Oficina de Seguridad del Internauta

ES UN **JUEGO** de 2 a 4 jugadores

TRIVIAL DE LA CIBERSEGURIDAD

¿Quién será el usuario más concienciado y protegido?

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA TERCERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

017 TU AYUDA EN CIBERSEGURIDAD

TRIVIAL OSI DE LA CIBERSEGURIDAD

Oficina de Seguridad del Internauta

ES UN **JUEGO** de 2 a 4 jugadores

INTRODUCCIÓN AL JUEGO

Si has llegado hasta aquí, es porque has recorrido un largo camino de experiencias positivas por Internet, pero también lleno de obstáculos y amenazas que has tenido que superar. ***Navegar por la red no está exento de riesgos***, pero has demostrado que eres un usuario concienciado y que no tienes nada que temer.

Es el momento de ponerte a prueba y medir tus conocimientos en ciberseguridad con tus amigos. ***¿Quién será el usuario más concienciado y protegido?***

¡Mucha suerte!

CÓMO SE JUEGA

Los jugadores comenzarán colocando sus fichas de jugador o Ciberfichas en el centro del tablero. El jugador que haya sacado ***la tirada más alta será el primero en jugar***. Deberá lanzar el dado y moverse tantas casillas como indique el número que haya salido. ***No existe una dirección de casillas establecida, y podrá elegir el camino a seguir.***

Al finalizar su movimiento, su ficha habrá quedado en una casilla con un color y una categoría determinada. Otro jugador, el que esté sentado a su derecha, deberá coger una tarjeta correspondiente a esa categoría y plantear la pregunta que haya en ella:

✓ ***Si el jugador la acierta, volverá a tirar el dado y repetir su turno. Podrá hacerlo tantas veces como preguntas acierte.***

✗ ***Si el jugador falla, el turno pasará al jugador siguiente.***

Las casillas especiales ofrecen la oportunidad de obtener un Ciberpunto si el jugador acierta la pregunta. Una vez obtenido, pasará a ser una casilla normal para ese jugador.

¿Cómo se gana en el juego?

El jugador que ***consiga obtener los seis Ciberpuntos*** antes que el resto de los jugadores, ***será el ganador del juego.***

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.*** 6 de estas casillas estarán resaltadas y corresponderán a preguntas con opción a Ciberpunto si el jugador responde correctamente.

60 Tarjetas con preguntas

sobre:

- ***Redes sociales y mensajería instantánea***
- ***Gestión de contraseñas***
- ***Compras online***
- ***Fraudes online***
- ***Navegación segura***
- ***Protección de dispositivos***

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

24 Ciberpuntos

(4 tarjetas por cada categoría)

Se proporcionarán al usuario que ***conteste correctamente a una pregunta en la casilla de Ciberpuntos*** de una categoría.

4 Ciberfichas

Fichas que los ***jugadores utilizarán para desplazarse por el tablero.***

TRIVIAL OSI DE LA CIBERSEGURIDAD

Oficina de Seguridad del Internauta

PREPARACIÓN

Imprime los materiales del juego, recórtalos y pégalos si es necesario. Además, necesitaras un dado de 6 caras para jugar.

Antes de comenzar a jugar, ***utiliza el dado para elegir al primer jugador de la partida que será el que obtenga el resultado más alto***, el jugador de tu derecha será el segundo, y así sucesivamente.

Aprovecha para ***barajar todas las cartas y colócalas en seis montones, uno por cada categoría.*** Luego, cada jugador deberá elegir la Ciberficha que va a utilizar durante la partida.

Una vez ***definido el orden de juego de los jugadores y habiendo escogido vuestra "Ciberficha", estaréis listos para jugar.***

MONTAJE DE LAS CARTAS

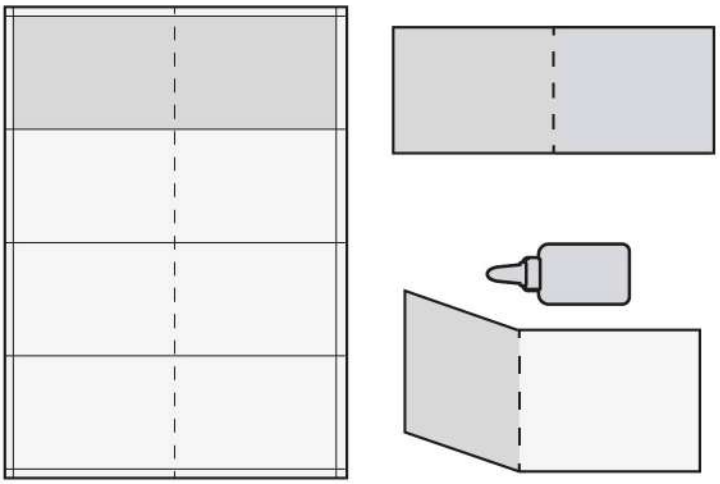
DOBLA LAS CARTAS Y USA PEGAMENTO

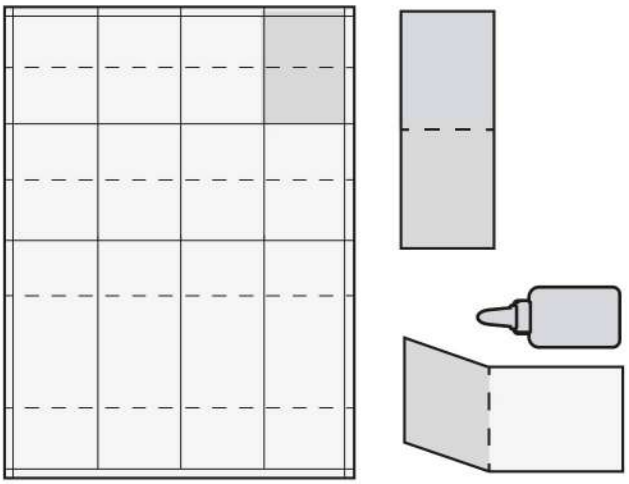
Para montar las cartas necesitaremos:
1-Tijeras o cúter.
2-Pegamento.

LA LÍNEA CONTINUA
Sigue la línea continua para cortar las cartas.

LA LÍNEA DISCONTINUA
Es por donde plegarás las cartas para unir ambas partes.

PEGAMENTO
El pegamento se usará en el lado contrario de la cartas, se pegará como si fuera un libro.





TRIVIAL OSI Oficina de Seguridad del Internauta

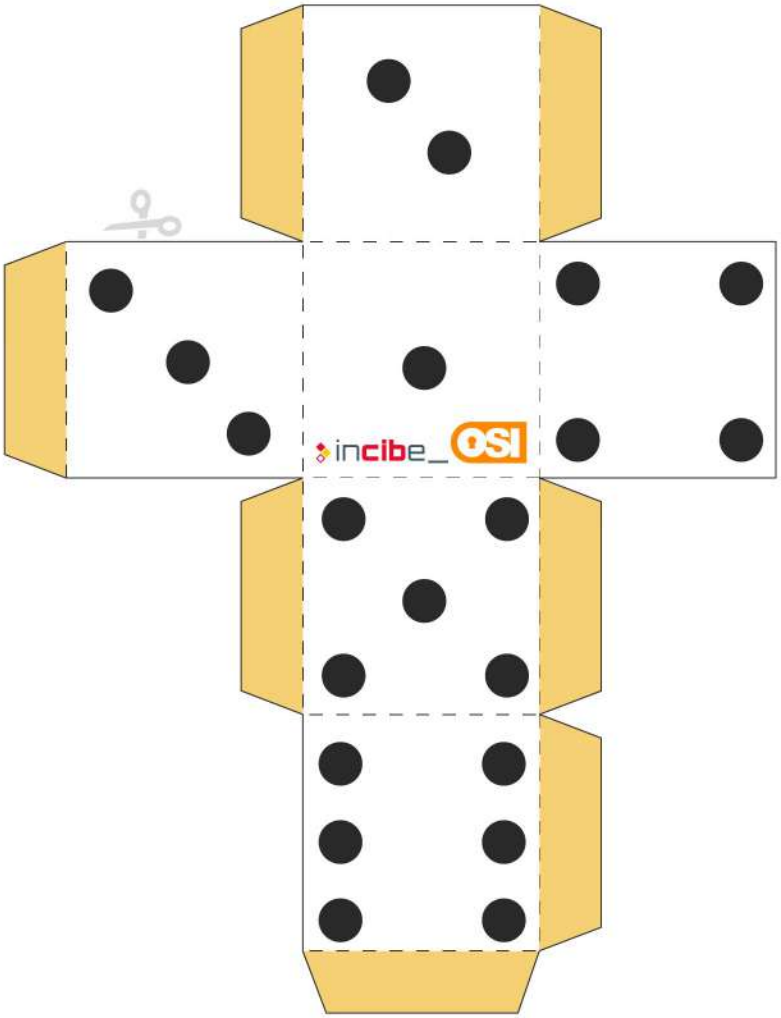
DE LA CIBERSEGURIDAD

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.



INSTRUCCIONES MONTAJE

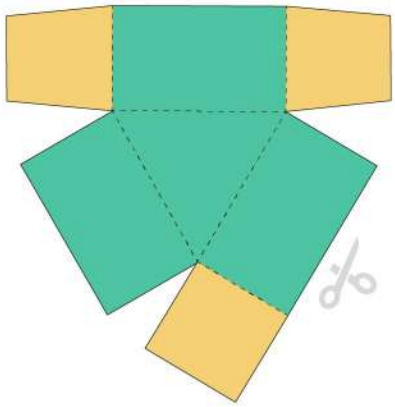
Para montar los elementos necesitaremos:
1-Tijeras de punta fina o cúter.
2-Pegamento.

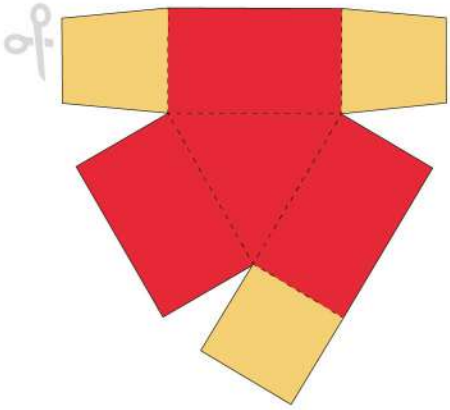
LA LÍNEA CONTINUA
Serán aquellas zonas que deban cortarse.

LA LÍNEA DISCONTINUA
Serán las zonas que solo tengas que plegar.

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

*Cuanto más gramaje tenga el papel más consistencia tendrán tus elementos.



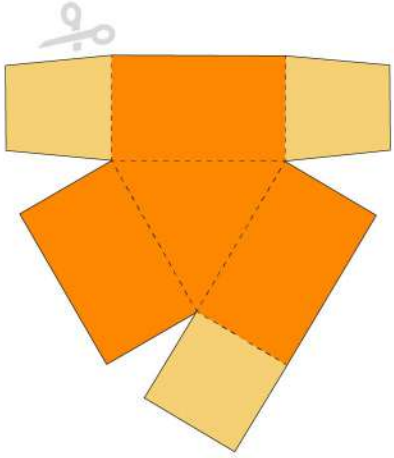


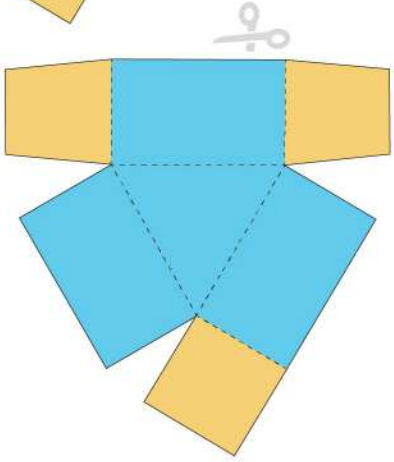
MONTAJE CIBERFICHAS

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

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

Sigue las instrucciones de la parte superior para crear tus fichas en 3D.





MONTAJE TABLERO 1 DE 2

SIGUE EL PASO A PASO DEL MONTAJE Y PLEGADO DEL TABLERO

Para montar el tablero donde se desarrollará el juego deberás imprimir éste y el siguiente folio, recortar y unirlos con pegamento.

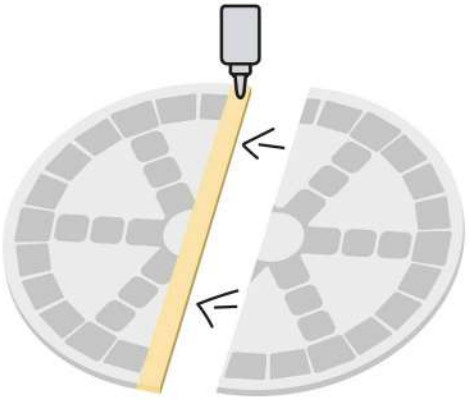
Para montar el tablero necesitaremos:
1-Tijeras de punta fina o cúter.
2-Pegamento.

LA LÍNEA CONTINUA

Sigue la línea continua para recortar el tablero.

PEGAMENTO

La zona coloreada en amarillo, es donde tendrás que untar pegamento para unir ambas mitades del tablero.



*Cuanto más gramaje tenga el papel más consistencia tendrá tu tablero.

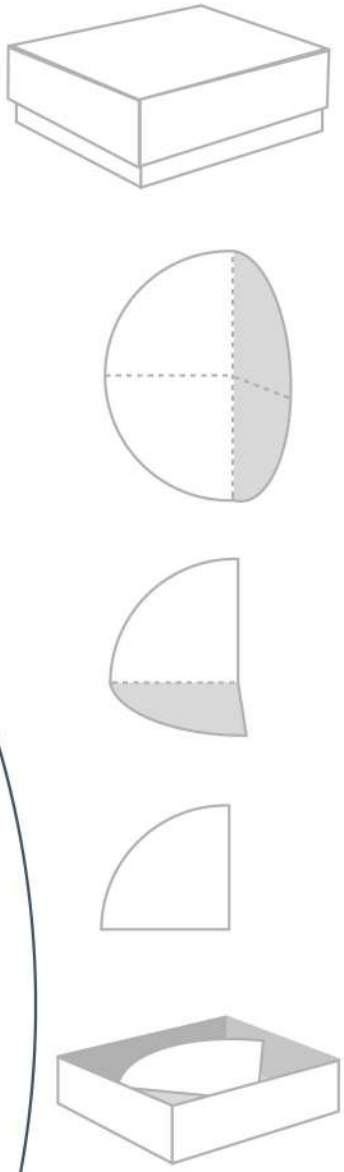
MONTAJE TABLERO 2 DE 2

SIGUE EL PASO A PASO DEL MONTAJE Y PLEGADO DEL TABLERO

Una vez montado el tablero, para colocarlo en la caja deberás plegarlo por ambas mitades, dejando el tablero plegado tal y como viene en las imágenes.

TRIVIAL DE LA CIBERSEGURIDAD

Oficina de Seguridad del Internauta



*Cuanto más gramaje tenga el papel más consistencia tendrá tu tablero.

MONTAJE DE LA CAJA 1 DE 2

SIGUE EL PASO A PASO DEL MONTAJE Y PLEGADO

TRIVIAL OSI Oficina de Seguridad del Internauta
DE LA CIBERSEGURIDAD

Para montar la base de la caja que contendrá nuestro juego necesitaremos:
1-Tijeras de punta fina o cúter.
2-Pegamento.

LA LÍNEA CONTINUA
Serán aquellas zonas que deban cortarse.

LA LÍNEA DISCONTINUA
Serán las zonas que solo tengas que plegar.

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

MONTAJE DE LA CAJA 2 DE 2

SIGUE EL PASO A PASO DEL MONTAJE Y PLEGADO

TRIVIAL DE LA CIBERSEGURIDAD

OSI Oficina de Seguridad del Internauta

Para montar la tapa de la caja que contendrá nuestro juego necesitaremos:
1-Tijeras de punta fina o cúter.
2-Pegamento.

LA LÍNEA CONTINUA ✂———

Serán aquellas zonas que deban cortarse.

LA LÍNEA DISCONTINUA - - - - - -

Serán las zonas que solo tengas que plegar.

PEGAMENTO

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

*Cuanto más gramaje tenga el papel más consistencia tendrá tu caja.

¿Quién será el usuario más concienciado y protegido?

OSI Oficina de Seguridad del Internauta

TRIVIAL DE LA CIBERSEGURIDAD

OSI Oficina de Seguridad del Internauta

TU AYUDA EN CIBERSEGURIDAD 017

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

ES UN JUEGO de 2 a 4 jugadores

Gestión de contraseñas

TRIVIAL OSI DE LA CIBERSEGURIDAD

¿Qué se considera una contraseña robusta?

- A| Aquella con más de 5 caracteres.
- ***B| Aquella que tiene números, mayúsculas, minúsculas y caracteres especiales.***
- C| Cualquiera, lo importante es poder recordarla.

Respuesta: Una contraseña robusta será aquella que contenga una combinación de letras, números, mayúsculas, minúsculas y caracteres especiales.

Gestión de contraseñas

TRIVIAL OSI DE LA CIBERSEGURIDAD

¿Qué debes hacer si recibes un correo que dice que tu cuenta ha podido ser vulnerada y te pide renovar la contraseña a través de un enlace?

- A| Hago clic en el enlace y la cambio.
- B| Respondo al correo con mis credenciales preguntando si mi cuenta ha sido afectada.
- ***C| No hago clic en el enlace y voy a mi navegador favorito.***

Respuesta: Para evitar ser víctimas de un fraude de tipo *phishing* (suplantación de identidad de un servicio), lo más seguro es no hacer clic y teclear directamente la URL legítima del servicio desde el navegador.

Gestión de contraseñas

TRIVIAL OSI DE LA CIBERSEGURIDAD

¿Cada cuánto tiempo es recomendable cambiar tus contraseñas?

- ***A| Entre 3 y 6 meses.***
- B| Entre 3 y 6 meses solo las del banco y correo.
- C| No es necesario, a no ser que hayan sido vulneradas.

Respuesta: Aunque depende de la criticidad de la cuenta, lo recomendable es hacer un cambio de contraseñas cada 3-6 meses.

Gestión de contraseñas

TRIVIAL OSI DE LA CIBERSEGURIDAD

¿Tiene riesgos utilizar siempre la misma contraseña?

- A| No, los ciberdelincuentes no centran sus ataques en las contraseñas.
- ***B| Sí, si se compromete una, el resto de las cuentas pueden ser hackeadas.***
- C| No, así no se me olvida.

Respuesta: Utilizar una misma contraseña para varias cuentas es muy peligroso. Una vez que una cuenta sea vulnerada, el resto podrían estar en peligro por efecto dominó.

Gestión de contraseñas

TRIVIAL DE LA CIBERSEGURIDAD

OSI Oficina de Seguridad del Internauta

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

017 TU AYUDA EN CIBERSEGURIDAD

TRIVIAL OSI Oficina de Seguridad del Internauta DE LA CIBERSEGURIDAD

¿Qué puede suceder si tienes una contraseña sencilla?

- A| Nada, así es más fácil recordarla.
- B| Nada crítico porque tengo antivirus instalado y, además, si alguien la adivina, no tengo nada que esconder.
- ***C| De todo. Es como dejar una puerta abierta para que roben todos tus datos.***

Respuesta: Una contraseña simple y fácil no supone un reto para los ciberdelincuentes. Utilizando determinados *software*, podrían descifrarla en cuestión de segundos.

Gestión de contraseñas

TRIVIAL DE LA CIBERSEGURIDAD

OSI Oficina de Seguridad del Internauta

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

017 TU AYUDA EN CIBERSEGURIDAD

TRIVIAL OSI Oficina de Seguridad del Internauta DE LA CIBERSEGURIDAD

¿Cuál de las siguientes contraseñas consideras que es más segura?

- A| 10002943
- ***B| R3p0ster1A!***
- C| 123QWEasd

Respuesta: La contraseña es robusta, al incluir mayúsculas, minúsculas, números y caracteres especiales.

Gestión de contraseñas

TRIVIAL DE LA CIBERSEGURIDAD

OSI Oficina de Seguridad del Internauta

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

017 TU AYUDA EN CIBERSEGURIDAD

TRIVIAL OSI Oficina de Seguridad del Internauta DE LA CIBERSEGURIDAD

Lo mejor para gestionar correctamente tus contraseñas es:

- A| Apuntarlas todas en una libreta y guardarla a buen recaudo.
- B| Utilizar una o dos contraseñas para todos nuestros servicios.
- ***C| Utilizar un gestor de contraseñas.***

Respuesta: Un gestor de contraseñas nos facilitará mucho el trabajo a la hora de crear contraseñas robustas, actualizarlas cada cierto tiempo y gestionar una gran cantidad de cuentas.

Gestión de contraseñas

TRIVIAL DE LA CIBERSEGURIDAD

OSI Oficina de Seguridad del Internauta

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

017 TU AYUDA EN CIBERSEGURIDAD

TRIVIAL OSI Oficina de Seguridad del Internauta DE LA CIBERSEGURIDAD

El ciberataque que realiza combinaciones de letras para averiguar nuestras contraseñas se conoce como:

- ***A| Ataque por fuerza bruta.***
- B| *Spidering*.
- C| *Passwording*.

Respuesta: Los ataques por fuerza bruta permiten a los ciberdelincuentes obtener nuestras contraseñas a base de realizar cientos de combinaciones de letras y números con alguna máquina diseñada para tal fin.

Gestión de contraseñas

TRIVIAL DE LA CIBERSEGURIDAD

OSI Oficina de Seguridad del Internauta

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

017 TU AYUDA EN CIBERSEGURIDAD

TRIVIAL OSI DE LA CIBERSEGURIDAD

Si para acceder a tus cuentas, además de la contraseña necesitas introducir otro dato, como un código recibido a través de un SMS, hablamos de:

- A| *Tokening.*
- ***B| Verificación en dos pasos.***
- C| *Multipassword.*

Respuesta: Una capa extra para la seguridad de nuestras credenciales es la verificación en dos pasos. En este proceso, se requiere la utilización de otro elemento además de nuestra contraseña para validar el acceso a un servicio.

Gestión de contraseñas

TRIVIAL DE LA CIBERSEGURIDAD

OSI Oficina de Seguridad del Internauta

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

017 TU AYUDA EN CIBERSEGURIDAD

TRIVIAL OSI DE LA CIBERSEGURIDAD

De las siguientes opciones, ¿cuál es la mejor para comenzar a crear una contraseña segura?

- A| Una combinación larga de números.
- ***B| Una combinación larga de palabras y números.***
- C| Una combinación de nuestra fecha de cumpleaños.

Respuesta: La mejor opción es recurrir a una frase o combinación larga de palabras y números, a la que ir aplicando otras como es alternar mayúsculas, minúsculas, números y caracteres especiales.

Compras online

TRIVIAL DE LA CIBERSEGURIDAD

OSI Oficina de Seguridad del Internauta

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

017 TU AYUDA EN CIBERSEGURIDAD

TRIVIAL OSI DE LA CIBERSEGURIDAD

Estás cerrando la compra de un artículo a través de una plataforma de compraventa. El vendedor te pide realizar una transferencia a un banco extranjero. ¿Es una transacción segura?

- A| Sí, las transferencias son el método de pago más seguro.
- B| Sí, siempre y cuando que el vendedor me envíe pruebas de estar en posesión del artículo por WhatsApp.
- ***C| No, si hubiese algún problema sería difícil recuperar mi dinero.***

Respuesta: El principal problema de realizar una transferencia a un banco extranjero es que, en caso de resultar ser víctima de un fraude y querer recuperar nuestro dinero, sería complicado.

Compras online

TRIVIAL DE LA CIBERSEGURIDAD

OSI Oficina de Seguridad del Internauta

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

017 TU AYUDA EN CIBERSEGURIDAD

TRIVIAL OSI DE LA CIBERSEGURIDAD

¿Qué aspectos comprobarías de un sitio web para saber si es fiable?

- ***A| Condiciones de devolución y reembolso.***
- B| Cantidad de ofertas y promociones.
- C| Número de visitas.

Respuesta: Si la tienda online carece de un apartado para las condiciones de devolución y reembolso, es sin duda una tienda online fraudulenta.

Compras online

TRIVIAL DE LA CIBERSEGURIDAD

OSI Oficina de Seguridad del Internauta

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

017 TU AYUDA EN CIBERSEGURIDAD

TRIVIAL OSI Oficina de Seguridad del Internauta DE LA CIBERSEGURIDAD

¿Cómo podemos asegurarnos de que la tienda online vela por nuestra privacidad y la seguridad de nuestras comunicaciones?

- ***A\| Dispone de un certificado digital y HTTPS.***
- B\| Dispone de un certificado digital y HTTP.
- C\| Tiene muchos comentarios positivos.

Respuesta: El certificado digital y el protocolo HTTPS nos aseguran que todas las comunicaciones que hagamos dentro de la web estarán cifradas.

Compras online

Compras online

TRIVIAL DE LA CIBERSEGURIDAD

OSI Oficina de Seguridad del Internauta

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

017 TU AYUDA EN CIBERSEGURIDAD

TRIVIAL OSI Oficina de Seguridad del Internauta DE LA CIBERSEGURIDAD

Encuentras una oferta en una tienda online pero esta no tiene apartado de términos y condiciones. ¿Confiarías en ella?

- A\| Sí, aunque solo en territorio nacional.
- B\| Sí, si dispone de redes sociales.
- ***C\| No, nunca.***

Respuesta: Si una tienda online carece de un apartado de términos y condiciones, hay que desconfiar.

Compras online

Compras online

TRIVIAL DE LA CIBERSEGURIDAD

OSI Oficina de Seguridad del Internauta

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

017 TU AYUDA EN CIBERSEGURIDAD

TRIVIAL OSI Oficina de Seguridad del Internauta DE LA CIBERSEGURIDAD

Has encontrado una oferta para un producto que andabas buscando. Parece que desde la web ofrecen varias formas de pago, pero en el último paso sólo acepta tarjeta de crédito. ¿Qué harías?

- A\| Utilizar una tarjeta secundaria.
- B\| Contactar con el vendedor.
- ***C\| Descartar la compra.***

Respuesta: En estos casos, lo mejor es descartar la compra. Puede que, utilizando una tarjeta solo para compras online, corramos menos riesgos pero quizás nunca lleguemos a recibir el producto. Ante la más mínima señal de fraude, lo más seguro es descartar la compra.

Compras online

Compras online

TRIVIAL DE LA CIBERSEGURIDAD

OSI Oficina de Seguridad del Internauta

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

017 TU AYUDA EN CIBERSEGURIDAD

TRIVIAL OSI Oficina de Seguridad del Internauta DE LA CIBERSEGURIDAD

¿Cuál de las siguientes recomendaciones nos asegura una compra online segura?

- A\| No comprar en época de rebajas.
- ***B\| Utilizar una tarjeta solo para compras online.***
- C\| Utilizar solo las promociones que nos lleguen por email.

Respuesta: Si utilizamos una tarjeta exclusivamente para nuestras compras online, en caso de sufrir un fraude, no perderemos más que los datos y/o el dinero almacenado en dicha tarjeta.

Compras online

Compras online

TRIVIAL DE LA CIBERSEGURIDAD

OSI Oficina de Seguridad del Internauta

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

017 TU AYUDA EN CIBERSEGURIDAD

TRIVIAL OSI DE LA CIBERSEGURIDAD

Algunas webs de compra online permiten almacenar los datos de tu tarjeta de crédito. ¿Cuándo puedes hacer uso de esta opción?

- A| Solo si tiene HTTPS.
- B| Solo si tiene certificado digital.
- ***C| Nunca.***

Respuesta: Aunque la web nos ofrezca la confianza de que nuestras comunicaciones no van a ser espiadas, no es recomendable almacenar este tipo de datos personales. No sabemos si la seguridad del servicio web puede llegar a ser vulnerada, y nuestros datos filtrados.

Compras online

Compras online

TRIVIAL DE LA CIBERSEGURIDAD

OSI Oficina de Seguridad del Internauta

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

017 TU AYUDA EN CIBERSEGURIDAD

TRIVIAL OSI DE LA CIBERSEGURIDAD

No siempre puedes evaluar la calidad del producto de una tienda online. ¿Cómo podrías identificar la fiabilidad de una tienda online?

- ***A| Calidad de la descripción e imágenes de los productos.***
- B| Variedad de productos ofertados.
- C| Presencia de marcas conocidas.

Respuesta: Las tiendas online fraudulentas suelen incluir descripciones pobres sobre sus productos, o imágenes de mala calidad o incluso robadas de otras webs.

Compras online

Compras online

TRIVIAL DE LA CIBERSEGURIDAD

OSI Oficina de Seguridad del Internauta

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

017 TU AYUDA EN CIBERSEGURIDAD

TRIVIAL OSI DE LA CIBERSEGURIDAD

¿Qué aspectos referentes al precio de un producto deben hacerte sospechar en una tienda online?

- A| Variedad de productos con un precio igual o similar.
- ***B| Precios anormalmente bajos.***
- C| Ambas opciones.

Respuesta: Una tienda online con precios demasiado bajos y productos similares con el mismo precio es candidata a ser un fraude.

Compras online

Compras online

TRIVIAL DE LA CIBERSEGURIDAD

OSI Oficina de Seguridad del Internauta

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

017 TU AYUDA EN CIBERSEGURIDAD

TRIVIAL OSI DE LA CIBERSEGURIDAD

De las siguientes opciones, ¿cuál sería una opción de pago seguro?

- ***A| Plataforma de pago seguro.***
- B| Transferencia bancaria.
- C| Ambas respuestas son correctas.

Respuesta: Las plataformas de pago actúan como intermediarias para evitar que nuestros datos se filtren, y nos ayudarán a la hora de recuperar nuestro dinero en caso de fraude.

Compras online

Redes Sociales y mensajería instantánea

TRIVIAL DE LA CIBERSEGURIDAD

OSI Oficina de Seguridad del Internauta

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

017 TU AYUDA EN CIBERSEGURIDAD

TRIVIAL OSI Oficina de Seguridad del Internauta DE LA CIBERSEGURIDAD

¿Cómo podemos detectar si un perfil es falso en una red social?

- ***A\| Comprobar las imágenes del perfil en Google imágenes.***
- B\| Ver el número de seguidores y seguidos.
- C\| Ambas opciones son correctas.

Respuesta: Para detectar un perfil falso, podemos analizar el número de seguidores que tiene en relación con los perfiles que sigue, o comprobar si su imagen de perfil o el resto de imágenes publicadas no sean suyas, mediante Google imágenes.

Redes Sociales y mensajería instantánea

Redes Sociales y mensajería instantánea

TRIVIAL DE LA CIBERSEGURIDAD

OSI Oficina de Seguridad del Internauta

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

017 TU AYUDA EN CIBERSEGURIDAD

TRIVIAL OSI Oficina de Seguridad del Internauta DE LA CIBERSEGURIDAD

Tras mucho esfuerzo, has conseguido sacarte el carnet de conducir, así que decides subir una foto de él a tus redes sociales. ¿Es una buena idea?

- A\| Sí, ¿qué peligro va a tener?
- B\| Sí, si tengo configurada correctamente las opciones de privacidad de mi cuenta.
- ***C\| No. La publicación de datos sensibles en Internet nunca lo es.***

Respuesta: Todo lo que publicamos en Internet permanecerá publicado. Si compartimos datos personales en las redes sociales, corremos el riesgo de que terceros se hagan con ellos para usos delictivos, como la suplantación de identidad.

Redes Sociales y mensajería instantánea

Redes Sociales y mensajería instantánea

TRIVIAL DE LA CIBERSEGURIDAD

OSI Oficina de Seguridad del Internauta

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

017 TU AYUDA EN CIBERSEGURIDAD

TRIVIAL OSI Oficina de Seguridad del Internauta DE LA CIBERSEGURIDAD

Has visto un meme en Internet que puede ser ofensivo para algunos colectivos, pero decides publicarlo igualmente. ¿Crees que tus publicaciones pueden afectarte negativamente en el futuro?

- ***A\| Sí, si se trata de contenido ofensivo o que afecta a mi identidad digital.***
- B\| Sí, pero solamente si publico información personal.
- C\| No, es mi muro y puedo publicar lo que quiera.

Respuesta: Publicar contenidos que puedan ser ofensivos en cualquier red social puede tener consecuencias negativas para tu identidad digital.

Redes Sociales y mensajería instantánea

Redes Sociales y mensajería instantánea

TRIVIAL DE LA CIBERSEGURIDAD

OSI Oficina de Seguridad del Internauta

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

017 TU AYUDA EN CIBERSEGURIDAD

TRIVIAL OSI Oficina de Seguridad del Internauta DE LA CIBERSEGURIDAD

La técnica utilizada por los ciberdelincuentes basadas en el engaño y la manipulación para hacerse con nuestros datos, se conoce como:

- A\| *Phishing*.
- ***B\| Ingeniería social.***
- C\| E-fraudes.

Respuesta: La ingeniería social se basa en el engaño y la manipulación para conseguir que los usuarios hagamos lo que nos piden los ciberdelincuentes, como por ejemplo, que demos nuestros datos personales.

Redes Sociales y mensajería instantánea

Redes Sociales y mensajería instantánea

TRIVIAL DE LA CIBERSEGURIDAD

OSI Oficina de Seguridad del Internauta

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

017 TU AYUDA EN CIBERSEGURIDAD

TRIVIAL OSI Oficina de Seguridad del Internauta DE LA CIBERSEGURIDAD

Tus aportaciones, publicaciones, comentarios y gustos en Internet conforman la imagen que los demás tienen de ti en la red. ¿Cómo se conoce a este concepto?

- A| *Egosurfing*.
- ***B| Identidad digital.***
- C| E-reputación.

Respuesta: La identidad digital es la imagen que proyectas sobre ti en la Red, es decir, cómo te ven y perciben el resto de usuarios.

Redes Sociales y mensajería instantánea

Redes Sociales y mensajería instantánea

TRIVIAL DE LA CIBERSEGURIDAD

OSI Oficina de Seguridad del Internauta

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

017 TU AYUDA EN CIBERSEGURIDAD

TRIVIAL OSI Oficina de Seguridad del Internauta DE LA CIBERSEGURIDAD

Un amigo comparte una noticia explosiva sobre un supuesto caso de corrupción en una gran multinacional en la que varios famosos están implicados. ¿Qué haces?

- ***A| Contrasto la noticia buscando información sobre el tema en otros medios.***
- B| Como confío totalmente en la persona que me lo envía, comparto la noticia.
- C| La comparto rápidamente entre mis contactos. ¡Que todo el mundo se entere!

Respuesta: Una buena práctica para combatir los bulos y las *fake news* es contrastar la información, buscando en fuentes de información confiables y con buena reputación.

Redes Sociales y mensajería instantánea

Redes Sociales y mensajería instantánea

TRIVIAL DE LA CIBERSEGURIDAD

OSI Oficina de Seguridad del Internauta

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

017 TU AYUDA EN CIBERSEGURIDAD

TRIVIAL OSI Oficina de Seguridad del Internauta DE LA CIBERSEGURIDAD

Un rumor en la red que no tiene ninguna base ni está apoyado en ninguna fuente fiable recibe el nombre de:

- A| Cadena.
- ***B| Hoax.***
- C| *Phishing*.

Respuesta: El término *Hoax* o bulo, hace referencia a cualquier rumor que circula por la Red infundado.

Redes Sociales y mensajería instantánea

Redes Sociales y mensajería instantánea

TRIVIAL DE LA CIBERSEGURIDAD

OSI Oficina de Seguridad del Internauta

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

017 TU AYUDA EN CIBERSEGURIDAD

TRIVIAL OSI Oficina de Seguridad del Internauta DE LA CIBERSEGURIDAD

Cuando creas una cuenta en una red social, ¿qué es lo primero que deberías hacer?

- A| No publicar ni utilizar ninguna foto personal.
- B| Agregar a mis familiares y amigos más íntimos.
- ***C| Configurar la seguridad y privacidad de mi perfil.***

Respuesta: Al crearnos una cuenta en cualquier red social, el primer paso siempre debe ser configurar debidamente las opciones de seguridad y privacidad.

Redes Sociales y mensajería instantánea

Redes Sociales y mensajería instantánea

TRIVIAL DE LA CIBERSEGURIDAD

OSI Oficina de Seguridad del Internauta

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

017 TU AYUDA EN CIBERSEGURIDAD

TRIVIAL OSI Oficina de Seguridad del Internauta DE LA CIBERSEGURIDAD

¿Cuál de las siguientes opciones puede ayudarte a identificar una noticia falsa (fake new)?

- A| Analizar el número de *likes* de la noticia.
- ***B| Comprobar la noticia en otras fuentes de información.***
- C| Ambas opciones son correctas.

Respuesta: Si una noticia te da mala espina y no te terminas de fiar, lo mejor será contrastarla con otras fuentes de información para ver si es cierta o no.

Redes Sociales y mensajería instantánea

TRIVIAL DE LA CIBERSEGURIDAD

OSI Oficina de Seguridad del Internauta

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

017 TU AYUDA EN CIBERSEGURIDAD

TRIVIAL OSI Oficina de Seguridad del Internauta DE LA CIBERSEGURIDAD

Buscar información sobre nosotros en Internet sirve para detectar perfiles falsos con nuestros datos. ¿Cómo se llama esta búsqueda?

- ***A| Egosurfing.***
- B| *Autophishing*.
- C| *Grooming*.

Respuesta: El *egosurfing* es una práctica muy útil para ver qué se dice sobre nosotros en la Red y para detectar perfiles falsos con nuestra información.

Protección de dispositivos

TRIVIAL DE LA CIBERSEGURIDAD

OSI Oficina de Seguridad del Internauta

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

017 TU AYUDA EN CIBERSEGURIDAD

TRIVIAL OSI Oficina de Seguridad del Internauta DE LA CIBERSEGURIDAD

De las siguientes opciones, ¿cuáles son medidas antimalware con las que proteger nuestro dispositivo?

- A| Contraseñas seguras.
- ***B| Antivirus y Cortafuegos.***
- C| *Phishing*.

Respuesta: Dentro de las medidas de protección, el antivirus y el cortafuegos (*firewall*) se encuentran entre las más básicas. Su función es la de protegernos ante distintos tipos de ataque a la seguridad de nuestro equipo.

Protección de dispositivos

TRIVIAL DE LA CIBERSEGURIDAD

OSI Oficina de Seguridad del Internauta

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

017 TU AYUDA EN CIBERSEGURIDAD

TRIVIAL OSI Oficina de Seguridad del Internauta DE LA CIBERSEGURIDAD

Quiero deshacerme de mi dispositivo móvil, pero me preocupa la información almacenada en él. ¿Qué sería lo adecuado?

- ***A| Crear una copia de seguridad de la información, eliminar los datos y cuentas manualmente y restablecer el dispositivo al estado de fábrica.***
- B| Volver el dispositivo al estado de fábrica, así queda como nuevo.
- C| Sacar la tarjeta de almacenamiento es suficiente, es donde se encuentra toda la información relevante del teléfono.

Respuesta: La mejor manera de eliminar toda la información de nuestro dispositivo de forma segura es eliminando los datos y cuentas manualmente y restableciéndolo luego al estado de fábrica. Si creamos antes una copia de seguridad, podremos volcar los datos a un nuevo dispositivo.

Protección de dispositivos

TRIVIAL DE LA CIBERSEGURIDAD

OSI Oficina de Seguridad del Internauta

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

017 TU AYUDA EN CIBERSEGURIDAD

TRIVIAL OSI Oficina de Seguridad del Internauta DE LA CIBERSEGURIDAD

Tu dispositivo ha comenzado a lanzar alertas sobre distintas actualizaciones pendientes de instalar. ¿Qué debes hacer?

- A| No hago caso al mensaje, no quiero nuevas funcionalidades ya que consumen más recursos.
- B| Dejo la actualización para otro día que tenga más tiempo.
- ***C| Aplico la actualización lo antes posible.***

Respuesta: Una actualización nos protege de posibles brechas de seguridad, por lo que es fundamental que las instalemos lo antes posible.

Protección de dispositivos

Protección de dispositivos

TRIVIAL DE LA CIBERSEGURIDAD

OSI Oficina de Seguridad del Internauta

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

017 TU AYUDA EN CIBERSEGURIDAD

TRIVIAL OSI Oficina de Seguridad del Internauta DE LA CIBERSEGURIDAD

Cuando se habla de rootear o hacer jailbreacking a un dispositivo, se refiere a:

- A| *Hackear* un dispositivo para tener acceso a todos sus datos.
- ***B| Liberar el dispositivo para adquirir permisos de administrador.***
- C| Devolver el dispositivo a su estado de fábrica.

Respuesta: Estos procedimientos permiten liberar el dispositivo de las restricciones del fabricante y adquirir permisos de administración. Sin embargo, no están exentos de riesgos, como la pérdida de garantía o mayor probabilidad de infección por *malware*.

Protección de dispositivos

Protección de dispositivos

TRIVIAL DE LA CIBERSEGURIDAD

OSI Oficina de Seguridad del Internauta

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

017 TU AYUDA EN CIBERSEGURIDAD

TRIVIAL OSI Oficina de Seguridad del Internauta DE LA CIBERSEGURIDAD

¿Qué haces si empiezas a visualizar anuncios en tu dispositivo, el ratón se mueve sólo o va mucho más lento?

- A| Reinicio el ordenador y conecto un USB para pasar mis archivos a otro equipo.
- B| Reinicio el ordenador a ver si se soluciona solo.
- ***C| Me aseguro de que el antivirus está actualizado y realizo un análisis con él.***

Respuesta: Ante los síntomas descritos, es probable que nuestro dispositivo esté infectado. Lo mejor es utilizar un antivirus actualizado para eliminar el *malware* que se haya podido instalar.

Protección de dispositivos

Protección de dispositivos

TRIVIAL DE LA CIBERSEGURIDAD

OSI Oficina de Seguridad del Internauta

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

017 TU AYUDA EN CIBERSEGURIDAD

TRIVIAL OSI Oficina de Seguridad del Internauta DE LA CIBERSEGURIDAD

Un malware capaz de cifrar todos tus ficheros para luego pedirte dinero a cambio se conoce como:

- ***A| Ransomware.***
- B| *Keylogger*.
- C| Troyano.

Respuesta: El *ransomware* es un tipo de *malware* que tiene como objetivo cifrar todo el contenido de nuestros dispositivos para pedir un rescate (dinero) a cambio de la clave de descifrado.

Protección de dispositivos

Protección de dispositivos

TRIVIAL DE LA CIBERSEGURIDAD

OSI Oficina de Seguridad del Internauta

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

017 TU AYUDA EN CIBERSEGURIDAD

TRIVIAL OSI Oficina de Seguridad del Internauta DE LA CIBERSEGURIDAD

Te has instalado una app con funcionalidad de linterna desde la tienda oficial y te pide los siguientes permisos: cámara, archivos multimedia, contactos, SMS. ¿Cuáles debes aceptar?

- A| Todos, ya que se ha descargado de una tienda oficial.
- B| Cámara, archivos multimedia y contactos.
- ***C| Cámara.***

Respuesta: Debemos aceptar únicamente los permisos imprescindibles para la función de la app. En el ejemplo, sólo es necesario el permiso de cámara para su funcionamiento.

Protección de dispositivos

TRIVIAL DE LA CIBERSEGURIDAD

OSI Oficina de Seguridad del Internauta

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

017 TU AYUDA EN CIBERSEGURIDAD

TRIVIAL OSI Oficina de Seguridad del Internauta DE LA CIBERSEGURIDAD

Una forma segura de proteger tu dispositivo y la información almacenada en él es:

- A| Cambiar el PIN frecuentemente.
- ***B| Cifrarlo y protegerlo con una clave o PIN.***
- C| No utilizar la conexión Bluetooth.

Respuesta: Al cifrar nuestro dispositivo, toda la información contenida en él también se cifrará, protegiéndola de terceros, especialmente en caso de pérdida o robo.

Protección de dispositivos

TRIVIAL DE LA CIBERSEGURIDAD

OSI Oficina de Seguridad del Internauta

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

017 TU AYUDA EN CIBERSEGURIDAD

TRIVIAL OSI Oficina de Seguridad del Internauta DE LA CIBERSEGURIDAD

¿Cuál de las siguientes recomendaciones deberías llevar a cabo si te encontrases en un lugar que proporciona una red wifi pública?

- A| Conectarse, así se ahorran datos móviles.
- B| Revisar las redes wifi disponibles y conectarte solo a la que tenga mejor señal.
- ***C| Desactivar la opción que permite al dispositivo conectarse automáticamente.***

Respuesta: Es conveniente desactivar la opción que permite conectarnos automáticamente a redes inalámbricas para minimizar los riesgos de conectarse a redes wifi.

Protección de dispositivos

TRIVIAL DE LA CIBERSEGURIDAD

OSI Oficina de Seguridad del Internauta

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

017 TU AYUDA EN CIBERSEGURIDAD

TRIVIAL OSI Oficina de Seguridad del Internauta DE LA CIBERSEGURIDAD

Cuando se trata de realizar copias de seguridad, lo ideal es seguir la regla 3-2-1, pero ¿qué significa?

- ***A| 3 copias en 2 soportes diferentes y 1 en un lugar físico distinto.***
- B| 3 copias de seguridad en 2 carpetas distintas y 1 cifrada.
- C| 3 copias de seguridad en 2 soportes diferentes y 1 en la nube.

Respuesta: La regla 3-2-1 se refiere a mantener 3 copias de seguridad, en 2 soportes distintos, como puede ser la nube y un disco duro externo, y 1 de las copias en un lugar físico distinto.

Navegación segura

TRIVIAL DE LA CIBERSEGURIDAD

OSI Oficina de Seguridad del Internauta

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

017 TU AYUDA EN CIBERSEGURIDAD

TRIVIAL OSI Oficina de Seguridad del Internauta DE LA CIBERSEGURIDAD

¿Los plugins, addons o complementos utilizados por los navegadores son siempre seguros?

- A| Solamente cuando los descargo de sitios no oficiales.
- B| Sí. Precisamente me ayudan a mejorar la seguridad.
- ***C| No. Incluso uno fiable puede presentar vulnerabilidades.***

Respuesta: Al igual que las aplicaciones, estos complementos pueden ser maliciosos o presentar vulnerabilidades. Lo mejor es descargarlos de sitios oficiales y revisar los comentarios y valoraciones de otros usuarios.

Navegación segura

Navegación segura

TRIVIAL DE LA CIBERSEGURIDAD

OSI Oficina de Seguridad del Internauta

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

017 TU AYUDA EN CIBERSEGURIDAD

TRIVIAL OSI Oficina de Seguridad del Internauta DE LA CIBERSEGURIDAD

¿Cómo puedes mejorar tu seguridad y privacidad cuando navegas por Internet?

- A| Manteniendo mi dispositivo actualizado y utilizando una conexión segura.
- ***B| Instalando una herramienta antivirus.***
- C| Ambas respuestas son correctas.

Respuesta: Manteniendo el dispositivo actualizado y contando con herramientas de protección, como el antivirus, nos aseguramos de que nuestro dispositivo está más protegido de posibles amenazas.

Navegación segura

Navegación segura

TRIVIAL DE LA CIBERSEGURIDAD

OSI Oficina de Seguridad del Internauta

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

017 TU AYUDA EN CIBERSEGURIDAD

TRIVIAL OSI Oficina de Seguridad del Internauta DE LA CIBERSEGURIDAD

¿De qué te protege una web que utiliza protocolo HTTPS?

- ***A| Del robo de datos y de la suplantación de identidad.***
- B| De un intento de *phishing*.
- C| De riesgos de explotación de vulnerabilidades

Respuesta: El protocolo HTTPS permite una conexión segura mediante un cifrado SSL que posibilita que los datos viajen de forma segura entre tu equipo y el servidor de la página web.

Navegación segura

Navegación segura

TRIVIAL DE LA CIBERSEGURIDAD

OSI Oficina de Seguridad del Internauta

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

017 TU AYUDA EN CIBERSEGURIDAD

TRIVIAL OSI Oficina de Seguridad del Internauta DE LA CIBERSEGURIDAD

Al entrar en la configuración del router, has visto varios dispositivos desconocidos conectados a tu red wifi. ¿Qué debes hacer?

- A| Debo bloquearlos y hacer un filtro de direcciones MAC.
- ***B| Debo cambiar la contraseña de acceso al router así como de conexión a la red wifi.***
- C| Ambas respuestas son correctas.

Respuesta: Una configuración segura de nuestro *router* pasa por cambiar la contraseña de acceso, la de la red wifi y, si en el caso de detectar dispositivos desconocidos, debemos bloquearlos y realizar un filtrado de direcciones MAC.

Navegación segura

Navegación segura

TRIVIAL DE LA CIBERSEGURIDAD

OSI Oficina de Seguridad del Internauta

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

017 TU AYUDA EN CIBERSEGURIDAD

TRIVIAL OSI Oficina de Seguridad del Internauta DE LA CIBERSEGURIDAD

¿Puede infectarte un documento, una imagen o un video recibido a través de un correo electrónico o descargado de una web?

- A| Una imagen no contiene *malware*.
- B| Los vídeos e imágenes no pueden contener *malware*.
- ***C| Cualquier archivo puede contener software malicioso.***

Respuesta: Cualquier archivo descargado de Internet puede contener *malware*. Incluso las páginas web pueden infectarnos con tan solo visitarlas. Por eso es fundamental contar con un buen antivirus y mantener actualizado el dispositivo.

Navegación segura

Navegación segura

TRIVIAL DE LA CIBERSEGURIDAD

OSI Oficina de Seguridad del Internauta

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

017 TU AYUDA EN CIBERSEGURIDAD

TRIVIAL OSI Oficina de Seguridad del Internauta DE LA CIBERSEGURIDAD

Necesitas hacer una búsqueda por Internet a través del equipo de otra persona. ¿Cuál de las siguientes opciones sería la forma más segura de no dejar rastro?

- ***A| Utilizando el modo incógnito.***
- B| Borrando las *cookies*.
- C| Utilizando el navegador de Mozilla Firefox.

Respuesta: Si no hay más remedio y debemos utilizar otro equipo, una buena opción será utilizar el modo incógnito del navegador, evitando introducir información personal en páginas web.

Navegación segura

Navegación segura

TRIVIAL DE LA CIBERSEGURIDAD

OSI Oficina de Seguridad del Internauta

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

017 TU AYUDA EN CIBERSEGURIDAD

TRIVIAL OSI Oficina de Seguridad del Internauta DE LA CIBERSEGURIDAD

Recibes un email de tu banco pidiéndote que accedas a un enlace para confirmar tus datos personales ¿Qué haces?

- A| Respondo al correo para que me faciliten más información.
- B| Lo abro y sigo las indicaciones del mensaje, parece un tema importante.
- ***C| Los bancos nunca piden estos datos por correo, lo elimino.***

Respuesta: Se debe tener precaución con los mensajes que solicitan información personal bajo alguna circunstancia. Una entidad financiera o servicio web con cierta reputación jamás nos pedirá nuestros datos personales por correo.

Navegación segura

Navegación segura

TRIVIAL DE LA CIBERSEGURIDAD

OSI Oficina de Seguridad del Internauta

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

017 TU AYUDA EN CIBERSEGURIDAD

TRIVIAL OSI Oficina de Seguridad del Internauta DE LA CIBERSEGURIDAD

A la hora de navegar por páginas web, la opción más segura es:

- A| Webs con HTTP.
- B| Webs con HTTP y certificado digital.
- ***C| Webs con HTTPS y certificado digital.***

Respuesta: El certificado digital y el protocolo HTTPS actúan como sellos de confianza que nos aseguran que las comunicaciones que hagamos dentro de la web estarán cifradas y serán seguras.

Navegación segura

Navegación segura

TRIVIAL DE LA CIBERSEGURIDAD

OSI Oficina de Seguridad del Internauta

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

017 TU AYUDA EN CIBERSEGURIDAD

TRIVIAL OSI DE LA CIBERSEGURIDAD

Un buen hábito cuando navegamos online es:

- A| Guardar las credenciales en nuestro navegador para no tener que introducirlas manualmente con frecuencia.
- ***B| Eliminar las cookies, la caché y el historial del navegador cada cierto tiempo.***
- C| Conectarse a redes wifi públicas.

Respuesta: De este modo, eliminaremos el rastro que vamos dejando cuando navegamos por Internet, protegiendo mejor nuestra privacidad y seguridad online.

Navegación segura

TRIVIAL DE LA CIBERSEGURIDAD

OSI Oficina de Seguridad del Internauta

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

017 TU AYUDA EN CIBERSEGURIDAD

TRIVIAL OSI DE LA CIBERSEGURIDAD

Para una navegación segura, el protocolo de seguridad que debes tener configurado en tu router es:

- ***A| Protocolo WPA2.***
- B| Protocolo WEP.
- C| Protocolo HTTPS.

Respuesta: Hoy en día, el protocolo WPA2 se considera el protocolo más seguro. El resto presentan vulnerabilidades que pueden ser aprovechadas por los ciberdelincuentes.

Fraudes Online

TRIVIAL DE LA CIBERSEGURIDAD

OSI Oficina de Seguridad del Internauta

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

017 TU AYUDA EN CIBERSEGURIDAD

TRIVIAL OSI DE LA CIBERSEGURIDAD

Uno de tus contactos te ha compartido una noticia sobre una cura para una enfermedad muy contagiosa. ¿Cómo comprobarías si se trata de una noticia real?

- A| Analizar los *likes* de la noticia.
- B| Revisar si la url tiene HTTPS.
- ***C| Buscar la fuente y contrastar.***

Respuesta: Internet está lleno de bulos y noticias falsas. Para combatir la desinformación, es recomendable contrastar la información con otras fuentes.

Fraudes Online

TRIVIAL DE LA CIBERSEGURIDAD

OSI Oficina de Seguridad del Internauta

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

017 TU AYUDA EN CIBERSEGURIDAD

TRIVIAL OSI DE LA CIBERSEGURIDAD

Te ha llegado un SMS sobre una ayuda económica de 350 €. Solo hay que acceder a un link y rellenar un formulario. ¿Qué haces?

- ***A| Investigo sobre la ayuda en Internet.***
- B| Accedo, ya que por SMS no hay riesgo.
- C| Copio el enlace y accedo desde modo incógnito.

Respuesta: Los ciberdelincuentes pueden utilizar estos formularios para hacerse con nuestra información más personal. Para evitarlo, recuerda contrastar e investigar la información del mensaje con otras fuentes y pasar el cursor por el link para asegurarte que te redirige a un sitio legítimo.

Fraudes Online

TRIVIAL DE LA CIBERSEGURIDAD

OSI Oficina de Seguridad del Internauta

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

017 TU AYUDA EN CIBERSEGURIDAD

TRIVIAL OSI DE LA CIBERSEGURIDAD

Has recibido un correo, donde un desconocido afirma tener material íntimo sobre ti. Te pide realizar un pago a cambio de no difundirlo.
¿Qué deberías hacer?

- ***A| Ignorar el mensaje.***
- B| ¿Y si es verdad? Pagas para evitar problemas.
- C| Desconfías. Le pides una prueba primero.

Respuesta: Este tipo de ataque se conoce como sextorsión. Tratan de asustarnos diciendo que tienen material comprometido sobre nosotros para que realicemos un pago a cambio de supuestamente no difundirlo.

Fraudes Online

Fraudes Online

TRIVIAL DE LA CIBERSEGURIDAD

OSI Oficina de Seguridad del Internauta

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

017 TU AYUDA EN CIBERSEGURIDAD

TRIVIAL OSI DE LA CIBERSEGURIDAD

Ante un fraude donde acaban suplantando tu identidad, debes ejercer tus derechos ARCO. ¿Qué significan sus siglas?¿Qué deberías hacer?

- A| Acceso, Rectificación, Comprobación y Oposición.
- ***B| Acceso, Rectificación, Cancelación y Oposición.***
- C| Afirmación, Rectificación, Comprobación y Oposición

Respuesta: Los derechos ARCO hacen referencia al derecho de Acceso, Rectificación, Cancelación y Oposición que tenemos en relación al uso que se hace de nuestros datos.

Fraudes Online

Fraudes Online

TRIVIAL DE LA CIBERSEGURIDAD

OSI Oficina de Seguridad del Internauta

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

017 TU AYUDA EN CIBERSEGURIDAD

TRIVIAL OSI DE LA CIBERSEGURIDAD

Recibes un SMS de tu compañía de teléfono informándote de un error en tu última factura. Te piden que hagas clic en un enlace, pero al entrar y descargar el archivo, se trataba de un malware. ¿Cómo se conoce a este fraude?

- A| *Grooming*.
- B| *Baitering*.
- ***C| Smishing.***

Respuesta: Este tipo de ciberataque se conoce como *smishing*, utilizan los SMS para engañarnos y hacer que nos descarguemos *malware* o que hagamos clic en webs maliciosas.

Fraudes Online

Fraudes Online

TRIVIAL DE LA CIBERSEGURIDAD

OSI Oficina de Seguridad del Internauta

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

017 TU AYUDA EN CIBERSEGURIDAD

TRIVIAL OSI DE LA CIBERSEGURIDAD

¿Qué factores te deberían hacer desconfiar al tratar con un vendedor de una web de compraventa online?

- A| Quiere utilizar la plataforma de pago de la web.
- ***B| Quiere seguir la comunicación por WhatsApp.***
- C| Tiene varios meses de antigüedad en la web con muchas valoraciones.

Respuesta: Si un vendedor trata de utilizar otro canal de comunicación o forma de pago distinto al de la web, podría tratarse de un fraude, es una práctica muy habitual utilizada entre los ciberdelincuentes.

Fraudes Online

Fraudes Online

TRIVIAL DE LA CIBERSEGURIDAD

OSI Oficina de Seguridad del Internauta

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

017 TU AYUDA EN CIBERSEGURIDAD

TRIVIAL OSI DE LA CIBERSEGURIDAD

Acaba de llegarte una oferta de trabajo muy interesante. Sin embargo, algo te huele mal. ¿Cuál de las siguientes opciones sería un indicio de fraude?

- ***A\| Pide contactar con un número de tarificación especial.***
- B\| Pide dinero como gastos de administración por adelantado.
- C\| Ambas opciones.

Respuesta: Aquellas ofertas de empleo que piden llamar a un teléfono de tarificación especial o solicitan un dinero por adelantado son candidatas a tratarse de un fraude.

Fraudes Online

Fraudes Online

TRIVIAL DE LA CIBERSEGURIDAD

OSI Oficina de Seguridad del Internauta

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

017 TU AYUDA EN CIBERSEGURIDAD

TRIVIAL OSI DE LA CIBERSEGURIDAD

Has recibido una llamada de un supuesto soporte técnico. Tras seguir los pasos indicados, te das cuenta de que ha podido tratarse de un fraude. ¿Qué deberías hacer?

- A\| Cambiar las contraseñas de todas tus cuentas.
- ***B\| Desinstalar las apps que hayan instalado en tu equipo.***
- C\| Todas las opciones son correctas.

Respuesta: Si creemos ser víctima de un posible fraude de este tipo, lo más importante es deshabilitar cualquier cambio en nuestra configuración, desinstalar cualquier app y cambiar las contraseñas de nuestros equipos. Un análisis con nuestro antivirus también sería recomendable.

Fraudes Online

Fraudes Online

TRIVIAL DE LA CIBERSEGURIDAD

OSI Oficina de Seguridad del Internauta

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

017 TU AYUDA EN CIBERSEGURIDAD

TRIVIAL OSI DE LA CIBERSEGURIDAD

Es hora de cambiarse de casa y estás mirando alquileres por tu zona. ¿Cuál de las siguientes opciones no te ayudará a evitar fraudes?

- A\| Comprobar las direcciones en Google maps.
- B\| Revisar las descripciones e imágenes en busca de fallos o dobles.
- ***C\| Desconfiar de las agencias.***

Respuesta: La clave para detectar posibles fraudes en los alquileres es revisar detenidamente las descripciones e imágenes. Además, conviene utilizar Google Maps y Google imágenes para comprobar que la dirección y las fotos utilizadas son reales.

Fraudes Online

Fraudes Online

TRIVIAL DE LA CIBERSEGURIDAD

OSI Oficina de Seguridad del Internauta

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

017 TU AYUDA EN CIBERSEGURIDAD

TRIVIAL OSI DE LA CIBERSEGURIDAD

Acabas de recibir un correo de tu marketplace favorita, donde te avisan de una promoción por la cual te regalan 50€. Solo tienes que acceder al enlace para obtener el código. ¿Qué debes hacer?

- A\| Acceder al enlace y reclamar el código.
- ***B\| Pasar el cursor sobre el enlace para ver si dirige a la web original.***
- C\|Copiar el enlace y acceder desde modo incógnito.

Respuesta: Para evitar acabar siendo víctima de un fraude, recuerda pasar el cursor por encima para ver la web real a la que te redirige.

Fraudes Online

CIBER PUNTO OSI incibe_ 017

CIBER PUNTO OSI incibe_ 017

CIBER PUNTO OSI incibe_ 017

OFERTA 60% SOLO HOY -50% AÑADIR AL CARRITO

CIBER PUNTO OSI incibe_ 017


www
CIBER
PUNTO
OSI
incibe_