Ciberseguridad: prevención, detección y protección frente a amenazas

JUSTIFICACIÓN

Los avances tecnológicos han traído consigo una amplia gama de amenazas cibernéticas, y a medida que las organizaciones invierten en soluciones de seguridad sofisticadas, también se han dado cuenta de que el eslabón más débil en esta cadena es el ser humano. Debido a ello, se hace evidente y fundamental dotar a los usuarios finales de los conocimientos y habilidades prácticas necesarias para prevenir, detectar y protegerse de los posibles ataques que puedan sufrir y, aumentar así su nivel de protección y concienciación frente a dichas amenazas.

CONTENIDOS

Módulo I: Introducción a la ciberseguridad (5 horas)

Módulo II: Seguridad en la navegación web (25 horas)

Módulo III: Seguridad en el correo electrónico (20 horas)

Módulo IV: Seguridad en los dispositivos móviles (20 horas)

Módulo V: Identificación y protección frente a fraudes online (10)

OBJETIVOS

Objetivos:

- Conocimiento práctico y atractivo sobre los términos más importantes que rodean al concepto de ciberseguridad
- Conocimiento teórico y práctico de las amenazas y medidas de protección asociados a la navegación web
- Conocimiento teórico y práctico de las amenazas y medidas de protección asociados al uso del correo electrónico
- Conocimiento teórico y práctico de las amenazas y medidas de protección asociados al uso de los dispositivos móviles
- Conocimiento teórico y práctico para la identificación y protección frente a fraudes que se producen en internet

80 horas / 8 semanas	**Nivel de profundidad: Básico***	**Modalidad:** *e-learning*	**Ampliar información:** web: www.ingenierosformacion.com e-mail: secretaria@ingenierosformacion.com Tlf: 985 73 28 91

* Partiendo de la base de que los cursos están dirigidos a un perfil mínimo de Ingeniero

Presentación

Esta acción formativa implementada en modalidad online proporciona los conocimientos teóricos y prácticos necesarios para prevenir, detectar y protegerse frente a las actuales amenazas a la que todos estamos expuestos en el

uso de las tecnologías, centrándose principalmente en la utilización del correo electrónico, la navegación web, dispositivos móviles y fraudes online . La realización del curso no sólo aporta labores de concienciación sino que todo su contenido está confeccionado con la intención de transferir al alumnado conceptos clave y habilidades totalmente útiles y aplicables al panorama actual de amenazas.

Modalidad

Modalidad e-learning.

El curso se impartirá integralmente vía Internet en la Plataforma de Formación (https://www.ingenierosformacion.com).

Carga lectiva

80 horas

Duración

8 semanas

Precio

Reseña del cálculo de precios

Precio base: 320€.

A este precio base se le podrán aplicar los siguientes descuentos:

Descuentos exclusivos para **asociados**

Descuento	Descripción
Asociados: descuento de 160€	Este descuento del 50% se aplica a todos los asociados de la AIU.

Mínimo de alumnos

Para que la acción formativa pueda llevarse a cabo se necesitará un número mínimo de **10** alumnos.

La matrícula se cerrará cuando se hayan alcanzado un número de **80** alumnos.

Nivel de profundidad

Nivel de profundidad 1

(Partiendo de la base de que todos los cursos están dirigidos a un perfil mínimo de Ingeniero, se valorará el curso que presenta con niveles de 1 a 3 de forma que el 1 significará que el curso es de carácter básico, 2 el curso es de carácter medio y 3 el curso es de carácter avanzado.)

Perfil de Destinatarios

Curso dirigido a cualquier persona que haga uso del correo electrónico, navegue por internet, utilice un dispositivo móvil y pueda ser objeto de fraudes online , es decir, hoy en dia prácticamente todo el mundo que haga un uso cotidiano de las tecnoclogías y desee aumentar sus nivel de protección frente al panorama actual y real de amenazas.

Escrito en un lenguaje cercano y con pocos tecnicismos, esta acción formativa se adecúa perfectamente a usuarios con un nivel básico o medio en el uso de las tecnologías.

Por último, dada su tranversabilidad encaja perfectamente tanto en entornos corporativos que deseen elevar el nivel de protección de sus empleados y, por consiguiente, el de los sistemas de información de la empresa, así como usuarios independientes que deseen aprender ciberseguridad sin tener que estudiar conceptos generales alejados del día a día.

Requisitos previos necesarios:

No se requieren conocimientos previos en ciberseguridad, únicamente un nivel básico o medio en el uso de las tecnologías.

Requisitos previos recomendados:

No se requieren conocimientos previos en ciberseguridad, únicamente un nivel básico o medio en el uso de las tecnologías.

Justificación

Los avances tecnológicos han traído consigo una amplia gama de amenazas cibernéticas, y a medida que las organizaciones invierten en soluciones de seguridad sofisticadas, también se han dado cuenta de que el eslabón más débil en esta cadena es el ser humano. Debido a ello, se hace evidente y fundamental dotar a los usuarios finales de los conocimientos y habilidades prácticas necesarias para prevenir, detectar y protegerse de los posibles ataques que puedan sufrir y, aumentar así su nivel de protección y concienciación frente a dichas amenazas.

Objetivos

Objetivos:

- Conocimiento práctico y atractivo sobre los términos más importantes que rodean al concepto de ciberseguridad
- Conocimiento teórico y práctico de las amenazas y medidas de protección asociados a la navegación web
- Conocimiento teórico y práctico de las amenazas y medidas de protección asociados al uso del correo electrónico
- Conocimiento teórico y práctico de las amenazas y medidas de protección asociados al uso de los dispositivos móviles
- Conocimiento teórico y práctico para la identificación y protección frente a fraudes que se producen en internet

Docente

Antonio José Gamero León

Tecnico/administrador en la **Unidad Técnica de Ciberseguridad** de EPICSA - **Diputación de Cádiz**

Contenido

Módulo I: Introducción a la ciberseguridad (5 horas)

1. Introducción
2. Ciberseguridad: definición y conceptos
3. Comencemos por algunos conceptos
4. Identificando a los ciberdelincuentes
5. Tipos de ciberataques
6. Ingeniería social
7. Buenas prácticas generales en el uso de las tecnologías

Módulo II: Seguridad en la navegación web (25 horas)

1. Introducción
2. Conociendo los navegadores web más populares
3. Familiarizándonos con la terminología

4. Extensiones: un riesgo y un aliado
5. Explorando los rincones de internet
6. Nuestra privacidad en línea está en peligro
6.1. Data brokers
7. El navegador recopila nuestra información, ¿lo sabías?
7.1. Fingerprinting
7.2. Modo incógnito, una forma de proteger nuestra privacidad
8. Cookies, conócelas a fondo
8.1. Antes de empezar, un poco de historia
8.2. Conociendo a las cookies
8.3. Puntualizaciones sobre el reglamento de la UE
8.4. Gestión de cookies recolectadas
9. Cuentas de Google y nuestra privacidad
9.1. Motivos por los que se te muestran ciertos anuncios
9.2. Qué tipo de anuncios me muestra Google
9.3. Cómo colabora Google con los anunciantes
9.4. Dónde se pueden mostrar los anuncios
10. Utiliza contraseñas seguras en sitios web
10.1. Errores más comunes cuando usamos contraseñas
10.2. Cómo nos roban las contraseñas
10.3. Creando una contraseñas robusta
10.4. Cuantas contraseñas diferentes debo usar
10.5. Frecuencia de cambio
10.6. Qué hacer si nuestras contraseñas se han filtrado
10.7. Registrarte con tu cuenta de Google, Facebook o Twitter
10.8. Gestores de contraseñas
11. Explorando el protocolo HTTPS
11.1. SSL/TLS y HTTPS
11.2. Cómo funciona HTTPS
11.3. Analizando la información de los sitios web
11.4. Riesgos de una navegación no segura
12. Motores de búsqueda
13. Conozcamos las VPN, hoy tan de moda
13.1. Su uso en la actualidad
13.2. Ventajas de las conexiones VPN
13.3. Su lado menos atractivo
13.4. Resumiendo
13.5. Oferta actual
14. Cómo nos atacan cuando navegamos por internet
14.1. Exploits
14.2. Ataques Cross-Site Scripting (XSS)
14.3. Uso de extensiones y plugins peligrosos
15. Recomendaciones de seguridad
16. Recomendaciones de privacidad
17. Resumen de recomendaciones importantes

Módulo III: Seguridad en el correo electrónico (20 horas)

1. Introduccion
2. Antes de comenzar, un poco de terminología no viene mal
3. El correo electrónico como fuente de engaños
4. Cómo identificar un correo electrónico malicioso
5. Mantente a salvo del phishing
6. Mal Spoofing
7. Analizando cabeceras de correo electrónico
7.1. Iniciandonos en MessageHeader de Google
8. Alguien está mandando correos en mi nimbre
9. Verificar si una dirección de correo es real
10. El peligro de las URL acortadas
11. Extensiones web, otro punto crítico
12. La importancia de las actualizaciones
13. Evita el spam con unas pautas sencillas
14. Profundizando en los filtros de correo antispam
15. CCO, protege los correos electrónicos
16. Cifrado de mensajes
16.1. Gmail y el cifrado de mensajes
17. Ficheros adjuntos
18. Cuentas robadas

19. Factor de doble autenticación
19.1. Biometría y ciberseguridad, ¿qué relación guardan?
20. Campañas fraudulentas que hacen uso del correo electrónico

Módulo IV: Seguridad en los dispositivos móviles (20 horas)

1. Introducción
2. Medidas de protección básicas
2.1. Protección física del dispositivo
2.2. Gestión de cuentas de usuario
2.2.1. Veamos cómo se hace en los smartphones XIAOMI
2.3. Creación de copias de seguridad
2.3.1. Motivos para realizar copias de seguridad
2.3.2. Cómo realizar copias de seguridad en Android
2.3.3. Cómo realizar copias de seguridad en IOS
2.3.4. Dónde debemos alojar nuestras copias de seguridad
2.3.4.1. Almacenamiento en la nube
2.3.4.1.1. Qué nos ofrece
2.3.4.1.2. Principales características
2.3.4.1.3. Qué riesgos puede conllevar
2.4. Cifrado de nuestros dispositivos móviles
2.4.1. Cifrado de dispositivos Android
2.4.2. Cifrado de dispositivos IOS
3. Apss y permisos asociados
3.1. Medidas que podemos tomar
3.2. Tipos de permisos que piden las apps
3.3. Qué puede suceder con una mala gestión de los permisos
4. Jailbreaking y rooting en dispositivos móviles
4.1. Ventajas
4.2. Riesgos
4.3. Legalidad
4.4. Para quién está destinado
5. Seguridad de las conexiones inalámbricas
5.1. Riesgos de redes Wifi
5.2. Riesgos de conexiones Bluetooth
5.3. Medidas de protección
6. Cómo actuar en caso de pérdida o robo de mi dispositivo móvil
6.1. Qué hacer para ser precavidos en caso de pérdida/robo
7. Códigos QR
7.1. Riesgos que puede suponer su uso
7.2. Cómo acceder a un código QR
7.3. Recomendaciones
8. La importancia de las actualizaciones
8.1. Comprobar actualizaciones en Android
8.2. Comprobar actualizaciones en IOS

Módulo V: Identificación y protección frente a fraudes online (10)

1. Introducción
2. Fakes News o bulos
2.1. Ejemplos de noticias falsas
2.2. Pasos para contrastar una noticia
3. Deepfakes
3.1. ¿Cómo se pueden detectar?
4. Búsquedas de imágenes inversas con Google
5. Fraudes en tiendas online
5.1. Cómo se las ingenian los ciberdelincuentes
5.2. Cómo detectar e identificar estas estafas
5.3. Medidas de protección que debemos tomar
6. Cómo Whatsapp actúa contra la ciberdelincuencia
7. Smishing
8. Vishing
9. Fraudes en plataformas de alquiler de viviendas
10. Sellos de confianza
11. Métodos de pagos online
12. Una vez efectuada la compra, ¿podemos hacer algo?

Desarrollo

El curso se desarrollará en el campus virtual de la plataforma de formación e-learning e-learning. (https://www.ingenierosformacion.com/campus/)

El día de inicio del curso los alumnos que hayan formalizado la prematrícula en la plataforma (www.ingenierosformacion.com) y hayan hecho efectivo el pago de la misma (bien por pasarela de pago, con tarjeta, directamente en el momento de la matriculación o bien por transferencia o ingreso bancario en el número de cuenta que se indica en la misma), podrán acceder al curso por medio de la plataforma, con las claves que utilizaron para registrarse como usuarios. Desde su perfil en “Mis Matrículas” podrán ver el enlace de acceso al curso.

Al ser la formación e-learning, los alumnos seguirán los distintos temas que se proponen en el curso al ritmo que ellos puedan, y en las horas que mejor se adapten a su horario.

NO se exigirá a los alumnos que estén las horas lectivas propuestas para el curso, aunque el número de horas lectivas indicado en cada curso es el recomendable para alcanzar los objetivos del curso y la adquisición de los conocimientos previstos, cada alumno va siguiendo a su ritmo los contenidos, de igual forma NO se cortará el acceso a la plataforma a aquellos alumnos que superen las horas propuestas para el curso. Sí se tendrá en cuenta que el alumno haya visto todos los contenidos o al menos la gran mayoría (más del 75 %) de los mismos durante el periodo que dura el curso, así como realizado con éxito las tareas o ejercicios, trabajos que se le vayan proponiendo durante el curso.

El alumno, además de ir estudiando los contenidos de los distintos temas, podrá participar en el foro del curso dejando sus dudas o sugerencias o intercambiando opiniones técnicas con otros alumnos, así como respondiendo aquellas que hayan dejado otros compañeros. Asimismo podrá hacer las consultas que estime oportunas al tutor del curso para que se las responda a través de la herramienta de mensajería que posee la plataforma y preferentemente en el mismo foro. Recomendamos encarecidamente el uso del foro por parte de todos los alumnos.

Para la obtención del certificado de aprovechamiento del curso el alumno tendrá que superar los objetivos mínimos marcados por el docente (superación de cuestionarios de evaluación, casos prácticos, participación, etc…).

De igual forma, los alumnos, deberán realizar la encuesta de satisfacción que nos ayudará en la mejora de la calidad de las acciones formativas que proponemos en la plataforma de formación. La encuesta estará accesible en el apartado “Mis matrículas” en la plataforma, a partir de la finalización del curso.

Matrícula

Para ampliar información mandar mail a secretaria@ingenierosformacion.com o llamando por teléfono al número 985 73 28 91.

Formación Bonificada

La formación bonificada está dirigida a trabajadores de empresas que estén **contratados por cuenta ajena**, es decir, trabajadores de empresas que, en el momento del comienzo de la acción formativa, coticen a la Seguridad Social por el Régimen General.

Están **excluidos** los autónomos, los funcionarios y el personal laboral al servicio de las Administraciones públicas.

Para beneficiarse de la Formación bonificada la empresa tiene que encontrarse al corriente en el cumplimiento de sus obligaciones tributarias y de la Seguridad Social.

Para aclarar cualquier duda relacionada con nuestros cursos o sobre la bonificación de la FUNDAE, pueden dirigirse a la página web de la plataforma **FORMACIÓN BONIFICADA** donde podrán ver la información de una manera mas detallada, así como descargarse los documentos necesarios para la obtención de esta bonificación.

También pueden ponerse en contacto con nosotros, en el teléfono 985 73 28 91 o en la dirección de correo electrónico secretaria@ingenierosformacion.com.