# Ciberseguridad. Amenazas 4.

1. ¿Qué es el ciberacoso?

a) Un programa malicioso que infecta los dispositivos electrónicos.

b) Una enfermedad causada por el uso excesivo de la tecnología.

c) Un tipo de juego en línea donde se compite contra otros usuarios.

d) Una forma de acoso o intimidación que ocurre en el entorno digital.

1. ¿Cuál es una característica del ciberacoso?

a) Solo ocurre en días laborables.

b) Se limita a un único medio de comunicación en línea.

c) Se puede llevar a cabo las 24 horas del día, los 7 días de la semana.

d) Solo afecta a personas mayores de 18 años.

1. ¿Cuál de las siguientes acciones es un ejemplo de ciberacoso?

a) Enviar mensajes ofensivos a través de redes sociales.

b) Publicar consejos útiles sobre seguridad en internet.

c) Compartir imágenes de mascotas lindas en línea.

d) Participar en una competencia de videojuegos en línea.

1. ¿Qué es el ciberbullying?

a) Enviar mensajes de amor y amistad a través de redes sociales.

b) Hacer bromas inofensivas en internet.

c) Utilizar las plataformas en línea para acosar o avergonzar repetidamente a alguien.

d) Compartir información útil sobre un tema específico en línea.

1. ¿Cuáles son algunas consecuencias del ciberacoso?

a) Impacto negativo en la reputación y la vida social de las víctimas.

b) Mayor rendimiento académico y éxito laboral.

c) Aumento de la popularidad en línea y el reconocimiento público.

d) Mejora de la autoestima y las relaciones personales de las víctimas.

1. ¿Cuál de las siguientes medidas es importante para protegerse del ciberacoso?

a) Responder a todos los mensajes y comentarios recibidos.

b) Compartir información personal con desconocidos.

c) Mantener la privacidad en línea.

d) No utilizar contraseñas seguras en las cuentas en línea.

1. ¿Qué se puede hacer para combatir el ciberacoso?

a) Vengarse del acosador publicando información personal sobre él.

b) Participar en foros en línea y expresar opiniones negativas sobre el ciberacoso.

c) Bloquear o reportar a los acosadores y denunciar ante las autoridades.

d) Ignorar por completo los mensajes y comentarios ofensivos.

1. ¿Cuál es una forma común de ciberacoso?

a) Compartir fotos de vacaciones con familiares en línea.

b) Difusión de rumores o mentiras sobre alguien en línea.

c) Envío de mensajes de agradecimiento a amigos en redes sociales.

d) Publicación de contenido educativo en línea.

1. ¿Por qué es importante buscar apoyo de adultos de confianza en situaciones de ciberacoso?

a) Los adultos no suelen entender el problema del ciberacoso.

b) No es necesario buscar apoyo, se puede resolver el problema solo.

c) Pueden brindar orientación y apoyo emocional.

d) Pueden resolver el problema sin la necesidad de tomar medidas adicionales.

1. ¿Qué se puede hacer para proteger la privacidad en línea?

a) Ajustar las configuraciones de privacidad en las redes sociales.

b) Compartir información personal con cualquier persona en línea.

c) Permitir que cualquier persona tenga acceso a tu información en línea.

d) Utilizar contraseñas débiles y fáciles de adivinar.

1. ¿Qué pueden hacer las víctimas de ciberacoso para protegerse?

a) No hacer nada y esperar que el acoso desaparezca por sí solo.

b) Compartir aún más información personal en línea.

c) Bloquear y reportar a los acosadores. Denunciar ante las autoridades.

d) Responder a los mensajes ofensivos con más agresividad.

1. ¿Qué pueden hacer los testigos de ciberacoso para ayudar?

a) Ignorar completamente la situación y no hacer nada al respecto.

b) Burlarse y unirse a los acosadores en línea.

c) No participar y comunicar el acoso a una autoridad competente.

d) Compartir y difundir el contenido ofensivo en línea.

1. ¿Cuál de las siguientes afirmaciones es cierta sobre el ciberacoso?

a) Solo ocurre en entornos escolares.

b) Es una forma inofensiva de expresión en línea.

c) Solo afecta a los adultos, no a los jóvenes.

d) Puede afectar negativamente la salud mental y emocional de las víctimas.

1. ¿Cuál es el objetivo del ciberacoso?

a) Molestar, hostigar, amenazar o humillar a otra persona.

b) Divertirse y pasar el tiempo en línea.

c) Promover la amistad y el respeto en línea.

d) Ayudar a las víctimas a mejorar su autoestima.

1. ¿Qué es un ataque de denegación de servicio (DoS)?

a) Una estrategia para mejorar la disponibilidad de los servicios en línea.

b) Un mecanismo para mejorar la velocidad y rendimiento de una red.

c) Un método para robar información y comprometer la seguridad de un sistema.

d) Una técnica utilizada para inundar un sistema o red con tráfico malicioso.

1. ¿Cuál es el objetivo principal de un ataque de denegación de servicio (DoS)?

a) Robar información confidencial de los usuarios.

b) Obtener acceso no autorizado a un sistema o red por parte de los ciberdelincuentes.

c) Mejorar la seguridad y protección de un sistema.

d) Interrumpir los servicios y causar inconvenientes o pérdidas económicas.

1. ¿Qué es un ataque de denegación de servicio distribuido (DDoS)?

a) Un ataque que utiliza múltiples dispositivos infectados para lanzar peticiones a un servicio web y colapsarlo.

b) Un ataque que se lleva a cabo desde una única ubicación geográfica hacia un servicio web para colapsarlo.

c) Un ataque que solo afecta a sistemas personales, no a redes empresariales.

d) Un ataque que tiene como objetivo robar información confidencial.

1. ¿Cuál es la principal diferencia entre un ataque DoS y un ataque DDoS?

a) Un ataque DoS solo afecta a sistemas personales, no a redes empresariales.

b) Un ataque DDoS utiliza múltiples dispositivos infectados distribuidos en diferentes ubicaciones.

c) Un ataque DDoS tiene como objetivo robar información confidencial.

d) Un ataque DoS tiene como objetivo hacer pasar a una persona por otra, con intenciones maliciosas.

1. ¿Cuál es el propósito de un ataque de inundación de tráfico?

a) Mejorar la velocidad y rendimiento de una red.

b) Sobrecargar el sistema objetivo y causar una interrupción en el servicio.

c) Robar información confidencial de los usuarios de una red.

d) Aumentar la disponibilidad de los servicios en línea.

1. ¿Qué tipo de daños pueden causar los ataques DoS?

a) Mejora del rendimiento y velocidad de los servicios en línea.

b) Aumento de la seguridad y protección de los sistemas y redes.

c) Mejora de la reputación y reconocimiento de una organización.

d) Pérdida de ingresos para las empresas, interrupción de servicios críticos y pérdida de reputación.

1. ¿Qué es una botnet en el contexto de los ataques DDoS?

a) Una red de dispositivos infectados utilizados para lanzar un ataque.

b) Un software de seguridad utilizado para proteger contra ataques DDoS.

c) Una técnica para mejorar la velocidad y rendimiento de una red.

d) Un protocolo de comunicación utilizado para coordinar ataques DDoS.

1. ¿Cuál es la finalidad de implementar medidas de seguridad y mitigación en los sistemas y redes?

a) Protegerse de los ataques de denegación de servicio y mantener la disponibilidad de los servicios en línea.

b) Reducir el acceso a los servicios en línea para los usuarios legítimos.

c) Aumentar la velocidad y rendimiento de una red.

d) Incrementar el robo de información confidencial.

1. ¿Cuál de las siguientes afirmaciones es cierta sobre los ataques DoS?

a) Solo afectan a sistemas personales y no a redes empresariales.

b) No tienen como objetivo robar información o comprometer la seguridad de un sistema.

c) Son técnicas legítimas utilizadas para mejorar la disponibilidad de los servicios en línea.

d) Se enfocan en mejorar la reputación de las organizaciones.

1. ¿Cuál es el objetivo principal de un ataque de denegación de servicio (DoS)?

a) Robar información confidencial de los usuarios.

b) Mejorar la seguridad y protección de un sistema.

c) Obtener acceso no autorizado a un sistema o red.

d) Interrumpir los servicios y causar inconvenientes o pérdidas económicas.

1. ¿Qué es el DNS poisoning?

a) Una técnica utilizada para alterar o corromper la información en la base de datos de nombres de dominio (DNS).

b) Una técnica para optimizar el rendimiento de los servidores DNS.

c) Una técnica utilizada para alterar o corromper la información en la base de datos de denegación de servicio (DNS).

d) Un sistema de seguridad utilizado para proteger los datos personales.

1. ¿Cuál es el objetivo principal del DNS poisoning?

a) Optimizar la seguridad de los servidores DNS.

b) Mejorar la velocidad y rendimiento de la conexión a Internet.

c) Proteger los datos personales de los usuarios.

d) Redirigir a los usuarios a sitios web maliciosos o falsos.

1. ¿Cómo manipulan los atacantes los datos en el DNS poisoning?

a) Mejorando la funcionalidad de los servidores DNS.

b) Alterando o corrompiendo los datos almacenados en los servidores DNS.

c) Aumentando la capacidad de almacenamiento de los servidores DNS.

d) Creando nuevos servidores DNS desde cero.

1. ¿Qué es el secuestro de DNS?

a) Un protocolo de comunicación utilizado en la administración de servidores DNS.

b) Una medida de seguridad utilizada para proteger los servidores DNS.

c) Un método para mejorar la velocidad de carga de los sitios web.

d) Un ejemplo de DNS poisoning donde los atacantes alteran los registros para redirigir a los usuarios a sitios web falsificados.

1. ¿Qué es el pharming?

a) Una técnica para mejorar el rendimiento de los servidores DNS.

b) Una medida de seguridad utilizada para proteger los datos personales.

c) Una forma de DNS poisoning donde los atacantes redirigen a los usuarios a sitios web falsos sin su conocimiento.

d) Un protocolo utilizado para administrar la seguridad en los servidores DNS de forma distribuida por parte de los administradores del sistema.

1. ¿Cuáles pueden ser las consecuencias del DNS poisoning?

a) Los usuarios experimentarán una mejora significativa en la velocidad de conexión a internet, aunque con cortes esporádicos.

b) Los servidores DNS se vuelven más eficientes y confiables.

c) Los usuarios pueden verse expuestos a sitios web maliciosos y corren el riesgo de robo de datos o propagación de malware.

d) Los ataques de phishing se vuelven más difíciles de detectar para los usuarios.

1. ¿Por qué puede ser difícil para los usuarios detectar el DNS poisoning?

a) Los usuarios generalmente no visitan sitios web maliciosos o falsos.

b) La redirección ocurre a nivel de los servidores DNS y no en el dispositivo del usuario.

c) Los servidores DNS son muy eficientes en la detección de ataques de envenenamiento.

d) Los usuarios no están familiarizados con los términos técnicos relacionados con el DNS poisoning.

1. ¿Qué medidas de seguridad se pueden tomar para protegerse del DNS poisoning?

a) Ignorar las posibles señales de phishing y no prestar atención a los sitios web que parecen sospechosos.

b) Utilizar cualquier servidor DNS disponible y no preocuparse por las actualizaciones de software.

c) Utilizar servidores DNS reconocidos y estar alerta ante señales de phishing o webs sospechosas.

d) Desactivar los firewalls y sistemas de detección de intrusiones para evitar bloqueos en los servidores DNS.

1. ¿Cuál es la función principal del servidor DNS?

a) Optimizar el rendimiento de la conexión a Internet y acelerar la carga de los sitios web.

b) Traducir los nombres de dominio legibles para los humanos en direcciones IP numéricas que las computadoras pueden entender.

c) Almacenar información confidencial de los usuarios y protegerla de accesos no autorizados.

d) Mejorar la seguridad de los sitios web y evitar ataques de envenenamiento de DNS.

1. ¿Qué se puede hacer para detectar y prevenir ataques de envenenamiento de DNS?

a) Configurar firewalls y sistemas de detección de intrusiones.

b) Proporcionar información personal en sitios web no verificados.

c) No utilizar servidores DNS confiables y evitar las actualizaciones de software.

d) Mantener el software y los sistemas operativos desactualizados.

1. ¿Qué tipo de información se encuentra en la base de datos de nombres de dominio (DNS)?

a) Los nombres de los países asociados con los dominios en Internet.

b) Las direcciones IP de los servidores DNS utilizados en una red.

c) Los registros que relacionan los nombres de dominio (www.google.com) con las direcciones https correspondientes.

d) Los registros que relacionan los nombres de dominio (www.google.com) con las direcciones IP correspondientes.

1. ¿Cuál es el propósito del envenenamiento de cachés DNS locales en los dispositivos de los usuarios?

a) Mejorar el rendimiento de los dispositivos y acelerar la conexión a Internet.

b) Redirigir a los usuarios a sitios web falsos o maliciosos.

c) Proteger los datos personales de los usuarios y evitar el robo de información.

d) Optimizar la seguridad de los servidores DNS y prevenir ataques de envenenamiento.

1. ¿Qué es una dirección IP?

a) Un código de seguridad utilizado para proteger las cuentas en línea.

b) Una técnica utilizada para corromper los datos almacenados en los servidores DNS.

c) Un nombre de dominio utilizado para acceder a sitios web específicos (por ejemplo https://www.google.com).

d) Una identificación numérica única asignada a cada dispositivo conectado a una red (por ejemplo 81.169.145.93).