# Ciberseguridad. Amenazas 3.

1. ¿Qué es una botnet?

a) Un servicio de almacenamiento en la nube.

b) Una red de dispositivos informáticos infectados y controlados por un atacante.

c) Un tipo de software antivirus confiable.

d) Un programa de seguridad utilizado para proteger los dispositivos de las amenazas de la red.

1. ¿Quién controla una botnet?

a) El botmaster.

b) El proveedor de servicios de Internet.

c) Los usuarios de los dispositivos infectados.

d) Los propietarios legítimos de los dispositivos infectados.

1. ¿Cuál es el objetivo principal de una botnet?

a) Mejorar el rendimiento de los dispositivos infectados.

b) Realizar actividades legítimas con el conocimiento y el consentimiento de los propietarios del equipo informático.

c) Proporcionar servicios de seguridad en línea.

d) Realizar actividades maliciosas sin el conocimiento ni el consentimiento de los propietarios legítimos.

1. ¿Qué tipo de dispositivos pueden formar parte de una botnet?

a) Computadoras personales, servidores, teléfonos inteligentes y otros dispositivos conectados a Internet.

b) Electrodomésticos como lavadoras y neveras.

c) Tarjetas de crédito y pasaportes.

d) Instrumentos musicales electrónicos y libros electrónicos.

1. ¿Por qué los ciberdelincuentes utilizan una botnet para realizar un ataque DDoS?

a) Para evitar ser identificados por las fuerzas de seguridad.

b) Para proteger sus propios dispositivos de posibles ataques.

c) Para demostrar sus habilidades en programación.

d) Para hacer el ataque más poderoso y difícil de rastrear.

1. ¿Cuál es un ejemplo común de uso de botnets?

a) La reparación de dispositivos electrónicos.

b) El envío masivo de correos electrónicos no deseados o spam.

c) La administración de redes sociales.

d) La creación de copias de seguridad de archivos importantes.

1. ¿Cómo pueden los botmasters obtener ganancias utilizando una botnet?

a) Cobrando una tarifa de suscripción a los propietarios legítimos de los dispositivos.

b) Solicitando rescates a las víctimas de ataques de botnet.

c) Vendiendo los dispositivos hardware infectados a otros ciberdelincuentes.

d) Alquilando su botnet a otros ciberdelincuentes en el mercado negro digital.

1. ¿Qué tipo de actividades ilegales pueden llevarse a cabo utilizando una botnet?

a) Transacciones bancarias seguras y compras en línea.

b) Juegos en línea y redes sociales.

c) Fraudes publicitarios y ataques DDoS.

d) Investigaciones científicas y desarrollo de software.

1. ¿Qué recomendaciones se mencionan para protegerse contra las botnets?

a) Mantener los dispositivos actualizados, utilizar software antivirus confiable y tener cuidado al descargar archivos o hacer clic en enlaces sospechosos.

b) Utilizar contraseñas débiles y desactivar las actualizaciones automáticas.

c) Ignorar las actualizaciones de seguridad y utilizar cualquier software antivirus disponible.

d) Compartir información personal en línea sin restricciones y descargar software de fuentes no confiables.

1. ¿Por qué es importante no hacer clic en enlaces sospechosos?

a) Para ayudar a los ciberdelincuentes a expandir su botnet.

b) Para evitar ser redirigido a sitios web maliciosos o fraudulentos.

c) Para acceder a información confiable y legítima en línea.

d) Para obtener descuentos y promociones exclusivas.

1. ¿Qué es una brecha de seguridad?

a) Un mecanismo de seguridad utilizado para proteger la información sensible de los ataques en línea.

b) Un punto débil o vulnerabilidad en un sistema o red que puede ser aprovechado por personas no autorizadas.

c) Un término que se refiere al proceso de actualizar software y contraseñas.

d) Una herramienta utilizada por expertos en ciberseguridad.

1. ¿Cuál puede ser una causa de una brecha de seguridad?

a) Abrir archivos adjuntos de correos electrónicos conocidos.

b) Utilizar contraseñas fuertes y diferentes para cada servicio online.

c) Compartir información confidencial con personas de confianza.

d) Una falta de actualizaciones de seguridad en un sistema.

1. ¿Cuál fue uno de los casos famosos de brecha de seguridad en 2017?

a) Robo de credenciales de acceso a través de ataques de phishing.

b) Ataque a la red de computadoras de Target, donde se comprometieron datos personales y financieros de clientes.

c) Ataque a Equifax, donde se expusieron los datos personales de millones de personas.

d) Infiltración en la red de la empresa Sony, donde se accedió a información confidencial.

1. ¿Cómo se logró el acceso a los sistemas de punto de venta de Target en 2013?

a) A través de una brecha de seguridad en el sistema de gestión de proveedores de la compañía.

b) Robando credenciales de acceso a través de ataques de phishing.

c) Mediante la explotación de vulnerabilidades en el sistema operativo.

d) Utilizando contraseñas débiles de los empleados de Target.

1. ¿Qué tipo de información fue comprometida en el ataque a la red de Sony en 2014?

a) Datos de acceso a cámaras y dispositivos de Internet de las Cosas.

b) Correos electrónicos internos, contratos, documentos financieros y datos personales de empleados y artistas.

c) Información personal de millones de clientes.

d) Datos de acceso a sistemas operativos y aplicaciones populares.

1. ¿Qué medidas se pueden tomar para mitigar las brechas de seguridad?

a) Ignorar posibles amenazas y no adoptar prácticas de seguridad cibernética.

b) Mantener actualizados los sistemas y utilizar contraseñas seguras.

c) Utilizar software no confiable y abrir archivos adjuntos de correos electrónicos desconocidos.

d) Compartir información confidencial con personas de confianza.

1. ¿Cuáles pueden ser las consecuencias de una brecha de seguridad?

a) Robo de datos personales, pérdida financiera y la interrupción de servicios.

b) Incremento de la confianza del público en una empresa.

c) Mejora de la reputación de una organización.

d) Disminución de la seguridad cibernética en general.

1. ¿Por qué es importante mantener actualizados los sistemas?

a) Para facilitar el acceso a información sensible.

b) Para aumentar la velocidad de los dispositivos.

c) Para protegerlos contra las últimas vulnerabilidades conocidas.

d) Para evitar el uso de contraseñas seguras.

1. ¿Cuál es una medida de seguridad cibernética sólida que se debe adoptar?

a) Utilizar contraseñas seguras y únicas.

b) Ignorar actualizaciones de seguridad y utilizar cualquier software disponible.

c) Compartir información confidencial en línea sin restricciones.

d) No prestar atención a posibles amenazas en línea.

1. ¿Qué se entiende por una puerta trasera no detectada?

a) Una técnica utilizada para proteger información confidencial en una red.

b) Una medida de seguridad adicional en un sistema que evita el acceso no autorizado.

c) Un tipo de software malicioso que se instala sin el conocimiento del usuario para encriptar toda su información y pedir un rescate.

d) Una debilidad en un sistema que permite el acceso no autorizado a tu ordenador sin ser detectado.

1. ¿Cuál es una debilidad común que puede llevar a una brecha de seguridad?

a) Compartir información confidencial solo con personas de confianza.

b) Utilizar software antivirus confiable.

c) Contraseñas débiles que son fáciles de adivinar.

d) Mantener los sistemas actualizados con las últimas actualizaciones de seguridad.

1. ¿Qué se puede hacer para evitar abrir archivos adjuntos de correos electrónicos desconocidos o sospechosos?

a) Verificar la fuente y el contenido del correo electrónico antes de abrir cualquier archivo adjunto.

b) No utilizar el correo electrónico como medio de comunicación para evitar cualquier tipo de amenaza.

c) Desactivar las actualizaciones automáticas de seguridad.

d) Abrir todos los archivos adjuntos sin importar su origen.

1. ¿Cuál es una forma común en la que se pueden explotar las brechas de seguridad en los dispositivos de Internet de las Cosas?

a) Acceso no autorizado a través de vulnerabilidades en la configuración de seguridad.

b) Actualizaciones automáticas de software y firmware.

c) Mantener los dispositivos desconectados de Internet.

d) Utilizar contraseñas seguras y únicas.

1. ¿Qué se debe hacer si se descubre una brecha de seguridad en un sistema o red?

a) Informar inmediatamente a los responsables de seguridad para que tomen medidas correctivas.

b) Compartir la información con personas no autorizadas.

c) Ignorar la brecha y esperar a que se solucione por sí sola.

d) No hacer nada y esperar a que otros descubran la brecha.

1. ¿Qué es el catfishing?

a) Un tipo de pesca con anzuelo especializado.

b) Una forma de engaño en línea en la cual una persona crea un perfil falso para engañar a otra persona.

c) Una técnica para obtener información personal y financiera de manera ilegal de los usuarios de internet.

d) Un documental que narra historias de amor en línea.

1. ¿Cuál es el objetivo principal del catfishing?

a) Promover la interacción social positiva en línea.

b) Engañar a otras personas haciéndoles creer que están interactuando con alguien genuino y confiable.

c) Divertirse a costa de los demás en las redes sociales.

d) Conseguir seguidores en las plataformas de redes sociales.

1. ¿Cómo se originó el término "catfishing"?

a) Por un famoso caso judicial relacionado con el engaño en línea.

b) A través de un experimento científico en línea.

c) A partir de un documental llamado "Catfish".

d) Por una canción popular sobre las redes sociales.

1. ¿Qué puede motivar a una persona a practicar el catfishing?

a) Ayudar a otras personas a encontrar el amor verdadero.

b) Obtención de información confidencial para fines maliciosos.

c) Diversión o entretenimiento a costa de los demás.

d) Búsqueda de seguidores y popularidad en línea.

1. ¿Qué recomendación se da para evitar caer en un catfishing?

a) No compartir información personal o financiera con personas desconocidas en línea.

b) Crear perfiles falsos para proteger nuestra identidad en línea.

c) Ignorar los instintos y confiar en cualquier perfil que parezca interesante.

d) Compartir información confidencial con cualquier persona en línea.

1. ¿Cuál es una pauta de seguridad en línea para verificar la autenticidad de una persona?

a) Compartir información personal y financiera con personas desconocidas en línea.

b) Realizar búsquedas en línea sobre la persona antes de entablar una relación o compartir información confidencial.

c) Confiar en la información proporcionada por perfiles en línea sin verificarla.

d) Crear perfiles falsos en línea para engañar a otras personas.

1. ¿Qué se puede sentir como consecuencia del catfishing?

a) Aumento de la confianza y la autoestima en línea.

b) Desinterés por las redes sociales y las aplicaciones de citas.

c) Mejora de las habilidades de comunicación en línea.

d) Daño emocional y pérdida de confianza en las interacciones en línea.

1. ¿Qué tipo de información se debe evitar compartir con personas desconocidas en línea?

a) Contraseñas y códigos de acceso.

b) Datos de ubicación en tiempo real.

c) Información personal o financiera.

d) Todas las respuestas son ciertas.

1. ¿Cuál es una señal de advertencia de que un perfil en línea podría ser falso?

a) Comparte información personal y financiera sin restricciones.

b) Muestra interés en entablar una relación amorosa.

c) Tiene muchas seguidores y "me gusta" en sus publicaciones.

d) Parece demasiado bueno para ser verdad.

1. ¿Qué se debe hacer si se sospecha que se está siendo víctima de catfishing?

a) Compartir más información personal y financiera para confirmar la autenticidad.

b) Cortar la comunicación con la persona y reportar el perfil a la plataforma.

c) Intentar rastrear la identidad de la persona por cuenta propia.

d) Ignorar la situación y esperar a que desaparezca por sí sola.

1. ¿Cuál es uno de los riesgos asociados con el catfishing?

a) Reducción de la interacción social en línea.

b) Mejora de las habilidades de comunicación en línea.

c) Aumento de la popularidad en las redes sociales.

d) Acoso y extorsión por parte del impostor.