

Reporte Generador de Escenarios de Aprendizaje

Nombre de Usuario:

Manolito

Consulta:

Quiero aprender acerca del phishing

Respuesta de la IA:

Hola, soy un experto en hackatones. Estoy aquí para ayudarte con tus preguntas sobre malware, programación y ciberseguridad.

Definición y descripción:

El phishing es un tipo de ataque cibernético en el que un atacante intenta engañar a las víctimas para que revelen información confidencial, como contraseñas o datos bancarios, haciéndose pasar por una entidad confiable a través de correos electrónicos, mensajes de texto o sitios web falsos.

Cómo te pueden infectar:

Un ejemplo de cómo puedes ser víctima de phishing es recibir un correo electrónico que parece ser de tu banco, solicitando que verifiques tu información haciendo clic en un enlace. Al hacerlo, puedes ser dirigido a un sitio web falso que roba tus credenciales.

Código de ejemplo:

```
python
import smtplib
from email.mime.text import MIMEText

def send_phishing_email():
    sender = "tu_email@ejemplo.com"
    recipient = "victima@ejemplo.com"
    subject = "Verificación de cuenta"
    body = "Estimado usuario, por favor verifique su cuenta haciendo clic en el siguiente enlace: http://sitio-falso.com"

    msg = MIMEText(body)
    msg['Subject'] = subject
    msg['From'] = sender
    msg['To'] = recipient

    with smtplib.SMTP('smtp.ejemplo.com') as server:
        server.login("tu_email@ejemplo.com", "tu_contraseña")
        server.sendmail(sender, recipient, msg.as_string())

send_phishing_email()
```

Ahora, por favor, inserta tu nombre: ____ y tu nota: ____.

Actividad:

1. Explica qué es el phishing y cómo se diferencia de otros tipos de ataques cibernéticos.
2. Describe un escenario en el que podrías ser víctima de un ataque de phishing. ¿Qué señales de advertencia podrías identificar?
3. ¿Cuáles son algunas medidas que puedes tomar para protegerte contra el phishing?

Respuestas de la actividad:

1. El phishing es un ataque que busca engañar a las personas para que revelen información confidencial, a diferencia de otros ataques que pueden involucrar malware o virus.
2. Un escenario podría ser recibir un correo de un banco solicitando verificar información. Las señales de advertencia incluyen errores gramaticales y enlaces sospechosos.
3. Medidas de protección incluyen no hacer clic en enlaces sospechosos, verificar la dirección del remitente y utilizar autenticación de dos factores.



Reporte del Usuario:

El código ofrecido en la consulta no es correcto