Seguridad de la Información | **Correo Electrónico, Ciberataques e Ingeniería Social**

Detalles del curso:

Duración: 4 h.

Modalidad: e-Learning

Información e inscripción:

685 457 610 - 615 844 193

formacion@laberit.com

LÃBERIT | CENTRO DE FORMACIÓN TIC.

Introducción

El correo electrónico es una importante herramienta de comunicación. A través de él puedes enviar, recibir, almacenar y organizar mensajes que proceden de diversas fuentes. Cuando utilizas el correo electrónico, hay buenas costumbres a tener en cuenta que debes conocer. Y aunque no te hayas dado cuenta, cuando utilizas tu correo electrónico te estás exponiendo a una gran cantidad de peligros y amenazas, los más comunes son: el Spam, el Phising y las Cadenas.

Cuando utilizas tu correo electrónico, además de escribir y enviar texto al destinatario, puedes enviarle todo tipo de archivos: imágenes, documentos, vídeos, archivos comprimidos, etc. Cualquier tipo de archivo enviado a través de correo electrónico se conoce como "archivo adjunto" del correo. Si bien los archivos adjuntos son muy útiles y enriquecen la comunicación por correo electrónico, son también uno de los medios preferidos por los ciberdelincuentes para cometer sus delitos. Por eso, debes tener especial cuidado con ellos, para evitar que te perjudiquen a ti particularmente como a tu empresa.

Funcionamiento lento de nuestro ordenador, archivos que desaparecen, mensajes inesperados en pantalla, cierre repentino de programas, etc. Antes nuestro ordenador funcionaba correctamente, pero con el tiempo se ha hecho más lento y cada vez funciona peor y es desesperante. De forma genérica, podemos definir el malware como los programas con comportamientos maliciosos y dañinos para nuestro equipo (ordenador, móvil o tablet).

La variedad de programas maliciosos que es muy grande; cada uno tiene sus propios efectos dañinos y una forma diferente de actuar e instalarse en nuestro equipo. Por supuesto, todo sin nuestro consentimiento. Para aprender a combatirlos y a protegernos de la mejor forma posible, es fundamental saber cómo logran los ciberdelincuentes instalar sus programas maliciosos en nuestros equipos.

En nuestro trabajo diario utilizando Internet, exponemos nuestra información privada a muchas amenazas. Al igual que existen los delincuentes en el mundo físico, también existen los "ciberdelincuentes" en Internet; su principal objetivo es robar nuestra información. El término "phishing" viene del inglés "pescar". La relación con Internet está en que los ciberdelincuentes nos hacer "morder el anzuelo" cuando nos engañan y terminamos ofreciéndoles nuestra información.

El ransomware (del inglés ransom, "rescate", y ware, término recortado de "software"), es un tipo de malware (programa malicioso) creado por un ciberdelincuente que impide a los usuarios acceder a su sistema informático o a sus archivos personales. A cambio de quitar esa restricción y poder acceder de nuevo a dichos archivos, el ciberdelincuente exigirá el pago de un rescate. A través del ransonware, los ciberdelincuentes han creado una forma muy fácil de

hacer grandes cantidades de dinero y coaccionar a los usuarios para que paguemos por recuperar algo que es nuestro y nos han "secuestrado": nuestros archivos.

Si alguien nos persuade para que realicemos una acción determinada que puede no estar dentro de nuestros principios e intereses, probablemente esté aplicando principios de ingeniería social. Ésta se basa en influenciar, engañar y manipular mental y psicológicamente a las personas para que, inconscientemente, acaben realizando determinadas acciones y aportando información confidencial.

En sus comienzos, la ingeniería social se basaba en llamadas telefónicas donde los delincuentes se hacían pasar por otra persona (suplantación de la identidad) y conseguían recabar información privada y confidencial de las personas a las que llamaban. Actualmente, además del teléfono, se utilizan las redes sociales, el correo electrónico, mensajería instantánea y hasta engaños presenciales. La efectividad del engaño depende del comportamiento de la víctima, quien muchas veces, de forma involuntaria, contribuye a que estos delincuentes se salgan con la suya.

¿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 el correo electrónico, descargas y abres archivos adjuntos y aprenderás una serie de buenas prácticas y costumbres que será importante seguir para evitar estos riesgos y peligros cuando uses el correo electrónico. También aprenderás a identificar y combatir los ciberataques más comunes que nos llegan por Internet, así como los engaños de la ingeniería social.

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 el correo electrónico o estás conectado a 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 correo electrónico, ciberataques e ingeniería social?

Con este curso conocerás los riesgos y peligros que podemos encontrarnos en el uso del correo electrónico y en la descarga de archivos adjuntos que pueden venir en sus mensajes. También conoceremos los principales ciberataques y engaños de ingeniería social a los que podemos enfrentarnos hoy en día, tanto en el entorno personal, como empresarial. Pero

también veremos una serie de consejos y buenas prácticas para luchar contra todos estos peligros y poderlos prevenir.

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 el correo electrónico y saber cómo actuar antes las constantes amenazas de ciberataques y engaños de ingeniería social.

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 el correo electrónico e Internet a diario 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 en el uso del correo electrónico, los peligros que puede acarrear la descarga y ejecución de archivos adjuntos en los mensajes y una serie de buenas prácticas y costumbres para evitar los riesgos y peligros en el uso del correo electrónico.
- Conocer qué es el malware, escenarios habituales de casos de malware y las medidas para evitar y prevenir los casos de malware.
- Conocer qué es el phishing y la información privada, escenarios habituales de casos de phishing y medidas para evitar y prevenir los casos de phishing.
- Conocer qué es el ransomware, cómo se produce el secuestro de archivos, las distintas opciones de recuperar nuestros archivos, las vías de infección del ransomware y saber qué hacer en el trato con el ciberdelincuente y qué equipos y dispositivos pueden ser afectados.

- Conocer qué es la ingeniería social y su evolución en el tiempo, escenarios habituales de casos de ingeniería social y las medidas para evitar y disminuir estos casos.

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 “Correo electrónico, ciberataques e ingeniería social” consta de 2 unidades de aprendizaje. Los títulos y contenidos son los siguientes:

UNIDA DE APENDIZAJE 1: CORREO ELECTRÓNICO: RIESGOS, ARCHIVOS ADJUNTOS Y BUENAS COSTUMBRES

Capítulo 1. Riesgos en el uso de correo electrónico

Tema 1.1.: Introducción.
Tema 1.2.: Escenario 1: Spam.
Tema 1.3.: Escenario 2: Phishing.
Tema 1.4.: Escenario 3: Cadenas.
Tema 1.5.: Consejos para combatir las amenazas.
Tema 1.6.: Conclusiones finales.

Capítulo 2. Descarga de archivos adjuntos

Tema 2.1.: Introducción.
Tema 2.2.: Escenario 1: Habilitar contenido/macros.
Tema 2.3.: Escenario 2: Archivos comprimidos.
Tema 2.4.: Escenario 3: Suplantación de identidad y programas desactualizados.
Tema 2.5.: Encriptación con ransomware de la información del equipo.
Tema 2.6.: Conclusión final.

Capítulo 3. Buenas costumbres en el uso del correo electrónico

Tema 3.1.: Introducción.
Tema 3.2.: Escenario 1: Asunto en los mensajes de correo.
Tema 3.3.: Escenario 2: Archivos adjuntos y enlaces.
Tema 3.4.: Escenario 3: Envío de mensajes de correo a varios destinatarios.
Tema 3.5.: Conclusiones finales.

UNIDA DE APENDIZAJE 2: CIBERATAQUES MÁS COMUNES E INGENIERÍA SOCIAL

Capítulo 1. Malware: programas maliciosos

Tema 1.1.: Introducción: conceptos básicos.
Tema 1.2.: Escenario 1: Medios extraíbles.
Tema 1.3.: Escenario 2: Demasiado bueno para ser cierto.
Tema 1.4.: Escenario 3: ¡Necesitas un antivirus!, ¿o quizás no?
Tema 1.5.: Peligros del malware, qué hacer en caso de infección y conclusión final.

Capítulo 2. Phishing: engaño en Internet

Tema 2.1.: Introducción: Información privada y concepto de phishing.
Tema 2.2.: Escenario 1: Mensajes que solicitan información privada.
Tema 2.3.: Escenario 2: Mensajes con suplantación de identidad.
Tema 2.4.: Escenario 3: Mensajes con archivos adjuntos y enlaces.
Tema 2.5.: Cómo disminuir los casos de Phishing. Conclusión final.

Capítulo 3. Ransomware: estafas en Internet

Tema 3.1.: Introducción: qué es y cómo funciona el ransomware.
Tema 3.2.: Secuestro de archivos.
Tema 3.3.: Negociación y trato con el ciberdelincuente. Pago del rescate.
Tema 3.4.: Copias de seguridad.
Tema 3.5.: Vías de infección del ransomware.
Tema 3.6.: Equipos y dispositivos afectados.
Tema 3.7.: Conclusiones finales.

Capítulo 4 Ingeniería social: víctimas de engaño

Tema 4.1.: Introducción: qué es la ingeniería social y su evolución.
Tema 4.2.: Escenario 1: Llamadas que requieren una acción inmediata.
Tema 4.3.: Escenario 2: Mensajes que llaman nuestra atención.
Tema 4.4.: Escenario 3: Víctimas de nuestras buenas intenciones.
Tema 4.5.: Conclusiones finales.

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