LÂBERIT | CENTRO DE FORMACIÓN TIC.

CERTIFICADO DE FORMACIÓN

Correo Electrónico, Ciberataques e Ingeniería Social - Versión 2

Duración: 4 h | Modalidad: Online

Fecha y lugar: Valencia, 13 de March de 2024

César Osvaldo Matelat Borneo

DNI:42268151Q

Firmado Responsable Formación

Programa

El curso “Seguridad de la Información | Correo Electrónico, Ciberataques e Ingeniería Social” consta de 2 unidades. 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.