

Ejercicios y actividades prácticas



Experiencia
SENIOR



5. ¡Qué no te estafen!

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?**

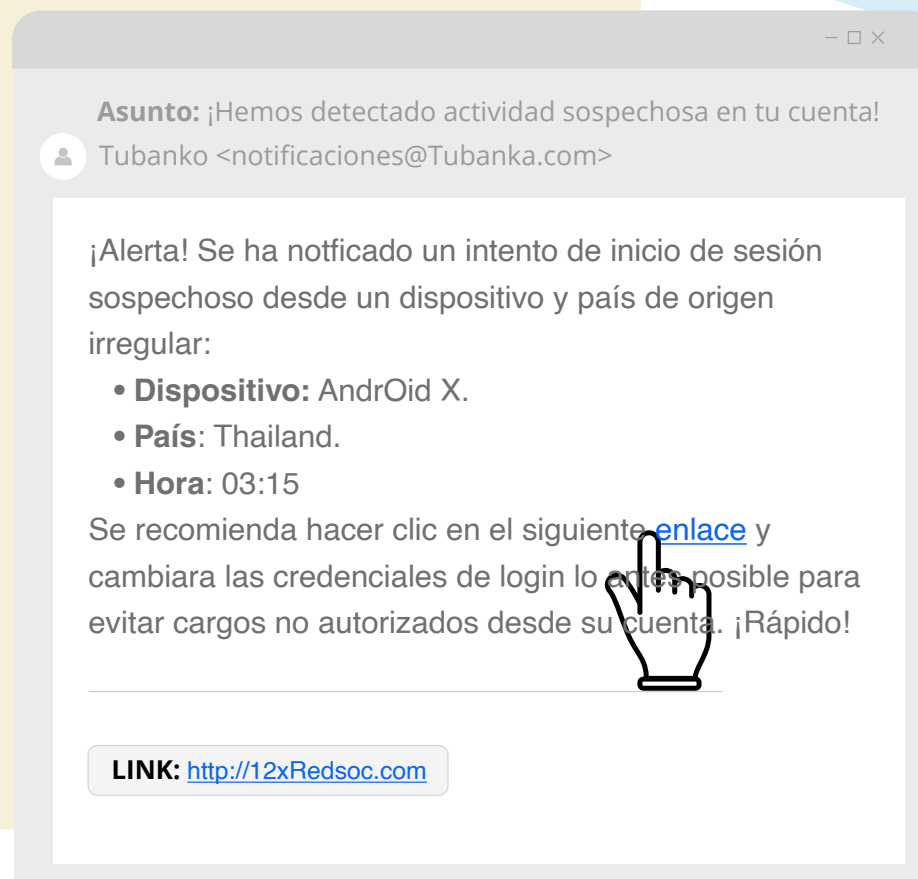
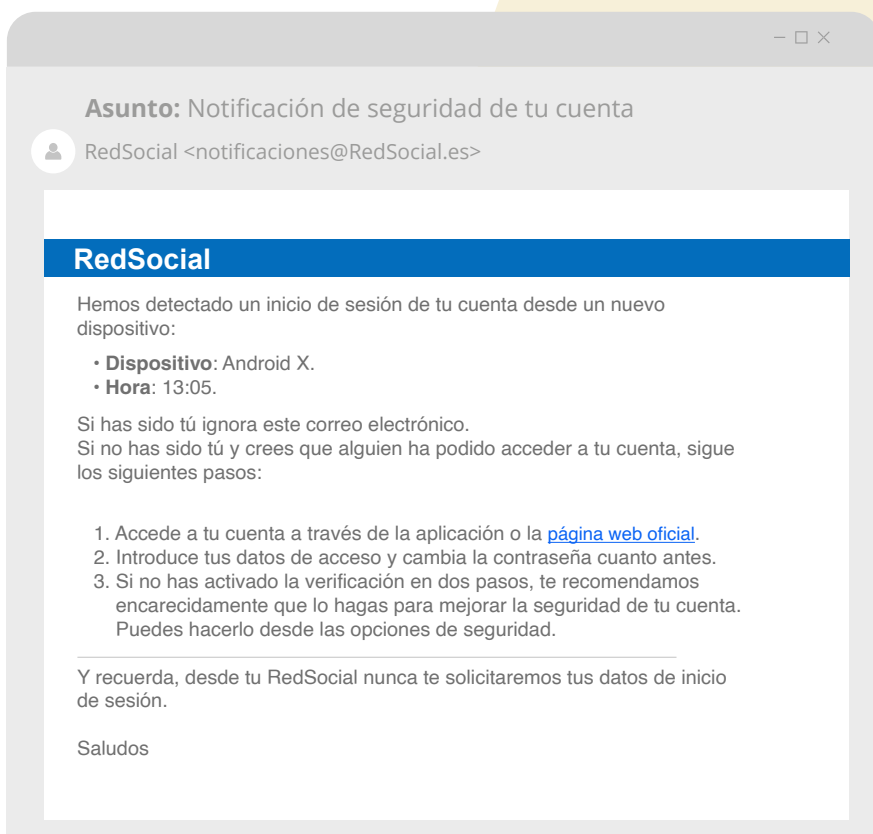
En este ejercicio te invitamos a que analices los distintos mensajes y trates de identificar aquellos que consideres fraudulentos.

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

¡Mucha suerte!

Situación 1:

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

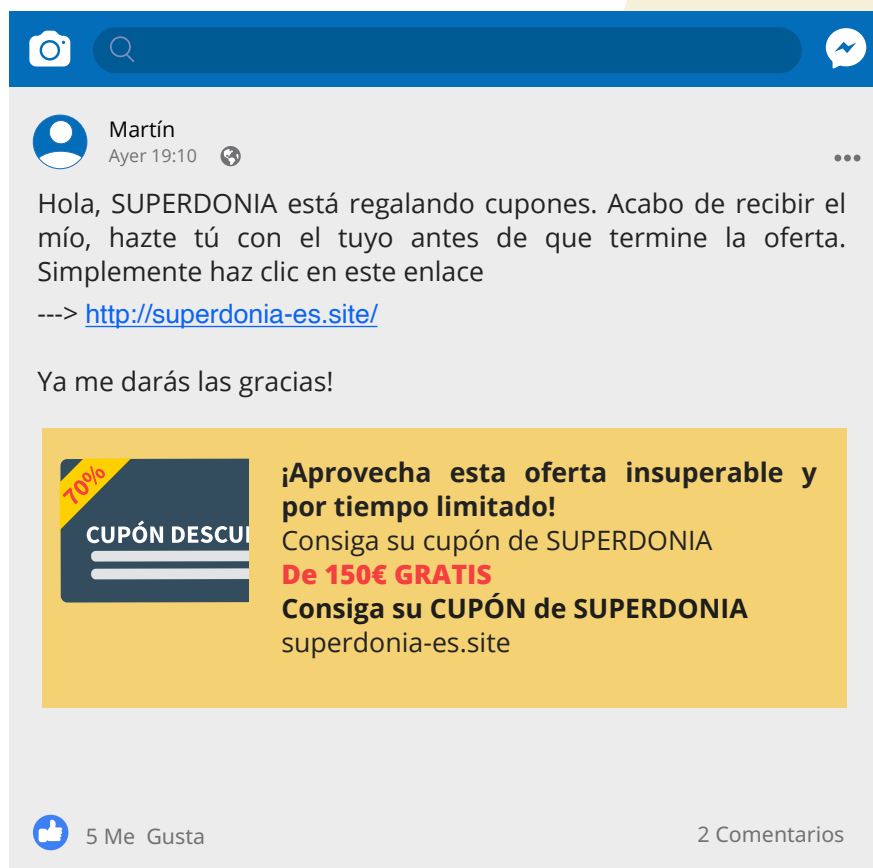


5. ¡Qué no te estafen!

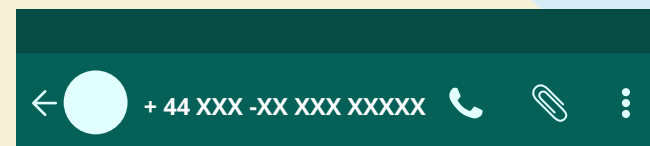
Experiencia
SENIOR

Situación 2:

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



Opción 1



**HOLA UN CORDIAL SALUDO DESDE EL SOPORTE
TÉCNICO DE [WHATSAPP]**

ESTIMADO USUARIO

Le informamos que recientemente alguien se ha registrado una cuenta de WhastApp con su número telefónico y no podemos determinar si se trata de un inicio de sesión legítimo.

Para proteger su cuenta y privacidad, le hemos enviado un código a través de un SMS a este número. Copie y pegue el código en esta conversación para validar su identidad.

Un saludo.

12:20 ✓

Opción 2

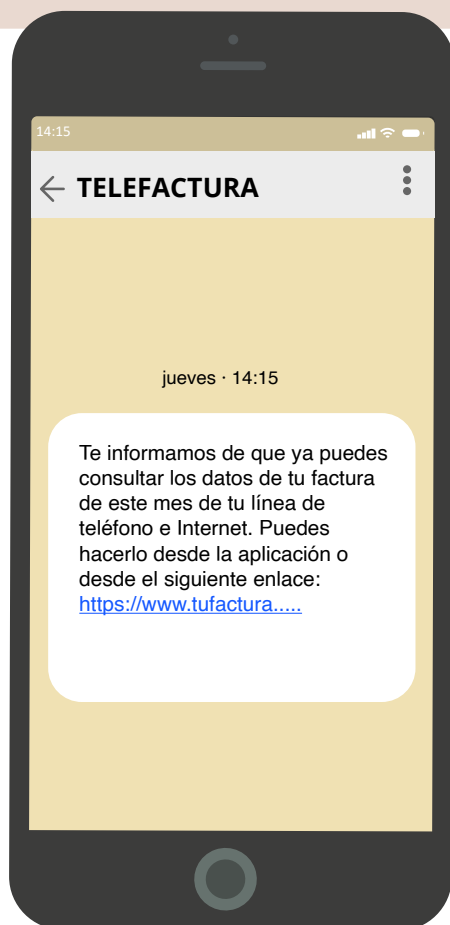
Hola, mi código es XXX-XXX-XXX

5. ¡Qué no te estafen!

Experiencia
SENIOR

Situación 3:

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



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.

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-XXXX-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.

5. ¡Qué no te estafen!

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.

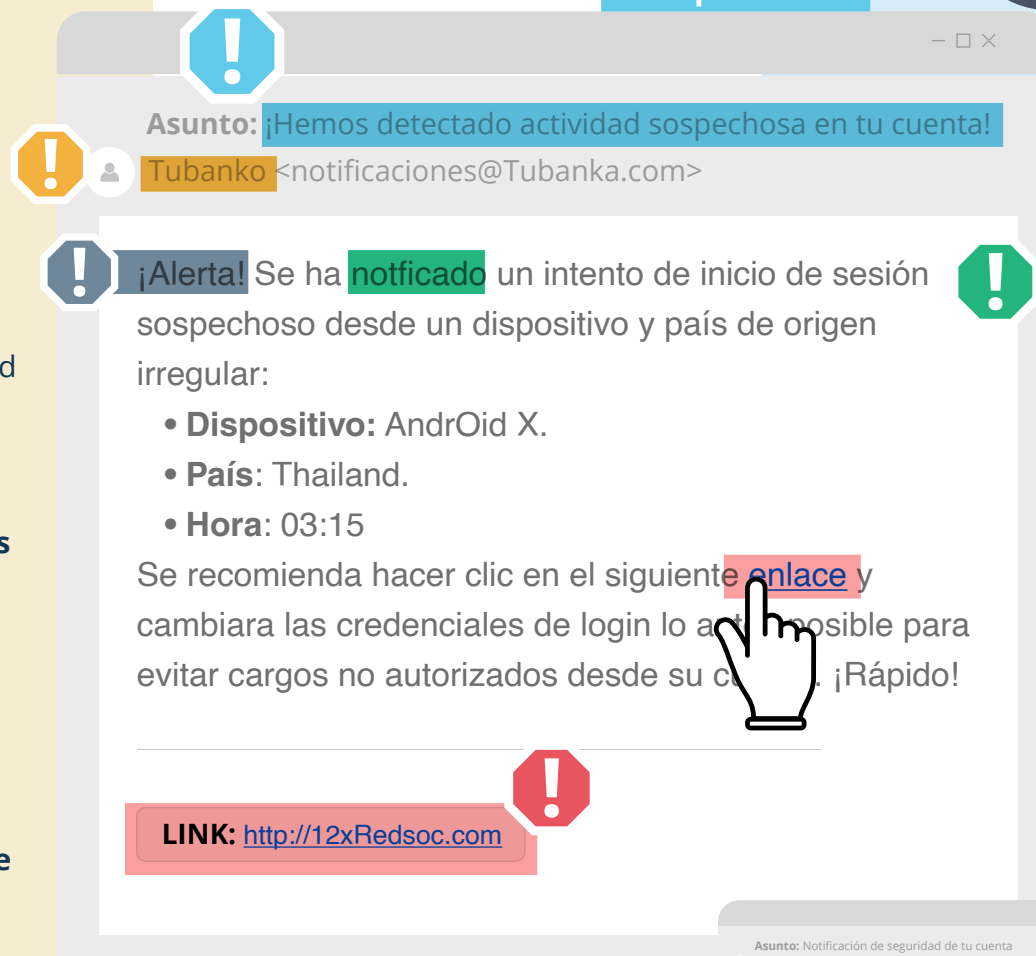
Remitente:

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

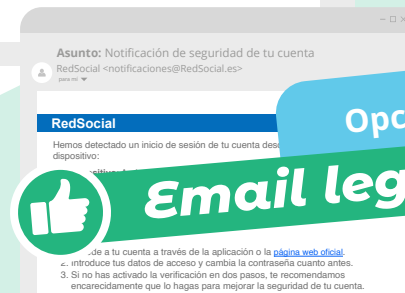


Experiencia
SENIOR

Opción 1



Email legítimo



5. ¡Qué no te estafen!

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.

Martín
Ayer 19:10

Hola, SUPERDONIA está regalando cupones. Acabo de recibir el mío, hazte tú con el tuyo antes de que termine la oferta. Simplemente haz clic en este enlace

---> <http://superdonia-es.site/>

Ya me darás las gracias!

¡Aprovecha esta oferta insuperable y por tiempo limitado!
Consiga su cupón de SUPERDONIA
De 150€ GRATIS
Consiga su CUPÓN de SUPERDONIA
superdonia-es.site

70% CUPÓN DESCU

5 Me Gusta 2 Comentarios

Opción 1

5. ¡Qué no te estafen!

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.

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!

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**.

Experiencia
SENIOR



**HOLA UN CORDIAL SALUDO DESDE EL SOPORTE
TÉCNICO DE [WHATSAPP]**

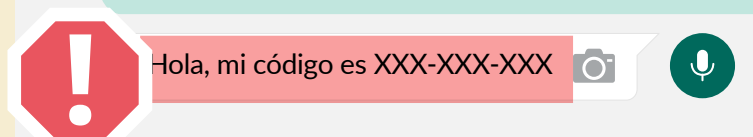
ESTIMADO USUARIO

Le informamos que recientemente alguien se ha registrado una cuenta de WhastApp con su número telefónico y no podemos determinar si se trata de un inicio de sesión legítimo.

Para proteger su cuenta y privacidad, le hemos enviado un código a través de un SMS a este número. Copie y pegue el código en esta conversación para validar su identidad.

Un saludo.

12:20



Opción 2

5. ¡Qué no te estafen!

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...).

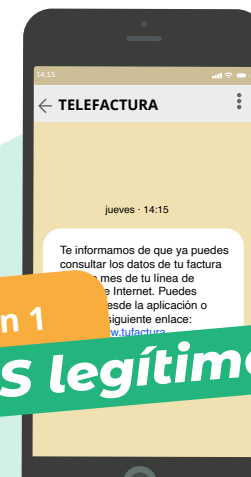


Experiencia
SENIOR

Opción 1



sms legítimo



5. ¡Qué no te estafen!

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.



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.



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



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



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

Experiencia
SENIOR



Vaya... ¿Qué necesitan?



Es 30-XX-XX-XX-X.



Pues es XXXX-XXXXX-XXXXX-XX



Es XX/XX y XXX.

