Cursos de concienciación y formación del servicio SIMULPHISHING de RedIRIS

Contenido

Introducción

En este documento se realiza un resumen de los dos cursos ofrecidos por la plataforma “Attack Simulator”, ambos cuentan con certificado de finalización.

En este resumen veremos una breve descripción de ambos cursos, un índice de su contenido, los idiomas disponibles y su duración.

El curso obligatorio a realizar es el curso de **Concienciación sobre la seguridad** para aquellos usuarios que terminen este curso y quieran aprender más acerca de la seguridad informática **pueden realizar de manera voluntaria el curso de Formación sobre ransomware** .

Concienciación sobre la seguridad

Duración del curso

Siguiendo los tiempos marcados por la plataforma “Attack Simulator” el tiempo estimado para la realización del curso “Concienciación sobre la seguridad” es de **4 horas**.

También hay que tener en cuenta que este tiempo podría variar dependiendo del conocimiento del usuario, la atención puesta durante el curso y la efectividad en realización a los cuestionarios.

Idiomas disponibles

El Curso cuenta con los siguientes idiomas disponibles:

- Inglés
- Castellano
- Rumano
- Catalán
- Griego
- Español latino
- Portugués

Descripción del curso

Mediante nuestro enfoque de formación interactiva, nos aseguramos de que sus empleados comprendan los peligros de los ciberataques y reconozcan que la responsabilidad de crear un entorno de trabajo seguro está en sus manos.

De acuerdo con nuestra visión, queremos estimular a todos los empleados para que perciban la concienciación sobre la seguridad como algo accesible y fácil de entender.

Pretendemos dar a la seguridad un significado positivo, convirtiéndola en un tema abierto, transparente y abordable, de modo que los empleados no tengan miedo de hablar de sus encuentros, se animen a informar de sucesos inusuales y dispongan de las herramientas necesarias para identificar posibles ataques.

Apoyamos el crecimiento de la seguridad mediante un compromiso unificado, lo que significa que todos los empleados deben cooperar para crear un entorno de trabajo seguro.

Contenido del curso

- Chapter 1: Introducción sections
  - Section 1.1: BienvenidosOne lesson
    - Lesson 1.1.1: Hola de AttackSimulator
  - Section 1.2: ¿Por qué necesita realizar este curso?
    - Lesson 1.2.1: Le puede suceder a usted
    - Lesson 1.2.2: Objetivos
    - Lesson 1.2.3: Estructura del curso
  - Section 1.3: Comenzar lentamenteOne lesson
    - Lesson 1.3.1: Qué es la Seguridad de la Información?
  - Section 1.4: Notas finalesOne lesson
    - Lesson 1.4.1: Conclusiones
  - Quiz: Cuestionario
- Chapter 2: Los ciberataques11 sections
  - Section 2.1: Información general5
    - Lesson 2.1.1: Introducción
    - Lesson 2.1.2: Tipos y Técnicas de Ataques
    - Lesson 2.1.3: Técnicas de Ataque
    - Lesson 2.1.4: Vectores y Tendencias de Ataques Modernos
    - Lesson 2.1.5: Tendencias
  - Section 2.2: Historia de los Ciberataques7
    - Lesson 2.2.1: Introducción
    - Lesson 2.2.2: Los Primeros Ataques
    - Lesson 2.2.3: Primeros años: el periodo blanco
    - Lesson 2.2.4: El amanecer de la era moderna
    - Lesson 2.2.5: Los años 2000: la era moderna
    - Lesson 2.2.6: 2010 – presente: los años calientes
    - Lesson 2.2.7: Ataques cibernéticos recientes
    - Quiz: Cuestionario
  - Section 2.3: Hackers5

- Lesson 2.3.1: Introducción
- Lesson 2.3.2: Historia temprana
- Lesson 2.3.3: Los hackers modernos
- Lesson 2.3.4: Hackers éticos
- Lesson 2.3.5: Hackers famosos

- Section 2.4: Malware6
  - Lesson 2.4.1: ¿Qué es el malware?
  - Lesson 2.4.2: Brechas de seguridad… ¡Por todas partes!
  - Lesson 2.4.3: Tipos de malware
  - Lesson 2.4.4: Ejemplos
  - Lesson 2.4.5: Historia
  - Lesson 2.4.6: Conclusiones
  - Quiz: Cuestionario
- Section 2.5: Ransomware7
  - Lesson 2.5.1: ¿Qué es el ransomware?
  - Lesson 2.5.2: Métodos de infección
  - Lesson 2.5.3: Componentes
  - Lesson 2.5.4: Cómo reconocer y evitar el ransomware
  - Lesson 2.5.5: ¿Pagar o no pagar?
  - Lesson 2.5.6: Métodos de defensa
  - Lesson 2.5.7: El futuro de ransomware
  - Quiz: Cuestionario Ransomware
- Section 2.6: Spyware y Keyloggers5
  - Lesson 2.6.1: Qué es el Spyware?
  - Lesson 2.6.2: ¿Cómo puede el spyware entrar en su equipo?
  - Lesson 2.6.3: ¿Quiénes son los actores detrás del espionaje?
  - Lesson 2.6.4: Tipos de información que un spyware puede recabar
  - Lesson 2.6.5: Reconocer el spyware
  - Quiz: Cuestionario
- Section 2.7: Phishing6
  - Lesson 2.7.1: Què és el phishing?

- Lesson 2.7.2: El mecanismo de phishing
- Lesson 2.7.3: Tipos de phishing
- Lesson 2.7.4: Reconocer el phishing
- Lesson 2.7.5: Señales de alerta
- Lesson 2.7.6: Ejemplos
- Quiz: Cuestionario

- Section 2.8: Vishing y Smishing5
  - Lesson 2.8.1: ¿Qué es el vishing?
  - Lesson 2.8.2: Cadena de ataque de vishing
  - Lesson 2.8.3: ¿Qué es el smishing?
  - Lesson 2.8.4: Cadena de ataque de smishing
  - Lesson 2.8.5: Qué hacer si usted sufre un ataque de Vishing o Smishing
  - Quiz: Cuestionario
- Section 2.9: Bots y Crypto-jacking5
  - Lesson 2.9.1: ¿Qué son los bots y botnets?
  - Lesson 2.9.2: Elementos en una operación de Botnet
  - Lesson 2.9.3: ¿Qué es el crypto-jacking?
  - Lesson 2.9.4: ¿Qué es el crypto-mining?
  - Lesson 2.9.5: Métodos de prevención
  - Quiz: Cuestionario
- Section 2.10: Ingeniería Social
  - Lesson 2.10.1: ¿Qué es la ingeniería social?
  - Lesson 2.10.2: El proceso de ingeniería social
  - Lesson 2.10.3: Técnicas de ataque
  - Lesson 2.10.4: Cómo evitar la Ingeniería Social
  - Quiz: Cuestionario
- Section 2.11: El robo de identidad
  - Lesson 2.11.1: ¿Qué es el robo de identidad?
  - Lesson 2.11.2: ¿Cómo puede ser posible el robo de identidad?
  - Lesson 2.11.3: ¿Qué se puede hacer para prevenir el robo de identidad?

        - Lesson 2.11.4: ¿Qué puede hacer si descubre que es víctima de robo de identidad?
        - Quiz: Cuestionario

- Chapter 3: Reglas y Directrices sections
    - Section 3.1: Piensa como un atacante
        - Lesson 3.1.1: Perfiles de atacantes
        - Lesson 3.1.2: El ciclo de un ataque
    - Section 3.2: Phishing - medidas de protección
        - Lesson 3.2.1: Detección
        - Lesson 3.2.2: Evitar los problemas
        - Lesson 3.2.3: Controlar el daño
    - Section 3.3: La seguridad del correo electrónico
        - Lesson 3.3.1: Cómo detectar el phishing
        - Lesson 3.3.2: Cómo detectar el spam y las estafas en línea
        - Lesson 3.3.3: Detectar el malware y el ransomware
    - Section 3.4: Navegación segura en Internet5
        - Lesson 3.4.1: Mantenga su navegador actualizado
        - Lesson 3.4.2: No utilice las opciones preconfiguradas
        - Lesson 3.4.3: La actividad de navegación
        - Lesson 3.4.4: Gestione las extensiones y los complementos del navegador
        - Lesson 3.4.5: Contenido pirateado
    - Section 3.5: Las contraseñas y el acceso seguro
        - Lesson 3.5.1: Riesgos de seguridad al usar contraseñas
        - Lesson 3.5.2: Recomendaciones generales
    - Section 3.6: Gestión de vulnerabilidades y parches
        - Lesson 3.6.1: Tipos
        - Lesson 3.6.2: Gestión de procesos
        - Lesson 3.6.3: ¿Qué puedes hacer?
    - Section 3.7: Acceso remoto seguro
        - Lesson 3.7.1: Riesgos de seguridad
        - Lesson 3.7.2: Garantizar un acceso seguro

- Section 3.8: Firewall y Anti-Virus
  - Lesson 3.8.1: ¿Qué es un firewall?
  - Lesson 3.8.2: ¿Qué es un anivirus?
  - Lesson 3.8.3: Las mejores prácticas
- Section 3.9: La seguridad en las redes sociales
  - Lesson 3.9.1: Social media y redes sociales
  - Lesson 3.9.2: Riesgos de seguridad
  - Lesson 3.9.3: Buenas prácticas
- Section 3.10: La seguridad física2
  - Lesson 3.10.1: Riesgos
  - Lesson 3.10.2: Buenas prácticas

Formación sobre ransomware

Duración del curso

Siguiendo los tiempos marcados por la plataforma “Attack Simulator” el tiempo estimado para la realización del curso “Concienciación sobre la seguridad” es de **2 horas**.

También hay que tener en cuenta que este tiempo podría variar dependiendo del conocimiento del usuario, la atención puesta durante el curso y la efectividad en realización a los cuestionarios.

Idiomas disponibles

El Curso cuenta con los siguientes idiomas disponibles:

- Inglés
- Castellano

Descripción del curso

Este curso proporcionará a los participantes una comprensión en profundidad del ransomware, cómo funciona y su impacto en individuos y organizaciones. Los participantes aprenderán a identificar posibles amenazas de ransomware, a evitar ser víctimas de un ataque y a desarrollar un plan de respuesta al ransomware para mitigar los posibles daños.

El curso abordará temas como los tipos más comunes de ransomware, las últimas tácticas utilizadas por los ciberdelincuentes y los indicadores clave de un ataque de ransomware. Además, los participantes aprenderán a aplicar medidas preventivas, como por ejemplo realizar copias de seguridad de los datos y su cifrado, para reducir el riesgo de sufrir un ataque.

En el caso de un ataque de ransomware, los participantes aprenderán cómo responder y recuperarse del ataque, incluyendo cómo negociar con los ciberdelincuentes y los pasos a seguir para minimizar los daños y restaurar los datos. El curso también cubre las consideraciones legales y éticas relacionadas con el ransomware, incluido el cumplimiento de la normativa correspondiente.

Al final del curso, los participantes dispondrán de los conocimientos y habilidades necesarios para protegerse a sí mismos y a sus organizaciones contra los ataques de ransomware, y responder eficazmente en caso de ataque.

- Chapter 1: Ransomware sections
  - Section 1.1: Introducción
    - Lesson 1.1.1: Un error caro

      Quiz: Un error caro
    - Lesson 1.1.2: ¿Qué es el ransomware?

      Quiz: ¿Qué es el ransomware?
    - Lesson 1.1.3: Los tipos de ransomware

      Quiz: Los tipos de ransomware
  - Section 1.2: Prevención5
    - Lesson 1.2.1: Los correos electrónicos maliciosos

      Quiz: Correos electrónicos maliciosos
    - Lesson 1.2.2: Los sitios web maliciosos

      Quiz: Sitios web maliciosos
    - Lesson 1.2.3: Las banderas rojas del ransomware - Primera parte

      Quiz: Las banderas rojas del ransomware primera parte
    - Lesson 1.2.4: Las banderas rojas del ransomware segunda parte

      Quiz: Las banderas rojas del ransomware segunda parte
    - Lesson 1.2.5: 6 consejos para evitar una infección de ransomware

      Quiz: 6 tips to avoid a ransomware infection
  - Section 1.3: Respuesta
    - Lesson 1.3.1: ¿Se debería pagar el rescate?

      Quiz: ¿Se debería pagar el rescate?
    - Lesson 1.3.2: ¿Cómo saber si estás infectado?

      Quiz: ¿Cómo saber si estás infectado?
    - Lesson 1.3.3: Como responder a un ataque de ransomware

      Quiz: Como responder a un ataque de ransomware

- Section 1.4: RevisiónOne lesson
  - Lesson 1.4.1: Lección final - Resumen del ransomware

Quiz: Lección final - Resumen del ransomware