Prácticas básicas sobre Ciberseguridad

Detalles del curso:

Duración: 25 horas

Modalidad: Teleformación

Información e inscripción:

685 457 610

615 844 193

960 075 817 (Ext. 257)

formacion@laberit.com

LÄBERIT | CENTRO DE FORMACIÓN TIC.

Prácticas básicas sobre Ciberseguridad

Introducción

Este curso ofrece al alumnado tres beneficios fundamentales: mejora de la seguridad personal y profesional frente a amenazas digitales comunes, comprensión clara y accesible de los principales riesgos cibernéticos, y adopción de buenas prácticas para el uso seguro de dispositivos y servicios online. A diferencia de otras formaciones más técnicas o teóricas, esta propuesta pone el foco en la aplicación práctica, el uso de escenarios reales y consejos útiles que cualquier persona puede implementar en su día a día digital.

¿Por qué hacer este curso?

En un contexto de creciente dependencia tecnológica, las amenazas digitales aumentan de forma constante. En este contexto este curso permite mejorar las competencias básicas en materia de seguridad digital, incrementar la empleabilidad y reducir el riesgo de incidentes de seguridad en el entorno profesional y personal. También representa una oportunidad para sentirse más preparado, seguro y autónomo en el uso de tecnología. Inscribirse en esta formación implica obtener herramientas y criterios prácticos para navegar, comunicarse y trabajar con confianza en el entorno digital actual.

¿En qué consiste la formación en Prácticas básicas sobre Ciberseguridad?

Esta formación está orientada a proporcionar conocimientos básicos, pero esenciales, sobre los principales riesgos y amenazas en el ámbito digital. A través de una metodología accesible y práctica, se enseñan medidas de protección frente a malware, phishing, amenazas en dispositivos móviles o accesos inseguros, navegación en Internet, uso de la nube y del correo electrónico. Además, se fomenta una cultura preventiva en materia de ciberseguridad y privacidad. No se requieren conocimientos técnicos previos, por lo que cualquier persona con un manejo habitual de la tecnología puede aprovechar este curso.

¿A quién va dirigido?

- Personas usuarias habituales de tecnologías de la información que deseen mejorar su seguridad digital.

- Estudiantes de ciclos formativos o grados no técnicos con interés en competencias digitales básicas.
- Personal administrativo, de atención al público o soporte que trabaja con ordenadores o correo electrónico.
- Cualquier profesional que necesite conocer prácticas de ciberseguridad esenciales en su entorno laboral o doméstico.

Objetivos didácticos

Objetivo general:

- Capacitar a los participantes en la identificación de amenazas digitales comunes y en la adopción de medidas básicas de protección y prevención, fomentando una cultura de ciberseguridad.

Objetivos específicos:

- Comprender los conceptos fundamentales de ciberseguridad.
- Identificar las principales amenazas digitales y sus riesgos asociados.
- Aplicar prácticas seguras en el uso de dispositivos, aplicaciones, navegación e intercambio de información.
- Proteger la información personal y profesional frente a ataques como phishing o ransomware.
- Reconocer situaciones de riesgo y saber cómo actuar frente a incidentes de seguridad.
- Desarrollar buenos hábitos y actitudes responsables en el uso de las TIC.

Metodología

El curso se imparte en modalidad de Teleformación mediante una plataforma online accesible 24/7. Combina contenidos teóricos y prácticos con un enfoque didáctico basado en escenarios reales y resolución de problemas. Además, incluye materiales multimedia, vídeos explicativos y ejercicios autoevaluativos. Cada unidad está acompañada de ejemplos y consejos de aplicación directa. La evaluación final, con preguntas tipo test, permitirá al alumnado comprobar los conocimientos adquiridos durante el curso de forma práctica y sencilla.

Salidas profesionales u opciones de promoción profesional

Al completar esta formación, el alumnado podrá aplicar sus conocimientos de ciberseguridad en cualquier entorno profesional que implique el uso de dispositivos, redes o servicios digitales. Personas que han cursado esta formación han logrado reducir incidentes en sus puestos de trabajo, mejorar sus competencias digitales en procesos de selección y contribuir activamente a la prevención de amenazas en sus organizaciones. Es una base recomendable para perfiles que busquen especializarse posteriormente en ámbitos más técnicos de la ciberseguridad.

Programa

Se presenta el desglose temático estructurado en **siete unidades de aprendizaje**:

UNIDAD 1. SEGURIDAD GENERAL. INTROUDCCIÓN A LA CIBERSEGURIDAD

Capítulo 1. Aspectos generales de la ciberseguridad.

Tema 1.1. Bienvenida al curso. Introducción.

Tema 1.2. Incidente de seguridad. INCIBE y OSI

Capítulo2. Malware: programas maliciosos.

Tema 2.1. Introducción. Peligros del “malware”.

Tema 2.2. Escenario 1: Medios extraíbles

Tema 2.3. Escenario 2: Demasiado bueno para ser cierto

Tema 2.4. Escenario 3: ¡Necesitas un antivirus!, ¿o quizás no?

Tema 2.5. Medidas de protección y consejos

UNIDAD 2. SEGURIDAD EN INTERNET

Capítulo 1. Seguridad en la navegación por Internet.

Tema 1.1.: Importancia de la navegación segura. Uso de los navegadores.

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 finales.

Prácticas básicas sobre Ciberseguridad

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.: Prevenir el acceso no autorizado a nuestros archivos. Conclusión final.

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 finales.

UNIDAD 3. SEGURIDAD EN EL CORREO ELECTRÓNICO

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 y 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.

UNIDAD 4. AMENAZAS SOBRE LOS DATOS PERSONALES Y LA PRIVACIDAD

Capítulo 1. Ingeniería social: víctimas de engaño

Tema 1.1.: Introducción: qué es la ingeniería social y su evolución.

Tema 1.2.: Escenario 1: Llamadas que requieren una acción inmediata.

Tema 1.3.: Escenario 2: Mensajes que llaman nuestra atención.

Tema 1.4.: Conclusiones finales.

Capítulo 2. Ransomware: estafas en Internet

Tema 2.1.: Introducción: qué es y cómo funciona el ransomware.

Tema 2.2.: Secuestro de archivos.

Tema 2.3.: Negociación y trato con el ciberdelincuente. Pago del rescate.

Tema 2.4.: Copias de seguridad.

Tema 2.5.: Vías de infección del ransomware.

Tema 2.6.: Equipos y dispositivos afectados.

Tema 2.7.: Conclusiones finales.

Capítulo 3. Phishing: engaño en Internet y robo de datos personales

Tema 3.1.: Introducción: Información privada y concepto de phishing.

Tema 3.2.: Escenario 1: Mensajes que solicitan información privada.

Tema 3.3.: Escenario 2: Mensajes con suplantación de identidad.

Tema 3.4.: Escenario 3: Mensajes con archivos adjuntos y enlaces.

Tema 3.5.: Cómo disminuir los casos de Phishing. Conclusión final.

UNIDAD 5. SEGURIDAD EN DISPOSITIVOS MÓVILES Y ACCESOS REMOTOS

Capítulo 1. Uso seguro de aplicaciones móviles: permisos, fuentes fiables y actualizaciones

Tema 1.1.: Introducción. Las Apps.

Tema 1.2.: Escenario 1: Cuidado con la concesión de permisos.

Tema 1.3.: Escenario 2: Cuidado con la instalación de apps gratuitas y/o no oficiales.

Tema 1.4.: Escenario 3: Cuidado con el escaneo de códigos QR.

Tema 1.5.: Actualización de aplicaciones. Conclusiones finales.

Capítulo 2. Configuración de seguridad y conexiones seguras en accesos remotos

Tema 2.1.: Introducción a la configuración de seguridad y conexiones seguras en accesos remotos.

Tema 2.2.: Escenario 1: Uso personal del ordenador de empresa.

Tema 2.3.: Escenario 2: Conexiones poco fiables.

Prácticas básicas sobre Ciberseguridad

UNIDAD 6. CULTURA DE CIBERSEGURIDAD

Capítulo 1. Riesgos en el puesto de trabajo. Reporte de incidentes de seguridad de la información. Copias de seguridad

Tema 1.1.: Riesgos en el puesto de trabajo.

Tema 1.2.: Reporte de incidentes de seguridad de la información.

Tema 1.3.: Copias de seguridad.

Capítulo 2. Seguridad en el puesto de trabajo: manual uso medios electrónicos para personal de la organización

Tema 2.1.: Aspectos generales en las normas de uso de medios electrónicos.

Tema 2.2.: Normas de aplicación específica de medios electrónicos.

Capítulo 3. Buenas prácticas en el uso y definición de contraseñas

Tema 3.1.: Introducción en el uso de las contraseñas.

Tema 3.2.: Reglas para crear contraseñas seguras y autenticación de dos factores.

UNIDAD 7. CIBERSEGURIDAD E INTELIGENCIA ARTIRICIAL

Capítulo 1. Descubriendo la Inteligencia Artificial

Tema 1. Introducción

Tema 2. ¿Qué es la Inteligencia Artificial?

Tema 3. La IA en nuestra vida diaria

Tema 4. Tipos de Inteligencia Artificial

Capítulo 2. Ciberataques con Inteligencia artificial

Tema 1. Phishing automatizado con IA

Tema 2. Clonación de voz para fraudes financieros

Tema 3. Deepfakes en estafa y manipulación

Tema 4. Ransomware impulsado por IA

LÂBERIT | CENTRO DE FORMACIÓN TIC.

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 VUE
Authorised Test Centre

CERTIPORT
A PEARSON VUE BUSINESS
AUTHORIZED TESTING CENTER

Microsoft
Office Specialist
Authorized Testing Center

LABORA
Servei Valencià d'Ocupació i Formació

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