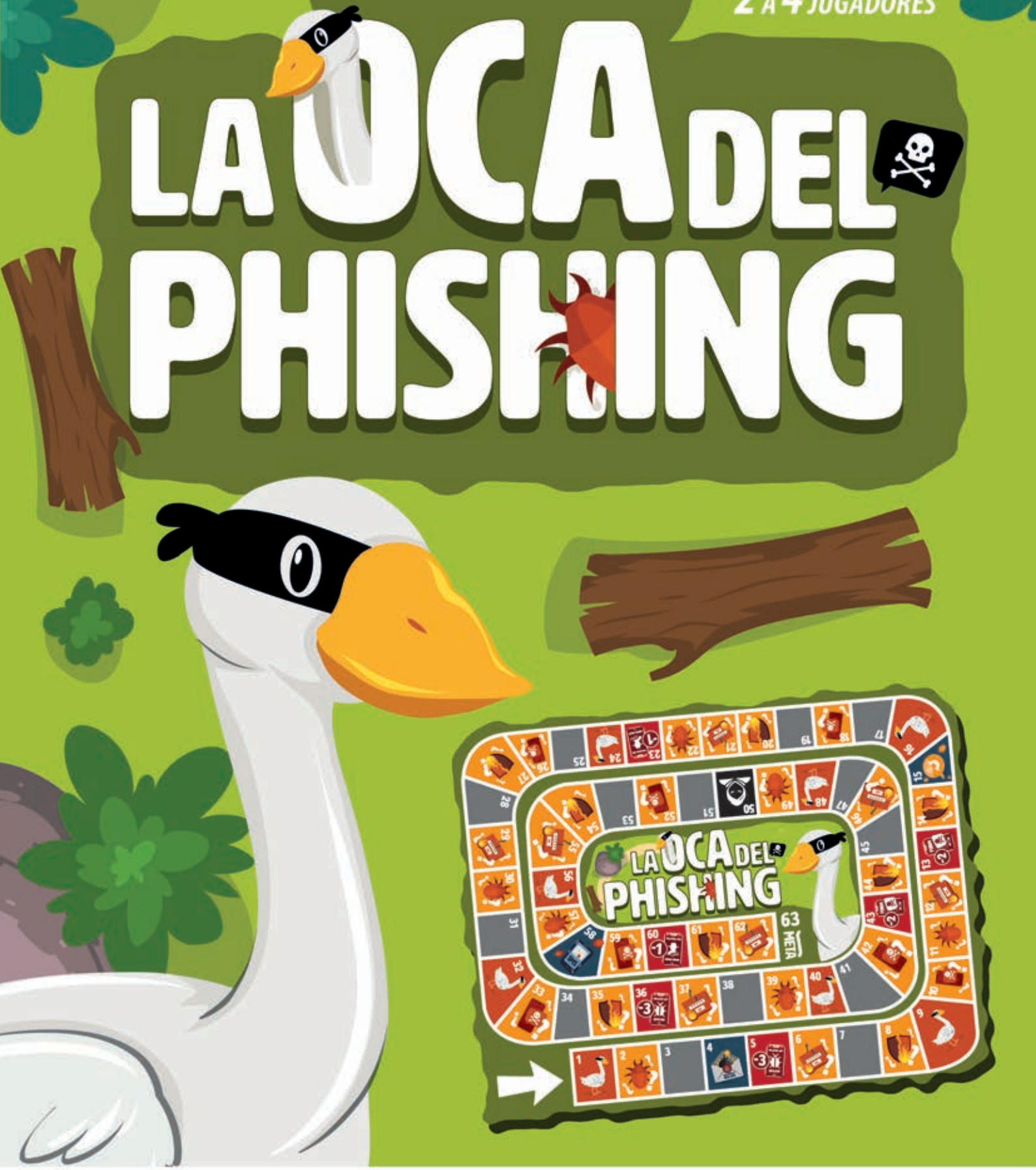
OSI Oficina de Seguridad del Internauta

ES UN JUEGO DE 2 A 4 JUGADORES

LA OCA DEL PHISHING



Financiado por la Unión Europea NextGenerationEU

Plan de Recuperación, Transformación y Resiliencia

España | digital 2026

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

017

INTRODUCCIÓN AL JUEGO

Todo/as recibimos correos, llamadas y SMS en el día a día, y no siempre es fácil detectar cuáles son fraudulentos y cuáles no, ¿o sí? **Juega a la 'Oca del Phishing', pon a prueba tus conocimientos sobre los fraudes de tipo *phishing, smishing y vishing*** e intenta llegar el primero a la meta sin caer en las trampas de los ciberdelincuentes.

¡Suerte!

CÓMO SE JUEGA

Primero, deberás descargarte e imprimir las instrucciones del juego, el dado, las fichas y el tablero.

Los jugadores situarán su ficha en la casilla de inicio del tablero. Cada jugador lanzará el dado y el que obtenga el valor más alto, comienza el juego.

El orden de los jugadores será en el sentido de las agujas del reloj.

El juego consistirá en lanzar el dado y avanzar tantas casillas como números refleje hasta detenerse en la casilla correspondiente. El objetivo del juego es llegar el/la primero/a a la meta del juego.

A medida que se avance por el tablero, los jugadores podrán caer en las siguientes casillas:

Casillas de "Oca"

Avanzas de Oca en Oca y vuelves a tirar. ("Y tiro porque me toca").

"Mensaje fraudulento"

Tendrás que responder 3 preguntas y únicamente perderás el número de turnos de las respuestas falladas.

Casillas vacías

No se hacen preguntas y pasas turno.

Casilla -1

Retrocedes una casilla.

Casilla -2

Retrocedes dos casillas.

Casilla -3

Retrocedes tres casillas.

Ciber Delincuente

Vuelves a la casilla de inicio.

ES UN JUEGO DE 2 A 4 JUGADORES

CONTENIDO DEL JUEGO

1 Tablero

El juego se desarrollará sobre un tablero, el cual contiene una serie de casillas alrededor. Cada casilla es de un color representando a cada categoría.

- 4 fichas de jugador.
- 1 dado recortable.
- 50 cartas de preguntas y respuestas.
- 1 tablero con 63 celdas:
  - 15 celdas vacías
  - 30 celdas de pregunta
  - 3 celdas de "Mensaje fraudulento"
  - 1 casilla de "Ciberdelincuente"
  - 8 casillas de "Oca"
  - 2 casillas de -3
  - 2 casillas de-2
  - 2 casillas de -1

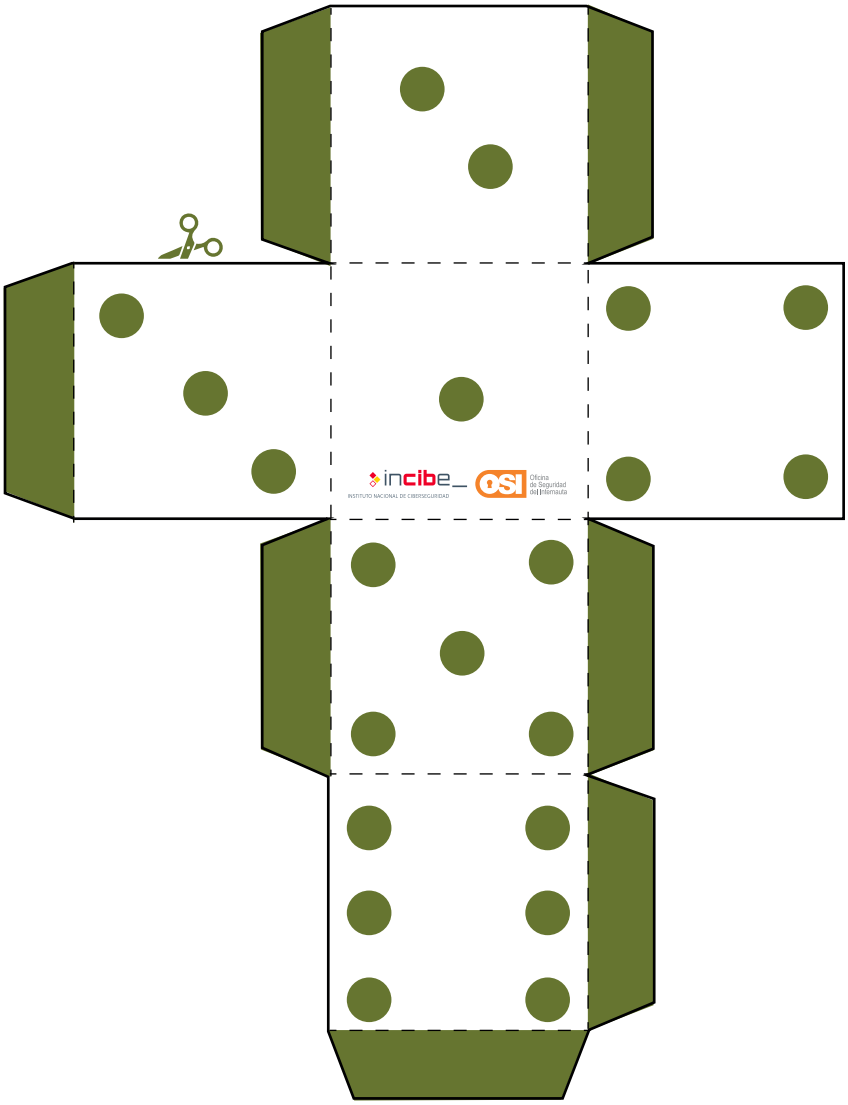
Cada tarjeta facilita la respuesta correcta a la pregunta con una breve explicación.

MONTAJE DADO

SIGUE EL PASO A PASO DEL MONTAJE Y PLEGADO DEL DADO

Si no tienes ningún dado a mano, no te preocupes, puedes utilizar este dado recortable que hemos creado para la ocasión.

Sigue las instrucciones para montar tu dado.



LA OCA DEL PHISHING

OSI Oficina de Seguridad del Internauta

INSTRUCCIONES MONTAJE

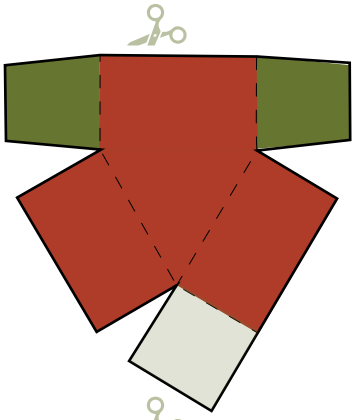
Para montar los elementos necesitaremos:

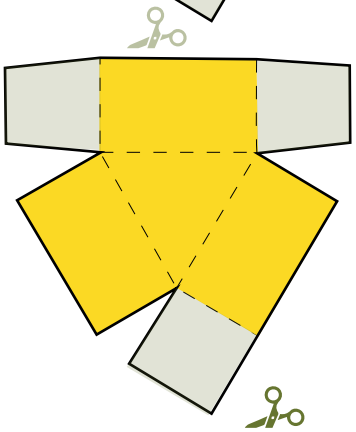
1- Tijeras de punta fina o cúter
2- Pegamento

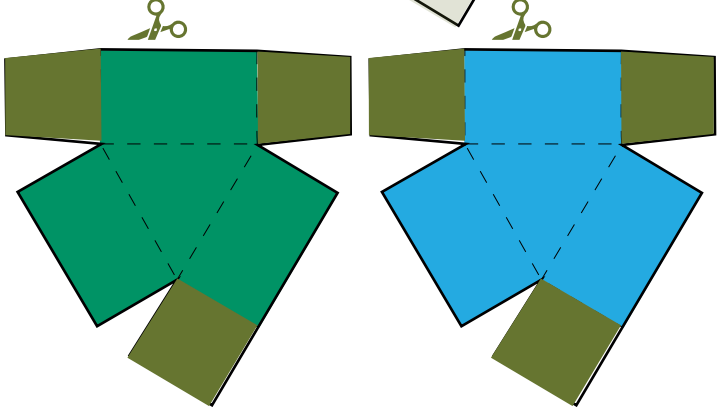
LA LÍNEA CONTINUA _____
Serán aquellas zonas que deban cortarse.

LA LÍNEA DISCONTINUA - - - - -
Serán aquellas zonas que solo tengas que plegar.

PEGAMENTO
Las zonas coloreadas en verde lima, es donde tendrás que untar pegamento, te servirá para unir los lados.







MONTAJE FICHAS

SIGUE EL PASO A PASO DEL MONTAJE Y PLEGADO DE LAS FICHAS

Tienes 2 opciones para crear tu ficha, recortar y montarla en 3D siguiendo los pasos para recortar, pegar y plegar los lados, o si prefieres puedes recortar el triángulo central y usar la ficha plana triangular.

Sigue las instrucciones para montar tus fichas.


incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD
017
LA OCA DEL PHISHING
63 META
OSI
Oficina de Seguridad del Internauta

LA OCA DEL PHISHING

OSI Oficina de Seguridad del Internauta

1 *¿Para qué quieren tus datos los ciberdelincuentes?*

- ***A) Ganar dinero a tu costa, ya sea por robo directo de tu cuenta, extorsión, etc.***
- *B) Para enviarte regalos.*
- *C) Para decirte si tus datos son erróneos.*

Respuesta: *A. Ganar dinero a tu costa, ya sea por robo directo de tu cuenta, extorsión,etc.*

LA OCA DEL PHISHING

OSI Oficina de Seguridad del Internauta

2 *¿Qué datos suelen solicitar a través del phishing?*

- ***A) DNI, datos bancarios y credenciales.***
- *B) Gustos sobre películas y libros.*
- *C) Talla de pie y ropa.*

Respuesta: *A. DNI, datos bancarios y credenciales.*

LA OCA DEL PHISHING

OSI Oficina de Seguridad del Internauta

3 *¿A través de qué medio se comete el phishing?*

- *A) SMS.*
- ***B) Correo electrónico.***
- *C) Redes sociales.*

Respuesta: *B. Correo electrónico.*

LA OCA DEL PHISHING

OSI Oficina de Seguridad del Internauta

4 *¿A través de qué medio se comete el smishing?*

- *A) Correo electrónico.*
- *B) Redes sociales.*
- ***C) SMS.***

Respuesta: *C. SMS.*

LA OCA DEL PHISHING OSI Oficina de Seguridad del Internauta

5 *¿A través de qué medio se comete el vishing?*

- *A) SMS.*
- ***B) Llamada telefónica.***
- *C) Redes sociales.*

Respuesta: *B. Llamada telefónica.*

LA OCA DEL PHISHING OSI Oficina de Seguridad del Internauta

6 *¿Qué datos no se deben dar por teléfono, correo o SMS?*

- *A) Nombre y apellidos, DNI, dirección o datos bancarios.*
- *B) DNI, dirección y datos bancarios.*
- ***C) Todas las anteriores son correctas.***

Respuesta: *C. Todas las anteriores son correctas.*

LA OCA DEL PHISHING OSI Oficina de Seguridad del Internauta

7 *¿Qué 3 características tienen los SMS o correos fraudulentos?*

- ***A) Faltas ortográficas o gramaticales, enlaces no oficiales y remitente desconocido.***
- *B) Procedencia de entidades bancarias, confirmación o códigos de autenticación.*
- *C) Ofertas, publicidad y enlaces a páginas webs.*

Respuesta: *A. Faltas ortográficas o gramaticales, enlace no oficial y remitente desconocido.*

LA OCA DEL PHISHING OSI Oficina de Seguridad del Internauta

8 *¿Cuál podría ser un mensaje sospechoso?*

- *A) Confirmamos su cita telefónica para el día 23/09/2022. Recibirá la llamada entre las 8:00 y 10:00h.*
- ***B) Detectado un acceso no autorizado a tu cuenta, entra en este enlace y bloquéalo. (URL).***
- *C) El pago con tu tarjeta ha sido denegado debido a que el uso de su tarjeta está desactivado. Entre en el menú de tarjetas en su aplicación.*

Respuesta: *B. Detectado un acceso no autorizado a tu cuenta, entra en este enlace y bloquéalo. (URL.)*

LA OCA DEL PHISHING OSI

9 *¿Qué medidas de seguridad debemos tener en cuenta antes de abrir un enlace?*

- *A) Revisar que comience por http.*
- ***B) Que la URL coincida con el dominio legítimo de la empresa.***
- *C) Que sea un enlace acortado.*

Respuesta: *B. Que la URL coincida con el dominio legítimo de la empresa.*

LA OCA DEL PHISHING OSI

10 *¿Cómo puedo protegerme del phishing?*

- ***A) No des tus datos a la ligera y comprueba que la web contiene https y el candado.***
- *B) No hagas clic en enlaces conocidos y descarga de páginas oficiales.*
- *C) Comprueba si el remitente del correo acaba en .com*

Respuesta: *A. No des tus datos a la ligera y comprueba que la web contiene https y el candado.*

LA OCA DEL PHISHING OSI

11 *¿Cuál de estas características nos dice que podríamos estar ante un correo de phishing?*

- *A) El mensaje habla de una campaña de nuestro banco de manera meramente informativa.*
- ***B) El remitente del correo es un banco diferente al nuestro.***
- *C) El correo te facilita información de nuevas medidas de seguridad de manera informativa.*

Respuesta: *B. El remitente del correo es un banco diferente al nuestro.*

LA OCA DEL PHISHING OSI

12 *¿Cuál de estas tres respuestas es un indicio de vishing?*

- *A) Nos llaman desde una compañía conocida para ofrecernos productos.*
- ***B) Nos solicitan información bancaria por algún motivo.***
- *C) Se dirigen a nosotros por nuestro nombre y apellido.*

Respuesta: *B. Nos solicitan información bancaria por algún motivo.*

LA OCA DEL PHISHING OSI

13 *¿Qué técnica pueden combinar los ciberdelincuentes especializados en vishing para mejorar su labor?*

- *A) Phishing.*
- *B) Smishing.*
- ***C) A y B son correctas.***

Respuesta: *C. A y B son correctas.*

LA OCA DEL PHISHING OSI

14 *¿Qué indicio no es válido para darnos cuenta al instante de que nos están llamando con intención de engañarnos?*

- *A) El teléfono nos avisa de que es spam.*
- *B) Es un número que no nos resulta familiar.*
- ***C) Llaman con un código de país diferente.***

Respuesta: *C. Llaman con un código de país diferente.*

LA OCA DEL PHISHING OSI

15 *¿Qué carpeta nos indica qué correos son potencialmente peligrosos?*

- ***A) Spam.***
- *B) Borradores.*
- *C) Papelera.*

Respuesta: *A. Spam.*

LA OCA DEL PHISHING OSI

16 *¿Cuál de estos indicios nos puede hacer diferenciar el spam del phishing?*

- *A) Información acerca de una promoción.*
- *B) Anuncio de novedades de un portal.*
- ***C) Textos mal redactados y contenidos mal maquetados.***

Respuesta: *C. Textos mal redactados y contenidos mal maquetados.*

LA OCA DEL PHISHING OSI

17 *Si dudamos de un correo informativo de nuestro banco, ¿qué debemos hacer?*

- ***A) Consultar directamente a la entidad a través de otros medios.***
- *B) Acceder al enlace adjunto para comprobar la veracidad.*
- *C) Ignorar las posibles advertencias de spam.*

Respuesta: *A. Consultar directamente a la entidad a través de otros medios.*

LA OCA DEL PHISHING OSI

18 *¿Qué debemos hacer si nos envían un SMS solicitando una llamada urgente a un número adjunto?*

- *A) Llamar al número.*
- ***B) Ignorar y bloquear el SMS.***
- *C) Cualquier de las opciones son correctas.*

Respuesta: *B. Ignorar y bloquear el SMS.*

LA OCA DEL PHISHING OSI

19 *¿Cómo se llaman los ataques de phishing a altos ejecutivos?*

- *A) Vishing.*
- ***B) Whaling.***
- *C) Big-phishing.*

Respuesta: *B. Whaling.*

LA OCA DEL PHISHING OSI

20 *¿Qué pasa si pulsamos sobre un enlace de un correo con indicios de phishing?*

- *A) Estaremos infectados automáticamente.*
- *B) Nos van a robar todo el dinero de nuestro banco.*
- ***C) Si no hemos facilitado información personal ni instalado nada, no tiene por qué pasar nada.***

Respuesta: *C. Si no hemos facilitado información personal ni instalado nada, no tiene por qué pasar nada.*

LA OCA DEL PHISHING OSI Oficina de Seguridad del Internauta

21 *¿Qué deberíamos hacer después de recibir una posible llamada fraudulenta?*

- *A) Colgar e ignorar.*
- ***B) Colgar y bloquear el número.***
- *C) Proporcionar la información necesaria.*

Respuesta: *B. Colgar y bloquear el número.*

LA OCA DEL PHISHING OSI Oficina de Seguridad del Internauta

22 *¿Cuándo deberíamos dar nuestra información bancaria en una llamada?*

- *A) Cuando quien nos llama se identifica como nuestro banco.*
- ***B) Nunca.***
- *C) Cuando ha podido ocurrir un problema con un pedido.*

Respuesta: *B. Nunca.*

LA OCA DEL PHISHING OSI Oficina de Seguridad del Internauta

23 *¿Cuál de estos tres ataques de ingeniería social es el más utilizado por los ciberdelincuentes?*

- ***A) Smishing.***
- *B) Vishing.*
- *C) Phishing.*

Respuesta: *A. Smishing.*

LA OCA DEL PHISHING OSI Oficina de Seguridad del Internauta

24 *¿En qué caso podemos confirmar que un mensaje bancario no es un smishing?*

- *A) Si nos solicita un cambio de contraseña sin motivo aparente.*
- ***B) Si nos proporciona un código tras activar la autenticación en dos pasos.***
- *C) Si nos informan de movimientos inusuales en nuestra cuenta bancaria.*

Respuesta: *B. Si nos proporciona un código tras activar la autenticación en dos pasos.*

LA OCA DEL PHISHING OSI

25 *¿De qué forma podemos saber que un SMS de una compañía de envío no es un smishing?*

- *A) Nos solicita un pago de aduanas sin proporcionarnos nuestro número de pedido.*
- ***B) Nos informa de una actualización del pedido con nuestro número de pedido.***
- *C) Nos invita a descargar una app para el seguimiento del pedido.*

Respuesta: *B. Nos informa de una actualización del pedido con nuestro número de pedido.*

LA OCA DEL PHISHING OSI

26 *¿Debemos pulsar algún enlace dentro de un correo sospechoso?*

- *A) El que tenga mejor aspecto.*
- *B) El que nos permita darnos de baja.*
- ***C) No, cualquiera puede ser peligroso.***

Respuesta: *C. No, cualquiera puede ser peligroso.*

LA OCA DEL PHISHING OSI

27 *Si pulsamos en Gmail el remitente de un correo potencialmente peligroso, ¿qué icono nos indicará que este no está cifrado?*

- A) Un símbolo de bacteria rojo.
- ***B) Un candado rojo.***
- *C) Una señal de advertencia amarilla.*

Respuesta: *B. Un candado rojo.*

LA OCA DEL PHISHING OSI

28 *¿Cuándo un SMS es spam y no smishing?*

- *A) Cuando proporciona un enlace que empieza por http.*
- ***B) Cuando tiene una opción para darte de baja de mensajes fiable.***
- *C) Cuando nos ofrecen un premio de un sorteo.*

Respuesta: *B. Cuando tiene una opción para darte de baja de mensajes fiable.*

LA OCA DEL PHISHING OSI Oficina de Seguridad del Internauta

29 *¿Es fiable la carpeta de spam?*

- *A)Sí, solo es un filtro automático de correos electrónicos.*
- *B) No, nunca.*
- ***C) No, pero nuestro correo a veces puede marcar como spam algo fiable.***

Respuesta: *C. No, pero nuestro correo a veces puede marcar como spam algo fiable.*

LA OCA DEL PHISHING OSI Oficina de Seguridad del Internauta

30 *Si dudamos acerca de un correo de aviso de cambio de contraseña, ¿qué podemos hacer?*

- ***A) Cambiar la contraseña de la cuenta afectada a través de la web oficial.***
- *B) Acceder al enlace adjunto para ver su contenido.*
- *C) Ignorarlo como el resto.*

Respuesta: *A. Cambiar la contraseña de la cuenta afectada a través de la web oficial.*

LA OCA DEL PHISHING OSI Oficina de Seguridad del Internauta

31 *¿Qué tipo de software malicioso no es una posible consecuencia del phishing y sus variantes?*

- ***A) Deathware.***
- *B) Malware.*
- *C) Ransomware.*

Respuesta: *A. Deathware.*

LA OCA DEL PHISHING OSI Oficina de Seguridad del Internauta

32 *¿Cuál debería ser nuestra reacción ante una llamada desde un número desconocido el cual aparentemente es alguien que conocemos gracias a la información que nos proporciona?*

- ***A) Fiarnos.***
- *B) Desconfiar e investigar.*
- *C) Colgar y bloquear.*

Respuesta: *B. Desconfiar e investigar.*

LA OCA DEL PHISHING OSI Oficina de Seguridad del Internauta

33 *En un ataque de vishing, ¿quién suele llamar primero?*

- *A) El criminal.*
- *B) La víctima.*
- ***C) Depende de la situación. En ocasiones, las víctimas obtienen el número malicioso por otras vías y es invitado a llamar bajo cualquier pretexto.***

Respuesta: *C. Depende de la situación. En ocasiones, las víctimas obtienen el número malicioso por otras vías y es invitado a llamar bajo cualquier pretexto.*

LA OCA DEL PHISHING OSI Oficina de Seguridad del Internauta

34 *¿Cuál es una manera fiable de evitar llamadas indeseadas?*

- *A) Solo cogiendo el número a numeros agregados.*
- ***B) Apuntándonos en la Lista Robinson.***
- *C) Solo cogiendo números provenientes de España.*

Respuesta: *B. Apuntándonos en la Lista Robinson.*

LA OCA DEL PHISHING OSI Oficina de Seguridad del Internauta

35 *¿Cómo se llama la técnica usada para monitorizar las llamadas con un ordenador con el fin de realizar ataques de phishing?*

- ***A) Wardialing.***
- *B) Networking.*
- *C) Fake-forwarding.*

Respuesta: *A. Wardialing.*

LA OCA DEL PHISHING OSI Oficina de Seguridad del Internauta

36 *¿Qué debes hacer si desconfías de un correo que te envió un amigo/a?*

- *A) Responder al correo directamente para preguntarle.*
- ***B) Contactar con él o ella por otra vía para confirmar el correo.***
- *C) Borrar el correo directamente.*

Respuesta: *B. Contactar con él o ella por otra vía para confirmar el correo.*

LA OCA DEL PHISHING OSI

37 *¿Cuál no es un método para obtener información a través de un smishing?*

- *A) Envío de enlace de descarga de programa malicioso o malware camuflado como app.*
- ***B) Envío de imágenes de ciberdelincuentes a través del SMS.***
- *C) Envío de enlace redirigiendo a web fraudulenta rellenando un formulario.*

Respuesta: *B. Envío de imágenes de ciberdelincuentes a través del SMS.*

LA OCA DEL PHISHING OSI

38 *¿Cuál de estas características no están presentes en un mensaje de phishing?*

- *A) Urgencia.*
- *B) Exclusividad.*
- ***C) Tranquilidad.***

Respuesta: *C. Tranquilidad.*

LA OCA DEL PHISHING OSI

39 *¿Que debemos hacer si hemos sido víctimas de un phishing y hemos facilitado la tarjeta?*

- *A) Utilizar otra tarjeta que tengamos.*
- ***B) Contactar con tu entidad bancaria y dar de baja la tarjeta.***
- *C) Desinstalar del móvil la aplicación del banco.*

Respuesta: *B. Contactar con tu entidad bancaria y dar de baja la tarjeta.*

LA OCA DEL PHISHING OSI

40 *¿Cuál no es una técnica de smishing?*

- *A) Hacer que el usuario llame a un número de tarificación especial.*
- *B) Hacer que el usuario se suscriba a un servicio SMS premium.*
- ***C) Hacer que el usuario entre en la app móvil de su entidad bancaria.***

Respuesta: *C. Hacer que el usuario entre en la app móvil de su entidad bancaria.*

LA OCA DEL PHISHING OSI

41 *¿Qué tipo de empresas o entidades pueden ser suplantadas a través de SMS?*

- *A) Bancos.*
- *B) Empresa de servicios de mensajería o reparto.*
- ***C) De todo tipo.***

Respuesta: *C. De todo tipo.*

LA OCA DEL PHISHING OSI

42 *¿Cómo se llama la técnica de manipulación detrás de los ataques de phishing y sus variantes?*

- *A) Stalking.*
- *B) Ciber-extorsión.*
- ***C) Ingeniería social.***

Respuesta: *C. Ingeniería social.*

LA OCA DEL PHISHING OSI

43 *¿Cuál es la principal razón por la cual el smishing es más efectivo que el phishing?*

- ***A) Una mayor confianza en SMS que en correos electrónicos.***
- *B) Un mensaje más corto.*
- *C) La dificultd de conocer un número.*

Respuesta: *A. Una mayor confianza en SMS que en correos electrónicos.*

LA OCA DEL PHISHING OSI

44 *¿Cómo se llama un ataque de phishing que tiene información detallada sobre nosotros, como trabajo o dirección?*

- *A) Menace-phishing.*
- ***B) Spear-phishing.***
- *C) Close-phishing.*

Respuesta: *B. Spear-phishing.*

LA OCA DEL PHISHING OSI Oficina de Seguridad del Internauta

45 *¿Cuál es la mejor forma de defenderse del phishing?*

- *A) Filtros antispam.*
- *B) Restringir correos.*
- ***C) Educación en phishing.***

Respuesta: *C. Educación en phishing.*

LA OCA DEL PHISHING OSI Oficina de Seguridad del Internauta

46 *¿Qué técnicas son efectivas para materializar ataques de vishing?*

- *A) Amenazas telefónicas.*
- *B) Facilitar teléfonos de tarificación especial en SMS.*
- ***C) Suplantar el servicio técnico de alguna empresa para resolver supuestos problemas de seguridad.***

Respuesta: *C. Suplantar el servicio técnico de alguna empresa para resolver supuestos problemas de seguridad.*

LA OCA DEL PHISHING OSI Oficina de Seguridad del Internauta

47 *¿Qué mensaje no es sospechoso en un SMS?*

- *A) Problemas de carácter técnico o de seguridad de la cuenta del usuario.*
- *B) Vales descuento, premios o regalos.*
- ***C) Avisarte de la fecha y hora de la próxima cita médica.***

Respuesta: *C. Avisarte de la fecha y hora de la próxima cita médica.*

LA OCA DEL PHISHING OSI Oficina de Seguridad del Internauta

48 *¿Cuál es el fraude más común?*

- ***A) Phishing y smishing.***
- *B) Smishing y vishing.*
- *C) Vishing y phishing.*

Respuesta: *A. Phishing y smishing.*

LA OCA DEL PHISHING OSI Oficina de Seguridad del Internauta

49 *¿De qué otras formas te puede afectar el vishing, además de recopilar tu información?*

- *A) Tomar el control de tu teléfono.*
- ***B) Grabar la conversación para extorsionarte posteriormente.***
- *C) Acceder a tus cuentas de usuario.*

Respuesta: *B. Grabar la conversación para extorsionarte posteriormente.*

LA OCA DEL PHISHING OSI Oficina de Seguridad del Internauta

50 *¿Cuál es una buena práctica para defendernos contra el vishing si vemos un número sospechoso?*

- ***A) Buscarlo en internet.***
- *B) Cogerlo y no responder.*
- *C) Entablar conversación.*

Respuesta: *A. Buscarlo en internet.*