Experiencia SENIOR

Ejercicios y actividades prácticas

Pon a prueba tus conocimientos

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA PRIMERA 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

OSI Oficina de Seguridad del Internauta

Experiencia SENIOR

Introducción:

Si estás empezando a ponerte al día en temas de ciberseguridad es el momento perfecto de ponerte a prueba.

Demuestra que has comprendido y adquirido los **conocimientos y términos** más básicos para desenvolverte con facilidad en este mundo.

Para ello te proponemos dos ejercicios: una sopa de letras y un crucigrama. **¿Te atreves?**

Experiencia SENIOR

Instrucciones de la sopa de letras:

Busca los **14 conceptos** de ciberseguridad escondidos en nuestra sopa de letras y vete rodeándolos.

Si no encuentras alguno, puedes recurrir a los recursos publicados en la campaña de concienciación Experiencia Senior de la **Oficina de Seguridad del Internauta de INCIBE** para conseguir alguna pista.
¡Mucha suerte!

V	I	Y	S	Z	R	M	E	I	I	X	F	P	H
P	H	I	S	H	I	N	G	S	T	X	U	X	T
C	O	R	T	A	F	U	E	G	O	S	T	I	T
F	L	S	Y	V	W	U	A	Z	U	E	C	E	P
D	I	P	H	I	S	T	O	R	I	A	L	T	S
U	N	A	L	Q	N	A	V	E	G	A	D	O	R
W	E	M	L	P	E	T	M	Z	V	O	S	Y	P
W	I	E	T	V	M	C	O	O	K	I	E	S	E
J	X	F	Q	H	P	M	A	L	W	A	R	E	R
H	V	T	I	A	S	O	F	T	W	A	R	E	M
A	C	T	U	A	L	I	Z	A	C	I	Ó	N	I
F	A	K	E	N	E	W	S	F	R	O	N	I	S
I	C	O	N	T	R	A	S	E	Ñ	A	S	N	O
B	A	N	T	I	V	I	R	U	S	V	C	B	S

Experiencia SENIOR

Instrucciones del crucigrama:

¿Sabrías identificar los **14 términos** de ciberseguridad a partir de sus descripciones? Trata de demostrarlo completando el crucigrama que te proponemos. Recuerda que puedes refrescar tus conocimientos en la **web de OSI.** ¡A por ello!

Conceptos crucigrama:

1.- Fraude que consiste en hacerse pasar por personal de una entidad de confianza a través de una llamada telefónica.

2.- Persona con muchos conocimientos técnicos en ciberseguridad dedicada a detectar fallos en los sistemas y resolverlos.

3.- Proceso que sirve para convertir un documento o un archivo en una versión ilegible para todas aquellas personas que no están autorizadas para verlo.

4.- Dispositivos que se conectan a nuestro equipo, como el ratón, teclado, pantalla, etc.

5.- Red formada por dispositivos infectados y controlados por un ciberdelincuente.

6.- Fallo de seguridad que sufre un programa informático y que puede ser aprovechado por los ciberdelincuentes.

7.- Dispositivo que nos permite conectarnos a Internet en nuestro hogar.

8. Herramienta para buscar información en Internet bajo términos o palabras concretas.

9.- Cadena de caracteres que permite acceder a una página web o contenido alojado en Internet.

10.- Programa que instalamos en nuestro navegador y que sirve para añadir alguna funcionalidad adicional.

11.- Mecanismo para bloquear el acceso a los dispositivos que utiliza algún elemento de nuestro cuerpo, como la huella dactilar o nuestro rostro.

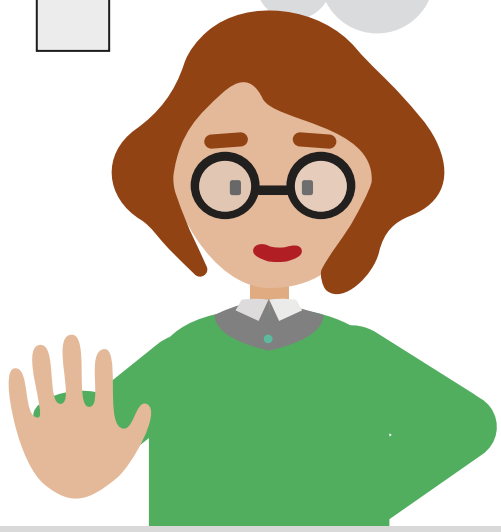
12.- Conexión inalámbrica que permite intercambiar información entre dos dispositivos y sincronizar o conectar dos dispositivos para que interactúen.

13.- Programa que instalamos en el dispositivo móvil, smartphone o tablet, y que nos proporciona alguna funcionalidad extra.

14.- Ataque en el que los ciberdelincuentes suplantan la identidad de una entidad enviando un SMS malicioso para engañar al usuario y que éste realice alguna acción.

1. Primeros pasos en ciberseguridad

Experiencia SENIOR



Experiencia SENIOR

Soluciones:

Conceptos sopa de letras:

Contraseñas, Wifi, Antivirus, Software, Spam, Phising, Navegador, Cookies, Permisos, Fake News, HTTPS, Historial, Cortafuegos, Actualización

2. Conoce tus dispositivos y protégelos

Experiencia SENIOR

Introducción:

Usamos nuestros dispositivos para una gran variedad de actividades en nuestro día a día. Entonces, **¿por qué no nos aseguramos de mantenerlos a punto y protegidos?**

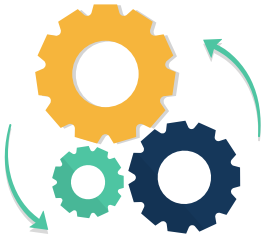
Repasa nuestra lista de acciones ciberseguras y comprueba que todos tus dispositivos están correctamente protegidos.

¡Y no te olvides de hacer una revisión de todos los puntos periódicamente!

2. Conoce tus dispositivos y protégelos

Experiencia SENIOR

Acciones:	Dispositivo:			
	Fecha:			
	SI	NO	SI	NO
Tengo instalado y activado un antivirus en mi dispositivo.				
El antivirus está actualizado a la última versión disponible.				
Analizo el dispositivo con el antivirus cada pocos días para asegurarme de estar libre de virus.				
Mi dispositivo está actualizado a la última versión disponible.				
Tengo automatizada la descarga e instalación de actualizaciones de mi dispositivo.				
Tengo activado un sistema de bloqueo para acceder a mi dispositivo (contraseña, PIN, patrón, huella dactilar, etc.).				
Solo yo conozco el sistema de bloqueo/ desbloqueo de mi dispositivo.				
En los dispositivos compartidos, tengo una cuenta de usuario para cada miembro.				



Acciones:	Dispositivo:			
	Fecha:			
	SI	NO	SI	NO
En los dispositivos compartidos, solo una de las cuentas corresponde al administrador y es gestionada por un único usuario.				
Tengo instalados solo programas y aplicaciones legítimas, descargados de repositorios de aplicaciones oficiales o de la web del fabricante.				
Antes de instalar una aplicación, compruebo los comentarios y valoraciones que han compartido otros usuarios sobre ella.				
He eliminado todas las aplicaciones y programas innecesarios que ya no utilizo.				
He revisado los permisos de mis aplicaciones y programas para evitar que tengan acceso a información personal. Además, antes de instalar una nueva aplicación también me fijo en los permisos que solicita.				

2. Conoce tus dispositivos y protégelos

Experiencia SENIOR

Analizo el dispositivo con el antivirus cada pocos días para asegurarme de estar libre de virus.

Es recomendable ***hacer un análisis con nuestro antivirus cada pocos días,*** especialmente si hemos estado descargando programas o archivos de Internet, navegando por la Red o intercambiando muchos correos electrónicos.

Tengo instalados solo programas y aplicaciones legítimas, descargados de repositorios de aplicaciones oficiales o de la web del fabricante.

A la hora de descargar e instalar cualquier aplicación o programa ***debemos asegurarnos de utilizar medios o sitios web fiables***, evitando versiones piratas o falsas que puedan tener un impacto negativo en nuestra seguridad.
Los programas y aplicaciones ilegítimos suelen ser una fuente de virus y amenazas que ponen en riesgo la seguridad de nuestro dispositivo y nuestra propia información personal.

Antes de instalar una aplicación, compruebo los comentarios y valoraciones que han compartido otros usuarios sobre ella.

Además de utilizar tiendas oficiales o las webs de los desarrolladores o fabricantes, ***es recomendable revisar las valoraciones y comentarios de otros usuarios***, comparar el nombre del programa en Internet para alertarnos de posibles fraudes y utilizar el sentido común.

Mi dispositivo está actualizado a la última versión disponible.

Nuestros dispositivos, ya utilicen un sistema operativo Windows, macOS, Android e iOS, ***necesitan actualizarse para resolver posibles fallos de seguridad*** y para ofrecernos mejoras en su funcionamiento.
Siempre que haya una actualización, el dispositivo nos informará y deberemos descargarla lo antes posible.

2. Conoce tus dispositivos y protégelos

Experiencia SENIOR

Tengo automatizada la descarga e instalación de actualizaciones de mi dispositivo.

El sistema operativo del dispositivo ***nos avisará cada vez que haya una nueva actualización.*** Por seguridad, es recomendable que ***accedamos a la configuración y confirmemos que está automatizada esta tarea.*** Así evitaremos que, por un despiste, no estemos actualizados a la última versión.

Tengo activado un sistema de bloqueo para acceder a mi dispositivo (contraseña, PIN, patrón, huella dactilar, etc.).

Nuestros dispositivos ***cuentan con una función de bloqueo para evitar que otros usuarios puedan acceder a su contenido.*** Hay muchos tipos, como una ***clave, un patrón, un código PIN o incluso factores biométricos***, como nuestra huella dactilar o nuestro rostro. Es uno de los primeros pasos que debemos configurar en nuestro dispositivo para evitar que un desconocido pueda acceder a su contenido.

Solo yo conozco el sistema de bloqueo/desbloqueo de mi dispositivo.

Al igual que nuestras contraseñas, ***los métodos de bloqueo son privados y no debemos compartirlos con ningún otro usuario.*** Si no, ***correríamos el riesgo de que un tercero pudiese acceder al contenido de nuestro dispositivo*** en un descuido.

En los dispositivos compartidos, tengo una cuenta de usuario para cada miembro.

En ocasiones, ***disponemos de dispositivos que son utilizados por toda la familia*** o por un grupo de usuarios. ***En estos casos, es recomendable asegurarnos de que cada uno tenga su propia cuenta para acceder al dispositivo***. Así, se evitará editar o borrar archivos de otros usuarios, poder instalar programas propios y realizar otras actividades sin que afecten al resto.

2. Conoce tus dispositivos y protégelos

Experiencia SENIOR

En los dispositivos compartidos, solo una de las cuentas corresponde al administrador y es gestionada por un único usuario.

Las cuentas de administrador son aquellas con más poderes dentro del dispositivo. ***Pueden crear más usuarios, realizar configuraciones del dispositivo, instalar y eliminar programas, etc.***

Por razones de seguridad, es recomendable que solo exista una de estas cuentas, y que sea gestionada por un único usuario. ***Así, las probabilidades de que la seguridad de esta y el resto de cuentas sea vulnerada será mucho menor.***

Tengo instalado y activado un antivirus en mi dispositivo.

Los ***antivirus son programas que analizan nuestros dispositivos en busca de virus*** y otras amenazas para eliminarlas. ***Es la herramienta de seguridad más básica que debemos tener instalada*** y, por norma general, todos los dispositivos tienen alguna preinstalada.
De cualquier modo, existen muchas alternativas, tanto de pago como gratuitas, que nos ayudarán a proteger nuestros dispositivos.

El antivirus está actualizado a la última versión disponible.

Como cualquier programa, ***los antivirus necesitan estar actualizados para ser capaces de realizar sus funciones***, adaptarse a las nuevas amenazas ***y resolver posibles fallos en su seguridad o funcionamiento.***

He eliminado todas las aplicaciones y programas innecesarios que ya no utilizo.

Algunas ***aplicaciones y programas con el tiempo sufren fallos de seguridad*** debido a la falta de actualizaciones por parte de los desarrolladores. ***Si tenemos instalados programas que ya no utilizamos desde hace tiempo, corremos el riesgo de que presenten estos fallos***, por lo que debemos desinstalarlos. Además, ganaremos espacio de almacenamiento en nuestros dispositivos.

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA PRIMERA 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
OSI Oficina de Seguridad del Internauta

2. Conoce tus dispositivos y protégelos

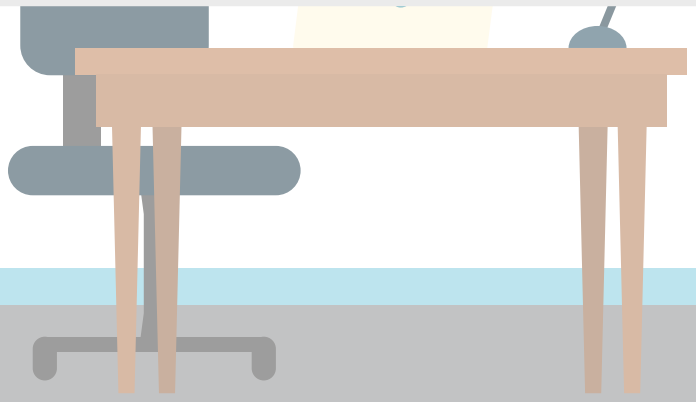
Experiencia SENIOR

Mis aplicaciones y programas están actualizados a la última versión disponible.

Las ***actualizaciones nos aseguran que las aplicaciones y programas instalados estén siempre a la última***, resolviendo fallos de seguridad, añadiendo nuevas funcionalidades y mejorándolos en todos los sentidos.
Siempre que veamos que un programa o aplicación necesita una actualización, deberemos descargarla e instalarla lo antes posible.

He revisado los permisos de mis aplicaciones y programas para evitar que tengan acceso a información personal. Además, antes de instalar una nueva aplicación también me fijo en los permisos que solicita.

Algunos programas o aplicaciones, especialmente en nuestros teléfonos o tablets, ***necesitan acceder a determinados datos o funciones de nuestros dispositivos para funcionar***. Esta petición es a lo que se conoce como permisos.
Debemos fijarnos detenidamente en qué permisos nos solicitan las aplicaciones antes de instalarlas y revisar los permisos concedidos de las que ya tenemos instaladas, cotejándolos con la función de la aplicación.



GOBIERNO DE ESPAÑA
VICEPRESIDENCIA PRIMERA 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
OSI Oficina de Seguridad del Internauta

3. Conéctate y navega de forma segura

Experiencia SENIOR

Introducción:

Navegar por Internet puede convertirse en un campo de minas si no sabes dónde hacer clic.

Por eso, te proponemos este ejercicio donde deberás **identificar aquellas acciones que puedan suponer un riesgo para tu privacidad y seguridad** cuando navegues por la Red.

Selecciona las opciones que consideres más peligrosas o que puedan comprometer tu seguridad y descubre sus consecuencias. **¿Acertarás?**

3. Conéctate y navega de forma segura

Experiencia SENIOR

Situación 1:

Te encuentras navegando por Internet en busca de un regalo de cumpleaños para tus sobrinos.
De pronto, mientras buscas ofertas en zapatillas de deporte, **una nueva ventana aparece en tu navegador con una oferta muy atractiva**. Parece que son de una marca muy conocida y podrían ser el regalo perfecto.

El anuncio ofrece un descuento del 50% para los 50 primeros solicitantes. Junto al texto aparece un enlace sobre el que debes hacer clic.

- **A** *Hago clic en el enlace, aunque sea solo para echar un vistazo y comprobar los precios.* ☐
- **B** *Ignoro el anuncio y centro mi búsqueda solo en la web oficial de la marca.* ☐
- **C** *Al ser el producto que quiero, hago clic y realizo la compra con descuento.* ☐

Experiencia SENIOR

Situación 2:

Te encuentras en la cafetería de un centro comercial descansando tras una mañana de compras. Aprovechas para revisar tus mensajes de WhatsApp o mirar tu correo o la prensa desde tu teléfono móvil.

Sin embargo, te preocupa quedarte sin datos móviles y el centro comercial cuenta con una **red wifi pública y gratuita** para sus clientes.

¿Qué haces?:

- **A** *Me conecto a la red wifi, al fin y al cabo solo voy a leer alguna noticia y contestar algunos mensajes y correos.* ☐
- **B** *Me conecto a la red wifi, pero solo para mirar la prensa y nada más.* ☐
- **C** *Prefiero consumir los datos de mi teléfono o esperar a llegar a casa para hacerlo.* ☐

Experiencia SENIOR

Situación 3:

Estás de visita en casa de unos amigos tras unas vacaciones.

Están deseando ver las fotos de tu viaje y **te han dejado su portátil para que te conectes a tu cuenta** de almacenamiento en la nube donde tienes subido el álbum de fotos (Google Fotos, Dropbox, OneDrive...).

¿Qué haces?

- **A** *Inicio sesión en el portátil de mis amigos para enseñarles las fotos.* ☐
- **B** *Abro una ventana de incógnito, inicio sesión y les enseño las fotos.* ☐
- **C** *Prefiero utilizar mi teléfono o compartir con ellos el álbum.* ☐

Experiencia SENIOR

Situación 4:

Te encuentras navegando por Internet desde tu portátil buscando sitios a los que poder ir el fin de semana que viene con tu familia y amigos.
De pronto, una **notificación** aparece en tu ventana del navegador:

¿Qué haces?

- **A** *Me pongo en contacto con el número indicado. No hay que ignorar ninguna alerta.* ☐
- **B** *Prefiero descargarme el antivirus del servicio técnico y utilizarlo.* ☐
- **C** *Ignoro el mensaje, cierro la web y analizo mi equipo con mi antivirus personal.* ☐

3. Conéctate y navega de forma segura

Experiencia SENIOR

Soluciones:

Veamos las consecuencias de tu decisión.
Busca la opción que habías seleccionado
y comprueba si has actuado bien o no:

Situación 1:

A ***Hago clic en el enlace, aunque sea solo para echar un vistazo y comprobar los precios.***

No es recomendable, aunque solo sea para echar un vistazo.
Al hacer clic podríamos terminar en una web maliciosa que nos infecte con algún malware, robe información almacenada en nuestro navegador o nos exponga a más anuncios fraudulentos.
Antes de abrir cualquier enlace o anuncio que nos genere dudas es recomendable comprobar en Internet qué dicen otros usuarios sobre dicha web para confirmar si se trata de un fraude, o por el contrario, si es fiable.

B ***Ignoro el anuncio y centro mi búsqueda solo en la web oficial de la marca.***

Es lo más seguro.
Así no **corremos el riesgo de terminar entrando en una web maliciosa que infecte nuestro dispositivo**, o una web falsa que simule ser otra web legítima, pero que a la hora de pagar se haga con nuestros datos personales y bancarios.

C ***Al ser el producto que quiero, hago clic y realizo la compra con descuento.***

No tan rápido, estos anuncios a veces tienen trampa.
Al hacer clic corremos el riesgo de terminar en una web maliciosa.
Si realizamos una compra o nos registramos, nuestros datos personales y bancarios podrían terminar en manos de un tercero con malas intenciones y, como consecuencia, podríamos encontrarnos cargos en nuestra cuenta bancaria.

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA PRIMERA 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
OSI Oficina de Seguridad del Internauta

3. Conéctate y navega de forma segura

Experiencia SENIOR

Soluciones:

Veamos las consecuencias de tu decisión.
Busca la opción que habías seleccionado
y comprueba si has actuado bien o no:

Situación 2:

A ***Me conecto a la red wifi, al fin y al cabo solo voy a leer alguna noticia y contestar algunos mensajes y correos.***

No lo hagas.
Al conectarte, navegar por la Red y acceder a tus cuentas **desde una red wifi pública, corres el riesgo de que toda tu actividad sea vigilada por un tercero**, ya que no sabes quién puede estar conectado a esa red, ni con qué intenciones.

B ***Me conecto a la red wifi, pero solo para mirar la prensa y nada más.***

Es seguro, pero ten cuidado.
Mientras **no accedas a ninguna de tus cuentas ni te descargues nada** no tendrás que preocuparte si te conectas a una red wifi pública. Sin embargo, no olvides que es mejor evitarlas.

C ***Prefiero consumir los datos de mi teléfono o esperar a llegar a casa para hacerlo.***

Es lo más seguro.
De este modo, **evitaremos correr riesgos innecesarios**, como el robo de información personal o la suplantación de tus cuentas al hacerse un tercero con tu usuario y contraseña.

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA PRIMERA 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
OSI Oficina de Seguridad del Internauta

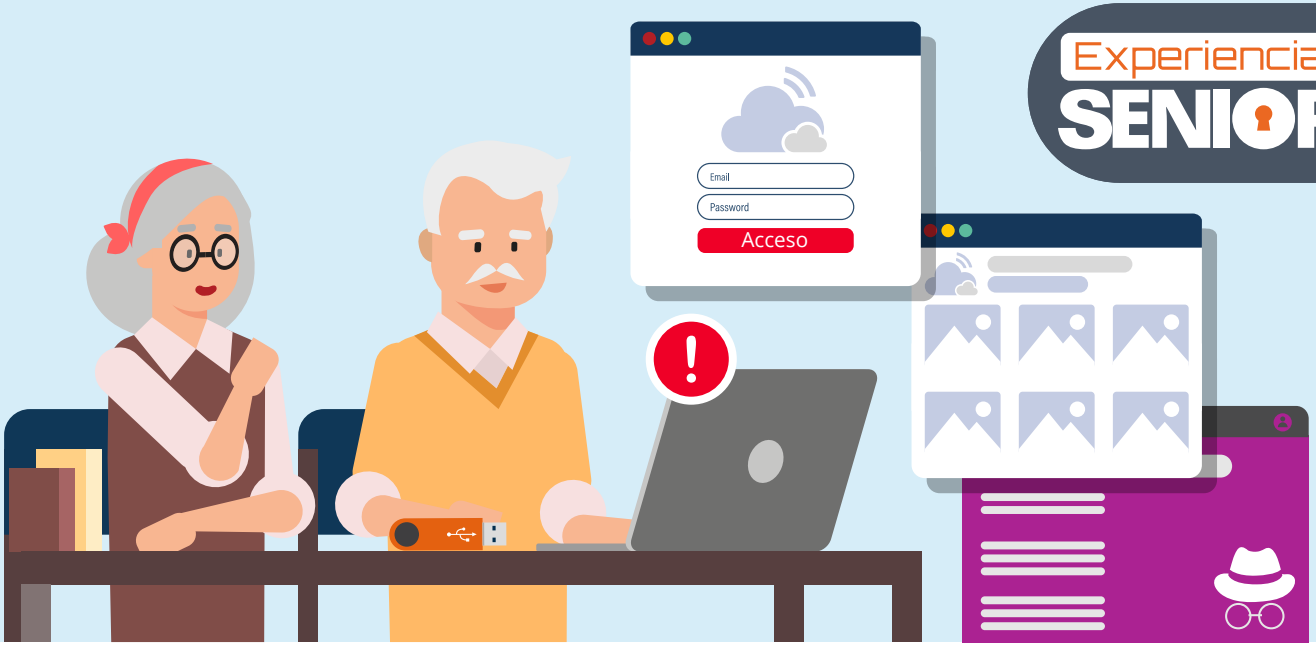
3. Conéctate y navega de forma segura

Experiencia SENIOR

Soluciones:

Veamos las consecuencias de tu decisión.
Busca la opción que habías seleccionado y comprueba si has actuado bien o no:

Situación 3:



A ***Inicio sesión en el portátil de mis amigos para enseñarles las fotos.***

Ten mucho cuidado.
Aunque sean amigos tuyos, **iniciar sesión en un dispositivo ajeno puede ser un problema para tu privacidad**, especialmente si te dejas la cuenta abierta, tus datos de navegación o tus contraseñas guardadas en el navegador.
Sin querer, podrían acceder a toda esta información, leer información privada o modificar alguna configuración de tu cuenta.

B ***Abro una ventana de incógnito, inicio sesión y les enseño las fotos.***

Es lo más seguro.
Así te asegurarás de mantener intacta tu privacidad y evitar que terceras personas puedan conectarse a tu cuenta después de ti o acceder al registro de tus **datos de navegación** (historial, cookies, contraseñas guardadas).

C ***Prefiero utilizar mi teléfono o compartir con ellos el álbum.***

Es buena idea.
Así **evitaremos dejar un rastro en su navegador y dispositivo** con nuestro usuario y contraseña al iniciar sesión.
Si compartimos con ellos una carpeta o álbum con las fotos que nos interesa, podremos gestionar hasta cuándo queremos hacerlo y seguiremos manteniendo a salvo nuestra privacidad.

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA PRIMERA 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
OSI Oficina de Seguridad del Internauta

3. Conéctate y navega de forma segura

Experiencia SENIOR

Soluciones:

Veamos las consecuencias de tu decisión.
Busca la opción que habías seleccionado y comprueba si has actuado bien o no:

Situación 4:

A ***Me pongo en contacto con el número indicado. No hay que ignorar ninguna alerta.***

Tiene pinta de ser una estafa.
El teléfono seguramente te suponga algún **cargo adicional en la factura telefónica**, o incluso que la persona al otro lado del teléfono intente tomar control de tu dispositivo haciéndote descargar algún programa malicioso que infecte tu dispositivo, o se encargue de recopilar datos, como números, contactos, información bancaria y compartirla con el atacante.

B ***Prefiero descargarme el antivirus del servicio técnico y utilizarlo.***

Es un riesgo descargar cosas pulsando en botones facilitados en anuncios. **Podrían ser ficheros maliciosos para infectar tu dispositivo, tomar su control** o compartir información con un ciberdelincuente.
Mejor acudir a fuentes de descarga de confianza, como página web del desarrollador o repositorios de aplicaciones oficiales.

C ***Ignoro el mensaje, cierro la web y analizo mi equipo con mi antivirus personal.***

Es lo más seguro.
Una alerta de este tipo cuando navegas por Internet suele ser sinónimo de **estafa**. Hacerle caso puede terminar con tu dispositivo infectado o con un ciberdelincuente robando tu información personal. Para mayor seguridad, puedes pasar el **antivirus** que tengas instalado en tu equipo y salir de dudas.

GOBIERNO DE ESPAÑA · VICEPRESIDENCIA PRIMERA 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
OSI Oficina de Seguridad del Internauta

Experiencia SENIOR

Introducción:

¿Te has planteado alguna vez la cantidad de información que tienes almacenada en tus cuentas de usuario de Internet y en los distintos dispositivos que manejas? **Su seguridad y privacidad depende de que seas consciente de ello.**

En este ejercicio te proponemos **identificar las medidas de protección** que encajan mejor con tus dispositivos y cuentas de usuario. Finalmente, podrás hacer un repaso sobre todo lo que tus dispositivos saben de ti. **¡Seguro que te sorprende!**

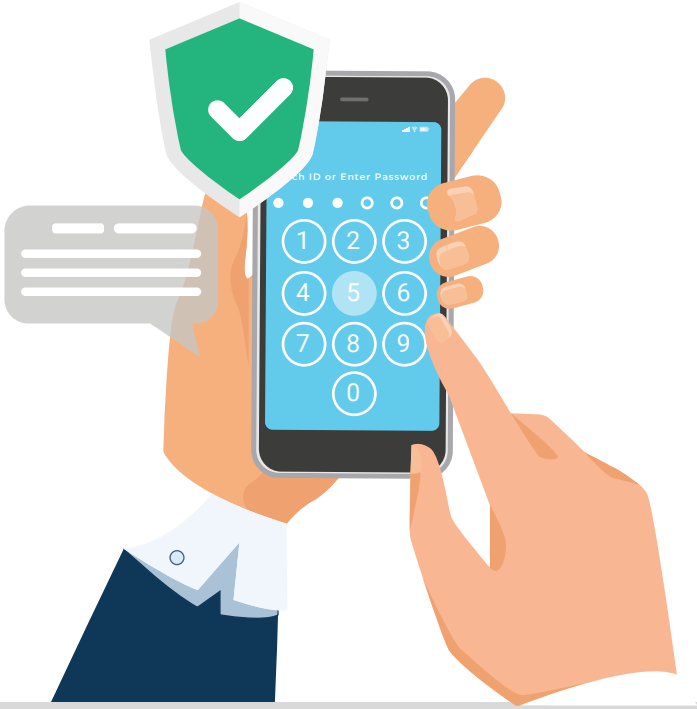
GOBIERNO DE ESPAÑA
VICEPRESIDENCIA PRIMERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
017 TU AYUDA EN CIBERSEGURIDAD
OSI Oficina de Seguridad del Internauta

Experiencia SENIOR

Ejercicio 1:

¿Cómo protegerías cada dispositivo o servicio y la información que contiene?

Une con flechas para asociar el tipo de dispositivo con las protecciones que se deberían aplicar para cada uno de ellos.



Tipo de dispositivo	
Ordenador	Contraseña
Teléfono móvil (smartphone)	Código PIN
Tablet	Patrón de bloqueo
Dispositivos inteligentes (asistentes, smartwatches,etc.)	Verificación en dos pasos
Disco duro externo	Bloqueo biométrico (huella dactilar o rostro)
Memoria USB	Copia de seguridad
	Cifrado
	Cuaderno con contraseñas
	Contraseña compartida

Experiencia SENIOR

Ejercicio 1:

¿Cómo protegerías cada dispositivo o servicio y la información que contiene?

Une con flechas para asociar el tipo de servicio con las protecciones que se deberían aplicar para cada uno de ellos.

Tipo de servicio online	Protecciones
Correo electrónico (Gmail, Outlook, Yahoo!, etc.)	Contraseña
Entretenimiento (Netflix, HBO, Amazon Prime Video, Spotify, etc.)	Código PIN
Redes sociales (Facebook, Instagram, Twitter, TikTok, etc.)	Patrón de bloqueo
Banca online u otros servicios financieros (PayPal, Bizum, etc.)	Verificación en dos pasos
Compras online (Amazon, Privalia, eBay, Zalando, etc.)	Bloqueo biométrico (huella dactilar o rostro)
Juegos (Nintendo, PlayStation 4, Xbox, etc.)	Copia de seguridad
	Cifrado
	Cuaderno con contraseñas
	Contraseña compartida

Experiencia SENIOR

Ejercicio 2:

Con el uso diario nuestros dispositivos van almacenando una gran cantidad de información sobre nosotros, casi como un registro de nuestra vida, que en ocasiones no llegamos a controlar.

Utiliza la información de la tabla para reflexionar sobre qué tipo de información puede contener cada uno de tus dispositivos y escríbelo en cada uno de ellos, según corresponda.

Puedes ampliarla si lo ves necesario:

Nombre y apellidos	Direcciones postales (casa, trabajo, etc.)	Rutinas y localizaciones habituales
Correo eletrónico	Nº de tarjetas de crédito	Fotografías
Empresa	Número de teléfono	DNI
Facturas, contratos y documentos oficiales	Datos de nuestros contactos (correos, teléfonos...)	Mensajes privados
Usuarios y contraseñas	Búsquedas de internet	Archivos y documentos personales
Tiendas online favoritas	Grabaciones de audio	Vídeos
Datos de salud	Transporte habitual	Patrones de sueño
Comida favorita	Talla de zapatos	Citas y fechas clave
Nombre de la mascota	Fecha de nacimiento	Lugares visitados
Entidad bancaria	Gustos e intereses para ocio	Redes sociales

Experiencia SENIOR

Escribe aquí tu información:

Smartphone:

Ordenador:

Experiencia SENIOR

Soluciones:

(ejercicio 1)

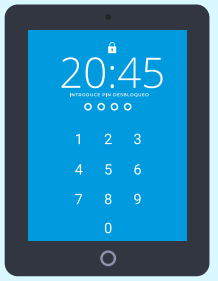
ORDENADOR

- Contraseña
- Código PIN
- Copia de seguridad
- Cifrado

SMARTPHONE

- Código PIN
- Patrón de bloqueo
- Bloqueo biométrico
- Copia de seguridad
- Cifrado

TABLET



- Código PIN
- Patrón de bloqueo
- Bloqueo biométrico
- Copia de seguridad
- Cifrado

• **Una contraseña robusta o un código PIN** nos ayudarán a proteger el acceso a nuestro dispositivo y nuestra cuenta de usuario de personas no autorizadas.

• **La copia de seguridad** nos ayudará a recuperar nuestros archivos y programas instalados, en caso de que se pierdan o se dañen. También, en caso de robo o si nuestro dispositivo deja de funcionar como debería, podemos utilizar la copia y restaurarla en otro dispositivo.

• **Cifrando** los archivos los protegeremos, haciéndolos inaccesibles para terceros que no conozcan la clave que permite acceder a ellos.

• **Una contraseña robusta, un código PIN, un patrón de bloqueo o un bloqueo biométrico** (como nuestra huella o el rostro) evitarán que otros usuarios no autorizados puedan acceder al dispositivo y a la información que contiene. Generalmente, podemos usar uno o dos métodos para desbloquear el dispositivo.

• La **copia de seguridad** nos ayudará a recuperar nuestros archivos y programas instalados, en caso de que se pierdan o se dañen. También, en caso de robo o si nuestro dispositivo deja de funcionar como debería, podemos utilizar la copia y restaurarla en otro dispositivo.

• **Cifrando los archivos** los protegeremos, haciéndolos inaccesibles para terceros que no conozcan la clave que permite acceder a ellos.

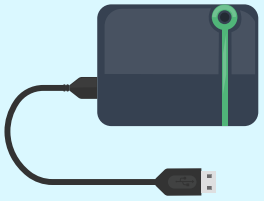
Experiencia SENIOR

Soluciones:

(ejercicio 1)

DISPOSITIVOS INTELIGENTES

- Contraseña
- Verificación en 2 pasos
- Bloqueo biométrico



DISCO DURO EXTERNO

- Copia de seguridad
- Cifrado

MEMORIA USB

- Copia de seguridad
- Cifrado

• **Una contraseña robusta** impedirá que otros usuarios puedan acceder a nuestro dispositivo, hacerse con la información o modificar la configuración.

Dependiendo del dispositivo inteligente, es posible encontrar algún otro mecanismo de protección, como los siguientes:

• **La verificación en dos pasos** añadirá una capa extra de seguridad, teniendo que introducir un código enviado a nuestro correo o teléfono cada vez que iniciemos sesión.

• **El bloqueo biométrico** supone una medida de seguridad alternativa a nuestra contraseña o PIN, ya que es complicado que alguien acceda a nuestras cuentas suplantando nuestra huella dactilar o rostro.

• **La copia de seguridad** nos ayudará a recuperar nuestros archivos y programas instalados, en caso de que se pierdan o se dañen. También, en caso de robo o si nuestro dispositivo deja de funcionar como debería, podemos utilizar la copia y restaurarla en otro dispositivo.

• **Cifrando los archivos los protegeremos,** haciéndolos inaccesibles para terceros que no conozcan la clave que permite acceder a ellos.

• **La copia de seguridad** nos ayudará a recuperar nuestros archivos y programas instalados, en caso de que se pierdan o se dañen. También, en caso de robo o si nuestro dispositivo deja de funcionar como debería, podemos utilizar la copia y restaurarla en otro dispositivo.

• **Cifrando los archivos** los protegeremos, haciéndolos inaccesibles para terceros que no conozcan la clave que permite acceder a ellos.

Experiencia SENIOR

Soluciones:

(ejercicio 1)

CORREO ELECTRÓNICO

- Contraseña
- Verificación en 2 pasos
- Copia de seguridad

ENTRETENIMIENTO

- Contraseña
- Verificación en 2 pasos

REDES SOCIALES

- Contraseña
- Verificación en 2 pasos
- Copia de seguridad

• **Una contraseña robusta** impedirá que otros usuarios puedan acceder a nuestra cuenta, robar información, modificar la configuración o hacerse pasar por nosotros.

• **La verificación en dos pasos** añadirá una capa extra de seguridad, teniendo que introducir un código enviado a nuestro correo o teléfono cada vez que iniciemos sesión. También es posible hacer uso de una aplicación específica (Google Authenticator o Microsoft Authenticator), que genera códigos aleatorios de un solo uso para acceder a la cuenta.

• **Disponer de una copia de todos nuestros mensajes y archivos almacenados en la bandeja de entrada** será muy útil, por ejemplo, en caso de que alguien tome el control de nuestra cuenta (hackeo) o se produzca un error en el servicio, de tal forma que siempre tendremos a mano una copia de esta información.

• **Una contraseña robusta** impedirá que otros usuarios puedan acceder a nuestra cuenta, robar información, modificar la configuración o hacerse pasar por nosotros.

• **La verificación en dos pasos** añadirá una capa extra de seguridad, teniendo que introducir un código enviado a nuestro correo o teléfono cada vez que iniciemos sesión. También es posible hacer uso de una aplicación específica (Google Authenticator o Microsoft Authenticator), que genera códigos aleatorios de un solo uso para acceder a la cuenta.

• **Una contraseña robusta** impedirá que otros usuarios puedan acceder a nuestra cuenta, robar información, modificar la configuración o hacerse pasar por nosotros.

• **La verificación en dos pasos** añadirá una capa extra de seguridad, teniendo que introducir un código enviado a nuestro correo o teléfono cada vez que iniciemos sesión. También es posible hacer uso de una aplicación específica (Google Authenticator o Microsoft Authenticator), que genera códigos aleatorios de un solo uso para acceder a la cuenta.

• **La copia de seguridad** nos ayudará a mantener a salvo nuestras publicaciones, fotografías, vídeos y otros momentos almacenados en nuestra cuenta de la red social. De este modo, siempre dispondremos de estos datos aunque cierren la cuenta o perdamos el control de la misma, por ejemplo, por el ataque de un ciberdelincuente.

Experiencia SENIOR

Soluciones:

(ejercicio 1)

BANCA Y SERVICIOS FINANCIEROS

- Contraseña
- Código PIN
- Verificación en 2 pasos
- Bloqueo biométrico

• **Una contraseña robusta o un código PIN** nos ayudarán a proteger el acceso a nuestra cuenta y a toda la información bancaria y personal almacenada en ella.

• **La verificación en dos pasos** añadirá una capa extra de seguridad, teniendo que introducir un código enviado a nuestro teléfono para confirmar una transacción bancaria.

• **El bloqueo biométrico** supone una medida de seguridad alternativa a nuestra contraseña o PIN, ya que es complicado que alguien acceda a nuestras cuentas suplantando nuestra huella dactilar o rostro.

COMPRAS ONLINE

- Contraseña
- Verificación en 2 pasos

• **Una contraseña robusta** impedirá que otros usuarios puedan acceder a nuestra cuenta, robar información, modificar la configuración o hacerse pasar por nosotros.

• **La verificación en dos pasos** añadirá una capa extra de seguridad, teniendo que introducir un código enviado a nuestro teléfono cada vez que iniciemos sesión. También es posible hacer uso de una aplicación específica (Google Authenticator o Microsoft Authenticator), que genera códigos aleatorios de un solo uso para acceder a la cuenta.

JUEGOS

- Contraseña
- Verificación en 2 pasos

• **Una contraseña robusta** impedirá que otros usuarios puedan acceder a nuestra cuenta, robar información, modificar la configuración o hacerse pasar por nosotros.

• **La verificación en dos pasos** añadirá una capa extra de seguridad, teniendo que introducir un código enviado a nuestro teléfono cada vez que iniciemos sesión. También es posible hacer uso de una aplicación específica (Google Authenticator o Microsoft Authenticator), que genera códigos aleatorios de un solo uso para acceder a la cuenta.

Experiencia SENIOR

Ejemplos de solución:

Soluciones:

(ejercicio 2)

¿Cuánta información almacenan tus dispositivos?
Quizás sea mucha más de la que crees:

Efectivamente, nuestros dispositivos almacenan muchísima información. En ocasiones se debe a que nosotros mismos la introducimos al utilizar una aplicación o guardar archivos o fotos, mientras que otras veces esta información es recogida automáticamente al hacer uso de cada uno de ellos.

Por esta razón, **es importante que los protejamos y los blindemos adecuadamente contra los ciberdelincuentes y otras amenazas.**

¡En nuestra web encontrarás toda la información que necesites para saber más!

Escribe aquí tu información:

Smartphone:

Nombre y apellidos	*Grabaciones de audio*
Direcciones postales	*Videos*
Rutinas y localizaciones	*Datos de salud*
Correo electrónico	*Transporte habitual*
Número de tarjeta de crédito	*Patrones de sueño*
Fotografías	*Comida favorita*
Empresa	*Talla de zapatos*
Número de teléfono	*Citas y fechas clave*
DNI	*Nombre de la mascota*
Facturas, contratos...	*Fecha de nacimiento*
Datos de nuestros contactos	*Lugares visitados*
Mensajes privados	*Entidad bancaria*
Usuarios y contraseñas	*Gustos e intereses para ocio*
Búsquedas de Internet	*Redes sociales*
Archivos y documentos	
Tiendas online favoritas	

Ordenador:

Nombre y apellidos	*Grabaciones de audio*
Direcciones postales	*Videos*
Rutinas y localizaciones	*Datos de salud*
Correo electrónico	*Transporte habitual*
Número de tarjeta de crédito	*Patrones de sueño*
Fotografías	*Comida favorita*
Empresa	*Talla de zapatos*
Número de teléfono	*Citas y fechas clave*
DNI	*Nombre de la mascota*
Facturas, contratos...	*Fecha de nacimiento*
Datos de nuestros contactos	*Lugares visitados*
Mensajes privados	*Entidad bancaria*
Usuarios y contraseñas	*Gustos e intereses para ocio*
Búsquedas de Internet	*Redes sociales*
Archivos y documentos	
Tiendas online favoritas	

5. ¡Qué no te estafen!

Experiencia SENIOR

Introducción:

Cada día te expones a una gran cantidad de fraudes y ataques basados en **ingeniería social** de los que no siempre eres consciente. **¿Crees que serías capaz de identificar uno de ellos si lo tuvieses delante?**

En este ejercicio te invitamos a que analices los distintos mensajes y trates de identificar aquellos que consideres fraudulentos.

Tómate tu tiempo, marca aquellos aspectos de las imágenes que te hagan sospechar y toma una decisión.
¡Mucha suerte!

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA PRIMERA 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
OSI Oficina de Seguridad del Internauta

Experiencia SENIOR

Situación 1:

Una notificación llega a tu teléfono móvil. Parece que te ha llegado un correo electrónico.

Opción 1

Asunto: Notificación de seguridad de tu cuenta

RedSocial <notificaciones@RedSocial.es>

RedSocial

Hemos detectado un inicio de sesión de tu cuenta desde un nuevo dispositivo:

- **Dispositivo**: Android X.
- **Hora**: 13:05.

Si has sido tú ignora este correo electrónico.
Si no has sido tú y crees que alguien ha podido acceder a tu cuenta, sigue los siguientes pasos:

1. Accede a tu cuenta a través de la aplicación o la página web oficial.
2. Introduce tus datos de acceso y cambia la contraseña cuanto antes.
3. Si no has activado la verificación en dos pasos, te recomendamos encarecidamente que lo hagas para mejorar la seguridad de tu cuenta. Puedes hacerlo desde las opciones de seguridad.

Y recuerda, desde tu RedSocial nunca te solicitaremos tus datos de inicio de sesión.

Saludos

Opción 2

Asunto: ¡Hemos detectado actividad sospechosa en tu cuenta!

Tubanko <notificaciones@Tubanka.com>

¡Alerta! Se ha notficado un intento de inicio de sesión sospechoso desde un dispositivo y país de origen irregular:

- **Dispositivo:** AndrOid X.
- **País**: Thailand.
- **Hora**: 03:15

Se recomienda hacer clic en el siguiente enlace y cambiara las credenciales de login lo antes posible para evitar cargos no autorizados desde su cuenta. ¡Rápido!

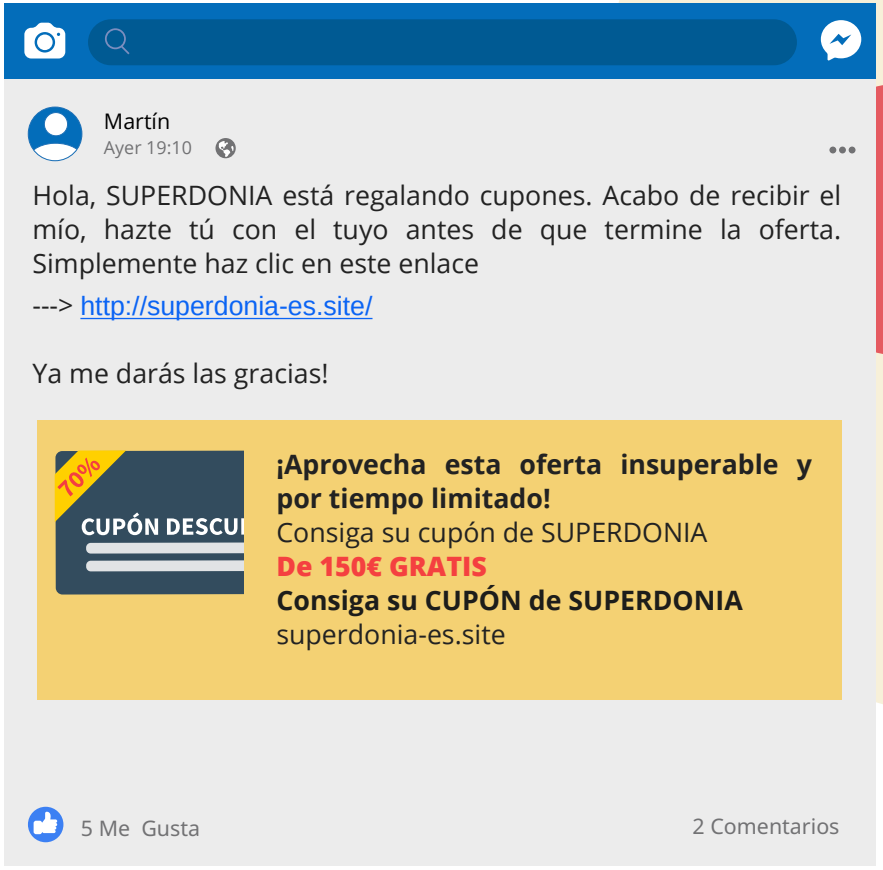
LINK: http://12xRedsoc.com

Experiencia SENIOR

Situación 2:

Ves una publicación sobre una promoción en la red social de uno de tus contactos:

Opción 1

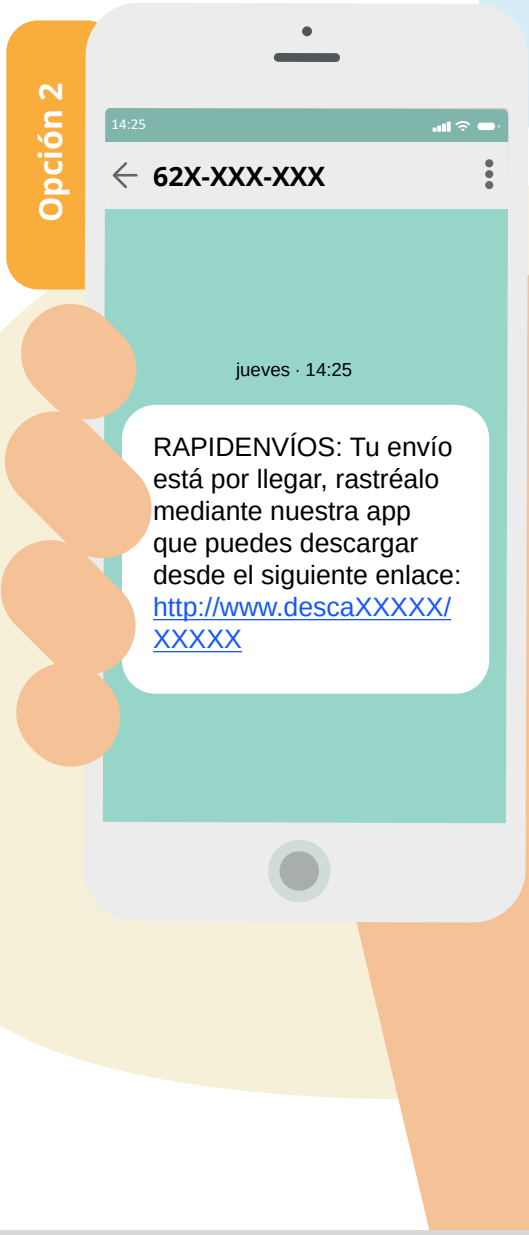


Opción 2

Experiencia SENIOR

Situación 3:

Estás tranquilamente echando un vistazo a tu teléfono móvil, cuando de pronto recibes un SMS:



Experiencia SENIOR

Situación 4:

Estás a punto de salir de casa, cuando tu teléfono empieza a sonar. Parece que se trata de una llamada...

Hola, buenas tardes. Le llamamos desde el departamento de seguridad y prevención de TUBANCO. El motivo es que hemos detectado algunos movimientos sospechosos de su cuenta vinculados a una de sus tarjetas de crédito y necesitamos confirmar con usted unos datos.

Por favor, dígame dígito a dígito su DNI.

Es 30-XX-XX-XX-X.

Muy bien, y los dígitos de su tarjeta de crédito.

Pues es XXXX-XXXXX-XXXXX-XX

Necesitamos también la fecha de caducidad y el código CVV que aparece en la parte trasera de la tarjeta:

Es XX/XX y XXX.

Muy bien, gracias por su colaboración. Parece que era una falsa alarma, si hay alguna otra novedad le mantendremos informado.

Experiencia SENIOR

Soluciones:

(Situación 1)

Comprueba si hubieras actuado bien o no:

Email fraudulento

Asunto:

un **asunto alarmante o de urgencia puede alertarnos** sobre un correo **fraudulento**.

Nombre:

nuestro banco siempre **se dirigiría a nosotros por nuestro nombre**, **no de forma genérica** usando expresiones del tipo “Estimado usuario”.

Enlace:

si pasamos **el cursor sobre el enlace del mensaje y vemos que no coincide con la URL original de nuestro banco** o de la entidad legítima que esté contactando supuestamente con nosotros, desconfiaremos.

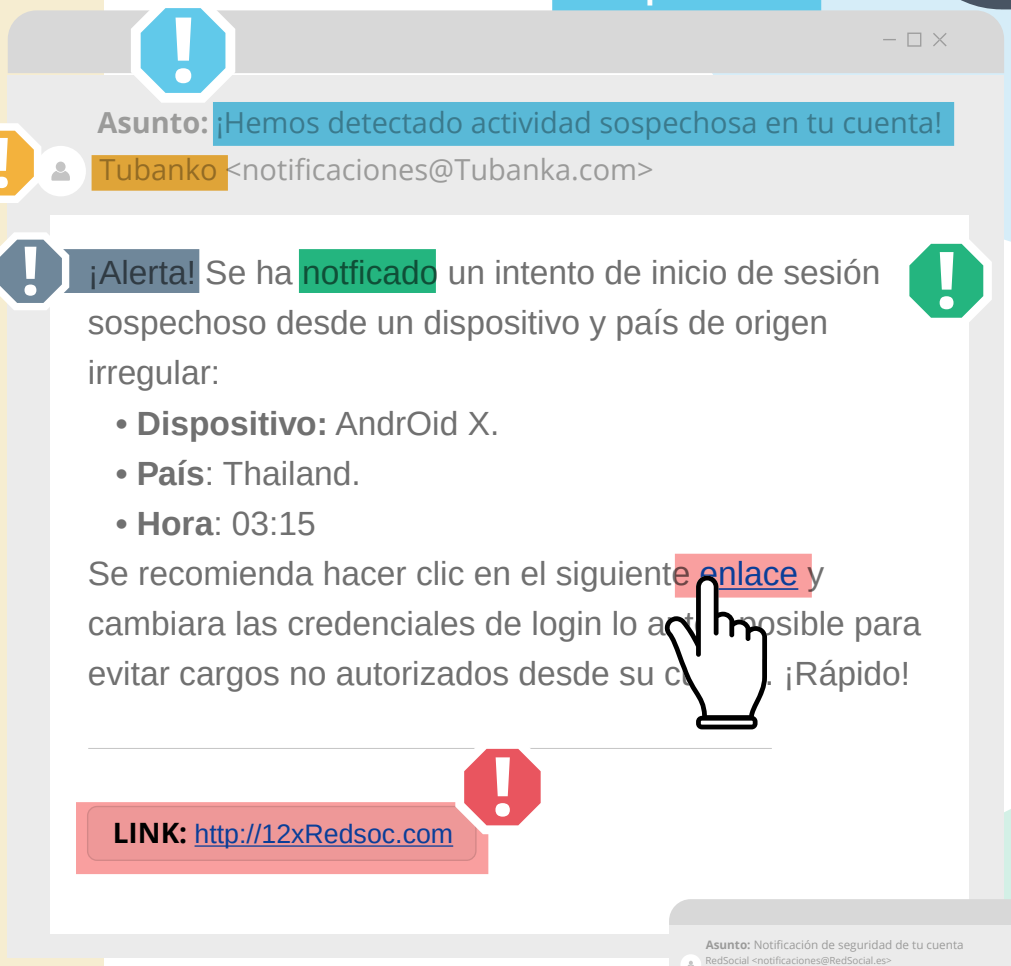
Remitente:

si no coincide con la entidad que dice ser, **difiere del correo original de dicha entidad o contacto** o contiene errores o caracteres extraños, **lo más probable es que se trate de un fraude.**

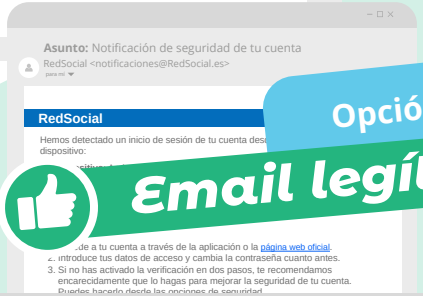
Mensaje:

si está mal redactado, **contiene errores ortográficos y el mensaje es alarmista o impactante** para que llevemos a cabo una acción rápidamente, **debemos sospechar.**

Opción 2



Opción 1



Email legítimo

Experiencia SENIOR

Soluciones:

(Situación 2)

Comprueba si hubieras actuado bien o no:

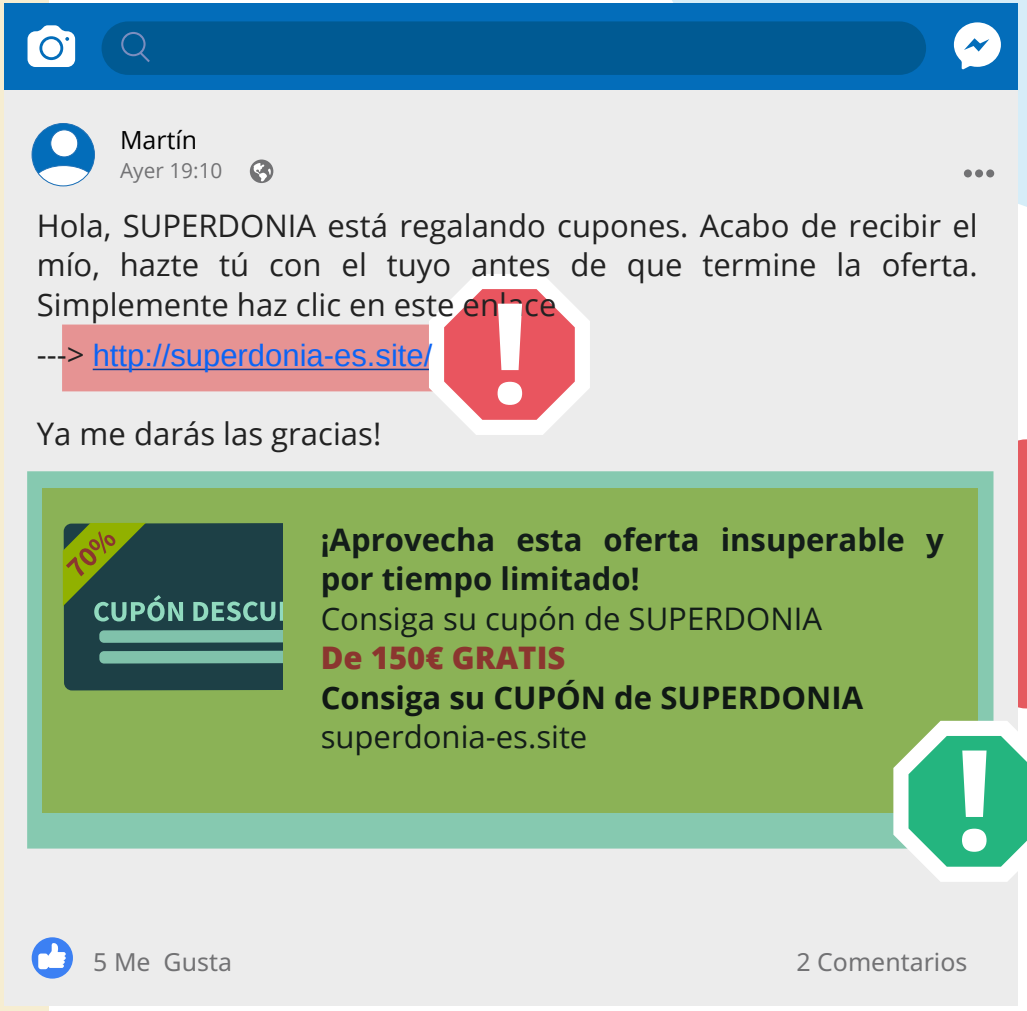
Publicación fraudulenta

Enlace:

si la URL de la **página web comienza por "http", será mejor desconfiar,** pues los datos que ingresemos no estarán protegidos y pueden acabar en malas manos. Probablemente nos redirija a un formulario que nos solicite muchos de nuestros datos personales (teléfono, correo, dirección...).

Mensaje:

es habitual utilizar **mensajes muy llamativos, invitándonos a disfrutar de una gran oportunidad irrechazable**. Esto es así para que no pensemos más allá del titular y sigamos las indicaciones para conseguir el beneficio prometido.



Opción 1

Experiencia SENIOR

Soluciones:

(Situación 2)

Comprueba si hubieras actuado bien o no:

Mensaje fraudulento

Remitente:

se trata de un número desconocido que se hace pasar por el servicio técnico de WhatsApp. **No es habitual a día de hoy que dicha empresa contacte con nosotros** de esta manera para hacer ningún tipo de comunicado.

Mensaje:

el mensaje **contiene errores ortográficos** que dan a entender que es una mala traducción o un texto escrito con prisas. Errores **que una empresa con cierta reputación jamás cometería.**

Código:

si compartimos el código que recibimos por SMS, estaremos permitiendo que **otro usuario pueda configurar la aplicación en un dispositivo desconocido, perdiendo el acceso a nuestra cuenta**. ¡No debemos facilitar a nadie este tipo de datos!

Opción 2

Experiencia SENIOR

Soluciones:

(Situación 3)

Comprueba si hubieras actuado bien o no:

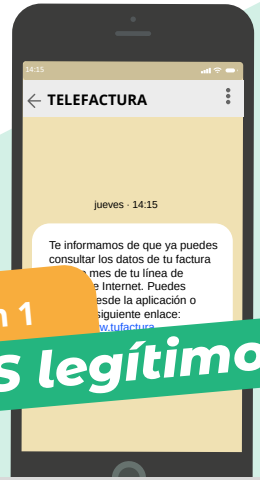
SMS fraudulento

Mensaje:

es habitual utilizar **mensajes muy llamativos, invitándonos a disfrutar de una gran oportunidad irrechazable**. Esto es así para que no pensemos más allá del titular y sigamos las indicaciones para conseguir el beneficio prometido.

Enlace:

Si la URL de **la página web comienza por "http", será mejor desconfiar**, pues los datos que ingresemos no estarán protegidos y pueden acabar en malas manos. Probablemente nos redirija a un formulario que nos solicite muchos de nuestros datos personales (teléfono, correo, dirección...).



Opción 1

sms legítimo

Soluciones:

(Situación 4)

Comprueba si hubieras actuado bien o no:

Llamada fraudulenta

Remitente:

El remitente dice pertenecer al servicio técnico de nuestra entidad bancaria. Sin embargo, **no se dirige a nosotros por nuestro nombre y nos pide información que ya debería tener.**

Información:

entre los datos solicitados se encuentran todos los asociados a nuestra tarjeta de crédito. **Los bancos no solicitan todos esos detalles por teléfono para ningún fin**, más aún sin ningún motivo aparente. Si tenemos dudas, será mejor acudir directamente a la sucursal más cercana.

Experiencia SENIOR

Hola, buenas tardes. Le llamamos desde el departamento de seguridad y prevención de TUBANCO. El motivo es que hemos detectado algunos movimientos sospechosos de su cuent vinculados a una de sus tarjetas de crédito y necesitamos confirmar con usted unos datos.

Vaya... ¿Qué necesitan?

Por favor, dígame dígito a dígito su DNI.

Es 30-XX-XX-XX-X.

Muy bien, y los dígitos de su tarjeta de crédito.

Pues es XXXX-XXXXX-XXXXX-XX

Necesitamos también la fecha de caducidad y el código CVV que aparece en la parte trasera de la tarjeta:

Es XX/XX y XXX.

Muy bien, gracias por su colaboración. Parece que era una falsa alarma, si hay alguna otra novedad le mantendremos informado.

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA PRIMERA 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
OSI Oficina de Seguridad del Internauta

6. Identifica bulos y noticias falsas

Experiencia SENIOR

Introducción:

Seguro que ya sabes que no todo lo que vemos en Internet tiene que ser cierto. **Las *Fake news*, los bulos y otros fraudes abundan en la Red.**

Por este motivo, queremos proponerte la siguiente actividad donde deberás **analizar diferentes noticias** y decidir si se tratan de una información falsa o no.
Míralas detenidamente, toma una decisión y comprueba la solución al final del ejercicio.

Presta atención, analiza la noticia y marca tu respuesta debajo de la misma o en una hoja de papel. Cuando hayas terminado, podrás comprobar tus respuestas.

¡Pon a prueba tu mirada crítica y no te dejes engañar!

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA PRIMERA 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
OSI Oficina de Seguridad del Internauta

6. Identifica bulos y noticias falsas

Experiencia SENIOR

Noticia 1:
WhatsApp comenzará a ser de pago.

"El sábado WhatsApp será facturado. Si tienes al menos 10 contactos enviales este mensaje. Así verán que eres un asiduo utilizador y tu logo se volverá azul y quedará gratuito. Se ha hablado de ello hoy en la prensa. WhatsApp costará 0,01 euro por mensaje. Envía este mensaje a 10 personas. Cuando lo hagas la luz se volverá azul de lo contrario Whatsapp activará la facturación"

VERDADERA **FALSA**

Experiencia SENIOR

Noticia 2:
La NASA descubre un universo paralelo

NASA /

Científicos de la NASA hallan evidencias de un universo paralelo donde el tiempo va hacia atrás

Científicos de la NASA han encontrado partículas que podrían explicarse con la existencia de un universo paralelo donde las leyes de la física serían al revés.

EN RESUMEN

- En ese universo las leyes de la física serían totalmente contrarias a las que conocemos
- Este descubrimiento sigue a debate dentro de la comunidad científica y ya ha generado diversas opiniones

VERDADERA **FALSA**

Haz **clic o copia la URL en tu navegador** para leer la noticia completa

https://archive.li/8rr4l

Experiencia SENIOR

Noticia 3:

Un perro con apariencia de león genera varios avisos para la Policía Local de Molina de Segura

VERDADERA **FALSA**

Experiencia SENIOR

Noticia 4:

Lidl regala un robot de cocina al participar en una encuesta

Felicitaciones!!

Hoy, 29 de septiembre de 2020, has sido seleccionado al azar para participar en esta encuesta. Solo te tomará un minuto y puedes recibir un premio: ¡un Silvercrest Monsieur Cuisine Connect!

VERDADERA

FALSA

Soluciones:

¡Buen trabajo! Ahora comprueba tus respuestas con nuestras soluciones y las evidencias y pruebas que te indicamos. ¿Has sido capaz de identificarlas todas?

Publicación falsa

Evidencias:

Como muchas otras cadenas de mensajes, **la mayoría de ellas son falsas.**
Comprobémoslo paso a paso:

- Primero, podemos **contrastar con la fuente oficial.** En este caso, revisaremos el blog oficial de WhatsApp en busca de alguna función de pago, pero no hay ninguna
  https://blog.whatsapp.com/?lang=eso

- **Comprobar en Internet otras fuentes que contrasten la noticia,** como sus canales en redes sociales: https://twitter.com/whatsapp?lang=es. No encontramos noticias al respecto. Si lo hacemos, comprobaremos que se trata de un bulo que circula por la aplicación.

Experiencia SENIOR

Noticia 1

WhatsApp comenzará a ser de pago.

Experiencia SENIOR

Soluciones

Publicación falsa

Evidencias:

En ocasiones, los redactores de los artículos **deciden mezclar o modificar un poco las palabras de un autor** para hacer la noticia más impactante y atraer a los lectores.
Comprobémoslo paso a paso:

- Primero, **analizaremos la URL** de la web para ver si dispone de certificado y si comienza con https:
(Haz click aquí para ver la noticia completa)

- Luego, **comprobaremos las fuentes** incluidas en la publicación para analizar si son fiables. Podemos hacer una búsqueda rápida en Internet para localizar las declaraciones del autor en la entrevista original:
(Haz click aquí para ver la noticia completa)

- Finalmente, **analizaremos el cuerpo de la noticia** y cotejaremos con la fuente original.

En este caso, las palabras del autor fueron **modificadas para generar la viralización de esta noticia.** Sin embargo, si investigamos sobre el estudio citado en el artículo o buscamos al autor, encontraremos rápidamente que se trata de un bulo.

Noticia 2

La NASA descubre un universo paralelo


NASA /

Científicos de la NASA hallan evidencias de un universo paralelo donde el tiempo va hacia atrás

Científicos de la NASA han encontrado partículas que podrían explicarse con la existencia de un universo paralelo donde las leyes de la física serían al revés.

EN RESUMEN

- En ese universo las leyes de la física serían totalmente contrarias a las que conocemos
- Este descubrimiento sigue a debate dentro de la comunidad científica y ya ha ge… s opiniones

Soluciones

Publicación verdadera

Evidencias:

Esta noticia fue publicada a través de redes sociales por la cuenta de la Policía Local del lugar. **Podría ser cierto, o una cuenta falsa.**
Comprobémoslo paso a paso:

- Si buscamos en la red social, veremos que la **publicación sigue estando activa**:
  (Haz click aquí para ver la noticia completa)

- Además, la cuenta desde la que se emitió es la **cuenta oficial** de la Policía Local de Molina de Segura:
  (Haz click aquí para ver la noticia completa)

- Una búsqueda en Internet sobre el titular de la noticia nos revelará **varias fuentes que apoyan la noticia**:
  (Haz click aquí para ver la noticia completa)

La Policía Local de Molina de Segura no tuvo más remedio que elaborar este tweet para calmar a los ciudadanos del lugar y que generó varias respuestas en tono de humor.

Experiencia SENIOR

Noticia 3

Un perro con apariencia de león genera varios avisos para la Policía Local de Molina del segura

Soluciones

Publicación falsa

Evidencias:

Las publicaciones de concursos y promociones en redes sociales **son muy variadas y abundan**, pero de vez en cuando **se cuela algún fraude**. Comprobémoslo paso a paso:

- Primero, **analizaremos la URL original**: ***spainrealty.info.*** Como podemos comprobar, no tiene nada que ver con la empresa Lidl.

- Luego, podremos realizar una **búsqueda en Internet** sobre la promoción para darnos cuenta de que aparecen varias fuentes alertando sobre el fraude: (Haz click aquí para ver la noticia completa)

En esta ocasión, **el timo estaba en conseguir que los lectores hiciesen clic en el enlace y compartiesen sus datos** personales pensando que recibirían el premio.

Experiencia SENIOR

Noticia 4

Lidl regala un robot de cocina al participar en una encuesta

Experiencia SENIOR

Introducción:

A todos **nos gusta disfrutar de los beneficios que nos ofrecen las redes sociales** a la hora de compartir momentos con nuestros familiares y conocidos. Para poder seguir haciéndolo, **es importante que también seamos capaces de identificar posibles fraudes o malas prácticas** que puedan ser negativas para nuestra privacidad.

Para prepararnos y poner en práctica nuestras habilidades, **hemos creado una serie de actividades que te ayudarán a identificar cualquier amenaza.**

¡Ten cuidado con dónde accedes y qué publicaciones compartes en tus redes!

Experiencia SENIOR

Ejercicio 1:

Compartir momentos y publicaciones en redes sociales u otras plataformas es siempre divertido y **nos ayuda a estar más cerca de nuestros amigos y familiares.** Sin embargo, **debemos tener cuidado** con qué compartimos, reenviamos o a dónde accedemos.

Revisa las siguientes publicaciones y únelas o escribe la opción que te parezca correcta:	Opción (A, B, C):
1. Reenviar una cadena de mensajes con un enlace a una noticia que no he contrastado en fuentes oficiales.	
2. Compartir una foto de mis nietos en su cumpleaños.	
3. Subir una foto de mi factura de la luz debido a un error en la misma.	
4. Subir una foto de mis últimos movimientos bancarios para pedir ayuda por unos cargos desconocidos.	
5. Darle *like* o 'me gusta' a una foto de uno de mis contactos.	
6. Agregar a un antiguo compañero del trabajo.	
7. Agregar a un contacto nuevo que no conocemos pero que quiere ser nuestro amigo.	
8. Reenviar una cadena de mensajes para evitar que tu aplicación se vuelva de pago.	
9. Etiquetar y compartir cada concurso o promoción que veas.	
10. Pedir o compartir fotografías íntimas con otros usuarios.	

A Bajo ningún concepto

B Solo bajo ciertas condiciones

C Sí, sin ningún problema

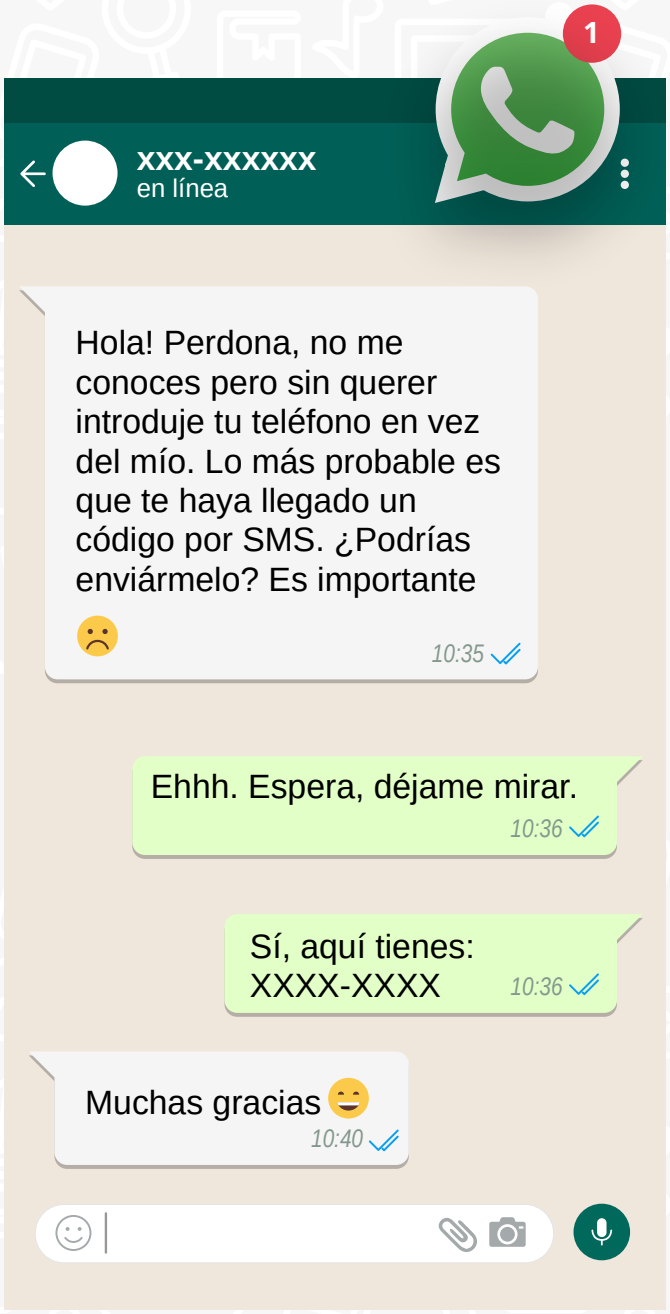
Experiencia SENIOR

Escena 1

Ejercicio 2:

En ocasiones **nos exponemos a situaciones, mensajes y publicaciones que pueden ser un riesgo para nosotros,** nuestra privacidad o la de nuestros contactos.

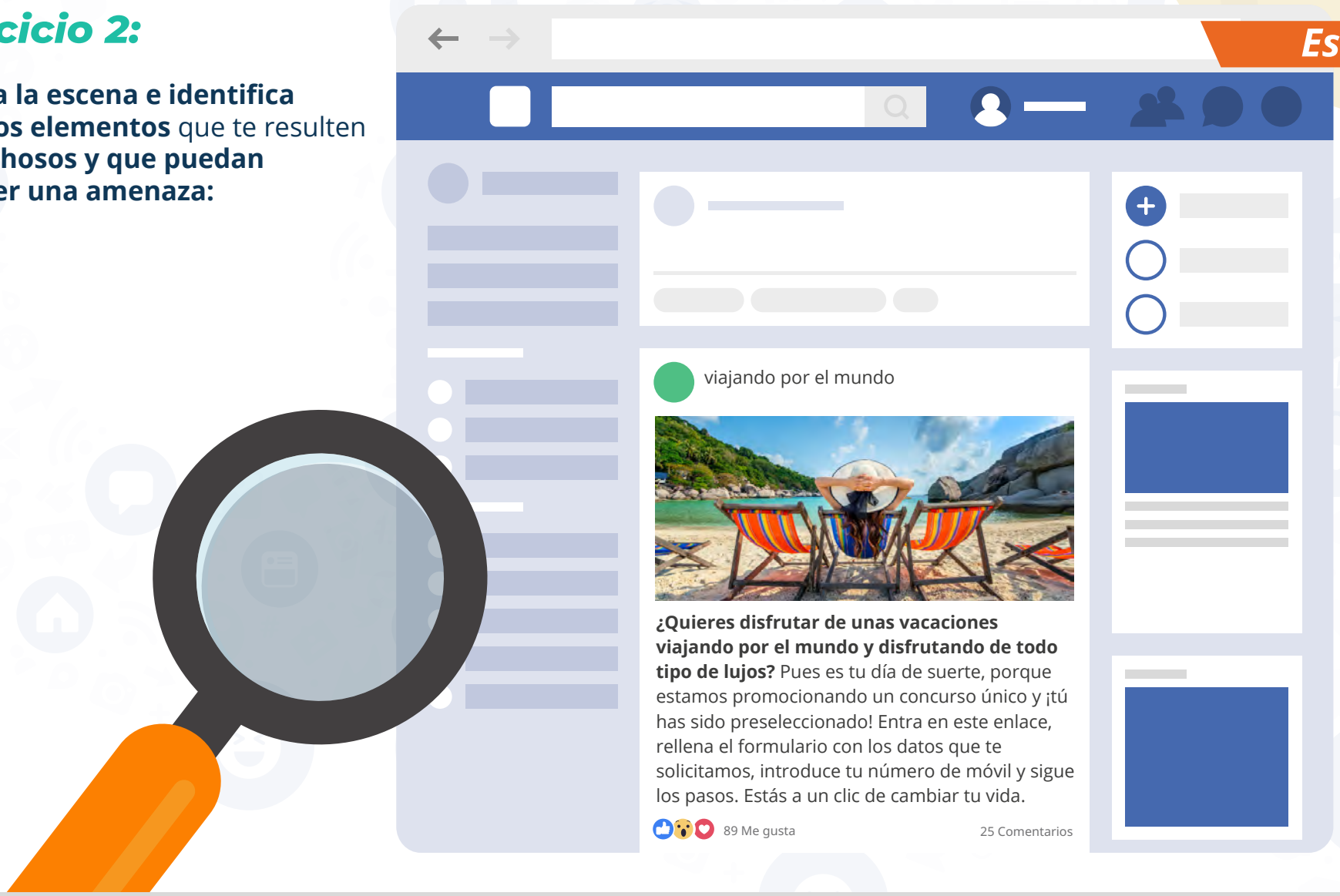
En esta actividad **te proponemos que analices tres escenas para que identifiques aquellos elementos que te resulten sospechosos y que puedan suponer una amenaza:**



Experiencia SENIOR

Ejercicio 2:

Analiza la escena e identifica aquellos elementos que te resulten **sospechosos y que puedan suponer una amenaza:**



Experiencia SENIOR

Ejercicio 2:

Analiza la escena e identifica aquellos elementos que te resulten **sospechosos y que puedan suponer una amenaza:**

Escena 3

Experiencia SENIOR

Soluciones:

Ejercicio 1

Es hora de comprobar si estás preparado para moverte seguro a través de las redes sociales, o si por el contrario es mejor que des otro repaso a los recursos de la campaña:

Comprueba si estás preparado para moverte seguro a través de las redes sociales:	Opción (A, B, C):
1. Reenviar una cadena de mensajes con un enlace a una noticia que no he contrastado en fuentes oficiales.	A
2. Compartir una foto de mis nietos en su cumpleaños.	C
3. Subir una foto de mi factura de la luz debido a un error en la misma.	A
4. Subir una foto de mis últimos movimientos bancarios para pedir ayuda por unos cargos desconocidos.	A
5. Darle *like* o 'me gusta' a una foto de uno de mis contactos.	B
6. Agregar a un antiguo compañero del trabajo.	B
7. Agregar a un contacto nuevo que no conocemos pero que quiere ser nuestro amigo.	C
8. Reenviar una cadena de mensajes para evitar que tu aplicación se vuelva de pago.	A
9. Etiquetar y compartir cada concurso o promoción que veas.	C
10. Pedir o compartir fotografías íntimas con otros usuarios.	C

A Bajo ningún concepto

B Solo bajo ciertas condiciones

C Sí, sin ningún problema

Experiencia SENIOR

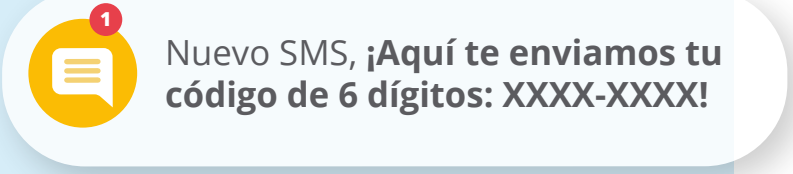
Soluciones:

Ejercicio 2

Escena 1

Se trata de un fraude muy común, donde los ciberdelincuentes **introducirán nuestro número de teléfono al instalar una famosa aplicación de mensajería en otro dispositivo.**

Al hacerlo, **nos llegará el SMS con el código, y si lo compartimos con los atacantes, perderemos el acceso a nuestra aplicación,** siendo víctimas de un secuestro de nuestra aplicación de mensajería.



Experiencia SENIOR

Soluciones:

Ejercicio 2

Escena 2

Muchos de los anuncios que vemos en redes sociales son reales y legítimos. Sin embargo, **algunos tratan de engañarnos con premios, descuentos o promociones muy atractivas.** Si nos fijamos, en el mensaje nos indican que ya hemos sido preseleccionados sin siquiera haber participado.

Además, **si hiciésemos clic en el enlace, accederíamos a un formulario donde nos preguntarían sobre muchos de nuestros datos personales.** El teléfono móvil pueden utilizarlo también para enviarnos publicidad o suscribirnos a algún servicio de tarificación especial sin nuestro consentimiento.

Experiencia SENIOR

Soluciones:

Ejercicio 2

Escena 3

A través de redes sociales también son frecuentes fraudes donde desconocidos tratan de ofrecer sus servicios o se hacen pasar por otras personas o entidades.

En este caso, **vemos que se presenta como una persona solidaria que quiere ayudarnos ofreciéndonos unos préstamos a muy bajo interés**, asequibles para cualquiera. Podemos ver que el **texto aparece mal redactado,** posiblemente, derivado de un traductor automático.
Lo más probable es que **si accediésemos, nos solicitase unos pagos previos a modo de gastos administrativos para luego desaparecer.**

8. Haz tus compras online más seguras

Experiencia ENIOR

Introducción:

Cuando se trata de comprar **Internet, siempre es una alternativa muy interesante, gracias a sus facilidades y a la cantidad de productos y servicios que puedes encontrar** con una simple búsqueda en cientos de webs online.

Sin embargo, **debes ser cauto, ya que navegando te encontrarás con anuncios y webs fraudulentas**, cuyo único objetivo es engañarte para hacerse con tu dinero o datos personales.

Para evitar estos riesgos, **hemos preparado una serie de actividades que te servirán de entrenamiento** para comprar en la Red con garantías de seguridad.

¡Sigue los pasos indicados, no te dejes engañar y realiza tus compras de forma segura!

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA PRIMERA 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
OSI Oficina de Seguridad del Internauta

Experiencia SENIOR

Ejercicio 1:

Comprar online no tiene por qué suponer un riesgo si sabemos cómo hacerlo de forma segura.

A continuación, verás una serie de **pasos que deberás ordenar** para garantizar que sigues un proceso de compra lógico y seguro; **pero presta atención, el ejercicio contiene algunas trampas**, ya que no todos los pasos que encontrarás corresponden a un proceso de compra segura.

Escribe el **orden correcto en el recuadro** y busca **qué pasos deberás eliminar**:

1. ***Conectar*** el dispositivo a una ***conexión a Internet segura.*** ☐

2. Hacer ***clic en el anuncio que me ha llegado por correo.*** ☐

3. Realizar la ***búsqueda en Internet del producto, tienda o servicio.*** ☐

4. ***Revisar el certificado de seguridad*** para comprobar que la web es de la empresa o servicio que dice ser. ☐

5. ***Comprobar que la web*** cifra la información intercambiada con ella ***(HTTPS)***. ☐

6. Comprobar que ***la URL comienza por HTTP.*** ☐

7. ***Echar un vistazo*** al aspecto general de la página web: ***calidad de las imágenes, redacción de los textos, precios, etc.*** ☐

8. ***Revisar*** que la web ***incluye información sobre la empresa***: domicilio fiscal; métodos de contacto; aviso legal; políticas de privacidad, envío, cancelación o devolución de pedidos, etc. ☐

9. ***Consultar las valoraciones y opiniones*** de otros compradores. ☐

10. Mirar la descripción y demás ***detalles del producto en el que se está interesado.***

11. Realizar el ***pago mediante MoneyGram, Western Union o transferencia bancaria.*** ☐

12. Cerciorarse de que el ***resumen del pedido es correcto y especifica claramente el desglose de todos los gastos.*** ☐

13. Revisar que los ***métodos de pago que admite la web son seguros: pasarela de pago del banco, PayPal, Android Pay, Apple Pay, Bizum, etc.*** ☐

14. ***Comprobar*** que he recibido la ***factura y un número de seguimiento del pedido.*** ☐

15. ***Revisar los movimientos bancarios*** para confirmar que el cargo efectuado es correcto. ☐

Experiencia SENIOR

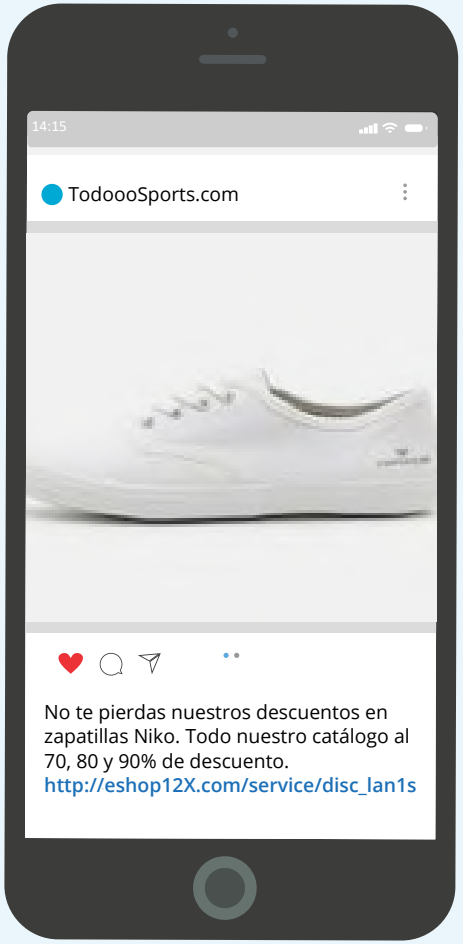
Ejercicio 2:

Revisa los casos y **averigua si estás ante un fraude o no.**

Marca la opción correcta y señala sobre el papel qué aspectos te han llevado a la conclusión:

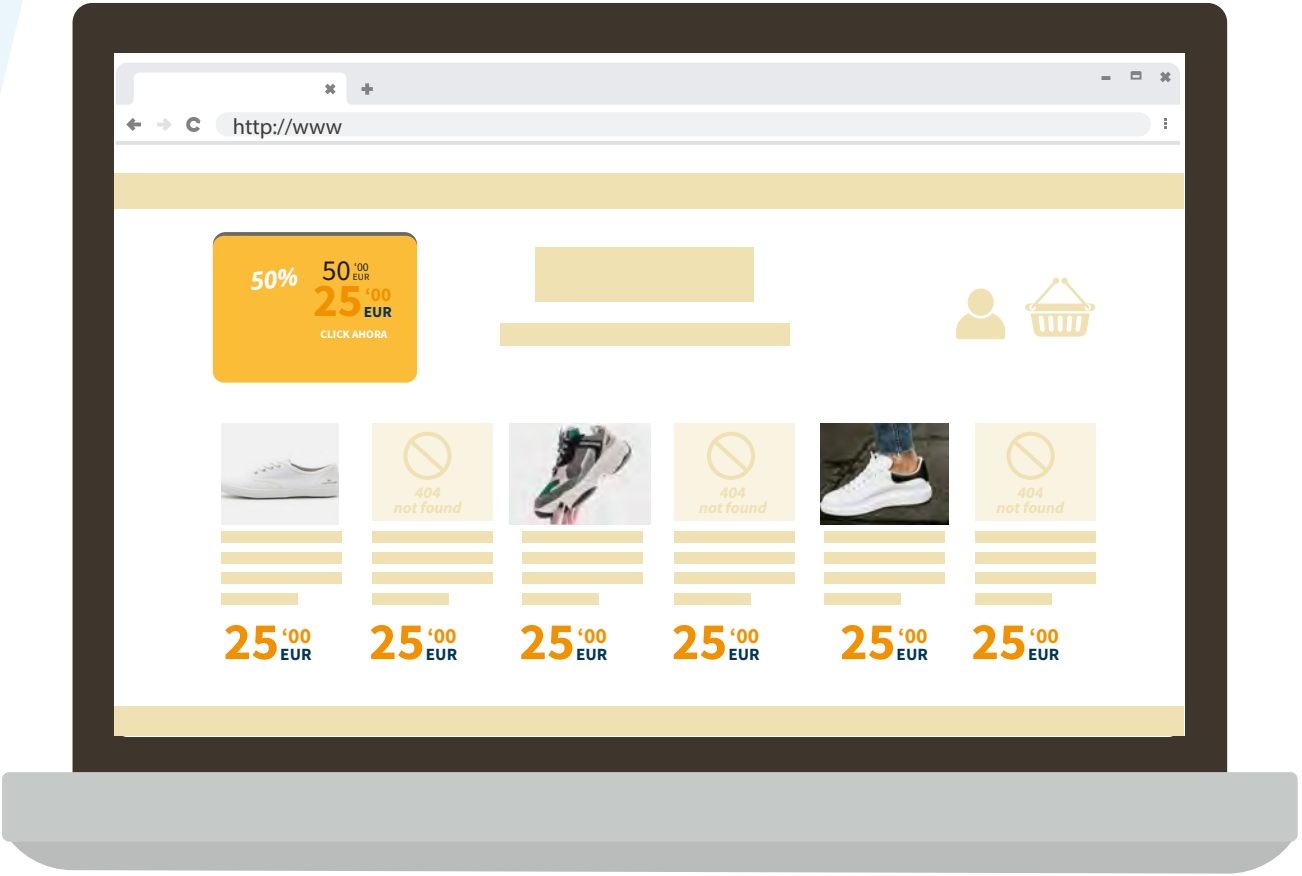
Caso 1

FRAUDE ☐ NO FRAUDE ☐



Caso 2

FRAUDE ☐ NO FRAUDE ☐



Experiencia SENIOR

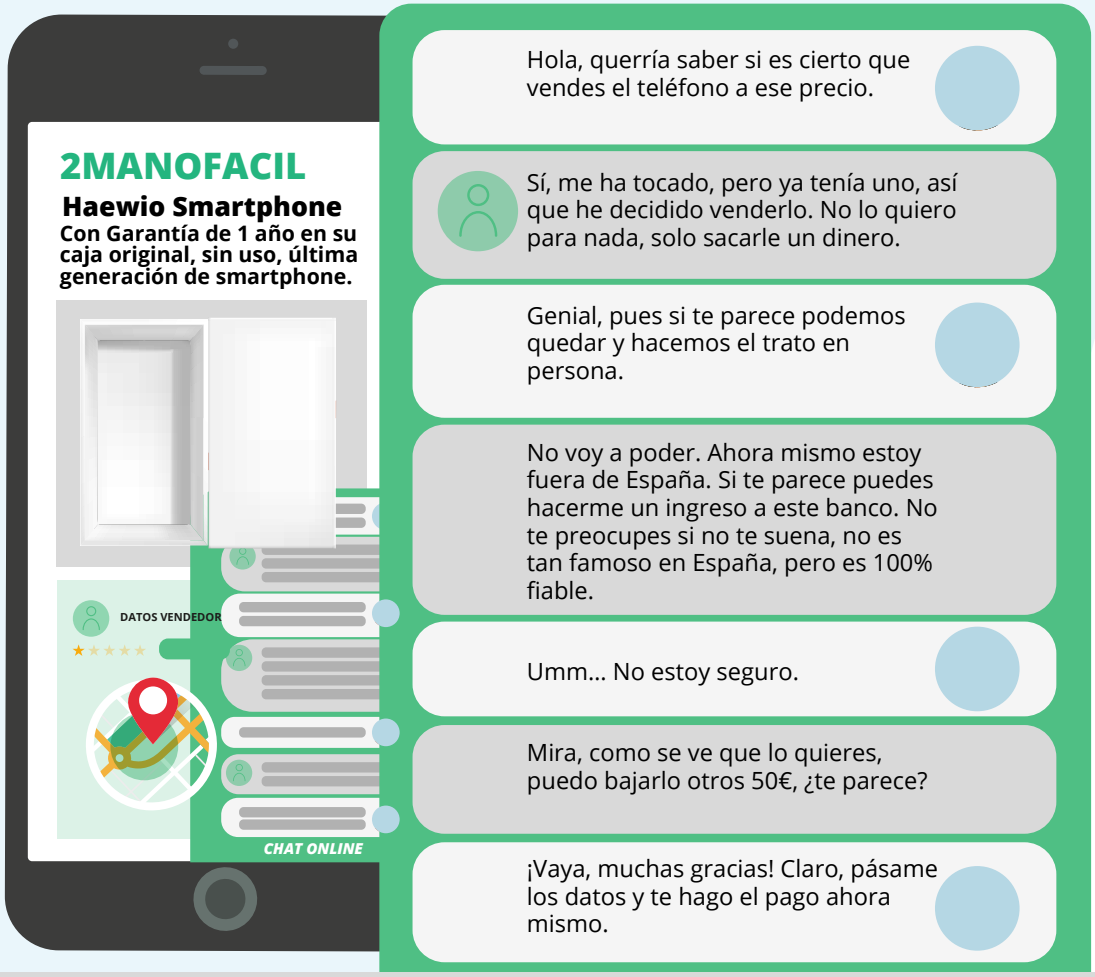
Ejercicio 2:

Revisa los casos y **averigua si estás ante un fraude o no.**

Marca la opción correcta y señala sobre el papel qué aspectos te han llevado a la conclusión:

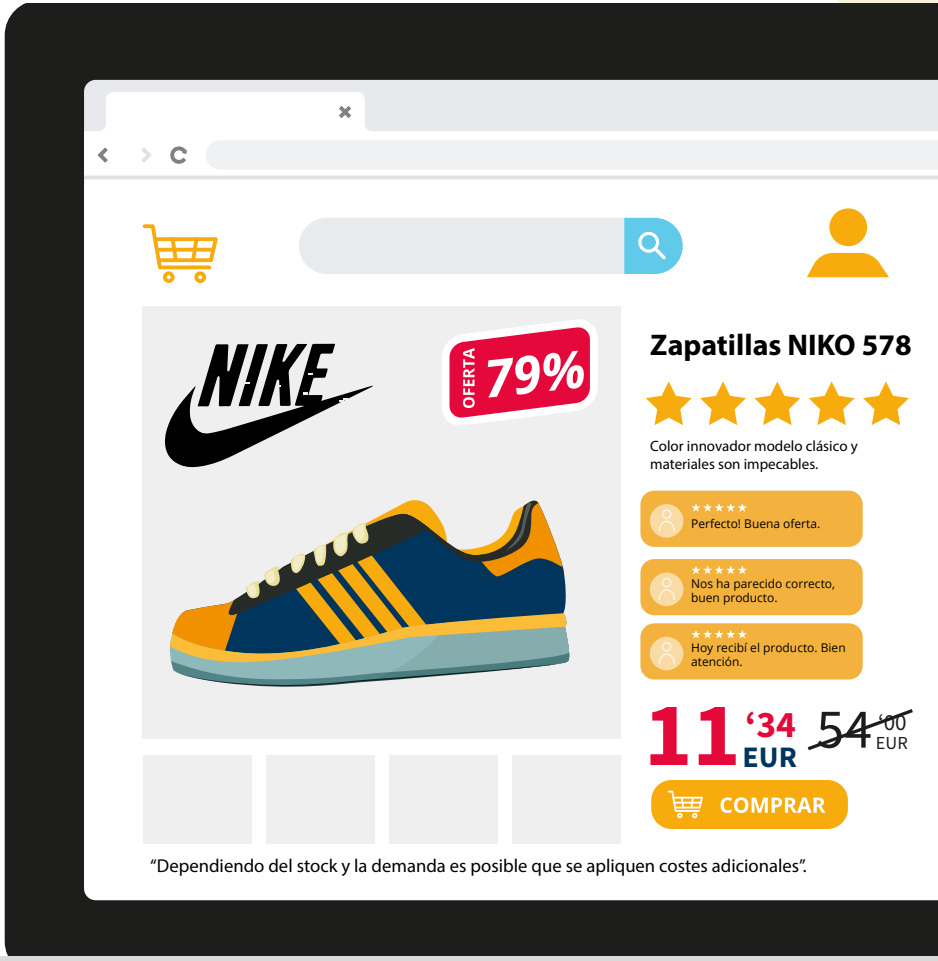
Caso 3

FRAUDE ☐ NO FRAUDE ☐



Caso 4

FRAUDE ☐ NO FRAUDE ☐



Experiencia SENIOR

Soluciones:

¡Muy bien! Comprueba ahora tus respuestas con las soluciones y **averigua si estás preparado para realizar tus compras online.** No te preocupes, nuestros recursos siempre estarán ahí para ayudarte.

Ejercicio 1

Estos son los pasos que debes seguir para realizar una compra online de forma segura.
No te preocupes si no lo has ordenado exactamente igual. Algunos pasos, como el 3, 4 y 5, pueden intercambiar posiciones:

Lista de orden correcto: ✓

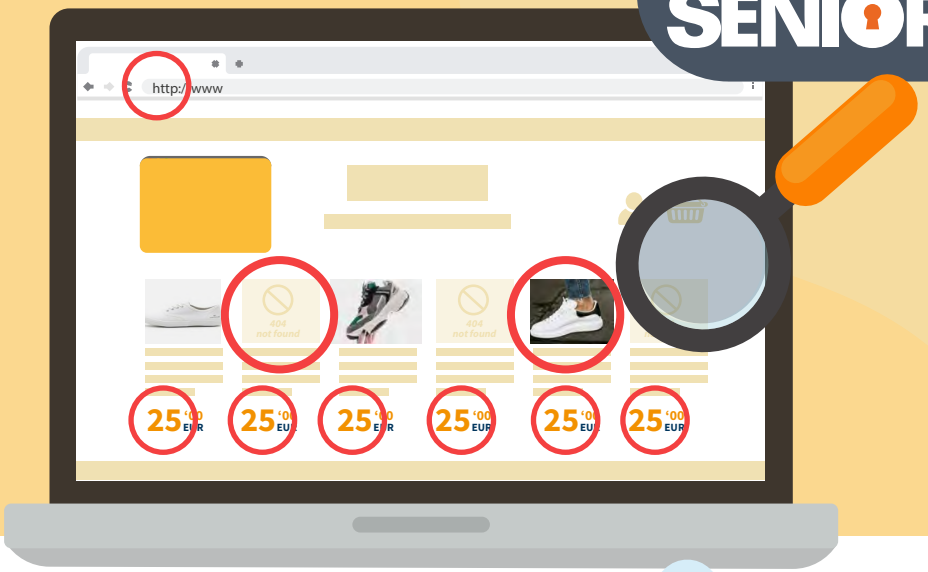
1. ***Conectar*** el dispositivo a una ***conexión a Internet segura.*** — 1
2. Hacer ***clic en el anuncio que me ha llegado por correo.*** — ✗
3. Realizar la ***búsqueda en Internet del producto, tienda o servicio.*** — 2
4. ***Revisar el certificado de seguridad*** para comprobar que la web es de la empresa o servicio que dice ser. — 3
5. ***Comprobar que la web*** cifra la información intercambiada con ella ***(HTTPS)***. — 4
6. Comprobar que ***la URL comienza por HTTP.*** — ✗
7. ***Echar un vistazo*** al aspecto general de la página web: ***calidad de las imágenes, redacción de los textos, precios, etc.*** — 5
8. ***Revisar*** que la web ***incluye información sobre la empresa***: domicilio fiscal; métodos de contacto; aviso legal; políticas de privacidad, envío, cancelación o devolución de pedidos, etc. — 6
9. ***Consultar las valoraciones y opiniones*** de otros compradores. — 7
10. Mirar la descripción y demás ***detalles del producto en el que se está interesado.*** — 8
11. Realizar el ***pago mediante MoneyGram, Western Union o transferencia bancaria.*** — ✗
12. Cerciorarse de que el ***resumen del pedido es correcto y especifica claramente el desglose de todos los gastos.*** — 9
13. Revisar que los ***métodos de pago que admite la web son seguros: pasarela de pago del banco, PayPal, Android Pay, Apple Pay, Bizum, etc.*** — 10
14. ***Comprobar*** que he recibido la ***factura y un número de seguimiento del pedido.*** — 11
15. ***Revisar los movimientos bancarios*** para confirmar que el cargo efectuado es correcto. — 12

Experiencia SENIOR

Soluciones:

Todos los casos que te hemos presentado tienen elementos que **evidencian que estás ante un posible fraude:**

Ejercicio 2



Caso 1

FRAUDE ☑ NO FRAUDE ☐

Los **anuncios en redes sociales son uno de los medios más utilizados por los ciberdelincuentes** para propagar sus fraudes.

En este caso, podrás ver un anuncio de una tienda online de zapatillas de una famosa marca. Sin embargo, **si prestas atención, verás que la URL no coincide con el nombre de la empresa**, ni dispone de certificado digital para confirmar si la empresa es quien dice ser, ni empieza por "https" que garantice que la información viaja cifrada por la Red.

Caso 2

FRAUDE ☐ NO FRAUDE ☐

Analizar la oferta de productos de una web puede proporcionarte **muchas pistas sobre si es de fiar o no**.

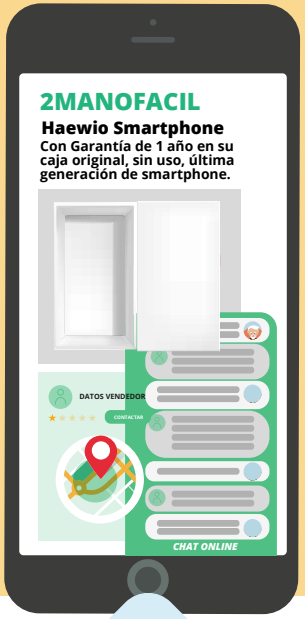
En este caso, los productos presentan el mismo precio en todos ellos. Además, el **aspecto visual de la web deja mucho que desear**, incluso con algunos productos sin imagen. Asimismo, **la URL indica** que no es una web segura al **no contar con "https" ni certificado digital.**

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA PRIMERA 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
OSI Oficina de Seguridad del Internauta

Soluciones:

Todos los casos que te hemos presentado tienen elementos que **evidencian que estás ante un posible fraude:**

Ejercicio 2



Caso 3

FRAUDE ☑ NO FRAUDE ☐

Algunos vendedores **intentan engañar a los usuarios utilizando como gancho precios muy bajos y atractivos.**

En este ejemplo, **el vendedor intentará que su víctima le haga la transacción a un banco extranjero** para que, cuando quiera recuperar su dinero al ver que el producto no llega, le sea **mucho más difícil hacerlo y comunicarse con él**. En otras ocasiones, utilizan otros métodos de pago no recomendables para transacciones online, como empresas de transferencia instantánea tipo Western Union. **También es habitual que intenten seguir la conversación fuera de la plataforma de compraventa para no dejar rastro de su estafa.**

Caso 4

FRAUDE ☑ NO FRAUDE ☐

A veces **es difícil identificar aquellas tiendas online que son fraudulentas**, pero si prestas atención a sus productos, podrás hacerlo.

En este caso, **podrás ver cómo tienes un producto con una gran rebaja, pero con una descripción mínima, pocas imágenes y de mala calidad.** Además, si prestas atención a **los comentarios** de otros compradores, verás que parecen **poco fiables y realizados por un bot** (máquina), a juzgar por los textos mal redactados

Experiencia SENIOR

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA PRIMERA 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

OSI Oficina de Seguridad del Internauta