



Social Engineering 101®

Comienza a dar tus primeros pasos en el hacking y ciberseguridad, pasos firmes y seguros.





CSASC es una organización formada por los hackers éticos más relevantes del mundo, con más de 10 años de experiencia.

ATO Organizaciones acreditada de entrenamiento

Inspire confianza en los cursos de capacitación de su organización

Solicite que su organización de capacitación esté acreditada para impartir cursos de capacitación para nuestros esquemas de certificación profesional. Únase a nuestra red de organizaciones de capacitación acreditadas (ATO) CSASC.

Recibir la acreditación de capacitación CSASC proporciona una gran cantidad de beneficios. Nuestro servicio de acreditación es integral: evalúa los entrenadores, los materiales del curso y la entrega de su organización. Esto garantiza que su organización se comprometa a brindar capacitación ejemplar.

Al mostrar el estado acreditado de CSASC, los clientes pueden confiar en el estándar de capacitación que proporcionará su organización.

Convertirse en un ATO también le permite a su organización entregar exámenes, reservar y entregar exámenes utilizando nuestros sistemas seguros en línea, completos con resultados provisionales instantáneos y nuestro portal de invigiladores seguro.

Surge la necesidad de crear un órgano que certifique de manera universal los conocimientos y habilidades en ciberseguridad, ayudando a las empresas a certificar sus profesionales encargados de explotar las vulnerabilidades, en búsqueda de fortalecer sus líneas de defensa.



Como organismo de acreditación global e instituto de examen, estamos comprometidos a garantizar excelentes estándares de servicio prestados por aquellos a quienes acreditamos.

CSASC está acreditado para los siguientes esquemas de certificación:

Pentesting 101®

Bug Bounty 101®

Social Engineering 101®

Vulnerability Scan 101®

STATISTICS

5

Países

400

Profesionales

15

Certificaciones

Temario



- 1 Introducción
- 1.1 ¿Qué es la ingeniería social?
- 1.2 Historia de la ingeniería social
- 1.3 Roles
- 2.0 Tipos de ataques de ingeniería social
- 2.1 Phishing
- 2.2 Spear Phishing
- 2.3 Vishing
- 2.4 Pretexting
- 2.5 Baiting
- 2.6 Traigating
- 2.7 Quid pro quo
- 3.0 Casos en la vida real
- 3.1 Estadísticas
- 3.2 Los casos más sonados
- 3.3 Demostraciones
- 4.0 Examen

La protección contra la ingeniería social comienza con la educación; los usuarios necesitan aprender que no deben hacer nunca clic en enlaces sospechosos y siempre deben proteger sus credenciales de inicio de sesión, incluso en la oficina y en el hogar. Sin embargo, si las tácticas sociales logran su objetivo, el resultado probable es una infección por malware. Para combatir los rootkits, troyanos y otros bots, es fundamental implementar una solución de seguridad de Internet de alta calidad que sea capaz de eliminar infecciones y ras-



No caer en los engaños de las personas es fácil cuando sabes que técnicas y/o herramientas usan. Protege los datos de tu organización con este curso.

Social Engineering 101

Curso diseñado para hacer conciencia de los peligros en la red, actualmente hay más ataques dirigidos a las personas, derivado a su falta de conocimiento, esto lo hacen debido a que las personas son el eslabón más débil de la organización.

La ingeniería social es un conjunto de técnicas o estrategias para engañar a las personas esto para obtener algún tipo de ventaja, en la actualidad tomaron este termino para engañar a empleados de miles de organizaciones y de esa forma atacarlas.





Sus participantes dominaran los siguientes temas

- 1.1 Identificar ataques de Ing social
- 1.2 Identificar correos falsos (Phishing)
- 1.3 Creación de contraseñas seguras
- 1.4 Entendimiento de protección de datos
- 1.5 Identificar documentos apócrifos
- 1.6 Protección de datos personales
- 1.7 Prevenir ataques a la organización
- 1.8 Que hacer en caso de ser engañado

Todo lo que necesita para su próximo entrenamiento



- Materiales de capacitación profesional listos para usar
- Proceso de compra fácil y flexible
- Opciones de licencia rentables y atractivos
- Para proveedores de capacitación

Social Engineering®

Duración:

1 días

Modalidades:

En sus instalaciones
En línea con instructor en vivo
Presencial

Créditos CSASC:

3 creditos



Audiencia

Usuarios de tecnologías de la información sin conocimientos técnicos.

Colaboradores clave que podrían ser víctimas de ciberataques.

Colaboradores que están en contacto con clientes y proveedores.

Condiciones

Ninguna

Examen de Certificación

Formato: Opción múltiple.

Preguntas: 20.

Idioma: Español.

Puntaje de aprobación: 14/20 o 70 %.

Duración: 60 minutos máximo.

Libro abierto: No.

Entrega: Este examen está disponible en línea y papel.

Supervisado: Será a discreción del Partner.

Si sus empleado empiezan a conocer estas técnicas y/o estrategias será difícil que un atacante pueda engañar a sus empleados

No caer en los engaños de las personas es fácil cuando sabes que técnicas y/o herramientas usan. Protege tus datos personales y los de tu organización con este curso.



www.csascouncil.org
contacto@csascouncil.net

CSASC es el proveedor líder de contenido en ciberseguridad. Ofrecemos a los proveedores de capacitación una forma completamente nueva de administrar sus negocios.

Torre de Cristal, Paseo de la Castellana 259C, Planta 18,
28046 Madrid, España

© 2020 Cybersecurity Association Council. All rights reserved.

