SEGURIDAD EN INTERNET

¿Qué hay que saber para que no me engañen cuando navego por Internet?

Lectura fácil

¿Qué es este documento?

En este documento te explicamos
los peligros que puedes encontrar
cuando navegas por Internet.

Las personas utilizan Internet cada vez más.
Algunas páginas web de compras
nos piden nuestros datos personales.

Debemos tener cuidado
cuando damos nuestros datos personales
porque nos pueden engañar.

Aquí podrás leer información
de los fraudes y las estafas más comunes
que puedes sufrir en Internet.

Si necesitas ayuda
puedes pedirla en la Unión de Consumidores de Aragón.

Puedes encontrar las direcciones
en la última página de este documento.

UCARAGÓN

La delincuencia en Internet.

Internet nos da herramientas y aplicaciones
que ayudan a hacer muchas tareas diarias.
Por ejemplo, podemos mandar mensajes
y hablar con personas que están lejos
con aplicaciones de Internet.

Pero hay personas que utilizan Internet
para hacer fraudes y estafas.
Los fraudes y las estafas ocurren
cuando una persona engaña a otra
para quitarle dinero o cosas de valor.

Estas personas se llaman ciberdelincuentes.
Los ciberdelincuentes se hacen pasar por bancos,
y por otras empresas
para engañar a las personas
y quitarles su dinero.

Para defendernos de los ciberdelincuentes
tenemos que conocer palabras
que se usan en Internet.
Estas palabras explican la forma de actuar
de los ciberdelincuentes.

Es importante estar bien informados
para navegar por Internet de forma segura.

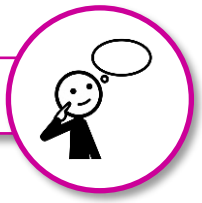
Ten cuidado con los mensajes.

Los ciberdelincuentes buscan nuevas formas
para ganar la confianza de las personas
y poder engañarlas.
Por eso, es importante estar alerta
cuando nos llega un mensaje con un enlace.

A veces, los mensajes que recibimos
parecen muy reales
y no sospechamos de ellos.

Por ejemplo, si recibimos un mensaje de un banco
donde no tenemos cuenta
podemos sospechar que es un fraude.
Pero si el mensaje dice que es de nuestro banco
es más fácil que confiemos
y que caigamos en un engaño.

Piensa antes de actuar.



Los ciberdelincuentes envían mensajes
que siempre son urgentes
para que tomemos decisiones rápidas.
Por eso, es muy importante pensar primero
y tomar el tiempo necesario
para comprobar si el mensaje es sospechoso.

Cuando recibas un mensaje
que te pide tomar una decisión rápida
lee bien el mensaje antes de hacer clic.

Busca elementos que te hagan desconfiar
y pide ayuda si la necesitas.

Pensar antes de actuar puede ayudarte
a no caer en un engaño.

Tipos de estafas por Internet.

Las estafas por Internet tienen nombres en inglés.

Las estafas más habituales son:

1. **Phishing**.
   Es una estafa donde un ciberdelincuente finge ser un banco
   o una empresa.
   El ciberdelincuente utiliza correos electrónicos.

2. **Smishing**.
   Es una estafa donde un ciberdelincuente finge ser un banco
   o una empresa.
   El ciberdelincuente utiliza mensajes SMS.

3. **Web spoofing**.
   Es una estafa donde un ciberdelincuente
   crea páginas web falsas
   que imitan a páginas web reales de bancos
   o de otras empresas.

4. **Vishing.**
   Es una estafa donde un ciberdelincuente finge ser un banco
   o una empresa.
   El ciberdelincuente utiliza llamadas telefónicas.

Phishing o fraudes por email.

¿Qué es el phishing?

El phishing es un tipo de fraude
que los ciberdelincuentes utilizan
para hacerse pasar por un banco
o por otras empresas
por medio de correos electrónicos.

¿Qué objetivo tiene el phishing?

El objetivo del phishing es robar a las personas
información personal o bancaria:

- Contraseñas.
- Datos bancarios de cuentas.
- Datos bancarios de tarjetas.

Los ciberdelincuentes utilizan la información personal
para quitarles el dinero.

¿Cómo funciona el phishing?

Los ciberdelincuentes envían correos electrónicos falsos
que parecen correos electrónicos de bancos
o de otras empresas.

Por ejemplo, recibes un correo electrónico
que parece que es de tu banco.
El correo dice que tu cuenta está bloqueada
o que se bloqueará en unos minutos.
El correo pide que confirmes tus datos personales
y tus contraseñas.
Los ciberdelincuentes te ofrecen un premio
o participar en un sorteo.

Smishing o fraudes por sms.

¿Qué es el smishing?

El smishing es un tipo de fraude
que los ciberdelincuentes utilizan
para hacerse pasar por un banco
o por otras empresas
por medio de mensajes SMS.

Los ciberdelincuentes emplean ingeniería social.
La ingeniería social es una técnica
para engañar a las personas
y conseguir su información personal y sus contraseñas.

Los ciberdelincuentes usan trucos
para ganarse nuestra confianza
por medio del engaño.

¿Qué objetivo tiene el smishing?

El objetivo del smishing es robar a las personas
información personal o bancaria:

- Contraseñas.
- Datos de cuentas bancarias.
- Datos de tarjetas bancarias.

¿Cómo funciona el smishing?

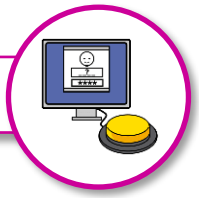
Recibimos un SMS que parece de nuestro banco
o de otra empresa que conocemos.
El mensaje alerta de un problema
con nuestra tarjeta bancaria
o con la banca online.
El mensaje dice que para solucionar el problema
debemos llamar a un número de teléfono
o hacer clic en un enlace.

Estos mensajes quieren asustarnos
para que hagamos clic en el enlace rápidamente
y no pensemos.

Por ejemplo, recibimos un SMS en el móvil
que parece de nuestro banco.
El SMS dice que hay un problema
con nuestra tarjeta de crédito
y para solucionar el problema
tenemos que hacer clic en un enlace.

El enlace lleva a una página web falsa
que imita a la página web del banco.
La página falsa pide nuestros datos personales
y los ciberdelincuentes los roban.

Web spoofing o fraudes por una página web.



¿Qué es el web spoofing?

Los ciberdelincuentes crean páginas web falsas
que imitan a las páginas web reales de bancos
y de otras empresas.

¿Qué objetivo tiene el web spoofing?

El objetivo del web spoofing es robar a las personas
información personal o bancaria:

- Contraseñas.
- Datos de cuentas bancarias.
- Datos de tarjetas bancarias.

¿Cómo funciona el web spoofing?

Los ciberdelincuentes crean una página web falsa
que imita la página web real de un banco
o de otra empresa.
Los ciberdelincuentes mandan un SMS o un correo electrónico
con un enlace que lleva a la página web falsa.

La persona cree que es la página real
y pone sus datos personales.

Por ejemplo, recibimos un SMS en el móvil
que parece de nuestro banco.
El mensaje dice que hay un problema
con la cuenta del banco
y que debemos cambiar la contraseña.

El mensaje tiene un enlace
que manda a una página web falsa
que imita a la página web de nuestro banco.

La página web falsa pide nuestra contraseña
y los ciberdelincuentes roban nuestros datos.

Vishing o fraude por llamadas de teléfono.

¿Qué es el vishing?

El vishing es un tipo de fraude
que los ciberdelincuentes utilizan
para hacerse pasar por un banco
o por otras empresas
por medio de llamadas de teléfono.

¿Qué objetivo tiene el vishing?

El objetivo del vishing es robar a las personas
información personal o bancaria:

- Contraseñas.
- Datos de cuentas bancarias.
- Datos de tarjetas bancarias.

¿Cómo funciona el vishing?

Recibimos una llamada telefónica
de una persona que dice que llama de nuestro banco
o de otra empresa.
La persona es un ciberdelincuente
que nos pide información personal
o un código SMS
para resolver un problema falso.

Si damos esa información
los ciberdelincuentes pueden hacer fraudes
y dirán que los hemos hecho nosotros.

Por ejemplo, una persona nos llama por teléfono
y nos dice que están usando nuestra tarjeta
para hacer una compra.
La persona nos pide un código SMS.
Si le damos el código SMS
el ciberdelincuente puede hacer fraudes.

Consejos para que no te engañen en internet.

1. Desconfía de mensajes o de llamadas urgentes.
   Si un mensaje o llamada dice
   que debes actuar rápido
   sospecha de ese mensaje o llamada.

2. No hagas clic en enlaces de correos electrónicos
   o de SMS que no esperas.
   No llames a los números de teléfono
   que salen en los enlaces
   de los SMS o de los correos electrónicos.

3. No descargues archivos adjuntos
   de correos electrónicos o de SMS
   que no esperas.

4. Bloquea a los remitentes
   de SMS y de correos electrónicos sospechosos
   para que no te manden más mensajes.

5. Cuelga el teléfono
   si recibes una llamada sospechosa de tu banco
   o de otras empresas.
   Bloquea el número de teléfono
   para que no recibas más llamadas.

6. Llama al teléfono de atención al cliente
   si tienes que contactar con tu banco
   o con otras empresas.

7. Tu banco no te pedirá datos personales por SMS,
   por correo electrónico o por teléfono.
   Tampoco te pedirá los datos de tu cuenta,
   los datos de tu tarjeta de crédito
   y tus contraseñas personales.

8. Si sufres una estafa por Internet
   llama a tu banco lo antes posible
   para que bloquee tu cuenta o tu tarjeta.

9. Llama a tu banco si tienes dudas
   para que puedan ayudarte.

10. Acude lo antes posible a la Policía,
    a la Guardia Civil o al Juzgado
    y pon una denuncia.

¿Cómo puedes protegerte de un fraude por Internet?

- Actualiza los programas de tu ordenador.
  Las actualizaciones mejoran la seguridad
  y te protegen de estafas en Internet.

- Utiliza contraseñas seguras.
  Una contraseña fuerte tiene 8 o más caracteres
  y lleva letras mayúsculas, números y símbolos.
  Utiliza contraseñas diferentes para cada cuenta.

- No compartas tu información personal
  con personas desconocidas.

- Instala programas antivirus en tus dispositivos.
  Los antivirus pueden encontrar y eliminar amenazas.

- Comparte esta información
  sobre seguridad en internet
  con tu familia y con tus amigos.

Puedes recibir más información en las oficinas de la Unión de Consumidores de Aragón

Oficina en Zaragoza

Calle Alfonso I, 20. Entresuelo, centro.

Código postal: 50.003 Zaragoza.

Teléfono: 976 39 76 02

Correo electrónico: info@ucaragon.com

Oficina en Huesca

Calle del Parque, 9.

Código postal: 22.003 Huesca.

Teléfono: 976 39 76 02

Correo electrónico: info@ucaragon.com

Oficina en Teruel

Calle Yagüe de Salas, 16. 4º izquierda.

Código postal: 44.001 Teruel.

Teléfono: 605 02 69 84

Correo electrónico: teruel@ucaragon.com

UCARAGÓN Unión de Consumidores de Aragón

Texto adaptado y validado por: Creando espacios accesibles Plena inclusión Aragón

Pictogramas de: ARASAAC

Financiado por: DIPUTACIÓN Đ ZARAGOZA