# Ciberseguridad. Amenazas 1.

1. ¿Cuál es el propósito principal del adware?

a) Mejorar la experiencia en línea

b) Aumentar la privacidad en línea

c) Proteger nuestros dispositivos

d) Mostrar anuncios no deseados

1. ¿Cómo se propaga principalmente el adware?

a) A través de descargas de software gratuitas, sitios web sospechosos y enlaces maliciosos

b) Por medio de actualizaciones automáticas del sistema operativo

c) Mediante el intercambio de archivos por correo electrónico

d) A través de redes sociales populares

1. ¿Qué son las ventanas emergentes (pop-ups) asociadas con el adware?

a) Ventanas que proporcionan información útil y relevante

b) Ventanas que muestran anuncios o promociones mientras navegamos por Internet

c) Ventanas que aparecen en el escritorio de nuestro dispositivo

d) Ventanas que solicitan la instalación de software adicional

1. ¿Qué efecto pueden tener las barras de herramientas no deseadas instaladas por el adware?

a) Modificar la configuración del navegador y redirigirnos a sitios web no deseados

b) Optimizar el rendimiento del dispositivo

c) Mejorar la velocidad de conexión a Internet

d) Proteger nuestros datos personales

1. ¿Cómo puede el adware alterar el comportamiento de nuestro navegador?

a) Bloqueando anuncios y ventanas emergentes

b) Mejorando la velocidad de carga de las páginas web

c) Redireccionando a sitios web diferentes a los que intentamos visitar

d) Restringiendo el acceso a ciertos sitios web

1. ¿Qué es la recopilación de datos personales por parte del adware?

a) Mejorar la calidad de los anuncios que se nos muestran

b) Permitirnos acceder a servicios en línea de forma más segura

c) Rastrear y recopilar información personal sin nuestro consentimiento

d) Proteger nuestros datos personales de terceros

1. ¿Qué impacto puede tener el adware en nuestros dispositivos?

a) Aumentar la capacidad de almacenamiento disponible

b) Optimizar la navegación por Internet

c) Ralentizar el rendimiento y consumir recursos del sistema

d) Mejorar la seguridad y privacidad en línea

1. ¿Cuál es una medida efectiva para protegernos del adware?

a) Descargar software solo de fuentes confiables y leer las opiniones de otros usuarios antes de instalarlo

b) Hacer clic en anuncios sospechosos para obtener más información

c) Utilizar contraseñas simples y fáciles de recordar

d) Desactivar las actualizaciones automáticas del sistema operativo

1. ¿Qué se recomienda hacer en caso de sospechar que hemos sido afectados por adware?

a) Compartir información sobre el incidente en las redes sociales

b) Ignorar cualquier cambio y esperar a que desaparezcan por sí solos

c) Reiniciar el dispositivo y borrar todos los archivos

d) Estar atentos a cualquier cambio inesperado en nuestro navegador o comportamiento del dispositivo y tomar medidas

1. ¿Cuál es una medida para evitar el adware?

a) Compartir nuestros datos personales en línea

b) Descargar software de cualquier fuente sin verificar su autenticidad

c) Hacer clic en cualquier anuncio para obtener ofertas especiales

d) Configurar nuestros navegadores para bloquear ventanas emergentes y desactivar la instalación automática de complementos o barras de herramientas

1. ¿Qué recomendación se da para mantener nuestros dispositivos protegidos contra el adware?

a) Descargar software desde cualquier fuente sin verificar su seguridad

b) Evitar utilizar software antivirus y antimalware

c) Mantener nuestros dispositivos actualizados con los últimos parches de seguridad y utilizar programas antivirus y antimalware confiables

d) Desactivar los programas de seguridad para mejorar el rendimiento del dispositivo

1. ¿Por qué es importante evitar hacer clic en anuncios sospechosos o enlaces desconocidos?

a) Porque aumentan nuestra experiencia en línea

b) Porque nos pueden llevar a páginas de descarga de software gratuito

c) Porque pueden contener adware o dirigirnos a sitios web maliciosos

d) Porque nos permiten obtener descuentos exclusivos

1. ¿Qué es la apropiación de formulario, también conocida como "formjacking" en inglés?

a) Una técnica para evitar el envío de formularios en línea.

b) Un método para mejorar la seguridad de los formularios en línea en los sitios web.

c) Un tipo de ataque que se centra en la explotación de redes sociales.

d) Una táctica empleada por los ciberdelincuentes para robar información confidencial de los formularios en línea presentes en sitios web legítimos.

1. ¿Cuál es el objetivo principal de la apropiación de formulario?

a) Impedir el acceso a los formularios en línea de los usuarios.

b) Aumentar la seguridad en los formularios en línea de los sitios web.

c) Robar información confidencial, especialmente datos de tarjetas de crédito, de los formularios en línea presentes en sitios web legítimos.

d) Interceptar correos electrónicos enviados a través de formularios en línea.

1. ¿Cómo logran los ciberdelincuentes insertar código malicioso en un sitio web comprometido?

a) Enviando correos electrónicos falsos a los administradores del sitio web.

b) Contratando a un programador para que realice la tarea.

c) Explotando vulnerabilidades en el software o en los complementos utilizados por el sitio web.

d) Utilizando técnicas de ingeniería social para obtener la contraseña del sitio web.

1. ¿Qué sucede cuando un usuario envía un formulario en un sitio web comprometido?

a) El formulario se bloquea y no se envía la información.

b) El código malicioso interfiere y copia los datos ingresados por el usuario.

c) El usuario recibe una confirmación de envío falsa.

d) El sitio web se cierra y se muestra un mensaje de error.

1. ¿Qué tipo de información pueden robar los ciberdelincuentes mediante la apropiación de formulario?

a) Contraseñas de redes sociales y direcciones de correo electrónico.

b) Historial de navegación y preferencias de compras.

c) Números de tarjetas de crédito, nombres, direcciones y otra información personal.

d) Documentos personales como el pasaporte o el carné de identidad.

1. ¿Cómo se envían los datos robados a los ciberdelincuentes después de un ataque de apropiación de formulario?

a) De manera encubierta a los servidores controlados por los ciberdelincuentes.

b) A través de un correo electrónico encriptado dirigido a los ciberdelincuentes.

c) Por medio de una llamada telefónica anónima.

d) Mediante una publicación en redes sociales.

1. ¿Cuál de las siguientes afirmaciones es un ejemplo de caso en el que se ha producido apropiación de formulario?

a) Ataque a cuentas de correo electrónico.

b) Ataque a servidores de videojuegos.

c) Ataque a cajeros automáticos.

d) Ataque a tiendas en línea.

1. ¿Qué tipo de organizaciones han sido víctimas de la apropiación de formulario?

a) Empresas de telecomunicaciones.

b) Redes sociales.

c) Agencias de viajes.

d) Organizaciones benéficas.

1. ¿En qué año se descubrió que los atacantes habían comprometido el sitio web de una organización benéfica británica llamada "National Emergencies Trust"?

a) 2018.

b) 2020.

c) 2019.

d) 2021.

1. ¿Qué tipo de sitios web también han sido objetivo de la apropiación de formulario?

a) Sitios web de música.

b) Sitios web de entretenimiento.

c) Sitios web de noticias.

d) Sitios web gubernamentales.

1. ¿Qué medidas de seguridad se recomienda tomar para protegerse de la apropiación de formulario?

a) Estar atento a las señales de advertencia, como cambios en la apariencia o el comportamiento de un sitio web.

b) Mantener el software y los sistemas operativos actualizados en todos los dispositivos.

c) Utilizar soluciones de seguridad confiables, como antivirus y firewalls.

d) Todas las anteriores.

1. ¿Qué se recomienda evitar para protegerse de la apropiación de formulario?

a) Actualizar constantemente los perfiles de redes sociales.

b) Abrir todos los enlaces recibidos en correos electrónicos.

c) Utilizar métodos de pago seguros, como servicios de pago en línea o tarjetas de crédito virtuales.

d) Proporcionar información personal o de pago en sitios web.

1. ¿Qué deben hacer los usuarios para proteger su información personal y financiera mientras navegan por Internet?

a) Desactivar todas las medidas de seguridad en los dispositivos.

b) No utilizar tarjetas de crédito en línea.

c) Ser conscientes de la amenaza de la apropiación de formulario y tomar las medidas necesarias de seguridad.

d) Evitar completamente el uso de formularios en línea.

1. ¿Qué es un ataque de abrevadero, también conocido como "watering hole attack"?

a) Un ataque físico en el que se utiliza un abrevadero para robar información confidencial.

b) Una medida de seguridad implementada en los sitios web para proteger a los usuarios.

c) Un método utilizado por los usuarios para proteger sus dispositivos de malware.

d) Una técnica utilizada por los ciberdelincuentes para comprometer la seguridad de los usuarios que visitan sitios web legítimos.

1. ¿Cuál es el objetivo principal de un ataque de abrevadero?

a) Evitar que los usuarios visiten sitios web legítimos.

b) Proteger la información confidencial de los usuarios en los sitios web legítimos.

c) Infectar a los usuarios desprevenidos con malware o robar. información confidencial.

d) Mejorar la seguridad de los sitios web confiables.

1. ¿Qué similitud existe entre un ataque de abrevadero y un depredador que acecha a sus presas?

a) Los ciberdelincuentes insertan código malicioso o redirigen a los usuarios a sitios web comprometidos.

b) Los usuarios visitan el sitio web comprometido y se descarga el malware.

c) Los ciberdelincuentes identifican sitios web de confianza frecuentados por un grupo particular.

d) Los ciberdelincuentes utilizan técnicas de ingeniería social para engañar a los usuarios.

1. ¿Qué puede hacer el malware descargado durante un ataque de abrevadero en un sistema infectado?

a) Mejorar el rendimiento del sistema infectado.

b) Robar información confidencial, como contraseñas, datos bancarios o información personal.

c) Actualizar automáticamente el software y los sistemas operativos.

d) Bloquear el acceso a otros sitios web.

1. ¿Qué técnica pueden utilizar los atacantes durante un ataque de abrevadero para engañar a los usuarios?

a) Técnicas de ingeniería social.

b) Contratar a expertos en ciberseguridad.

c) Crear sitios web legítimos.

d) Restringir el acceso a los sitios web comprometidos.

1. ¿En qué año ocurrió el ataque de abrevadero dirigido a los sitios web del Gobierno de los Estados Unidos?

a) 2014.

b) 2012.

c) 2013.

d) 2018.

1. ¿A qué tipo de empresas se dirigió el ataque de abrevadero descubierto en 2019 en Asia?

a) Empresas de alimentación.

b) Empresas tecnológicas.

c) Empresas de moda.

d) Empresas de transporte.

1. ¿Qué tipo de sitios web se han comentado como objetivos de ataques de abrevadero?

a) Sitios web gubernamentales exclusivamente.

b) Foros y sitios web frecuentados por comunidades en línea.

c) Sitios web de noticias internacionales.

d) Sitios web de música y entretenimiento.

1. ¿Cómo pueden protegerse los usuarios de los ataques de abrevadero?

a) Manteniendo el software y los sistemas operativos actualizados.

b) Siendo cautelosos al hacer clic en enlaces y descargar archivos de sitios web desconocidos o sospechosos.

c) Todas son correctas.

d) Utilizando soluciones de seguridad confiables, como antivirus y firewalls.

1. ¿Qué tipo de sitios web son identificados como sitios de confianza para llevar a cabo un ataque de abrevadero?

a) Sitios web de compras en línea.

b) Todas son correctas.

c) Sitios web gubernamentales.

d) Sitios web de redes sociales.

1. ¿Por qué los ataques de abrevadero son difíciles de detectar?

a) Porque los sitios web legítimos tienen medidas de seguridad avanzadas.

b) Porque los ataques de abrevadero son poco comunes.

c) Porque los usuarios están más atentos a los ataques de phishing.

d) Porque se aprovechan de la confianza depositada en los sitios web legítimos que se visitan con frecuencia.

1. ¿Qué se recomienda hacer al hacer clic en enlaces y descargar archivos de sitios web desconocidos o sospechosos?

a) Ser cauteloso y verificar la confiabilidad del sitio web antes de hacer clic o descargar.

b) Evitar completamente hacer clic en enlaces y descargar archivos.

c) Utilizar una conexión VPN para mayor seguridad.

d) Desactivar todas las medidas de seguridad en los dispositivos antes de hacer clic o descargar.

1. ¿Cuál es la finalidad principal de utilizar soluciones de seguridad confiables, como antivirus y firewalls, para protegerse de los ataques de abrevadero?

a) Crear una barrera física entre el usuario y el atacante.

b) Mejorar la velocidad de conexión a Internet.

c) Evitar el acceso a sitios web legítimos.

d) Detectar y bloquear posibles amenazas de malware.