Guía

Aprendiendo a identificar fraudes online

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

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

OSI Oficina de Seguridad del Internauta

Índice

OSI Oficina de Seguridad del Internauta

Desde la aparición de Internet y el auge de las nuevas tecnologías, los usuarios hemos tenido que adaptarnos a un mundo en constante cambio y actualización. Dentro de éste, también han aparecido nuevos riesgos y peligros asociados que debemos conocer.

Desde la **OSI** hemos preparado un recurso con el que recoger y compartir la información y buenas prácticas necesarias para que todos los usuarios seamos capaces de disfrutar de las ventajas que nos ofrece Internet, sin caer en las trampas con las que los ciberdelincuentes tratan de obtener un beneficio a nuestra costa.

A través de esta guía haremos un repaso de los tipos de fraudes más comunes que circulan por la Red, detallando en qué consisten y cómo detectar cada uno de ellos. Esta información evitará que caigamos en los engaños y nos permitirá disfrutar de Internet con mayor seguridad.

¡Nuestra mejor defensa es estar informados!

"Recibí un email, supuestamente de mi tienda online favorita, que detallaba que estaban regalando varios productos por tiempo limitado. Solo tenía que entrar en el enlace y completar varios campos.

Me interesó, así que los rellené, incluyendo mi nombre, dirección y datos de mi tarjeta de crédito. Días más tarde me di cuenta de que faltaban 600€ en mi cuenta."

¿Cómo nos afectaría?

Suplantando la identidad de personas, entidades y servicios conocidos, **el ciberdelincuente es capaz de engañarnos para que le facilitemos información personal.** Para ello, crean correos electrónicos y mensajes que utilizan como reclamo para que finalmente accedamos a una web fraudulenta.

Recomendaciones "Buenas prácticas del cibernauta"

Comprobar la ortografía y redacción

Muchos de los correos de phishing contienen errores ortográficos y de redacción, no son propios de entidades debido al uso de traductores automatizados.

Verificar que la cuenta es original

Debemos comprobar que el email coincide con la empresa que nos envía el correo. Generalmente utilizan dominios públicos o que se parecen al que sería el correo oficial.

Por ejemplo: gooogle.com en vez de **google.com**

Revisar la URL

Los enlaces del correo deben ser comprobados. Antes de hacer clic, podemos colocar el cursor del ratón sobre el hipertexto para ver la URL a la que nos redirige.

No descargar archivos adjuntos

Bajo ningún concepto descargaremos archivos adjuntos del email si no podemos confirmar que se trata de un mensaje legítimo.

Enlaces relacionados

- Conoce a fondo qué es el phishing
- No hagas clic en todo lo que lees
- Phishing. No muerdas el anzuelo

"Tras regresar de unas merecidas vacaciones, las tuberías del baño de nuestra casa se habían roto. La verdad es que nos habíamos gastado casi todos nuestros ahorros en el viaje.

Desesperados, buscamos un préstamo de bajo interés online sin pararnos a leer las condiciones. Fue la peor decisión que pudimos tomar."

¿Cómo nos afectaría?

Los ciberdelincuentes nos **ofrecen, a través de anuncios y webs de Internet, préstamos muy atractivos** con el **objetivo de engañarnos**, para que solicitemos uno y finamente **robarnos dinero y hacerse con nuestros datos personales.**

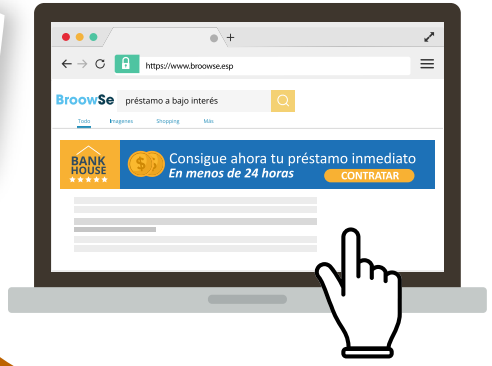
Investigar al prestamista

Comprobar que datos como, nombre y apellidos, correo electrónico o el número de teléfono que nos proporciona, no hayan sido utilizados en otras estafas.

Acudir a entidades oficiales de crédito

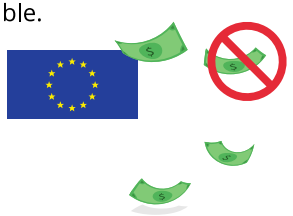
Una rápida búsqueda por Internet nos dará pistas de si se trata de una entidad fiable o si, por el contrario, estamos ante un fraude.

Recomendaciones "Buenas prácticas del cibernauta"



Comprobar normativa interbancaria EU

Debemos ser conscientes de que es difícil que un prestamista de otro país nos preste dinero sin pedir nada a cambio o a un interés tan bajo que hace que el préstamo no sea rentable.



Revisar ortografía y gramática

Es frecuente que los anuncios y mensajes enviados por los ciberdelincuentes contengan errores gramaticales y ortográficos que nos hagan sospechar del engaño.

Denunciar ante el banco

Denunciar ante el banco correspondiente la cuenta fraudulenta en la que se debía depositar el pago, para que así dicho banco proceda a su cancelación.

Enlaces relacionados

- Fraudes online. Préstamos de dinero a particulares
- ¿Buscas un préstamo a bajo interés? ¡Cuidado!
- Pedí un préstamo a un falso banco, e intentaron estafarme hasta tres veces.

"Me encontraba navegando por Internet, buscando un par de zapatos nuevos que comprar, cuando encontré una oferta estupenda.

Estaban un 40% más baratos que en la tienda oficial, y me decidí a comprarlos. La web parecía fiable, aunque ya han pasado dos meses desde que los pedí y aún no me han llegado."

¿Cómo nos afectaría?

Robo de nuestro dinero e información personal al acceder a las tiendas online a través de anuncios con ofertas irresistibles. Además, **lo más habitual es que no recibamos el producto comprado** o de recibirlo, que se trate de una falsificación.

Recomendaciones "Buenas prácticas del cibernauta"

Observar el aspecto visual

Una web mal construida y poco atractiva puede ser debido a que se ha hecho con prisas y/o tratando de copiar el estilo de una tienda oficial.

Monitorizar opiniones

Antes de comprar un producto revisaremos las opiniones de otros usuarios haciendo una búsqueda por Internet.

© Comprobar información legal empresa

El NIF de la empresa y otros datos como la razón social o los datos de contactos son necesarios para identificar a una tienda online fiable.

€ Fijarse en los precios

Deben hacernos sospechar los precios demasiado bajos con respecto a las tiendas oficiales o al precio de mercado.

Comprobar certificado SSL ON

Las tiendas online fiables tendrán una conexión segura por HTTPS y contarán con un certificado de seguridad.

Leer condiciones y políticas GDPR

Seamos conscientes de las condiciones del servicio que se nos está ofreciendo, así como de las políticas de privacidad de la plataforma. Esta información suele incluirse dentro del "Aviso legal" de la web, y debemos sospechar si no lo vemos por ningún lado.

$ Analizar pagos permitidos

Evitaremos páginas que, aunque contengan los logos de muchos métodos de pago online, a la hora de la verdad solo permiten transferencias a depósitos y pagos con tarjeta.

★ Contrastar reputación en la red

Un rápido vistazo por Internet, buscando por el nombre de la empresa o del vendedor, nos dirá si nos encontramos ante una estafa o fraude.

Enlaces relacionados

- Campaña concienciación sobre "Compras seguras online"
- Guía de "Compra segura en Internet"
- Tiendas online fraudulentas

OSI Oficina de Seguridad del Internauta

"Mi novia y yo planeábamos alquilar un piso en la playa en verano. Buscando en una app de alquileres vacacionales dimos con un anuncio muy interesante. El precio era mucho mejor que el de otros apartamentos de la zona, así que decidimos alquilarlo.
Cuando llegamos al destino nos encontramos con que el supuesto apartamento no era del propietario con el que habíamos contactado. De hecho, ni si quiera estaba en alquiler."

¿Cómo nos afectaría?

Ponen en circulación **anuncios de inmuebles demasiado buenos** como para dejarlos pasar. **Una vez mostramos interés**, **tratarán de obtener nuestro dinero** lo antes posible pidiendo, por ejemplo, **pequeños pagos en concepto de fianza o reserva.**

Recomendaciones "Buenas prácticas del cibernauta"

Revisar las descripciones

Descripciones que contengan errores ortográficos o frases inconexas pueden indicar que el anuncio es falso.

Comparar el precio con el de mercado

Los "chollos" demasiado buenos para ser ciertos (precios muy bajos, ubicación inmejorable, calidades muy buenas...) pueden ser el gancho perfecto para captar nuestra atención.

Analizar el perfil vendedor

Revisaremos el perfil del vendedor, leeremos las valoraciones de otros clientes y comprobaremos la antigüedad del perfil o los datos de contacto.

Excusas y problemas

Desconfiar si existe imposibilidad de enseñarnos el inmueble antes de alquilarlo o si nos obligan a continuar la comunicación fuera de la plataforma de anuncios.

No aceptar cualquier método pago

Los servicios de envío de dinero en efectivo, o transferencias a cuentas bancarias de países extranjeros, no nos permiten o dificultan la recuperación del dinero en caso de problemas o fraude.

Buscar en Google Maps

Podemos buscar la dirección del inmueble a través de Google Maps para comprobar si es real y se corresponde con la descripción del inmueble anunciado.

Enlaces relacionados

•Campaña concienciación sobre "Alquileres vacacionales"

"Estaba en mi ordenador trabajando en mi tesis, al mismo tiempo que navegaba por Internet buscando información en diversas fuentes. De pronto, una ventana apareció por pantalla indicando que mi ordenador estaba infectado, que no lo apagara y que llamara al número de soporte técnico que allí aparecía.

Tras hablar con el supuesto técnico, me explicó cómo instalar un programa para que él pudiese conectarse a mi ordenador y desinfectarlo de forma remota."

¿Cómo nos afectaría?

Los ciberdelincuentes podrían pedirnos dinero por hacer una **falsa reparación** del dispositivo o, incluso, **instalarnos programas maliciosos en él** para robar información privada y **realizar acciones maliciosas o ilegales desde él.**

Recomendaciones "Buenas prácticas del cibernauta"

Restablecer el dispositivo

Si hemos concedido acceso a los estafadores, consideremos la posibilidad de restablecer el dispositivo.

Actualizaciones de seguridad

Aplicar todas las actualizaciones de seguridad en cuanto estén disponibles.

Desinstalar las Apps

Desinstalar lo antesposible las aplicaciones que los estafadores te hayan pedido instalar.

Instalar Apps originales

Instalar aplicaciones originales, solo desde las páginas webs oficiales.

Descarga Disponible Google play

Descarga Disponible App Store

Cambiar las credenciales

Cambiar las claves de acceso a nuestras aplicaciones y servicios.

Reportar el incidente

Si nos mintieron diciendo que eran el asistente oficial de un software, podremos reportarlo al proveedor original.

Llamar a nuestro Banco

Llamar a nuestro banco para cancelar los pagos al soporte técnico falso.

Enlaces relacionados

- ¿Microsoft te ha llamado sin haberlo solicitado?
- Mensajes fraudulentos, invitan llamar a un falso soporte técnico.
- Llamadas desde el falso soporte técnico.
- Servicio técnico falso, pero estafa real.

"Llevaba solo un par de meses en un nuevo trabajo cuando recibí un correo electrónico con una oferta de trabajo muchísimo mejor de la que tenía.

Decidí mandarles el CV y a los pocos días me contactaron informándome de que había sido elegido para el puesto. Únicamente debía hacer una transferencia de dinero por adelantado en concepto de pago de la mitad del seguro de salud. Tras hacerlo, no volví a saber nada de la empresa."

¿Cómo nos afectaría?

Muchas personas sin empleo confían en Internet para encontrar ofertas de trabajo. Los **ciberdelincuentes se aprovechan, publicando falsas ofertas de empleo** con las que **obtener un beneficio económico** solicitando pagos por adelantado en concepto de gestión, seguro métido, formación inicial, etc.

Recomendaciones "Buenas prácticas del cibernauta"

Revisar la web de la empresa

Buscaremos información de la empresa por Internet y revisaremos su página web para contrastar la información del anuncio. Los comentarios de otros usuarios pueden ayudarnos.

Llamadas a tlf de tarificación especial

Si la empresa anunciante nos pide contactar a través de números que comienzan por 803, 806, 807, 905, 907, 70X..., hay que sospechar.

$ Compra material

También puede darse el caso de que nos pidan hacer un esfuerzo económico comprándoles los materiales con los que desempeñaríamos nuestro trabajo.

Revisar la redacción oferta

Si no está bien redactada, la descripción de la misma es vaga o contiene bastantes faltas de ortografía, lo más probable es que sea fraudulenta, ya que ninguna empresa de prestigio cometerá ese tipo de errores.

Utilizar portales fiables

Emplearemos portales de búsqueda de empleo contrastados y de instituciones u organismos oficiales.

Revisar la política protección datos

Nos aseguraremos de que la empresa cumple con la política de protección de datos personales.

$ ← Solicitud de dinero

En el caso de que nos soliciten un pago por adelantado, no continuaremos.

Enlaces relacionados

- Falsas ofertas de empleo
- Recibí un e-mail con la oferta de trabajo ideal, ¡pero tenía truco!
- ¿Buscas trabajo? Antes de dar el primer paso, analiza la oferta

"Mi hijo me comentó que, cuando estaba jugando en su ordenador, alguien le había enviado un mensaje al móvil amenazándolo con publicar en Internet unas fotos comprometedoras suyas si no pagaba una cantidad de dinero en menos de 24 horas.

En dicho mensaje se detallaba cómo habían obtenido sus fotos y cómo pensaban extorsionarle si no accedía a las peticiones."

¿Cómo nos afectaría?

Este tipo de extorsión **consiste en chantajearnos con la publicación de fotos, vídeos** o información íntima de nosotros, si no pagamos. En la mayoría de casos, **no tienen nada, pero se sirven del miedo y el desconocimiento** para engañarnos.

No revelar información

Seremos cuidadosos con quién compartimos nuestra información personal, como fotos o vídeos.

Mantener la calma

Lo primero es no alarmarnos ya que puede tratarse de un engaño, y que no tengan los archivos que dicen tener.

Recomendaciones "Buenas prácticas del cibernauta"

Desconectar webcam y micrófono

Si no estamos utilizando la cámara u otros dispositivos de audio como el micrófono, es mejor desconectarlos. Tampoco es recomendable que permitamos que cualquier app tengan acceso a la cámara del dispositivo.

No abrir archivos adjuntos

Si recibimos correos dudosos, no abriremos los archivos adjuntos, ya que podrán contener algún tipo de malware.

No enviar dinero

Realizar un pago no garantiza que no sigan extorsionándonos. Es más, estaremos favoreciendo este tipo de prácticas.

Enlaces relacionados

- ¿Buscas pareja por Internet? ¡Ten cuidado!
- Detectada una estafa a través de correo electrónico extorsionando con supuestas imágenes de contenido sexual
- Cuidado con las sesiones de fotos

Oficina de Seguridad del Internauta

"Estaba chateando con mis amigos cuando de pronto, un chico al que no conocía me abrió chat y empezó a hablarme como si me conociese.
Cuando le pregunté, me dijo que me había conocido a través de una app de citas en la que no me había registrado nunca. Fui a comprobarlo y efectivamente, alguien había creado un perfil falso con mi información y datos de contacto."

¿Cómo nos afectaría?

Los motivos que hay detrás de la creación de perfiles falsos son muy variados: **dañar nuestra reputación online**, extorsionarnos e incluso robarnos datos personales para cometer otras actividades fraudulentas. **Debemos tener cuidado con la información que publicamos en Internet**.

Recomendaciones "Buenas prácticas del cibernauta"

Ejercer derechos ARCO

Son los derechos de acceso, rectificación, cancelación y oposición de datos para la protección de nuestros datos personales.

Recopilar pruebas

Si nuestra identidad ha sido suplantada, deberemos recopilar todas las pruebas que podamos y reportar la situación a la web donde esté registrado el perfil falso.

Hacer "Egosurfing"

Una rápida búsqueda online sobre nosotros nos dirá si se han usado nuestros datos en alguna web que no conocemos o utilizamos.

Mejorar la privacidad en la redes sociales

Toda red social pone a nuestra disposición la opción de decidir cuánta información queremos que se haga pública y a quienes queremos que llegue.

No aceptar peticiones de desconocidos

Si su descripción es escasa, no tiene fotos asociadas y además no le conocemos, ni tenemos conocidos en común, no le aceptaremos. Es posible que se trate de una cuenta falsa.

Ser selectivo

Agregaremos a usuarios que realmente conozcamos. Existen perfiles que solo buscan llamar la atención publicando bulos o creando polémica y discusiones entre los usuarios.

Enlaces relacionados

- Un doble en la Red
- Perfiles falsos en redes sociales, ¿cómo actuar?
- Qué hacer ante una suplantación de identidad
- ¡SOS! Alguien ha creado un perfil con mi foto

"Llevaba meses buscando comprar una videoconsola nueva a buen precio a través de una app de compraventa de productos, hasta que encontré un vendedor que la ofertaba a un precio muy bajo.

Me pidió que le pagara por adelantado haciendo una transferencia bancaria, él a continuación me enviaría la videoconsola. Sin embargo, tras efectuar el ingreso, el envío nunca llegó y cuando fui a preguntar al usuario, éste había desparecido y su perfil ya no figuraba en la aplicación."

¿Cómo nos afectaría?

El principal riesgo de los procesos de compraventa de productos es que **el vendedor o comprador nos engañe**, de tal manera que realicemos el **pago de un producto que nunca nos llegará** o que enviemos el nuestro y no recibamos el pago.

Recomendaciones "Buenas prácticas del cibernauta"

Observar el anuncio

Los estafadores suelen usar imágenes falsas sacadas de Internet u ofertar productos falsificados. Si dudamos, debemos pedir más imágenes o información al vendedor para cerciorarnos de que es real.

Revisar comentarios

Siempre es útil revisar qué dicen otros usuarios sobre el vendedor. Si no tiene valoraciones o son pocas y negativas, desconfiemos.

No fiarse de ofertas muy agresivas

Desconfiar de productos con precios muy inferiores a los de mercado ya que son la excusa perfecta para engañarnos.

Sospechar de las excusas

Seguir la comunicación fuera de la plataforma, solicitud de dinero por adelantado y ofrecer pagar más cantidad de dinero por el producto sin ningún motivo son síntomas claros de que están intentando engañarnos.

Revisar el perfil vendedor/comprador

Normalmente los perfiles de estafadores llevan muy poco tiempo creados, no tienen fotos reales ni datos de contacto verificados. Además, suelen tener urgencia en llevar a cabo la transacción. Si somos el vendedor, desconfiaremos de compradores con perfiles extraños o de países extranjeros que dicen tener urgencia en la compra bajo cualquier condición.

Aceptar métodos de pago seguros

Si vamos a pagar a distancia, acudir preferentemente a sistemas de pago, como son el pago contrareembolso, PayPal o Wallapop Envíos, etc. que aseguren que recibimos el dinero o el producto.

Denunciar anuncio fraudulento

Si tenemos motivos para pensar que un anuncio es falso, se lo notificaremos a la plataforma que lo aloja para que pueda ser revisado y eliminado.

Enlaces relacionados

- Servicios de compraventa y subastas online
- ¿Qué son los sistemas de reputación?

“Los ciberdelincuentes no descansan y siempre están planeando nuevas formas de engañarnos para hacernos caer en sus trampas.”

En ocasiones podrá ser poniendo en circulación por la Red **anuncios con chollos y ofertas demasiado llamativas** como para que las dejemos pasar. En otras haciéndose pasar por otras personas, empresas, servicios e instituciones oficiales para ganarse nuestra confianza, e incluso **difundiendo mensajes extorsionadores y chantajes** con los que sacar un beneficio a nuestra costa.

Por tanto, no nos confiemos, permanezcamos informados y usemos el sentido común para no caer en ningún fraude online.

TU AYUDA EN
CIBERSEGURIDAD

incibe_

Si después de leer esta guía aún nos surgen dudas y necesitamos más información sobre los temas abordados en ella o cualquier otro relacionado con la ciberseguridad, recordemos que está disponible la Línea de Ayuda en Ciberseguridad de INCIBE.

www.osi.es

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

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

OSI Oficina de Seguridad del Internauta