8

SEGURIDAD EN LA RED II

ABRIL
2017

Infokontsumoa

PRÁCTICAS FRAUDULENTAS

SANTURTZI udala - ayuntamiento

IUB OMIC

kontsumoBIDE
KONTSUMOKO EUSKAL INSTITUTUA
INSTITUTO VASCO DE CONSUMO

FALSAS TIENDAS ONLINE

CÓMO IDENTIFICARLAS

- **Aspecto visual de la página**: si no hay homogeneidad en el diseño (por ejemplo varios tipos de letra), la foto de portada es falsa o la página no está dividida en apartados (política de privacidad, aviso legal…).
- **Información legal de la empresa**: ésta no existe o no está redactada de una forma coherente y correcta.
- Si venden productos a **precios muy bajos** o presentan ofertas demasiado buenas.
- **Forma de contacto**: únicamente a través de un formulario, correo electrónico o número de teléfono móvil. No aparecen los datos de la sede física.
- **Forma de pago**: no hay alternativas a la forma de pago, aceptando tan solo pagos por western unión o similares, o a través de trasferencia bancaria.

- **Política de devoluciones**: no existe o no cumple con las exigencias mínimas legales, por ley, en las compras realizadas a distancia existe el derecho de desistir del contrato en un plazo de 14 días naturales.

CÓMO COMPROBARLO

- A través de búsqueda en internet de información sobre la supuesta tienda.
- Consultando las opiniones de otros usuarios y usuarias sobre dicha página web.
- Mediante búsqueda inversa de fotos en GOOGLE, para ello debes entrar en IMÁGENES y hacer clic en el icono de la cámara de fotos. Con ello puedes comprobar si esa imagen aparece en distintas páginas web.
- Verificar si tienen sellos de confianza online y si éstos son reales, pinchando en el propio sello debe dirigirte directamente a la página web oficial de confianza online.

trust ECOMMERCE EUROPE

CONFIANZA ONLINE

SANTURTZI Stz

EIUB OMIC

kontsumoBIDE

PHISING

- Es un ciberdelito que consiste en **engañar a las personas** para **robar información privada mediante el envío de un correo electrónico, por mensajería instantánea, SMS, redes sociales**, etc.

- También pueden usarlo para **infectar tu ordenador o dispositivo móvil** con el fin de impedir que accedas a tus archivos hasta que pagues un rescate.

- Generalmente simulan ser una entidad legítima —entidades bancarias, organismos públicos, comercios, ….

- En esos mensajes se pide que actualices o confirmes datos personales o se te informa de que has obtenido algún premio y suelen dirigirte a un enlace con apariencia similar a la web oficial con el fin de que introduzcas tus datos.

- El contenido del mensaje suele ser inusual y habitualmente con faltas de ortografía y errores gramaticales.

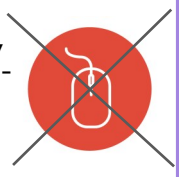
EJEMPLO:

Recibes un mensaje supuestamente de tu entidad bancaria informándote de que ha habido algún problema de seguridad y que debes confirmar urgentemente tus datos para verificar que tu cuenta no ha sido comprometida, introduciendo tus claves a través de un enlace que te facilitan.

CÓMO EVITARLO

- Usa los filtros anti spam y la configuración antiphising de los clientes de correo electrónico.

- Utiliza una contraseña robusta y segura (con mayúsculas, minúsculas símbolos y números) y cámbialas cada cierto tiempo.



- Si recibes uno de esos mensajes, no respondas. Si hubiera algún enlace, no lo pinches. Y, si tiene algún archivo adjunto, no lo abras. Debes eliminar el correo.

- Verifica la legitimación del sitio web, fíjate siempre en la URL para asegurarte que estas en la página web oficial en la que querías estar.

- En caso de duda, ponte en contacto directamente con la entidad o persona emisora para verificar su identidad.

Fuentes:
Kontsumobide, www.kontsumobide.euskadi.eus
Oficina de Seguridad del Internauta (OSI), www.osi.es

RECOMENDACIONES

- Evita las redes wifi públicas (aunque tengan contraseña) para realizar gestiones online, son más vulnerables que las redes privadas.
- Introduce tus datos confidenciales únicamente en páginas webs seguras: URLs que comiencen por http**s**:// y en las que aparezca el símbolo del candado cerrado y/o una llave.

- En algunos navegadores aparece el símbolo ⓘ por delante de la dirección web, si lo pinchas puedes ver qué tipo de conexión es.
- Cierra siempre la sesión cuando salgas de una página en la que te hayas autenticado con usuario y contraseña.
- Mantén el navegador actualizado a la última versión.
- Protege tus dispositivos con antivirus actualizado.
- Realiza periódicamente copias de seguridad de la información que almacenas en tus dispositivos.

CÓMO Y DÓNDE RECLAMAR

Para cualquier consulta o reclamación acudir a:

OMIC Santurtzi

Oficina Municipal de Información a la Persona Consumidora

Avda. Murrieta, 25. (Junto al Palacio de Oriol)

Horario de atención: 9:30-13:30 Lunes a Viernes

SANTURTZI udala · ayuntamiento

IUB OMIC

kontsumoBIDE