LÃBERIT

Boost your performance

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

Detalles del curso:
Duración: 4 horas
Modalidad: Teleformación

Información e inscripción:
685 457 610
615 844 193
960 075 817 (Ext. 274)
formacion@laberit.com

La información contenida en este documento va dirigida exclusivamente al destinatario/grupos de personas y contiene información confidencial. No se puede realizar ninguna revisión, copia, distribución, otro uso, u otra acción basada en ella, sin el permiso explícito por parte del propietario de este documento: Laberit Sistemas S.L. con C.I.F. B98064462.

IÃ Rev. 1

ÍNDICE

1. INTRODUCCIÓN 3
2. ¿POR QUÉ HACER ESTE CURSO? 3
3. ¿EN QUÉ CONSISTE LA FORMACIÓN EN SEGURIDAD DE LA INFORMACIÓN | CORREO ELECTRÓNICO, CIBERATAQUES E INGENIERÍA SOCIAL? 4
4. ¿A QUIÉN VA DIRIGIDO? 4
5. OBJETIVOS DIDÁCTICOS 4
6. METODOLOGÍA 5
7. SALIDAS PROFESIONALES U OPCIONES DE PROMOCIÓN PROFESIONAL 5
8. PROGRAMA 6
8.1. UNIDAD DE APENDIZAJE 1: CORREO ELECTRÓNICO: RIESGOS, ARCHIVOS ADJUNTOS Y BUENAS COSTUMBRES 6
8.2. UNIDAD DE APENDIZAJE 2: CIBERATAQUES MÁS COMUNES E INGENIERÍA SOCIAL 7

1. INTRODUCCIÓN

El uso cotidiano del correo electrónico e Internet exige aplicar criterios de seguridad claros, prácticos y sostenibles. Esta formación permite identificar los riesgos más habituales del correo electrónico, reconocer ataques frecuentes como phishing, malware o ransomware, y adoptar buenas prácticas para proteger la información personal y corporativa. Frente a otras soluciones más generales, el curso se diferencia por su enfoque directo, orientado a situaciones reales de uso, por su duración concentrada de 4 horas y por su planteamiento accesible para cualquier persona que trabaje o se comunique en entornos digitales.

Beneficios principales:

- Reconocer amenazas habituales asociadas al correo electrónico, los archivos adjuntos y la navegación por Internet.
- Aplicar hábitos de prevención para reducir riesgos de infección, fraude, pérdida de información o suplantación de identidad.
- Mejorar la capacidad de reacción ante mensajes sospechosos, ciberataques e intentos de manipulación mediante ingeniería social.

Diferenciales del curso respecto a otras soluciones:

- Contenido breve, concreto y aplicable desde el primer día, sin requerir conocimientos técnicos avanzados.
- Tratamiento integrado de correo electrónico, malware, phishing, ransomware e ingeniería social dentro de una misma acción formativa.
- Orientación preventiva basada en escenarios habituales, consejos prácticos y hábitos seguros para el ámbito profesional y personal.

2. ¿POR QUÉ HACER ESTE CURSO?

La seguridad digital ya no es una competencia exclusiva de perfiles técnicos: cualquier persona que utiliza correo electrónico, abre documentos, navega por Internet o comparte información necesita saber detectar señales de alerta y actuar con criterio. Realizar este curso ayuda a trabajar con mayor confianza, reduce errores que pueden comprometer equipos o datos y aporta una base útil para desenvolverse mejor en puestos vinculados a entornos digitales, administrativos, comerciales, educativos o de atención al cliente. Además, permite reforzar la responsabilidad profesional, ganar autonomía ante situaciones sospechosas y contribuir a una cultura de protección de la información dentro de la organización.

3. ¿EN QUÉ CONSISTE LA FORMACIÓN EN SEGURIDAD DE LA INFORMACIÓN | CORREO ELECTRÓNICO, CIBERATAQUES E INGENIERÍA SOCIAL?

La formación en Seguridad de la Información | Correo Electrónico, Ciberataques e Ingeniería Social consiste en aprender a identificar los riesgos que aparecen en comunicaciones digitales habituales y a aplicar pautas de prevención antes de que un incidente afecte a la información o a los dispositivos. A través del curso se revisan situaciones frecuentes relacionadas con spam, phishing, cadenas, archivos adjuntos, programas maliciosos, ransomware y técnicas de manipulación utilizadas por ciberdelincuentes. El objetivo es que el alumnado comprenda qué puede ocurrir, por qué ocurre y qué medidas debe aplicar para protegerse de forma sencilla, responsable y eficaz.

4. ¿A QUIÉN VA DIRIGIDO?

Esta formación está dirigida a personas que utilizan herramientas digitales y correo electrónico en su actividad diaria y desean mejorar su seguridad en el uso de Internet:

- Profesionales de cualquier área que gestionan comunicaciones, documentación o información mediante correo electrónico.
- Personal administrativo, comercial, técnico, docente o de atención al cliente que trabaja con mensajes, enlaces y archivos adjuntos.
- Usuarios/as de equipos informáticos, móviles o tabletas que quieren prevenir riesgos habituales en su entorno personal o laboral.
- Personas que desean adquirir hábitos básicos de ciberseguridad sin partir de conocimientos técnicos especializados.
- Organizaciones que buscan sensibilizar a sus equipos frente a fraudes digitales, suplantaciones e ingeniería social.

5. OBJETIVOS DIDÁCTICOS

Objetivo general:

- Adquirir hábitos de seguridad en el uso del correo electrónico e Internet para prevenir riesgos asociados a archivos adjuntos, malware, phishing, ransomware e ingeniería social.

Objetivos específicos:

- Identificar los riesgos más habituales en el uso del correo electrónico y aplicar buenas prácticas para reducirlos.
- Reconocer los peligros vinculados a la descarga y apertura de archivos adjuntos.
- Comprender qué es el malware, cómo puede afectar a equipos y dispositivos, y qué medidas ayudan a prevenirlo.
- Detectar intentos de phishing y proteger la información privada frente a mensajes fraudulentos.
- Explicar qué es el ransomware, cuáles son sus vías de infección y cómo actuar para disminuir su impacto.
- Reconocer técnicas de ingeniería social y adoptar conductas que dificulten el engaño y la manipulación.

6. METODOLOGÍA

La metodología combina exposición guiada de contenidos con ejemplos prácticos y escenarios habituales de uso del correo electrónico e Internet. El aprendizaje se plantea de forma progresiva, con explicaciones claras, ejercicios de reconocimiento de situaciones de riesgo y recomendaciones aplicables al entorno laboral y personal.

El curso se desarrolla en modalidad de teleformación mediante una plataforma online, con navegación secuencial durante la fase formativa y posibilidad de consulta posterior de los contenidos ya trabajados. El alumnado cuenta con guía de uso, unidades didácticas estructuradas, actividades prácticas y recursos orientados a consolidar hábitos seguros en el manejo de la información digital.

7. SALIDAS PROFESIONALES U OPCIONES DE PROMOCIÓN PROFESIONAL

Completar esta formación refuerza una competencia transversal muy valorada en cualquier puesto que implique uso de correo electrónico, gestión documental, atención a usuarios, comunicación interna o manejo de información sensible. La capacitación puede favorecer la mejora del desempeño en funciones administrativas, comerciales, técnicas, educativas o de soporte, al demostrar mayor criterio preventivo y responsabilidad en el uso de herramientas digitales.

También puede contribuir a la promoción interna o a la participación en proyectos donde se requiera sensibilización en ciberseguridad, cumplimiento de buenas prácticas, protección de datos o apoyo a procesos de digitalización segura.

8. PROGRAMA

8.1. UNIDAD 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.

8.2. UNIDAD 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.

ACREDITADO

Microsoft Imagine Academy
Program Member

CertiProf® | Partner

Fundación Estatal
PARA LA FORMACIÓN EN EL EMPLEO

Networking Academy
cisco

Linux Professional Institute

Microsoft
Technology Associate

Pearson
Professional Assessments

CERTIPORT
A PEARSON VUE BUSINESS
AUTHORIZED TESTING CENTER

Microsoft
Office Specialist
Authorized Testing Center

LABORA
Servei Valencià d'Ocupació i Formació

IC3
DIGITAL LITERACY
CERTIFICATION