# Ciberseguridad. Amenazas I.

1. ¿Qué es la "apropiación de formulario" en ciberseguridad?

a) Una técnica para proteger los datos en línea.

b) Una estrategia para crear formularios más atractivos visualmente para los usuarios que rellenan información en línea.

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

d) Una táctica para obtener información personal y sensible de los usuarios a través de formularios en línea.

1. ¿Cómo pueden los ciberdelincuentes llevar a cabo la apropiación de formulario?

a) Mediante el uso de sitios web fraudulentos que solicitan información confidencial.

b) Utilizando herramientas de encriptación para proteger los datos de los usuarios.

c) Implementando medidas de autenticación de dos factores en los formularios.

d) A través de la optimización de la seguridad de los formularios en línea.

1. ¿Qué es un ejemplo común de apropiación de formulario?

a) La ingeniería social.

b) El phishing.

c) El spam.

d) El malware.

1. ¿Cómo pueden los ciberdelincuentes llevar a cabo el phishing?

a) Enviando correos electrónicos fraudulentos que dirigen a los usuarios a sitios web falsos.

b) Utilizando antivirus para proteger la información personal de los usuarios.

c) Enviando mensajes de texto solicitando información personal a los usuarios.

d) A través de la configuración de firewalls en los dispositivos de los usuarios.

1. ¿Qué hacen los ciberdelincuentes una vez que los usuarios completan los formularios falsos?

a) No hacer nada, ya que los formularios son falsos.

b) Borrar la información para no dejar rastro.

c) Utilizar la información para cometer fraudes o robar identidades.

d) Utilizar la información para mejorar la seguridad en línea de los usuarios.

1. ¿Qué precauciones pueden tomar los usuarios para protegerse contra la apropiación de formulario?

a) Ignorar los avisos de seguridad en los navegadores web.

b) Compartir contraseñas con amigos para mayor seguridad.

c) Verificar la autenticidad de los sitios web antes de ingresar información personal.

d) Completar formularios en línea con información personal sin importar su procedencia.

1. ¿Qué tipo de información pueden solicitar los formularios fraudulentos?

a) Preferencias de entretenimiento, como películas favoritas.

b) Datos de contacto, como direcciones de correo electrónico del usuario.

c) Credenciales de inicio de sesión, como nombres de usuario y contraseñas.

d) Información médica confidencial del usuario.

1. ¿Cómo pueden los usuarios identificar un formulario falso en línea?

a) Verificando la legitimidad del sitio web y revisando la URL.

b) Completando el formulario y esperando los resultados.

c) Ignorando las advertencias de seguridad del navegador.

d) Haciendo clic en todos los enlaces proporcionados en el formulario.

1. ¿Por qué es importante que los usuarios estén alerta ante la apropiación de formulario?

a) Para evitar recibir correos electrónicos no deseados.

b) Para aumentar la velocidad de carga de los sitios web.

c) Para mejorar la funcionalidad de los formularios en línea.

d) Para proteger su información personal y evitar el fraude.

1. ¿Qué recomendación se da para protegerse contra la apropiación de formulario?

a) Utilizar contraseñas simples y fáciles de recordar en todas las cuentas en línea.

b) Proporcionar información personal sin importar la procedencia del formulario.

c) Compartir contraseñas con amigos cercanos para mayor seguridad.

d) Verificar la autenticidad de los sitios web y las aplicaciones antes de proporcionar información personal.

1. ¿Qué se sugiere hacer con las contraseñas para mitigar el riesgo de apropiación de formulario?

a) Guardar las contraseñas en un archivo de texto en el escritorio del dispositivo.

b) Compartir las contraseñas con amigos para mantenerlas seguras.

c) Utilizar contraseñas seguras y no reutilizar las mismas credenciales en múltiples cuentas.

d) Utilizar contraseñas simples y fáciles de recordar en todas las cuentas en línea.

1. ¿Por qué es importante verificar la autenticidad de los sitios web y aplicaciones antes de proporcionar información personal?

a) Para acelerar el proceso de registro en línea.

b) Porque todas las solicitudes de información en línea son seguras y legítimas.

c) Para evitar caer en trampas de apropiación de formulario y proteger la privacidad.

d) Porque los ciberdelincuentes no son capaces de crear sitios web falsos.

1. ¿Qué es el "ataque de abrevadero"?

a) Un método para proteger los dispositivos contra el malware.

b) Una técnica para mejorar la velocidad de descarga de archivos en línea.

c) Una táctica para evitar la detección de virus en los sistemas informáticos.

d) Una estrategia de ciberataque que aprovecha la confianza de los usuarios en sitios web o recursos legítimos para infectar sus dispositivos con malware.

1. ¿En qué se basa el "ataque de abrevadero"?

a) En la instalación de programas antivirus en los dispositivos.

b) En el uso de tácticas agresivas para dañar los sistemas informáticos.

c) En la idea de que los usuarios son más propensos a hacer clic en enlaces o descargar archivos adjuntos de fuentes que consideran seguras.

d) En la generación de contraseñas seguras para proteger los datos en línea.

1. ¿Qué hacen los ciberdelincuentes en un ataque de abrevadero?

a) Ayudan a los usuarios a proteger sus dispositivos contra el malware.

b) Ofrecen descargas gratuitas de software legítimo para mejorar la experiencia del usuario.

c) Crean sitios web falsos o comprometen sitios web legítimos para distribuir malware.

d) Envían correos electrónicos promocionales a los contactos de la víctima.

1. ¿Cómo pueden los ciberdelincuentes distribuir malware en un ataque de abrevadero?

a) Enviando correos electrónicos de phishing a personas desconocidas.

b) Creando una página web falsa que se parece a un sitio de descarga de software confiable.

c) Utilizando software antivirus para infectar los dispositivos de los usuarios.

d) Publicando anuncios en línea con enlaces maliciosos.

1. ¿Qué hacen los usuarios en un ataque de abrevadero?

a) Desconfían de cualquier enlace o archivo adjunto que provenga de fuentes conocidas.

b) Informan a las autoridades sobre cualquier actividad sospechosa en línea.

c) Descargan lo que creen que es un software legítimo, pero en realidad están descargando malware en sus dispositivos.

d) Actualizan regularmente su software de seguridad para proteger sus dispositivos.

1. ¿Cuál es un ejemplo común de ataque de abrevadero?

a) Crear una página web falsa que se ve y se comporta como un sitio de descarga de software confiable.

b) Enviar correos electrónicos promocionales a contactos desconocidos.

c) Compartir enlaces a sitios web legítimos en redes sociales.

d) Publicar anuncios en línea con enlaces maliciosos.

1. ¿Qué hacen los ciberdelincuentes una vez que los usuarios hacen clic en los enlaces maliciosos?

a) Envían un mensaje de advertencia a los usuarios sobre posibles amenazas en línea.

b) Ofrecen software gratuito para proteger los dispositivos contra el malware.

c) Solicitan un rescate económico a cambio de eliminar el malware de los dispositivos de los usuarios.

d) Redirigen a los usuarios a un sitio web falso que descarga malware en sus dispositivos.

1. ¿Qué pueden hacer los ciberdelincuentes cuando comprometen una cuenta de correo electrónico legítima en un ataque de abrevadero?

a) Compartir información útil y valiosa con los contactos de la víctima.

b) Enviar correos electrónicos de agradecimiento a los contactos de la víctima.

c) Comunicarse con los contactos de la víctima para verificar la autenticidad de los mensajes recibidos.

d) Enviar correos electrónicos con enlaces maliciosos a los contactos de la víctima.

1. ¿Por qué los usuarios pueden ser más propensos a hacer clic en enlaces maliciosos en un ataque de abrevadero?

a) Porque tienen instalado software antivirus que los protege de cualquier amenaza.

b) Porque siempre están atentos a posibles amenazas en línea.

c) Porque reciben los correos electrónicos de personas en quienes confían.

d) Porque comparten contraseñas con amigos cercanos para mayor seguridad.

1. ¿Cuál es una recomendación para protegerse contra los ataques de abrevadero?

a) Compartir contraseñas con amigos para mejorar la seguridad en línea.

b) Hacer clic en todos los enlaces que provengan de fuentes conocidas.

c) Descargar archivos adjuntos sin verificar su origen.

d) Estar siempre alerta y desconfiar de los enlaces o archivos adjuntos inesperados.

1. ¿Por qué es importante practicar buenos hábitos de seguridad en línea para prevenir los ataques de abrevadero?

a) Porque permite descargar archivos adjuntos de forma segura.

b) Porque puede ayudar a proteger los dispositivos contra el malware.

c) Porque aumenta la velocidad de navegación en Internet.

d) Porque no tiene impacto en la seguridad en línea.

1. ¿Qué puede ayudar a prevenir los ataques de abrevadero?

a) Hacer clic en todos los enlaces que parezcan seguros.

b) Descargar archivos adjuntos sin verificar su origen.

c) Compartir contraseñas con amigos.

d) Contar con un software antivirus actualizado.

1. ¿Qué es un ataque de día cero?

a) Un ataque que solo ocurre durante el día.

b) Un ataque que solo afecta a los dispositivos móviles.

c) Un ciberataque que explota vulnerabilidades de seguridad desconocidas para las cuales no hay parche disponible.

d) Un ataque que se produce todos los días a la misma hora.

1. ¿Por qué se llaman "día cero" las vulnerabilidades explotadas en un ataque de día cero?

a) Porque solo afectan a los sistemas operativos lanzados en un día específico.

b) Porque solo se pueden explotar durante el día.

c) Porque ocurren en el primer día del mes.

d) Porque son descubiertas por los atacantes antes de que los desarrolladores de software sean conscientes de ellas.

1. ¿Qué ventaja tienen los atacantes en un ataque de día cero?

a) No necesitan conocimientos técnicos para llevar a cabo el ataque.

b) Tienen acceso a herramientas avanzadas de hacking.

c) Pueden aprovechar la vulnerabilidad antes de que se desarrolle un parche de seguridad.

d) Pueden predecir cuándo ocurrirá el ataque.

1. ¿Qué hace un hacker en un ataque de día cero?

a) Revela públicamente las vulnerabilidades de seguridad.

b) Reporta las vulnerabilidades a los desarrolladores de software.

c) Desarrolla un malware que explota una vulnerabilidad recién descubierta.

d) Espera a que los desarrolladores de software creen un parche de seguridad.

1. ¿Cómo pueden los usuarios protegerse contra un ataque de día cero?

a) Ignorando cualquier actualización de seguridad que aparezca en su dispositivo.

b) Manteniendo sus sistemas actualizados con los últimos parches de seguridad.

c) Compartiendo sus contraseñas con amigos cercanos.

d) Descargando software de fuentes no confiables.

1. ¿Cuál es un ejemplo de un ataque de día cero?

a) Cuando un hacker desarrolla un malware que explota una vulnerabilidad en un sistema operativo popular.

b) Cuando un hacker informa a los desarrolladores de software sobre una vulnerabilidad recién descubierta.

c) Cuando un usuario instala una actualización de seguridad en su dispositivo.

d) Cuando un dispositivo es infectado por malware después de aplicar un parche de seguridad.

1. ¿Qué tipo de sitios pueden ser utilizados para distribuir exploits en un ataque de día cero?

a) Foros en línea donde se discuten temas de seguridad.

b) Redes sociales populares como Facebook o Instagram.

c) Sitios web comprometidos o correos electrónicos de phishing.

d) Sitios web oficiales de empresas reconocidas.

1. ¿Qué pueden hacer los usuarios para protegerse contra un ataque de día cero?

a) Compartir contraseñas con amigos cercanos.

b) Mantener sus sistemas y aplicaciones actualizados con los últimos parches de seguridad.

c) Descargar software de fuentes no confiables.

d) Ignorar cualquier advertencia de actualización en sus dispositivos.