salvo.

Completaremos la formación con un repaso de aspectos legales dentro del mundo de la ciberseguridad con ejemplos de situaciones reales.

- 1. La seguridad en los sistemas de información**
 - a. Conceptos de seguridad
 - b. Clasificación de las medidas de seguridad
 - c. Requerimientos de seguridad en los sistemas
 - d. "Hacker"
 - e. ¿Y los ataques de países del Este?
- 2. Ciberseguridad**
 - a. Concepto de ciberseguridad
 - b. Vulnerabilidades
 - c. Amenazas más frecuentes
 - d. Tecnologías de seguridad
 - e. Gestión de la seguridad informática
 - f. Copias de seguridad
- 3. Software peligroso**
 - a. Conceptos sobre software dañino
 - b. Clasificación de software dañino
 - c. Descripción de las amenazas. Virus
 - d. Otras amenazas
 - e. Amenazas avanzadas y en los móviles
- 4. Seguridad en redes inalámbricas (Wifi)**
 - a. El entorno inalámbrico
 - b. Protocolos Wifi
 - c. Protocolos de seguridad
 - d. Canales
 - e. Cómo realizar una intrusión en una red WiFi
 - f. Wifi profesional: 802.1x
 - g. NFC
- 5. Herramientas de seguridad**
 - a. Herramientas de seguridad
 - b. Autenticación de usuarios
 - c. Control de acceso a Internet
- 6. Reglamentos y aspectos legales**
 - a. Crisis del "coronavirus"
 - b. RGPD
 - c. ISO 270001. Seguridad de la información
 - d. Supuestos legales
 - e. Protección ante compras y fraude en Internet
 - f. Derecho al olvido

Dirigido a

Dirigido a todos los que estamos en el mundo digital.

Usuarios aunque también se incluyen pequeñas recomendaciones para los casos de tener una pequeña red de trabajo.

TELEFORMACIÓN

Modalidad y duración

- **25 horas** de duración
- Plataforma, contenidos y sistema tutorial adaptado a Bonificaciones de Fundae con acceso a:
 - Contenido Multimedia.
 - Videotutoriales
 - Recursos Adicionales
 - Foros de Debate
 - Pruebas de evaluación

Fechas

Del 17 Febrero al 26 Mayo de 2022

Francisco Javier Moreno

Formador, consultor y speaker internacional.

25 años de experiencia en entidades financieras (Santander y Caixabank)

Colaborador en Escuelas de negocios y universidades (UPM, Nebrija...)

Profesor en áreas como big data, small data, data analytics, gestión de riesgos, business intelligence durante más de 10 años.

Colaborador en consultoras y grandes empresas (Telefonica, Indra).

Tutor en proyectos formativos online desde hace 20 años.



El tutor

PRESUPUESTO		
Hasta 9 alumnos	De 10 a 25 alumnos	De 26 en adelante
187,5 €/alumno	175 €/alumno	150 €/alumno
(7,5 €/h/alumno)	(7 €/h/alumno)	(6 €/h/alumno)

Este curso es 100% bonificable ante Fundae.

Desde BAI ofrecemos realizar la gestión sin coste adicional para la empresa.