

Protección Penal de Consumidores y Usuarios ante los delitos de estafa

GUÍA PRÁCTICA



San Bernardo 97-99 Edificio Colomina 2F . Madrid 28015
Telef.: 91 594 5089 . Fax: 91 594 5124
E-mail: ceaccu@ceaccu.org
www.ceaccu.org



Esta publicación ha sido subvencionada por el Ministerio de Sanidad
y Consumo, Instituto Nacional de Consumo.
El contenido de la misma es responsabilidad de CEACCU.

Las Guías Prácticas de CEACCU



100 Consejos para ser una perfecta ama de casa ecológica



100 Consejos para llevar una vida saludable



100 Consejos para una alimentación sana



Cómo comprar y contratar en Internet



Guía práctica sobre el euro para el ama de casa



Cómo obtener el máximo provecho de su dinero



Cómo evitar los accidentes en el hogar



Cómo evitar los accidentes en el hogar: la cocina



Guía práctica sobre seguridad alimentaria



Seguridad alimentaria: la EEB, guía práctica



Derechos de los usuarios de la telefonía



Cómo reciclar en el hogar



Cómo evitar el sobreendeudamiento



Manual sobre productos y servicios en el hogar



¿Pantallas amigas? Niños y niñas, televisión y nuevas tecnologías



Ahorro Energética, Guía Práctica



Autocuidado de la salud, Guía Práctica



Sobreendeudamiento Familiar: ¿Cómo evitarlo?



Cómo prevenir los accidentes domésticos y de ocio

CEACCU, 2008

El contenido de esta publicación puede reproducirse, siempre que se indique su procedencia.

Editado y elaborado por: CEACCU
© de esta edición: CEACCU, 2008

Coordinación y contenidos: Eugenio Ribón Seisdedos (CEACCU)

Depósito Legal: M-23094-2008
ISBN-13: 978-84-691-3375-0

Esta publicación ha sido subvencionada por el Ministerio de Sanidad y Consumo-Instituto Nacional del Consumo. El contenido de la misma es responsabilidad de CEACCU.

Diseño, Fotomecánica y Producción Gráfica: Servigrafía. servigrafia.ag@telefonica.net - servigrafia.ag@hotmail.com

Nuestras publicaciones son GRATUITAS.
Más información en: www.ceaccu.org

Índice

0.	Introducción	3
1.	¿Dónde reclamo? ¿Qué cauces existen y cómo elegir el adecuado?	5
2.	Elementos del delito de estafa	9
3.	Principales tipos de estafas	11
4.	¿Qué hacer si he sido víctima de una estafa?	31
5.	Direcciones de utilidad	33

0. Introducción

En los últimos tiempos hemos asistido a una radicalización de los abusos cometidos contra los consumidores y usuarios. Más allá de las meras irregularidades administrativas, los cumplimientos defectuosos de los contratos, o incluso los incumplimientos flagrantes, se extienden auténticas redes criminales inmersas en variadas prácticas delictivas que apuntan como objetivo por su mayor debilidad al consumidor final. Dentro del amplio abanico de delitos que comprende nuestro Código Penal, las estafas a consumidores comienzan a ser realidades demasiado reiteradas en nuestro entorno social.

Las nuevas tecnologías han abierto una brecha desconocida para la comisión de los más variados fraudes, hallando como víctimas a usuarios todavía poco familiarizados con los peligros que entrañan y confiados en la seguridad que ofrece la denominada sociedad de la información.

Frente a estas actuaciones especialmente voraces, se alza un último instrumento de protección, capaz de dar respuesta a los peores ataques que padecen los usuarios, el Derecho Penal.

Ante muchas de estas conductas, el usuario es cierto que no tiene mayor protección que la que le puedan dispensar las fuerzas y cuerpos de seguridad y administración de justicia, sin embargo conocer las principales prácticas delictivas que nos acechan como consumidores, y en su caso, cuáles son los recursos existentes para su persecución, contribuye a una mejor prevención y solución del problema si ya hemos sido víctima del delito. Ofrecer esta aproximación a los usuarios, centrados en las defraudaciones o estafas, de un modo práctico y sencillo es el modesto objetivo de esta guía.

1. ¿Dónde reclamo? ¿Qué cauces existen y cómo elegir el adecuado?

1. ¿Dónde reclamo? ¿Qué cauces existen y cómo elegir el adecuado?

Los consumidores padecemos frecuentemente muchas situaciones injustas, imposición de cláusulas abusivas, trabajos mal ejecutados, servicios no cumplidos, interminables esperas para la recepción de lo prometido, información incorrecta por el comerciante... En todas estas realidades el consumidor puede reclamar, y existen diversas posibilidades, pero ha de saber hacia dónde dirigir sus pasos para tener éxito en su pretensión y obtener la satisfacción justa de sus intereses. Podemos distinguir cuatro grandes vías de reclamación, cuyas notas esenciales sintetizamos de modo muy esquemático por lo que aquí interesa:

- A) **Procedimiento Administrativo.** Totalmente gratuito para el usuario, sin necesidad de abogado ni procurador. Consiste en la comunicación a la administración competente (que puede ser la Dirección General de Consumo de su Comunidad Autónoma u organismo equivalente -vea el Anexo I de direcciones de utilidad-) de un determinado hecho que puede ser constitutivo de una infracción administrativa. En este caso la Administración estudiará su denuncia y si halla responsabilidad administrativa podrá aplicar una sanción a la empresa infractora, pero en términos generales no recibirá usted ninguna indemnización o restitución. Es una vía de reclamación acumulable a los siguientes cauces, y a pesar de que no vaya a obtener

directamente la reparación del perjuicio padecido, contribuirá a que otros usuarios no se encuentren en su misma situación.

- B) **Procedimiento Civil.** Podrá acudir directamente a este procedimiento sin necesidad de abogado y procurador sólo si su reclamación es inferior a 900 euros. Si el importe reclamado es mayor, tendrá que contratar a su costa a estos profesionales, salvo que por sus ingresos pueda acogerse al beneficio de justicia gratuita (ingresos inferiores al doble del salario mínimo interprofesional). Se tramitará ante el Juzgado de 1ª Instancia (o de lo mercantil en determinados casos de reclamaciones por transportes). A través de este procedimiento podrá reclamar la reparación de los daños y perjuicios que haya padecido. Es compatible con todas los demás procedimientos excepto el procedimiento arbitral de consumo.
- C) **Procedimiento Arbitral** de Consumo. Totalmente gratuito, sin necesidad de abogado ni procurador y sin ningún límite económico. Es un sistema de resolución de conflictos voluntario para ambas partes, por lo que requiere la aceptación del reclamado de someterse a éste. Se tramitara ante las Juntas Arbitrales de Consumo (vea anexo I de direcciones de utilidad). Es incompatible con el procedimiento civil y en la mayoría de los supuestos con el procedimiento penal.
- D) **Procedimiento Penal.** Totalmente gratuito para el usuario. No precisa abogado ni procurador, ya que el Ministerio Fiscal

asumirá, si procede, la defensa de sus intereses como perjudicado. Está reservado para los casos más graves en que más allá de una infracción de consumo o un contrato mal cumplido nos hallamos ante un delito o falta. Puede iniciarse mediante una denuncia ante la Comisaría más próxima de cualquiera de los cuerpos y fuerzas de seguridad del Estado o ante el Juzgado de Guardia. Tiene carácter preferente sobre cualquier otro procedimiento.

Ser prudente en la elección de uno u otro sistema tiene importantes consecuencias, ya que aunque pueda tener razón en su pretensión y le corresponda una indemnización por los daños o perjuicios que haya padecido, si en una reclamación civil (ej. un producto en garantía defectuoso) opta por el procedimiento penal, su denuncia se archivará por no revestir caracteres de delito sin lograr su objetivo. Por otra parte existen vías que pueden ser incompatibles entre sí (ej. procedimiento civil y procedimiento arbitral de consumo) y otras que permiten su acumulación (ej. procedimiento administrativo y procedimiento civil). Si tiene dudas sobre el cauce adecuado para iniciar su reclamación, contacte con CEACCU.

2. Elementos del delito de estafa.

No toda compra o venta mal hecha es una estafa, ni siquiera todo engaño en un proceso de contratación ha de concluir con la existencia de estafa. Nuestro Código Penal exige la concurrencia de tres requisitos para que los tribunales puedan apreciar la existencia de estafa:

- A) **Beneficio para el defraudador** (ánimo de lucro). El defraudador ha de obtener o pretender al menos una ventaja patrimonial como consecuencia de su actuación (ej. obtener 1000 euros)
- B) **Existencia de un perjuicio.** Como consecuencia de la acción desarrollada por el defraudador el consumidor o un tercero ha de padecer o exponerse a un perjuicio real (ej. pérdida de 1000 euros)
- C) **Engaño bastante.** No basta que el consumidor haya sido levemente engañado, sino que nuestro Código impone que el engaño sea de cierta entidad, difícilmente perceptible para cualquier usuario medio o de las circunstancias personales en que se halla la víctima (ej. utilización de disfraz, documentación falsa, simulación de un determinado cargo o profesión...)

Sólo si concurren estos tres requisitos de modo conjunto podremos hablar de estafa, que resultará perseguible, incluso aunque el estafador finalmente no haya tenido éxito en su plan.

3. Principales tipos de estafas

3.1. Las de toda la vida, aún vigentes.

A pesar de su larga tradición hay un importante número de ciudadanos que siguen cayendo año tras año en las estafas más convencionales. Con frecuencia los estafadores prefieren elegir como víctimas personas de edad avanzada, aunque ninguno estamos exentos de riesgo. Si pese a todo, Vd. ha sido víctima de un delito, no se avergüence por ello y presente la correspondiente denuncia.

A) EL TIMO DE LA ESTAMPITA.

Probablemente es la estafa convencional más extendida. Se desarrolla a través del acuerdo de dos timadores en el que uno asume el papel de “tonto” y el otro de “listo” convenciendo a la víctima de que el “tonto” ha encontrado un gran número de billetes con los que juega o pretende entregar en algún convento o entidad de caridad sin ser consciente del valor que realmente tienen. El “listo” que hace de gancho, propone a la víctima cambiar la bolsa de dinero por una cantidad inferior y repartírsela. Con frecuencia “el listo” se ofrecerá a acompañar a la víctima al banco o a su domicilio para obtener su botín. Una vez que la víctima accede y entrega un importe en efectivo inferior al ofrecido por el “tonto”, ambos timadores (“tonto” y “listo”) desaparecen comprobando la víctima que lo que se ofrecía como una importante cantidad de dinero no son sino recortes de papel.

B) EL TIMO DEL TOCOMOCHO.

El timo del tocomucho no es sino una variante del de la estampita, sustituyendo en su desarrollo el dinero hallado por el gancho por billetes de lotería (ONCE, Primitiva, Nacional...). El timador que actúa como “tonto” y simula una disminución psíquica, se dirige a la víctima y exhibe unos billetes de lotería, que frecuentemente denomina papelitos, estampitas o cromos, preguntándole por la dirección del organismo de lotería u otra excusa para entablar conversación y transmitir la idea de deficiencia, haciéndole creer con el auxilio del listo, que interviene con posterioridad en escena que estos han resultado agraciados con un sustancioso premio. Así se le propone en síntesis a la víctima facilitárseles a cambio de una cantidad en efectivo notablemente inferior al premio o acudir a cobrarlo entre los tres y repartirse de un modo favorable para la víctima el importe. Recaudado en dinero de la víctima por los timadores, estos desaparecen antes de que



el perjudicado compruebe finalmente que se trata de billetes falsos.

Con frecuencia, el timado conjuga un sentimiento mixto de humillación y deshonestidad por su pretendida acción de defraudar a su vez a un deficiente mental, prefiere guardar silencio de lo ocurrido. Si a pesar de ello, Vd. ha sido víctima de un delito, no se calle, denúncielo.

C) LA ESTAFA DEL NAZARENO.

El timo del nazareno es otro de los más frecuentes, cuya comisión, lejos de disminuir en nuestros días parece ir en alza. Consistente en la compra o encargo de una gran cantidad de productos de sencilla comercialización, con apariencia de solvencia y sin la menor intención de abonarlos, normalmente se dirige contra empresarios más que hacia particulares, si bien admite su modalidad inversa haciendo creer al usuario el envío de ciertos productos que jamás son remitidos. Para evitar la persecución del delito suelen emplearse establecimientos comerciales fugaces que se alquilan con facilitación falsa de los datos de los timadores y mediante el cobro a través de medios de pago carentes de rastros (efectivo, cheques al portador).

D) EL TINTADO DE BILLETES O LOS BILLETES MÁGICOS.



En esta modalidad defraudatoria el timador hace creer a la víctima que tiene acceso a un sofisticado sistema para elaborar dinero o bien que posee una importante cantidad de billetes de curso legal que tratará de justificar con cualquier extraña procedencia (Ej. provenir del gobierno de un país africano del que los ha tenido que sacar ocultos mediante su camuflaje con una tinta especial o de cualquier actividad ilícita) a los que es necesario someter a un proceso químico para recuperar su apariencia normal. Con frecuencia la estafa se desarrolla mediante la inyección de un “líquido especial” en unos supuestos fardos de billetes embalados con cinta. Tras lograr el convencimiento de la víctima mediante una demostración en la que parece transformarse un papel negro o blanco en un billete auténtico mediante la aplicación de un reactivo químico y que se ofrece a ésta para su comprobación, se le invita a participar en la operación mediante la aportación de una determinada cantidad de dinero para adquirir los productos necesarios para el “lavado” de los billetes tintados, con la promesa de unos elevados beneficios. El perjudicado al que se dejan varios ejemplares de billetes auténticos manipulados ante su presencia y tras comprobar en cualquier banco que efectivamente se trata de moneda de curso legal confía en los estafadores a los que les entrega su cuota económica de participación

en el negocio, recibiendo a cambio los supuestos billetes tintados que con posterioridad comprobará no son sino trozos de vulgar papel.

E) LA ESTAFA DE SEGURO.

En otras ocasiones son los propios consumidores quienes pretenden obtener un beneficio a cargo de su aseguradora. A través de la denominada estafa de seguro, el defraudador, asegurado, simula un siniestro en el objeto cubierto por póliza de seguro o acomete directamente un daño contra su patrimonio o su integridad, con objeto de beneficiarse de la cobertura de la póliza induciendo a error al asegurador para que abone la correspondiente indemnización. Habida cuenta de la variedad de pólizas existentes y las múltiples posibilidades de cobertura, la tipología que presenta la estafa de seguro es casi infinita desde accidentes de tráfico ficticios a incendios en bienes propios. Sea consciente de que este tipo de actuaciones constituye un delito por el que podrá conllevar una pena de hasta tres años de prisión.

3.2. Nuevo tipos de estafas contra los consumidores.

A) EL FALSO REVISOR DEL GAS.

Extraordinariamente extendido en su



práctica y reiteradamente alertado por asociaciones de consumidores y usuarios resulta el fraude del falso revisor del gas. Ataviados con un mono de trabajo y caja de herramientas en mano, simulados revisores o inspectores de gas, se identifican como personal de la empresa instaladora o suministradora aduciendo la necesidad de realizar una inspección de la instalación. Tras la apariencia fingida de realizar alguna operación de mantenimiento o reparación, que en ocasiones viene motivada por la propia avería dolosamente causada por el agente falsario, se solicita al usuario el pago de su intervención, con frecuencia de modo abusivo, llegando a expedir incluso una factura por los servicios prestados.

Nuevamente los autores de este tipo delictivo seleccionan con frecuencia hogares con usuarios de avanzada edad que vivan solos para facilitar la perfección de su comisión delictiva. En caso de no conseguir el acceso al domicilio, los falsos inspectores suelen amenazar con un supuesto corte del suministro de gas, logrando así atemorizar a sus víctimas con un perjuicio mayor.

Nunca permita el acceso a su domicilio de ninguna persona sobre la que albergue cualquier duda por muy uniformado que aparezca. Consulte con su compañía suministradora antes de permitir cualquier intervención sobre sus instalaciones. Consulte también con cualquier vecino en caso de sospechas. Piense que si la intervención es cierta, siempre podrá volver

otro día el técnico tras sus comprobaciones.

B) SERVICIOS DE TARIFICACIÓN ADICIONAL.

Los servicios de tarificación adicional son aquellos que se prestan a través de la línea telefónica mediante una llamada o envío de mensaje y que tienen un coste para el usuario superior al de una llamada convencional.

Actualmente están reconocidos como códigos para la prestación de servicios de tarificación adicional el 803, 806, 807 y 907 y los denominados mensajes de texto Premium (SMS) que comienzan por 2, 3, 79 y 99. No obstante existen otros números similares como el 905 o algunos “servicios de información”, que aún no teniendo el carácter legal de tarificación adicional presentan las mismas características.

Obviando las estafas informáticas a las que más adelante nos referiremos, los fraudes más frecuentes se articulan a través de las siguientes técnicas:

a) **Falsas promociones comerciales, concursos y publicidad engañosa.**

Consisten en el ofrecimiento de un presunto regalo u oferta comercial. Es frecuente que el usuario reciba directamente una comunicación (carta, e-mail, o SMS), informándole que ha sido agraciado con determinada oferta o

premio, indicándole la necesidad de llamar al número de tarificación adicional (en ocasiones disimulado mediante la alteración habitual de la indicación del código: Ej. 80-60-XX-YYY).

Evidentemente, una vez realizada la llamada por el usuario, se procurará su máxima retención posible, e incluso la realización de varias llamadas para poder recibir el premio ofrecido, que no suele existir.

Especiales escándalos, ha desatado la proliferación de concursos televisivos, frecuentemente difundidos por las televisiones locales, en los que bajo la formulación de una pregunta cuya respuesta es evidente, se incita a los televidentes a llamar al servicio de tarificación adicional para la obtención de un premio, prolongándose la llamada del usuario hasta una hipotética entrada en directo en el programa y cuyo fruto final siempre suele ser el de un laurel inexistente, o la obtención de un premio consistente en jamones o llamadas gratuitas durante seis meses, un viaje para dos personas gratis... promociones éstas con falsos premios en una gran mayoría de los casos.

b) **Falsos contactos (ofertas de trabajo, relaciones o situaciones de emergencia).**

Anunciadas generalmente en las páginas de ofertas de empleo de los diarios, ofrecen puestos asequibles con una

interesante remuneración. Una vez realizada la llamada por el demandante de empleo, los teleoperadores realizarán un extenso cuestionario, con objeto de retener la llamada el máximo tiempo posible, solicitando incluso en ocasiones con objeto de dar la mayor credibilidad una fotografía o curriculum vitae (en general dirigido a una dirección inexistente).

Una especialidad curiosa dentro de este grupo, es la consistente en el anuncio de contactos personales dirigidos fundamentalmente a individuos de sexo masculino. Este tipo de anuncios ofrecen relaciones sexuales remuneradas dentro del ámbito geográfico del usuario llamante. Finalmente, el usuario comprobará que lejos de entablar una relación, se enfrentará a una elevada factura telefónica, sin haber logrado establecer ningún contacto.

El caso más extremo parece desarrollarse entorno a supuestas actuaciones sanitarias. Se ha detectado una estafa consistente en la recepción por parte del usuario de una llamada telefónica o mensaje que dice proceder de algún centro público sanitario y que insta al usuario a ponerse en contacto urgentemente con determinada gerencia de un Hospital o departamento de pacientes de un centro de salud con relación a un familiar o para la actualización de unos datos. También

bajo el abrigado manto de la salud, se han realizado estafas alegando la realización de unas encuestas de salud realizadas por técnicos municipales.

c) **La instalación de dialers o programas marcadores.**

Es una variante de las estafas cometidas a través de números de tarificación adicional, pero en lugar de realizarse mediante una llamada de voz, es el módem de nuestro ordenador quien realiza la llamada. El delincuente oculto tras determinadas páginas Web y con frecuencia con el gancho de sencillos programas de descarga gratuita, logra la instalación en el ordenador de la víctima de un programa de marcación telefónica automática. A partir de este momento, dicho programa instalado sin el conocimiento ni consentimiento de la víctima se conecta automáticamente a un número de tarificación adicional (un 907 o cualquier otro situado en el extranjero) al ejecutar determinado comando (ej. ver tu horóscopo diario, información metereológica...)

En general el usuario no advierte el fraude sino hasta recibir la primera factura con un elevado importe.

Como prevención además de solicitar la desconexión de los servicios de tarificación adicional a su operador, si no desea hacer uso de ellos, existen antivirus

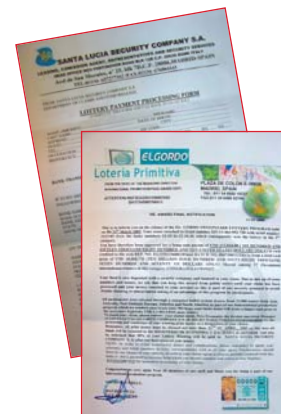
que protegen su ordenador. Puede comprobar el estado de sus conexiones a través de su “acceso telefónico a redes”

Si ya ha sido víctima de un delito, no borre ningún archivo para permitir la investigación policial.

Como eficaz medio de prevención frente a este tipo de estafas, si no desea hacer uso de los servicios de tarificación adicional, puede solicitar a su operador telefónico (tanto de fijo como de móvil), la solicitud de **DESCONEXIÓN DE LOS SERVICIOS DE TARIFICACION ADICIONAL**. Solicítelo por escrito dejando constancia de su petición o si lo realiza telefónicamente pida una confirmación documental de su solicitud.

C) LA ESTAFA DE LA LOTERÍA NIGERIANA.

La denominada estafa de la lotería nigeriana comienza con la recepción de una carta o correo por la víctima en la que se le comunica que ha sido agraciado con un premio de lotería. Para tener acceso al premio anunciado se solicita a la víctima que envíe una determinada cantidad de dinero con objeto de cumplimentar los trámites administrativos necesarios para su entrega, impuestos, etc. Esta cantidad de dinero es la que pierde el usuario y obtiene el delincuente, constituyendo la esencia de la estafa. Huelga decir que jamás existe ningún premio.



Naturalmente esta estafa ha desarrollado numerosas variantes entre las que destaca la oferta a la víctima de recibir una gran cantidad de dinero a cambio de permitir emplear su número de cuenta para recibir una cuantiosa transferencia, de la que recibirá un porcentaje.

Este tipo de estafas se arropan de una compleja estructura con teléfonos, faxes y páginas web auténticas, incluso si es preciso a través de un contacto personal entre víctima y estafador con objeto de afianzar la creencia de la víctima en las iniciales averiguaciones que desarrollará sobre el gancho ofrecido.

D) SUBASTAS Y VENTAS POR INTERNET.

Las subastas y ventas por Internet se han constituido también en un nicho importante de estafas. Una modalidad ligada a esas operaciones es la inexistencia del producto ofrecido. La técnica habitual consiste en el ofrecimiento o publicidad de bienes de segunda mano (con frecuencia vehículos o material informático), procedentes de stocks, o con pequeñas taras ofertados a un precio muy atractivo. El estafador solicita el pago por giro sin rastro (empresas de servicios de transferencias en minutos a cualquier parte del mundo, envío de dinero desde locutorios, especializadas en remesas de inmigrantes...) logrando el dinero y sin entrega alguna de producto.

Como precaución trate siempre de pagar

contra reembolso y compruebe la mercancía antes de abonarla (aunque haga esperar al transportista). Evite las transferencias bancarias y pagos a través de empresas de transferencias de dinero. Y finalmente, desconfíe de precios ridículos fuera de la lógica comercial.

Otra modalidad inversa consiste en que un determinado vendedor honesto recibe una oferta intensamente interesada en la adquisición del bien que se compromete a pagar incluso a un precio superior del solicitado, requiriendo el bien con urgencia. El objetivo será lograr el número completo de cuenta corriente de la víctima bajo el pretexto de realizarle una transferencia y una vez obtenida poder utilizarla de modo fraudulento.

E) LA PESCA DE DATOS O EL PHISING BANCARIO.

El phishing (pesca de datos), consiste en la captación ilícita de datos personales, principalmente relacionados con claves para el acceso a servicios bancarios y financieros a través de correos electrónicos o páginas Web que imitan y copian la imagen o apariencia de una entidad bancaria o financiera.

Prevaliéndose del prestigio o confianza que ofrece al usuario la entidad suplantada los defraudadores solicitan los datos de acceso, en general con la excusa de cualquier comprobación urgente de seguridad.

Cuatro cautelas básicas para evitar ser víctimas del phishing son:

- a) Recordar que la banca nunca solicita nuestras claves personales de acceso por ningún medio.
- b) Comprobar que la navegación es segura, identificada con la dirección **https** o por la presencia de un candado cerrado en la parte inferior de su navegador.
- c) Verificar el certificado de seguridad a través del candado amarillo que deberá aparecer en la parte inferior de la pantalla.
- d) No acceder a ninguna página web de servicios bancarios o financieros a través de vínculos alojados en correos electrónicos. Conviene dirigirse a las páginas Web directamente a través del navegador.

F) OBTENCIÓN DE LA NUMERACIÓN DE LA TARJETA, CLAVE DE SEGURIDAD Y REALIZACIÓN DE COMPRAS A CARGO DEL USUARIO.

Las tarjetas de crédito abren todo un universo de compras. Muchas de ellas es posible realizarlas a distancia (por teléfono, fax, correo, Internet...) sin la necesidad de su presentación física. Por ello, algunos delincuentes tratan de obtener los datos de las tarjetas de usuarios mediante engaño,

haciéndose pasar por la entidad emisora o con supuestos controles de seguridad, para realizar compras fraudulentas con cargo a la víctima y desaparecer después.

Para determinadas compras además de la identificación del titular, numeración de la tarjeta y fecha de caducidad se exige la clave de seguridad que esta compuesta por 3 o cuatro dígitos en el anverso o reverso de la tarjeta. No facilite nunca ningún dato. Los consejos para evitar ser víctima de esta estafa son similares a los expuestos para el phishing, pues no es sino una variante de este.

G) PHARMING.

Otra técnica que procura la captación de datos personales de los usuarios consiste en la creación de una página falsa (fenómeno conocido como web spoofing) con apariencia similar a otra bien reputada con la finalidad de suplantar a los usuarios una vez que se han obtenido sus claves, en la convicción de estos de que accedían a la página Web correspondiente a su banco. El pharming es probablemente una de las estafas informáticas más peligrosas por la dificultad que entraña para su percepción por el usuario.

El desvío del tráfico de la página Web original a la suplantada se realiza mediante el denominado “envenenamiento de DNS”, logrando la asociación de la Web verdadera

con su dirección IP. Una vez que el usuario ha sido redirigido a la falsa página Web, confiando en encontrarse en un sitio seguro, introduce su nombre de usuario y contraseña, que son capturados por el delincuente

Como consejos preventivos han de reiterarse los expuestos anteriormente con relación al phishing.

H) SCAM.

El scam es la captación de personas por medio de correos electrónicos, anuncios en web de trabajo, chats, irc, etc., donde empresas ficticias le ofrecen trabajar cómodamente desde casa y cobrando unos beneficios muy altos. Unas veces sin saberlo y otras con ignorancia deliberada, la víctima esta blanqueando dinero obtenido por medio del phishing (procedente de estafas bancarias).

Cierra el círculo de la estafa y el blanqueo la petición a la víctima de remisión de las cantidades recibidas en su cuenta mediante giros anónimos de rastro, manteniendo una parte por su contribución.

Tenga presente que en determinados casos, si usted puede ser consciente de la estafa y por obtener un beneficio coopera con ello, se convertirá en delincuente y podrá ser juzgado también como estafador con penas de hasta 3 años de prisión.

I) KEYLOGGERS.

El keylogger o “registro de tecleo” consiste en un programa maligno (malware), de tipo espía (spyware) que logra instalarse en el ordenador de la víctima sin su conocimiento (generalmente a través de descargas gratuitas) buscando determinadas secuencias introducidas por el usuario, que normalmente son combinaciones de nombres de usuarios y contraseñas o login y password. Una vez obtenidas, el programa envía los datos al estafador sin conocimiento del usuario. A partir de entonces, el delincuente simplemente tiene que suplantar a la víctima para lograr el desplazamiento patrimonial pretendido.

J) EL LAZO LIBANÉS.

Este tipo de estafa suele desarrollarse del modo siguiente: los timadores introducen el llamado "lazo" -que suele ser, la mayoría de las veces, una cinta magnetoscópica, generalmente película de cassette de video- para que el cajero no reconozca la introducción de una tarjeta en el mismo. De esta manera, la víctima, cuando llega al cajero para realizar cualquier transacción, enseguida comprueba que la tarjeta se ha quedado atascada en la ranura y que no puede operar.

En ese momento aparece uno de los timadores, haciéndose pasar por buen samaritano y ofreciéndole ayuda, bien le

facilita su teléfono móvil y le sugiere que se comunique con la sucursal bancaria para que allí le aconsejen o bien le invita a pulsar nuevamente su código para recuperar su tarjeta, momento este en que percibe la clave. Al otro lado de la línea se encuentra el segundo timador, que le pide a la víctima que marque ocho cifras en el teléfono; las últimas cuatro deben de ser las del número de seguridad de la tarjeta de crédito. Cuando se ha realizado esta operación, la víctima contempla con estupefacción que, pese a todo, la tarjeta de crédito no es devuelta por el cajero, así que finalmente abandona el lugar, momento en el cual los timadores aprovechan para recoger la misma y utilizarla, al conocer el código de acceso a la misma.

K) CLONACIÓN DE TARJETAS Y UTILIZACIÓN DE LAS MISMAS.

La clonación o duplicado de tarjetas de crédito constituye por sí sola un grave delito, asimilado a la falsificación de moneda en nuestro Código Penal.

Se realiza a través de sofisticados programas informáticos y un equipo especial para obtener los datos de la banda magnética de la tarjeta.

Aunque su prevención para no ser víctima del delito es compleja para el usuario por lo avanzados que resultan los métodos empleados la mejor cautela es exigir

siempre que se realice cualquier pago que la tarjeta sea pasada por el terminal ante nuestra vista, para ello cada vez se van extendiendo más los terminales inalámbricos. Junto a ello escriba en el reverso de su tarjeta: SOLICITAR SIEMPRE DNI, pida a su banco la inserción digital de su fotografía en la tarjeta y exíjale que le envíe un SMS de confirmación con cada compra que realice.

El usuario suele ser consciente del delito una vez que comienza a recibir elevadas facturas asociadas a su tarjeta por compras que jamás ha realizado y frecuentemente en exóticos lugares que nunca visitó. Tan pronto como sea consciente de ello, anule su tarjeta, presente una denuncia inmediata a la policía y reclame a su banco la devolución del importe indebidamente cobrado.



4. ¿Qué hacer si he sido víctima de una estafa?

4. ¿Qué hacer si he sido víctima de una estafa?



Si usted ya ha sido víctima de una estafa o sospecha que puede estar siéndolo, le sugerimos los siguientes pasos:

- 1º) No se avergüence de haber sido víctima de una estafa.
- 2º) Conserve todos los documentos o datos que puedan contribuir a la comprobación del delito y averiguación del delincuente (Ej. correos electrónicos, facturas telefónicas con detalle de las llamadas realizadas, chats, claves de acceso, login, passwords, extractos de cuentas bancarias, recibos de cualquier pago, ingreso o transferencia, historial de su navegador, archivos temporales de Internet, cookies). Si es posible realice copia en soporte digital e imprima también los documentos.
- 3º) Si ha establecido también comunicación visual con el presunto delincuente trate de recordar los máximos detalles posibles para su identificación (descripción física del delincuente –altura, peso, complexión, cabello o barba, ojos, tatuajes-, indumentaria -vestimenta, anillos, pulseras, cadenas, tipo de ropa-, acento o déficit en la pronunciación, vehículo del delincuente –marca, modelo, color, matrícula-, lugar

dónde se conocieron o encontraron, día y hora...).

- 4º) Presente una denuncia en cualquier comisaría de las fuerzas y cuerpos de seguridad, aportando cuantos datos y documentos pueda ofrecer para facilitar la investigación. Confíe en la labor de los agentes. Recuerde que existen unidades especializadas en delincuencia tecnológica, que según los supuestos podrán desarrollar una investigación con mejores medios (ver direcciones de utilidad).
- 5º) Si cualquier empresa o entidad (operadora de telecomunicaciones, Banco o Caja de Ahorros, financiera...) le reclama el pago de cualquier deuda derivada de la estafa, contacte con CEACCU antes de realizar cualquier pago.



5. Direcciones de utilidad

CEACCU

C/ San Bernardo 97-99, Edif. Colomina, 2º F
28015 Madrid

www.ceaccu.org

Correo electrónico: **ceaccu@ceaccu.org**

Teléfono: 915945089

Fax: 915945124

INSTITUTO NACIONAL DE CONSUMO (I.N.C.)

C/ Príncipe de Vergara, 54
28006 Madrid

www.consumo-inc.es

Teléfono: 918 224 444

Correo electrónico: inc@consumo-inc.es

ORGANISMOS AUTONÓMICOS DE CONSUMO

INSTITUTO GALLEGO DE CONSUMO

C/ San Caetano, s/n. Edif. Administrativo. Bloque 5
15704 La Coruña

Teléfono: 900 23 11 23

Fax: 981/54 45 99

Correo electrónico: gerencia.igc@xunta.es

<http://www.igc.xunta.es>

DIRECCIÓN GENERAL DE CONSUMO DE ARAGÓN

Vía universitaria, 36 - 6º planta.

50017 Zaragoza

Teléfono: 900 12 13 14; 976/71 71 41 11

Fax: 976/71 56 09

Correo electrónico: consumo.doc@aragon.es

<http://www.aragob.es/consumo>

AGENCIA REGIONAL DE SANIDAD AMBIENTAL Y CONSUMO DE ASTURIAS

C/ Santa Susana, 20-2º
33007 Oviedo
Teléfono: 012; 901 50 10 50; 985/27 91 00; 985/10 83 02
Fax: 985/10 83 10
[http:// www.asturias.es](http://www.asturias.es)

DIRECCIÓN GENERAL DE CONSUMO DE ANDALUCÍA

Plaza Nueva, 4
41071 Sevilla
Teléfono: 900 84 90 90
Fax: 95/504 41 61 y 95/504 14 49
Correo electrónico:
dg.consumo.cgob@juntadeandalucia.es
[http:// www.juntadeandalucia.es/gobernacion](http://www.juntadeandalucia.es/gobernacion)

DIRECCIÓN GENERAL DE CONSUMO DE BALEARES

Pº del Borne, 17-1ª Planta
07012 Palma de Mallorca
Teléfono: 900 166 000; 971/17 62 62
Fax: 971/17 62 52
Correo electrónico: mgarcia@dgconsum.caib.es
<http://www.dgconsum.caib.es>

DIRECCIÓN GENERAL DE CONSUMO DE CANARIAS

C/ León y Castillo, 200. Edf. Usos Múltiples III-1ª Planta
35071 Las Palmas
Teléfono: 928 89 93 60
Fax: 928 89 97 67
Correo electrónico: dgconsgc@gobiernodecanarias.org
[http:// www.gobcan.es](http://www.gobcan.es)

DIRECCIÓN GENERAL DE COMERCIO Y CONSUMO DE CANTABRIA

C/ Hernán Cortés, 9-4ª Planta
39003 Santander

Teléfono: 942/20 79 36; 20 75 18
Fax: 942/20 75 28
[http:// www.csanidadcantabria.com](http://www.csanidadcantabria.com)

DIRECCIÓN GENERAL DE CONSUMO DE CASTILLA-LA MANCHA

C/ Berna, 1-1ª Planta. Edif. Iberdrola
45071 Toledo
Teléfono: 900 50 10 89; 925/28 45 29
Fax: 925/22 62 06
Correo electrónico: infoconsumodgc@jccm.es
[http:// www.jccm.es/sanidad/consumo/index.htm](http://www.jccm.es/sanidad/consumo/index.htm)

DIRECCIÓN GENERAL DE PROTECCIÓN CIVIL Y CONSUMO DE CASTILLA Y LEÓN

C/ García Morato, 24
47007 Valladolid
Teléfono: 902 47 77 47; 983/41 25 68; 41 13 80
Fax: 983/41 41 00 78
[http:// www.jcyl.es](http://www.jcyl.es)

AGENCIA DE CONSUMO DE CATALUÑA

Avda. Diagonal, 405 . Bis - 2ª Planta
08008 Barcelona
Teléfono: 93/484 93 00
Fax: 93/484 93 20
Correo electrónico: consum@consumcat.net
[http:// www.consum.cat](http://www.consum.cat)

CONSEJERÍA DE SANIDAD Y CONSUMO DE CEUTA

C/ San Amaro, 12
51001 Ceuta
Teléfono: 956/20 06 80
Fax: 956/20 07 23
Correo electrónico: sanidad-bsocial@ceuta.info
[http:// www.ceuta.es](http://www.ceuta.es)

DIRECCIÓN GENERAL DE CONSUMO DE EXTREMADURA

C/ Juan Pablo Forner, 9
6800 Badajoz
Teléfono: 924/00 85 20
Fax: 924/00 85 21
correo electrónico: dgpspc@sc.juntaex.es
[http:// www.juntaex.es](http://www.juntaex.es)

DIRECCIÓN GENERAL DE SALUD PÚBLICA Y CONSUMO DE LA RIOJA

C/ Belchite, 2
26071 La Rioja
Teléfono: 941/29 11 09
Fax: 941/29 11 41
Correo electrónico: dg.salud@larioja.org
[http:// www.larioja.org](http://www.larioja.org)

DIRECCIÓN GENERAL DE CONSUMO Y ATENCIÓN AL CIUDADANO DE MADRID

C/ Ventura Rodríguez, 7-4ª Planta
28008 Madrid
Teléfono: 012; 91/420 58 80
Fax: 91/580 33 39
Correo electrónico: consultas.consumo@madrid.org
[http:// www.madrid.org](http://www.madrid.org)

DIRECCIÓN GENERAL DE CONSUMO DE MELILLA

C/ Duque de Ahumada, s/n. Edificio Mantelete
52801 Melilla
Teléfono: 952/69 92 71
Fax: 952/69 92 72
Correo electrónico: nmarti01@melilla.es
[http:// www.camelilla.es](http://www.camelilla.es)

DIRECCION GENERAL DE CONSUMO DE MURCIA

Calderón de la Barca, 14 . Edif. Atlas. 1ª planta
30071 MURCIA

Teléfono: 968/35 71 88
Fax: 968/22 83 76
<http://www.murciaconsumo.com>

DIRECCION GENERAL DE FAMILIA, INFANCIA Y CONSUMO DE NAVARRA

Parque Tomas Caballero, 1 - 2ª planta. Edif. Fuerte del Príncipe II
31005 Pamplona (Navarra)
Teléfono: 848 42 77 33
Fax: 948/42 35 90; 96
Correo electrónico: infoconsumo@cfnavarra.es
[http:// www.cfnavarra.es](http://www.cfnavarra.es)

DIRECCIÓN GENERAL DE COMERCIO Y CONSUMO DE PAÍS VASCO

C/ Donostia San Sebastián, 1
07071 Vitoria - Gasteiz
Teléfono: 945/01 99 23
Fax: 945/01 99 31, 945 01 99 47
Correo electrónico: consumo@ej-gv.es
[http:// www.euskadi.net/consumo](http://www.euskadi.net/consumo)

DIRECCIÓN GENERAL DE COMERCIO Y CONSUMO DE VALENCIA

C/ Colón, 32
46004 Valencia
Teléfono: 012; 96/318 42 19
Fax: 96/368 42 16; 963 98 51 70
[http:// www.gva.es/inicio.html](http://www.gva.es/inicio.html)

GUARDIA CIVIL

- <http://www.guardiacivil.es>
- Teléfono de emergencias: 062 y 112
- Para delitos telemáticos:
<https://www.gdt.guardiacivil.es>

- Correo del grupo de delitos telemáticos:
delitostelematicos@guardiacivil.org

POLICÍA NACIONAL

- **<http://www.policia.es/>**
- Teléfono de denuncias 902102112
(posteriormente tendrá que acudir a la comisaría que desee solo a firmarla ahorrándose tiempo de espera)
- Teléfono de emergencias 091 y 112
- Brigada de Investigación Tecnológica

- CENTRO POLICIAL DE CANILLAS

C/Julián González Segador, s/n
28043 – Madrid

- Consultas genéricas:

delitos.tecnologicos@policia.es
91 582 27 47

- Fraudes en Telecomunicaciones

delitos.telecomunicaciones@policia.es
91 582 27 48

- Fraudes en Internet

fraudeinternet@policia.es
91 582 27 54

MOSSOS D'ESCUADRA

- **<http://www.gencat.net/mossos>**
- Teléfono de emergencias: 088 y 112

ERTZAINZA

- **<http://www.ertzaintza.net>**
- Para delitos informáticos puede contactar con
delitosinformaticos@ertzaintza.net
- Teléfono de emergencias: 112