FRAUDE EN INTERNET

Internet es un potentísimo medio de comunicación, y particularmente se ha convertido en una herramienta muy importante para realizar todo tipo de transacciones comerciales y financieras: desde la compra de productos en tiendas virtuales hasta negocios entre empresas pasando por las operaciones que permite la banca online. Todo esto hace que por la red circule una gran cantidad de información que en manos de estafadores puede derivar en un fraude.

A primera vista parece alarmante, pero no lo es tanto si nos damos cuenta de que en realidad con las transacciones en la vida real corremos un peligro similar. Al entregar nuestra tarjeta de crédito en una tienda, al teclear la clave en nuestro cajero, al descuidar nuestra cartera, al abrir la puerta a vendedores no identificados, al hacer caso de publicidad engañosa de nuestro buzón...

En Internet no tendremos que hacer ni más ni menos de lo que hacemos frente a los fraudes en nuestra vida cotidiana: tomar precauciones y, si tenemos la mala suerte de ser víctimas de un fraude, simplemente denunciarlo. Como siempre, hay que usar en lo posible el sentido común.

Vamos a repasar los principales tipos de fraude que se realizan en Internet para estar prevenidos en lo posible.

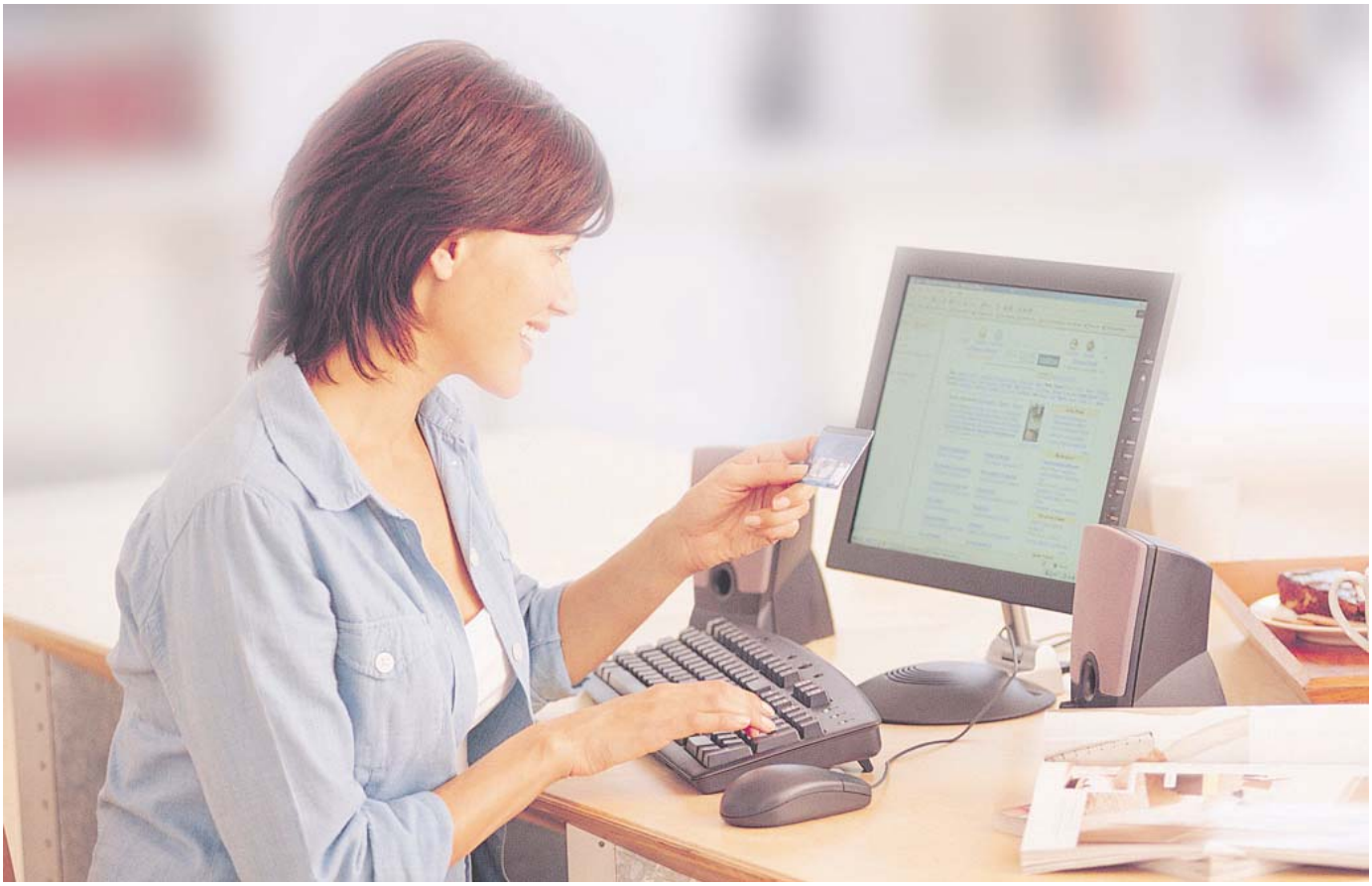
TIPOS DE FRAUDE

1.COMPRAS FRAUDULENTAS:

El vendedor puede hacerse pasar por una tienda virtual o simplemente ofrecer en un sitio de subastas un producto y, una vez realizado el pago, no enviar lo prometido.

•Cómo prevenirlo:

Asegurarse de la identidad del que nos vende, l**as tiendas online tienen la obligación de tener una sede física** y publicar sus datos en la página web (incluido el NIF). Tomemos nota de cómo se pueden realizar reclamaciones. En el caso de webs de subastas, revisar la puntuación del vendedor y comprobar si es fiable.



2.PHISHING:

Se trata de una técnica por la que **un banco o institución financiera nos remite aparentemente un correo electrónico para solicitarnos los datos de nuestra cuenta para realizar ciertos trámites.** Suelen incorporar el logotipo de la institución y su redacción no induce a sospechas, pero en realidad se trata de una suplantación del verdadero organismo. También suele incluirse una dirección web aparentemente legítima, construida especialmente para que introduzcamos los datos que utilizamos en las distintas operaciones relativas al servicio electrónico.

•Cómo prevenirlo:

Los bancos o instituciones financieras no solicitan datos confidenciales por correo electrónico. Si recibimos ese tipo de mensajes hay que notificarlo directamente a fraude@cert.inteco.es. Las transacciones siempre tendremos que realizarlas en la página web segura con la dirección web legítima del banco.

3.ROBO DE DATOS DEL USUARIO:

Pueden ser realizados por delincuentes informáticos que consigan datos del archivo de una tienda online o de otras instituciones, o por parte de empleados de dichas organizaciones. Normalmente se trata de datos de tarjetas de crédito para realizar compras, pero pueden ser todo tipo de datos personales que puedan ser utilizados para un uso fraudulento.

•Cómo prevenirlo:

Asegurarse de que el servidor donde realizamos las transacciones dispone de todos los sistemas de encriptación y seguridad. Podremos distinguirlas porque aparecerá el icono de un candado en la parte inferior derecha de la ventana de nuestro navegador.

4.PHARMING:

Algunos servidores o un equipo individual pueden ser atacados de diversas formas para conseguir que la dirección de un sitio de Internet lleve a un servidor en vez de a otro. Es como modificar las páginas amarillas y cambiar el número de teléfono que aparece, por ejemplo, de una tienda por el de otro sitio. De esta forma el **estafador puede llevar a su propia web a clientes o usuarios de cierto servicio sin que estos se den cuenta.**

•Cómo prevenirlo:

En primer lugar, teniendo **siempre actualizado y activado el programa de antivirus** para prevenir el que esté actuando un programa malicioso. Cuando accedamos a la página donde vamos a introducir nuestra clave, asegurarnos de que la dirección de la página empieza por HTTPS, es decir, que se trata de una página web segura. En este tipo de páginas el navegador comprueba la identidad del proveedor de servicio con un certificado digital. También podemos comprobar que aparece el símbolo de un candado en la parte inferior derecha del navegador. Para asegurarnos de que el certificado de seguridad de la página es válido y corresponde al servidor al que se supone que estamos accediendo, basta con hacer doble click con el ratón sobre ese candado.

Reconocer una página Web fraudulenta.

5.FRAUDES

BASADOS EN FALSAS OFERTAS:

Se trata de estafas que utilizan ofertas muy atractivas con el fin de que los usuarios se confíen bien apelando a su sensibilidad, bien apelando a su codicia o a sus necesidades. El estafador entra en contacto con el usuario por correo electrónico aportando en ocasiones incluso documentación aparentemente real. En inglés estas técnicas para ganar la confianza de la víctima reciben el nombre de Scam.

•Servicios gratuitos o de prueba:

Podemos recibir por correo electrónico una oferta irresistible para acceder a un servicio o producto gratuito, de precio reducido o de prueba. Una vez en la página web se nos pedirá, entre otros datos, los de nuestra tarjeta de crédito para obtener lo prometido.

• Cómo prevenirlo:

Desconfiemos de las ofertas, identifiquemos siempre a la empresa que nos va a prestar cualquier servicio, aunque sea gratuito. Comprobemos que se publican sus datos en la página web. En general no dar los datos de nuestra tarjeta de crédito o débito por muy atractiva que nos parezca la oferta, salvo que se

utilicen pasarelas de pago con tarjeta reconocidas.

•La estafa nigeriana:

Un fraude que se ha extendido mucho por el mundo. Consiste en prometer una gran suma de dinero al receptor, aportando documentos falsos de todo tipo, para la que es necesario realizar ciertos gastos en concepto de trámites. El nombre es debido a que los primeros casos detectados de esta estafa estaban dirigidos por un grupo de delincuentes de Nigeria. La estafa se puede alargar con varios intercambios y más documentación falsa sobre la supuesta suma de dinero que se va a recibir. Puede ser un político que no puede sacar el dinero del país y supuestamente nos recompensará por usar nuestra cuenta bancaria, una herencia, el premio de una lotería que el estafador supuestamente no puede cobrar...

•Cómo prevenirlo:

En este caso **el sentido común será la más valiosa de las herramientas.** No debemos confiar en personas que nos ofrecen grandes sumas a cambio de realizar pequeñas aportaciones de capital, pero esto no sólo vale para Internet...

•Ofertas de trabajo falsas:

Consiste en ofrecer a la víctima la posibilidad de ganar dinero mediante un supuesto trabajo en el que se deberán realizar diversos movimientos de dinero. Una vez concedido el trabajo, el usuario recibe una cantidad de dinero en su cuenta bancaria (normalmente desde el extranjero) o un cheque por correo y tiene que transferir ese dinero a otra cuenta. La empresa que contacta tiene una apariencia seria y justifica la operación con supuestos ahorros fiscales. Al tomar parte en este trabajo se puede llegar a participar en un delito de blanqueo de dinero (normalmente obtenido en otros fraudes electrónicos) o correr el riesgo de recibir cheques falsos a cambio de una transferencia legal.

•Cómo prevenirlo:

Como en la mayoría de los casos de fraudes o timos en general, siendo precavidos y no aceptando ofertas

de trabajo de desconocidos por muy atractiva que parezca.

• Falsas campañas de donación:

En este caso se solicitan donaciones para supuestas víctimas de desgracias naturales o menores enfermos para las que se proporciona a veces incluso una cuenta bancaria para depositarlas.

•Cómo prevenirlo:

Siempre que pueda procure comprobar que las donaciones se realizan a través de una ONG o institución autorizada. Compruebe que la organización existe y que se puede contactar. Compruebe con dicha organización que esa iniciativa es real y que los datos son correctos.

6.PROGRAMAS MALICIOSOS AL SERVICIO DEL FRAUDE:

En ocasiones los estafadores son expertos en informática y en vez de confiar en la debilidad de sus víctimas, realizan programas para sustraer datos de sus ordenadores o simular que accedemos a determinados servicios sin nuestro consentimiento. Algunas estafas ya mencionadas, como el Pharming o el robo de datos, también pueden utilizar este tipo de programas. Existen varias modalidades de programas.

•Spyware:

Se trata de **programas que se introducen en el ordenador de la víctima** de diversas formas y toman en parte el control del mismo sin que lo sepa. Mediante Spyware un estafador puede engordar las estadísticas de su página web haciendo que nuestro ordenador la visite sin que lo sepamos, sustraer información almacenada en el disco, mostrar publicidad (Adware), detectar qué páginas visitamos y otras muchas prácticas.

•Cómo prevenirlo:

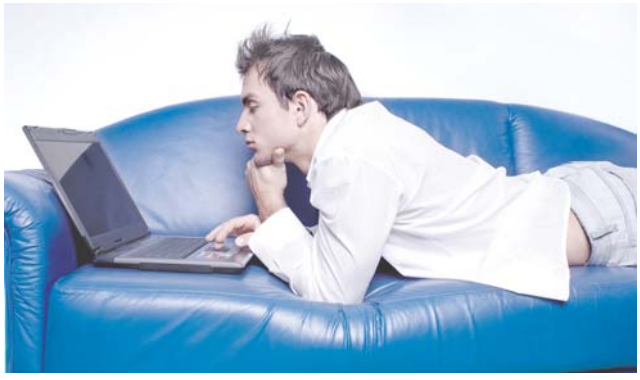
Evitando visitar páginas web poco fiables y realizando periódicamente una limpieza mediante un programa anti-spyware. Podemos descargar programas anti-spyware gratuitos desde "programas de seguridad".

•Código para robo de credenciales:

Son programas maliciosos especializados en el robo de credenciales de acceso a diversos servicios electrónicos. Los más conocidos son los **Keyloggers** (roban todos los caracteres introducidos por el teclado del sistema comprometido) aunque últimamente son más utilizados los **troyanos bancarios** (detectan las visitas a ciertos sitios web y superponen un formulario al legítimo de la entidad para que el usuario introduzca los datos en él de forma que queden registrados en el ordenador del estafador).

•Cómo prevenirlo:

Utilizar un programa antivirus en nuestro equipo para detectar este tipo de códigos maliciosos. Disponemos de información de programas antivirus en las sección de "útiles gratuitos".



PRECAUCIONES GENERALES

En general podemos resumir las precauciones a tomar frente a los fraudes en Internet con las siguientes:

•Identifica:

Procurar **tener perfectamente identificado al interlocutor** o prestador de servicios si vamos a realizar alguna operación.
Comprobar su certificado digital.

•Desconfía:

Nunca prestar crédito a promesas de dinero fácil, de productos o servicios gratuitos, de donaciones sin identificar la organización que las gestiona o a trabajos bien remunerados sin comprobar a conciencia de dónde proviene esa oferta.

•Comprueba:

Es conveniente **tener siempre bajo control la cuenta asociada a nuestra tarjeta de crédito** para detectar un posible uso indebido. Algunos bancos ofrecen un servicio de aviso por SMS por cada operación realizada. Puede ser conveniente tenerlo activado para prevenir problemas.

•Filtra:

Desconfiar siempre de un correo electrónico que nos dirige alguien que no conocemos y que no nos ofrece una explicación convincente de cómo ha conseguido nuestra dirección. **Filtra los mensajes de remitentes desconocidos** para que no aparezcan en la bandeja de entrada.

•Infórmate:

Es bueno permanecer atentos a las noticias de nuevas formas de fraude por Internet para estar prevenidos. Un buen lugar de información es la propia página web de Inteco: www.inteco.es en su sección de noticias de seguridad o dirigiéndote al buzón fraude@cert.inteco.es.

•Asegúrate:

Cuando hagamos alguna operación con nuestros datos bancarios o de nuestra tarjeta de crédito, **comprobar que la página web a la que accedemos es segura** y el certificado de la empresa es el correcto. Si es posible, exigir que el banco utilice medidas de seguridad complementarias (físicas) para proteger el acceso. Activar los mecanismos de pago seguro por internet de las tarjetas de crédito o débito y efectuar los pagos en sitios web que dispongan de este mecanismo.

•Limpia:

Un ordenador conectado a Internet puede ser el objetivo de Spyware o códigos maliciosos, es conveniente disponer de una herramienta adecuada y **realizar un análisis completo del sistema periódicamente.**

•Usa el sentido común:

Como hemos dicho: la herramienta más valiosa. No hacer click en enlaces en los que no confiamos, no creer en ofertas milagrosas, no descargar programas que no conocemos y ser prudentes con los desconocidos forman parte de este sentido común. Pero hay muchas cosas más de las que podemos enumerar y que el sentido común es capaz de detectar sin necesidad de programas especiales.

QUE HACER
SI SOMOS **VICTIMAS** DE UN FRAUDE

Si a pesar de nuestras precauciones somos víctimas de un fraude por Internet, es conveniente que sigamos las siguientes pautas.

•Vigilar:

Es bueno **tener siempre bajo control nuestras cuentas corrientes y los movimientos de la tarjeta de crédito** e investigar si vemos algo sospechoso. Ante cualquier duda sobre una compra que no hayamos hecho, consultar con el banco para conocer qué pasos hay que seguir.

•Cambiar:

También es importante **cambiar las contraseñas que utilizamos para acceder a nuestro banco por Internet** o a otros servicios que sospechamos que están siendo utilizados por otras personas a nuestro nombre. Para asegurarnos de que nuestras contraseñas son seguras es bueno seguir ciertas recomendaciones: "contraseñas seguras".

•Informar:

Además de informar del posible fraude a Inteco escribiendo un correo electrónico lo más detallado posible a la dirección fraude@cert.inteco.es también deberemos **denunciar personalmente la estafa ante alguna de las Fuerzas y Cuerpos de seguridad del Estado**, tal como se indica en la sección "Gestión de Fraude Electrónico".