Dirigido a: ENTIDADES FINANCIERAS, EMISORES, TÉCNICOS Y USUARIOS AVANZADOS

catálogo técnico europeo contra el fraude

Conozca con ADICAE el funcionamiento del fraude en medios de pago y sus posibles soluciones

ADICAE
Asociación de usuarios de Bancos, Cajas y seguros

Programa de Gestión de la Prevención, Preparación y Gestión del Terrorismo y otros Riesgos relativos a la Seguridad
Comisión Europea, Dirección General de Justicia, Libertad y Seguridad

Edita:

ADICAE
Asociación de Usuarios de Bancos, Cajas y Seguros

Servicios Centrales

c/ Gavín, 12 local - 50001 Zaragoza
Tel.: 976 39 00 60
Fax: 976 39 01 99
email: aicar.adicae@adicae.net
www.adicae.net

ÍNDICE

Un proyecto europeo para todos los consumidores

Las operaciones efectuadas mediante instrumentos diferentes del efectivo representan una proporción cada vez mayor de los pagos nacionales y transfronterizos, tanto por su volumen (número de operaciones) como por su valor (cantidad de dinero que se transfiere), y está previsto que su uso aumente aún más.

Pero estos cambios, muchas veces fomentados por las propias entidades financieras y empresas del sector, exigen que estos medios sean eficaces, fáciles de usar, ampliamente aceptados, fiables y disponibles para la mayoría de la población europea. El carácter transnacional del fraude hace necesaria una estrategia coherente de prevención a nivel europeo,

toda vez que, a pesar de su eficacia, las medidas que han adoptado los Estados miembros no son suficientes para contrarrestar la amenaza que representa el fraude en los medios de pago. Esta estrategia para combatir el fraude y sus efectos requiere la colaboración de todos.

Por ello, **ADICAE**, la única asociación de consumidores española especializada en bancos, cajas y seguros, preocupada por la situación de desprotección en la que están los usuarios de estos medios de pago en la actualidad afronta el proyecto europeodenominado **"Creación de un catálogo europeo técnico del fraude a disposición de las autoridades judiciales y policiales en base a una red de alertas e información facilitada por entidades y ciudadanos"** subvencionado por la Comisión Europea y en el que colabora con otras asociaciones de consumidores europeas.

En particular, con este catálogo, se pretende informar y alertar a los usuarios de las características técnicas de los medios de pago, así como de la operativa técnica concreta de los fraudes. No solo eso, sino que también sirva como una herramienta más de los operadores profesionales del mercado de medios de pago, los organismos policiales y judiciales responsables del fraude y diversas instituciones económicas, ya que este catálogo posee porpuestas de mejora dirigigas hacia todo tipo de actores, oprganizaciones y entidades.

En este proyecto participan junto con ADICE las siguientes asociaciones de consumidores europeas:

PARTE 1

Dimensión globalizada de los medios de pago distintos del efectivo

- **Situación actual en la Unión Europea y España**

  Evolución y expectativas

- **El impacto del fraude y su repercusión en los consumidores europeos**

Situación actual en la Unión Europea y España

El avance mundial de los medios de pago distintos del efectivo es indiscutible, tarjetas, transferencias, cheques, nuevos métodos de pago a través de Internet, pago por móvil ... están al alcance de todos los usuarios. Según el estudio "World Payments Report 2008" realizado por Capgemini, Royal Bank of Scothland (RBS) y la Asociación europea de Dirección y Márketing Financiero (EFMA), las tarjetas representan el 54% del volumen de pago en todo el mundo. Este medio de pago ha evolucionado en segundo lugar tras el efectivo, con una evolución anual entre 2001 y 2006 del 16% a nivel mundial y de un 11% en Europa. También las transacciones electrónicas de pago han experimentado un notable ascenso, llegando en todo el mundo aproximadamente a 210.000 millones de operaciones.

Evolución y expectativas

La circunstancia de que la emisión de medios de pago, fundamentalmente tarjetas, está creciendo a la vez que el volumen de operaciones de manera vertiginosa en todo el mundo y en especial en Europa queda constatado con las últimas cifras disponibles. En la zonaEuro existen actualmente más de 350 millones de tarjetas en circulación que se utilizan para realizar más de 12.000 millones de operaciones de pago y de 6.000 millones de retiradas de efectivo cada año. En cuanto a las tarjetas de crédito sólo en España llegaron a los 43,78 millones en marzo de 2008 y las de débito estaban en 31,46 millones, según los últimos datos disponibles del Banco de España.

El mercado europeo de medios de pago distintos al efectivo continúa creciendo. Un total de 70 billones de transacciones distintas al efectivo

se realizaron en Europa en 2006, cantidad equivalente a un tercio del mercado global. Los países de la Eurozona supusieron cerca del 73% del total; y tan sólo cinco países coparon el 85% del total de todas las transacciones de la Eurozona.

En 2006, según el informe anual del Banco de Italia de 2007, **España era el país con el mayor número de terminales de punto de venta** (TPV ó POS (en inglés)) con 1.291.000 unidades – 1276 operaciones por terminal y un importe medio de 52 euros -, seguido de Francia con 1.142.000 terminales – 4.938 operaciones por terminal y un importe medio de 51 euros – e Italia con 1.117.000 terminales, con 690 operaciones por terminal y un importe medio de 93 euros. El país europeo en el que se efectuó el mayor número de operaciones en TPV fue Finlandia con 7.799 transacciones, por un valor medio de 35 euros en sus 105.000 terminales. Por el contrario es Irlanda con 94 euros el país con el mayor importe medio por transacción con tarjetas de crédito y de débito, aunque el número de terminales instaladas en dicho país apenas se eleva a 53.000.

En cuanto al número de cajeros automáticos, éste creció un 4% durante el primer trimestre del año 2008, según los últimos datos oficiales del Banco de España, siendo el segundo país del mundo después de Japón en este aspecto. Así la red de cajeros automáticos de España era de 61.467 unidades en esa fecha, siendo la mayor de toda la Eurozona, seguida de la alemana. Durante ese período de tiempo, tres meses, los usuarios realizaron 240, 42 millones de operaciones de retirada de efectivo de los cajeros situados en España con tarjetas emitidas por cualquier entidad, un 1,74% más que el año anterior.

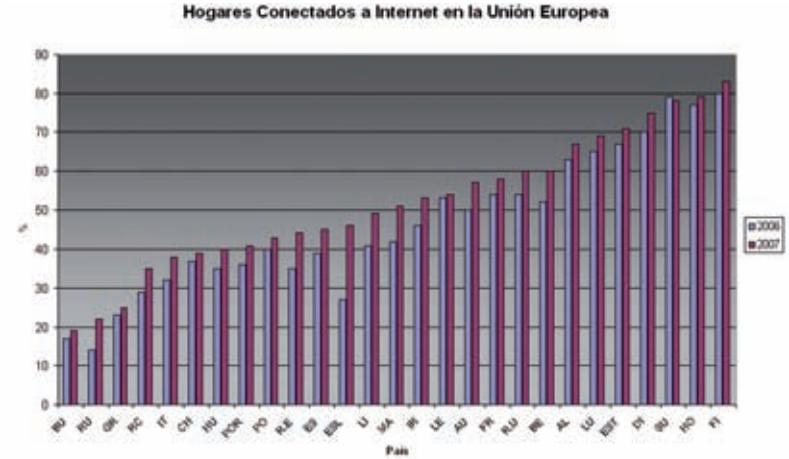
Las costumbres locales todavía determinan la preferencia de los instrumentos de pago por país. Sin embargo, existen dos tendencias en general válidas:

1 **Las tarjetas son el principal medio de pago distinto al efectivo,** con un uso constantemente creciente a una tasa de 11% por año entre 2001 y 2006.

2 **El uso de los cheques está disminuyendo,** aunque todavía no hay alternativa real para algunos tipos de pagos P2P (transacciones entre usuarios, p.ej. Ebay).

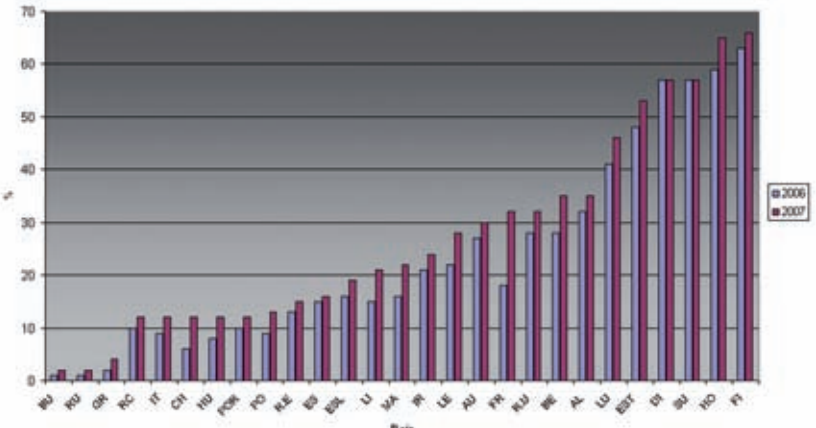
En mayor o menor medida, la presencia de Internet en el entorno de los hogares viene experimentando una tendencia alcista en todos los países de la Unión Europea a lo largo de los últimos años. En el conjunto de la UE15 el porcentaje de hogares con acceso a Internet se sitúa en el 59% a lo largo de 2007, lo que supone un incremento de 5 puntos porcentuales con respecto al valor del año anterior. Para el agregado de la UE27 las cifras son del 54% para el año 2007.

HOGARES CONECTADOS A INTERNET EN LA UNIÓN EUROPEA



Fuente: Word Payments Report 2008. Capgenini, RBS y EFMA

USUARIOS DE BANCA ELECTRÓNICA



Fuente: Word Payments Report 2008. Capgenini, RBS y EFMA

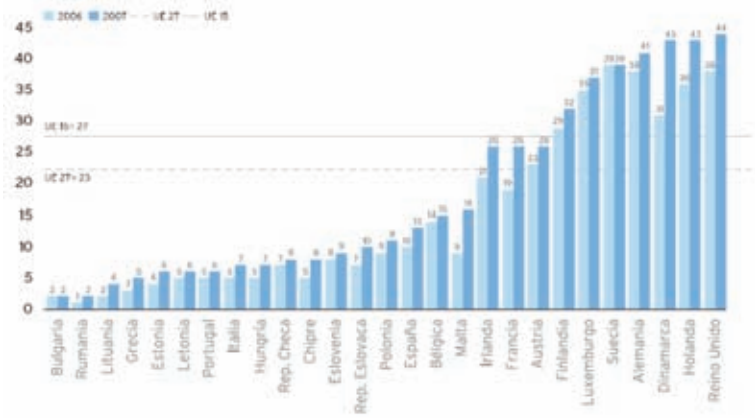
El número de individuos que usan e-banking está creciendo en toda Europa (p. ej., la proporción de la banca on-line en la UE-27 aumentó del 16% en 2004 al 24% en 2007). Si la tendencia observada continúa, se llegará a tasas del 50%-60% en 2020, un nivel que ya es común en los países nórdicos y el BENELUX (datos de Deutsche banks, 2008). La proporción de la población que usa banca electronica es, tal y como se observa en el gráfico, altamente dependiente de la localización geográfica del usuario.

El comercio electrónico un fenómeno creciente

La compra-venta de bienes y servicios se constituye como uno de los principales usos que tanto ciudadanos como empresas realizan a través de Internet.

A la vista del informe "Comercio Electrónico B2C, 2008" realizado por el Observatorio Nacional de las Telecomunicaciones y de la SI (ONTSI), podemos decir que el detalle de la buena situación del comercio electrónico en Europa aparece reflejado en el creciente porcentaje de particulares que utilizan la Red para ordenar o comprar bienes o servicios de uso privado. Reino Unido ocupa la primera posición del conjunto de países de la UE 27, con un porcentaje del 44%. Le siguen de cerca Holanda y Dinamarca con valores del 43% en ambos casos. Por el contrario, Bulgaria, Rumania y Lituania, cuentan con por-

PARTICULARES QUE HAN ORDENADO O COMPRADO BIENES O SERVICIOS DE USO PRIVADO POR INTERNET EN LOS TRES ÚLTIMOS MESES (%)



Fuente: Consumers in Europe: Facts and figures or services of general interest: 2007 edition. Eurostat

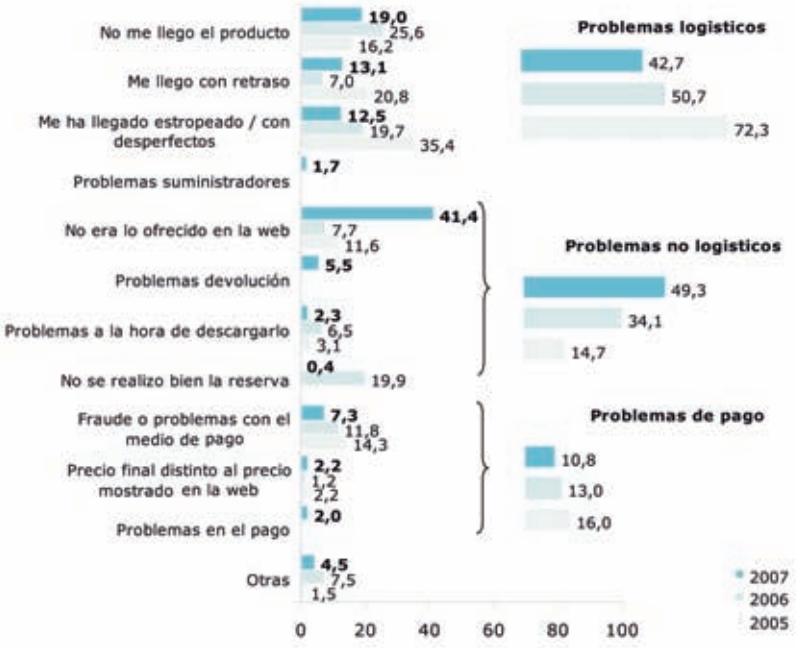
centajes que no superan el 4% y les sitúan en las últimas posiciones del ranking a nivel europeo.

Por término medio, en la UE15 el porcentaje asciende a un 27% de la población, frente al 23% que se puede contabilizar en la ampliación al grupo de los 27.

El problema fundamental que se ha detectado en las compras on-line es que el producto o servicio adquirido no responde a lo que se ofrecía en la web.

De hecho, éste es el problema que denuncian cuatro de cada diez compradores que han sufrido alguna dificultad en sus compras durante 2007.

¿QUÉ TIPO DE PROBLEMAS HA TENIDO EN LAS COMPRAS REALIZADAS POR INTERNET?



Fuente: Informe anual 2008 ONTSI

El resto de problemas con peso son de carácter logístico, o bien que no llega el producto (19%) o que llegó con retraso (13,1%), o incluso estropeado (12,5%).

Los problemas de pago (fraudes con medios de pago, precio final diferente al pactado o problemas con el pago), a pesar de ser los que generan mayores frenos entre los no compradores, tienen menos peso en el conjunto de los problemas, apenas un 10,8% de los mismos declara haber sufrido un contratiempo de esta categoría, frente al 42,7% que denuncia problemas logísticos.

El futuro de los medios de pago en la Unión Europea

Basándonos en los datos anteriormente citados, intentaremos echar la vista al futuro para ver cual será la evolución de los medios de pago distintos del efectivo. Pudiendo resaltar las siguientes apreciaciones:

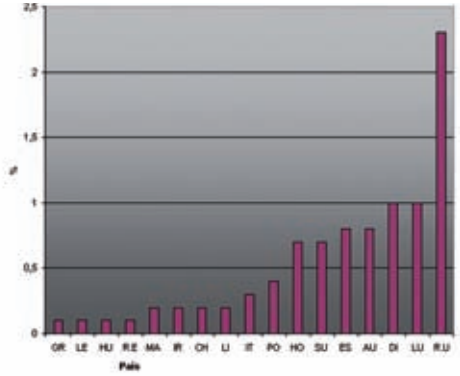
- **El esquema de los pagos europeos seguirá evolucionando.** Se espera un aumento generalizado.
- Asumiendo que la SEPA (Área Única de Pagos en Euros) ejerce una influencia notable sobre la convergencia en pagos distintos al efectivo, **el número de transacciones por habitante debería crecer a una tasa de un 9% hasta 2013.** Más concretamente, aquellos países donde las transacciones por habitante fueron menos de 150 en el año 2006, el uso debería de ser el doble para 2013.
- **El uso de tarjetas debería también aumentar radicalmente,** debido a que el número de comerciantes que acepta tarjetas crece, así como el número de productos que se comercializan. Sería positivo que el uso relativo de tarjetas sea especialmente destacado en países como Italia, Polonia y Grecia; donde el actual uso por habitante es pequeño.
- En los dos mayores países emisores de cheques, **Francia y Reino Unido, el conjunto de los medios de pago debería continuar evolucionando para pasar de los cheques hacia las transferencias,** tarjetas y domiciliaciones.

El impacto del fraude y su repercusión en los consumidores europeos

El fraude en Europa

Ante la amplia implantación de los medios de pago distintos del efectivo, han proliferado numerosos tipos de fraudes, como ya comentábamos al principio de este dossier. A continuación hacemos uso del informe Ontsi 2008, que se encuentra publicado en la web de Eurostat, para poder exponer este hecho con cifras. Es imprescindible destacar que es muy difícil obtener datos sobre este tipo de fraudes, ya que muchos son tratados con suma confidencialidad por las autoridades y otros nunca llegan a ver la luz.

FRAUDE CON TARJETAS EN INTERNET EN LA UE

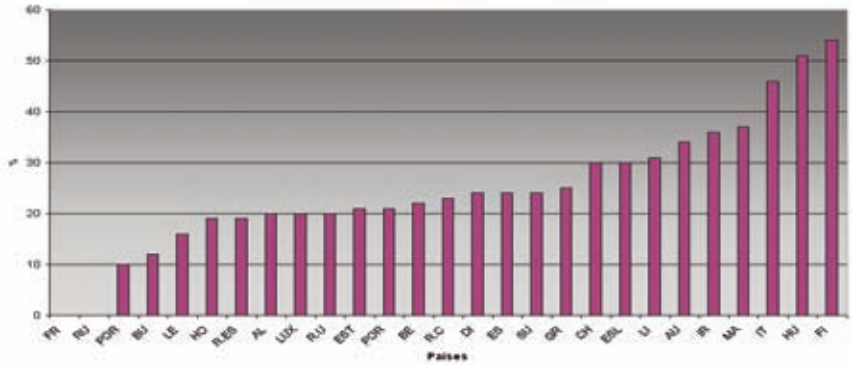


Fuente: Word Payments Report 2008. Capgenini, RBS y EFMA

En el gráfico vemos que en Reino Unido los fraudes llegan al 2,3 %, cifra que despunta con respecto al resto.

Observamos que los problemas que los virus causan en la seguridad de los datos son muy elevados, alcanzando cifras que rondan el 50% en Italia, Hungría y Finlandia.

PROBLEMAS DE SEGURIDAD CAUSADOS POR VIRUS INFORMÁTICOS EN LA UE



Fuente: Word Payments Report 2008. Capgenini, RBS y EFMA

El fraude en España

Según las autoridades españolas, **el 46% de los fraudes que se han producido en España en el último año 2009 se corresponden con estafas,** la mayoría de ellas relacionadas con medios de pago. La problemática abarca desde estafas en cajeros hasta robos electrónicos, pasando por incidencias ocurridas con todos y cada uno de los medios de pago que están al alcance del consumidor.

La implantación de las nuevas tecnologías en España, problemas de seguridad

Según el Informe Anual "La Sociedad en Red 2007", elaborado por ONTSI (Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información), seis de cada diez personas han accedido a Internet en alguna ocasión. Las Comunidades que presentan mayores porcentajes de internautas son Madrid, Cataluña y Baleares. Considerando la frecuencia de acceso a la Red, el 52,3% accedieron en el último mes y el 46,6% lo hicieron de una forma más intensa, ya que se conectaron en la última semana.

En cuanto a los problemas de seguridad más frecuentes relacionados con el uso del ordenador se encuentran los correos no deseados o spam (62,6% de los usuarios de Internet) y los virus informáticos (49,1% de los usuarios de ordenador). La recepción de correos no deseados es más frecuente en las Comunidades de Cataluña, Cantabria y Madrid. Por otro lado, Cataluña, Canarias y Aragón tienen los porcentajes más elevados de problemas relacionados con virus informáticos.

PROBLEMAS DE SEGURIDAD SUFRIDOS POR LOS USUARIOS
POR COMUNIDAD AUTÓNOMA

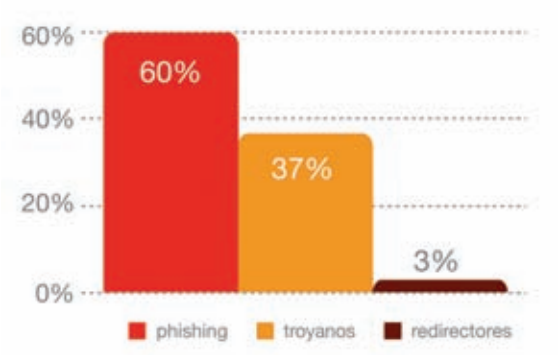
Fuente: SETSI y ONTSI

El nuevo fenómeno del ciberfraude en España

Basándonos en el "Informe de fraude online 2007 y primer semestre 2008 ", elaborado por la unidad e-crime de S21sec (Empresa de seguridad especializada en fraudes por Internet), podemos extraer las siguientes cifras sobre los ciberfraudes en España.

A lo largo de los primeros 6 meses de 2008, la unidad e-crime de S21sec detectó un total de 1.842 casos de fraude en Internet dirigidos a entidades financieras en España, lo que refleja una cantidad superior al número de casos total de 2007.

CASOS DE FRAUDE DETECTADOS
EN EL PRIMER TRIMESTRE DE 2008



Fuente: "Informe de fraude online 2007 y primer semestre 2008 . S21sec"

El phishing continúa siendo una de las principales preocupaciones aunque desciende en relación con años anteriores -60% de los casos de fraude hasta junio de 2008, 66% en 2007, 85% en 2006-, los ataques a través de Internet evolucionan de forma vertiginosa hacia técnicas más sofisticadas.

En el primer semestre del 2008 la utilización de **códigos maliciosos,** programas que se descargan sigilosamente en el ordenador del usuario mientras navega por Internet, se ha incrementado aunque muy levemente respecto a 2007, representando el 37% de los casos frente al 31% detectado el pasado año. Los redirectores, técnica utilizada para dificultar el cierre de los sitios cambiando la redirección de la página de phishing de forma dinámica, han supuesto el 3% de los casos.

El cajero, objetivo habitual de fraude

Como ya hemos dicho anteriormente, España es el país europeo que tiene más cantidad de cajeros automáticos por habitante, con una red que se aproxima a las 61.000 unidades. Por lo que es un objetivo muy apetecible para los delincuentes. En estos terminales suelen producirse dos tipos de robo distintos: el físico, en el que se incurre en violencia o intimidación, y el electrónico. Según consta en los anuarios del Ministerio del Interior, cada año tienen lugar 450 robos con violencia o intimidación en los cajeros automáticos. Una encuesta realizada por la multinacional NCR, especialista en seguridad electrónica para bancos y entidades financieras, desveló que en España uno de cada tres usuarios de cajeros automáticos considera insuficientes las medidas de seguridad. Este temor se explica porque, además de los **asaltos físicos,** también existen los **electrónicos,** que son mucho más frecuentes y sutiles, hasta el punto de que alguien puede ser robado sin que se de cuenta de ello en el momento.

PARTE 2

Catálogo técnico de medios de pago

- **La diversidad y complejidad de los medios de pago tradicionales distintos del efectivo**

  Tarjetas, transferencias, cheque, etc.

- **Nuevas fórmulas y métodos para pagar ¿Son seguros?**

  El chip en las tarjetas, pagos en el comercio electrónico

  Pago por móvil, banca on-line, Pay-pal, etc.

La diversidad y complejidad de los medios de pago tradicionales distintos al efectivo

Cada vez son más los posibles medios que tienen los consumidores para efectuar sus pagos. Los avances tecnológicos hacen que todos estos medios sustituyan y desplacen al uso de dinero en efectivo para cualquier tipo de compra, aunque ésta sea ya de escasa cuantía, ya que éstos son más rápidos, cómodos y efectivos. Las empresas emisoras de medios de pago y las entidades financieras cada vez ofrecen un mayor espectro, con lo que en la actualidad no hay posible usuario que no tenga un tipo de medio de pago que se acomode a sus características. Esto conlleva unas ventajas en cuanto a su funcionalidad y uso, pero también un mayor número de peligros para los usuarios. De ahí que gracias a los avances y mejoras dentro de este sector tanto comodidad como seguridad tenga que ir unidas.

No obstante existe una gama de medios de pago tradicionales que continúan siendo muy utilizados y sobre los que ha existido y continúa existiendo una amenaza constante de fraude.

Tarjetas, diferentes medios para diferentes usos

En la actualidad el uso de tarjetas está plenamente generalizado, es más, la media de tarjetas por persona en España es de casi 3, triplicándose el número de tarjetas en activo desde el año 2000 hasta el año 2007. Existe una amplia variedad de tarjetas, tanto en formato como en características y funciones.

Por desgracia esta multiplicación del número de tarjetas y sus tipos no ha venido aparejada de sustanciales mejoras en la seguridad ya que la banda magnética ha resultado ser muy vulnerable.

	TIPO	FOTO	COMENTARIO
DAN O NO CRÉDITO	Débito		Para poder extraer efectivo o realizar transacciones en establecimientos comerciales, es necesario tener vinculada una cuenta corriente en la entidad que la emite con saldo positivo; si no, la extracción o la compra nos será denegada.
	Crédito		La diferencia existente con la tarjeta de débito es que ofrece la posibilidad de pagar los gastos realizados en fechas posteriores a las que se han producido. Si el pago se realiza de forma fraccionada tiene unos intereses asociados.
ÁMBITO GEOGRÁFICO	Nacionales		Su uso se limita a la realización de transacciones en la moneda y país de su emisión.
	Internacionales		Se pueden utilizar en la compra de artículos en cualquier país del mundo y admiten compras en cualquier tipo de moneda.
OTROS	Mini		Son iguales a las tarjetas habituales pero de dimensiones más reducidas. No permiten sacar efectivo de cajero debido a sus dimensiones.
	Comerciales		Es un tipo de tarjeta, normalmente de crédito, emitido por grandes superficies, cadenas comerciales y asociaciones de comerciantes.
	Monedero		Permite ir cargando en la tarjeta importes de poco valor; su función es la de suplir al dinero en efectivo en los pagos cotidianos. Incorpora un microchip que registra la cantidad de dinero que se va descargando en los sucesivos pagos.

Sistema de tarjeta de banda magnética frente al Sistema EMV

En tarjetas clásicas de banda magnética, técnicamente su procedimiento cuando se pasa la banda por el lector tiene varias fases: adquisición de datos de pista de la banda, empaquetado y generación de un bloque de PIN cifrado y por último, envío a centro autorizador, que determinará, en función de si la tarjeta es propia o ajena, quien es reponsable de autorizar o denegar la operación. Es muy normal que además de los centros autorizadores de cada entidad financiera haya centros independientes que interconectan a las entidades, lo que permite que podamos operar con cualquier tipo de tarjeta en cualquier cajero, sea de nuestra entidad o no.

Por otro lado, el chip contiene una criptografía suficiente para generar criptogramas robustos, individuales para cada tarjeta (porque cada tarjeta tiene sus propias llaves), que serán enviados a los centros autorizadores, y en los que también viajan los datos de la tarjeta y el PIN introducido en el teclado para ser verificados y así poder conceder la preceptiva autorización o denegación a la transacción solicitada. En el caso de tarjetas EMV, también se pretende mejorar los procesos de autorización offline (sin acceso a centro autorizador).

La gran ventaja respecto al sistema tradicional es que en el caso de banda, la tarjeta no aporta nada al transporte criptográfico de bloque de PIN y datos de tarjeta al centro autorizador. En EMV, el chip sí permite aportar tratamiento criptográfico al proceso, porque el chip es ante todo eso: un elemento que genera criptogramas.

Paso de la banda magnética al chip

Tienen la misión de almacenar cierta información, como el nombre del titular, el número de su cuenta, el tipo de tarjeta y el PIN (Personal Identification Number). Básicamente se puede decir que identifica al usuario con la máquina con la que se pone en contacto (ATM, TPV...), y esta máquina o dispositivo, sola en ciertas operaciones, o conectándose on-line con otros dispositivos en otras, gestiona una serie de operaciones y guarda cierta información de cada transacción. La banda magnética es grabada o leída mediante contacto físico pasándola a través de una cabeza lectora/escritora gracias al fenómeno de la inducción magnética.

Propuestas de ADICAE
Mejoras técnicas en tarjetas para erradicar los fraudes

- **Mecanismos de autodefensa en cajeros automáticos.** Es decir, que los programas informáticos implantados en la gestión de cajeros automáticos cuenten con mecanismos de autodefensa que delatan cualquier movimiento de fondos extraño, ya sea por el lugar en el que se realiza la extracción, la frecuencia de las operaciones o la cuantía de las mismas.

- **Utilización del teléfono móvil como un segundo canal para autenticar y validar el pago.** El usuario de la tarjeta a través de su móvil recibiría un mensaje para autorizar la operación.

- **La obligación de solicitar el código CVV2 en las transacciones en la Red.** El código CVV2 (Card Verification Value) es un código de seguridad elaborado por las compañías de las tarjetas. Con este mecanismo de autenticación se identifica la posesión de la tarjeta empleada para el pago en las transacciones realizadas a través de la Red. Este código se debe introducir en el momento de la transacción económica por Internet para verificar que la tarjeta de crédito está en manos de su propietario, introduciendo un nivel de seguridad adicional a las transacciones realizadas.

- **Indicadores de nivel de fraude.** Consistiría en la introducción de un sistema inteligente que permita al usuario conocer, en función de los datos requeridos para una determinada operación, el nivel de riesgo que conllevaría su interceptación maliciosa antes de realizar dicha operación. Por ejemplo, sucesivos intentos de validación de datos sobre un mismo número de tarjeta de crédito variando su fecha de caducidad o el código CVV2 puede ser síntoma de un intento de uso fraudulento.

- **Instauración de tarjetas de crédito virtuales como medio de pago generalizado en vez de las tarjetas tradicionales.** Estas tarjetas en realidad son números que se solicitan a la entidad financiera. Este número se introduce en los formularios de pago cuando se realiza alguna compra por internet o por teléfono. Son de prepago, por lo que se debe cargar previamente transfiriendo dinero desde una cuenta corriente o desde otra tarjeta de crédito. Se puede cargar el dinero que se desee, por lo que el propio usuario limita el riesgo en caso de fraude. Las hay que tienen una duración limitada, de forma que sólo sirven para un periodo determinado, cancelándose una vez transcurrido este vencimiento, medida también muy útil contra el fraude.

Transferencias

Las transferencias bancarias y domiciliaciones constituyen un modo rápido de transferir dinero de una cuenta bancaria a otra. Es una manera de traspasar fondos entre cuentas bancarias sin sacar físicamente el dinero. Se llevan a cabo entre cuentas de una misma persona física o jurídica en un mismo banco o también entre diferentes bancos en diferentes países o entre cuentas de diferentes titulares.

Tipos de transferencias

- **Según el ámbito de aplicación:**
  - Transferencias nacionales: se trata de las transferencias realizadas entre un ordenante y un beneficiario los cuales se encuentran en el mismo país.
  - Transferencias exteriores o transnacionales: son aquellas realizadas por un ordenante y un beneficiario los cuales se encuentran en países distintos.

- **Según la importancia:**
  - Ordinarias: las realizadas en el plazo normal de ejecución.
  - Urgentes: las realizadas en un plazo inferior al estipulado.

Consecuencias de las transferencias fallidas o deficientes

La falta de realización de una transferencia dará lugar a una obligación de reembolso a favor del ordenante y a cargo de la entidad a la que éste ordenó la ejecución de aquella. El importe de ese reembolso está limitado en el caso de las transferencias transfronterizas hasta un total de 12.500 euros. El reembolso está compuesto por el importe de la transferencia, más el de los gastos que el ordenante hubiere abonado y el correspondiente interés legal. El reembolso deberá tener como presupuesto una solicitud formal del ordenante que, como es lógico, solo podrá presentarse una vez que se hubiere agotado el plazo convencional o normativo previsto para la ejecución de la transferencia que se reconoce al ordenante, se impone la obligación de llevar a cabo ese reembolso en el plazo de 14 días contados a partir de la fecha de la solicitud.

Domiciliación bancaria

Es el cargo que se realiza automáticamente a nuestra cuenta previo acuerdo con la empresa (con la que contratamos el servicio) y con el banco para que autorice los desembolsos. Esta modalidad de pago es muy frecuente para realizar desembolsos de carácter periódico como abonar la cuota del gas, luz, teléfono, etc. Las domiciliaciones bancarias suelen cobrarse de manera anual o semestral según se establezca de manera previa.

Propuestas de ADICAE
Mejoras técnicas en transferencias y domiciliaciones bancarias para erradicar el fraude

- Informar, vía teléfono móvil u otro medio de consulta habitual del cliente, de la realización de la transferencia y que éste disponga de un periodo de tiempo para cancelarla. De este modo se podrían cancelar transferencias fraudulentas.
- Pedir autorización al titular de la cuenta a la que va dirigida la transferencia con objeto de que compruebe que no hay ningún error en su importe y que conoce a la persona o empresa que la ordena.
- Envío de notificación previa a la realización de la transferencia, tanto a ordenante como a beneficiario; informando del importe más las comisiones que han de soportar cada uno. De este modo el usuario tendría la posibilidad de sopesar la realización del pago por otro medio si considera las comisiones abusivas.
- Instruir a la población sobre la necesidad de revisar periódicamente su libreta bancaria, para detectar domiciliaciones incorrectas o fraudulentas; en caso contrario podemos ser víctimas de este tipo de fraude durante mucho tiempo, ya que las domiciliaciones se producen de forma periódica.

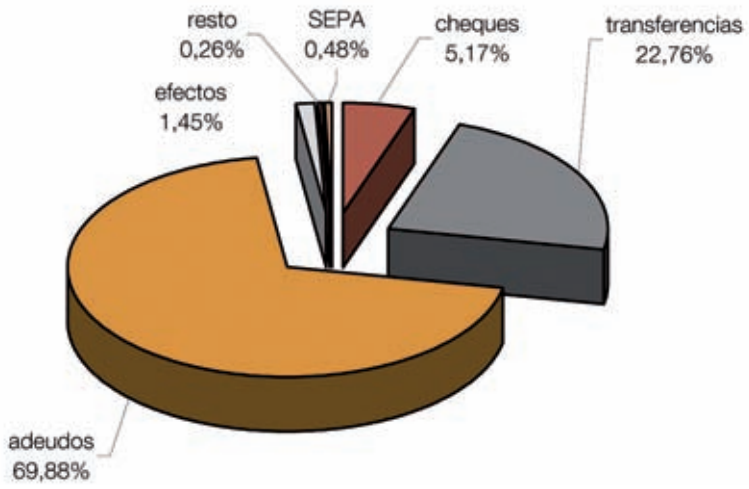
El sistema nacional de compensación electrónica: La llave de muchos de sus pagos

El SNCE es un sistema descentralizado que procesa las transacciones relacionadas con los instrumentos de pago al por menor. Debido a la variedad de instrumentos de pago, el esquema operativo del SNCE se estructura alrededor de varios subsistemas de compensación, cada uno de los cuales está especializado en un único instrumento.

Actualmente, de acuerdo con su Reglamento, estos subsistemas son: cheques, transferencias, adeudos, efectos y operaciones diversas. Este último subsistema fue creado en el año 2001 para el procesamiento de operaciones de distinta naturaleza (documentos no normalizados, comisiones y tasas de créditos y/o remesas documentadas, intercambio de moneda extranjera, etc.).

La mayor parte de los bancos, cajas de ahorro y cooperativas de crédito pertenecen al SNCE ya que éste se ha convertido en la forma más rápida y eficiente de comunicar los datos necesarios para una rápida compensación de los pagos al por menor.

Nº DE OPERACIONES POR SUBSISTEMA (AÑO 2009 - EN PORCENTAJE)



Fuente: Banco de España (datos hasta mayo de 2009)

El SNCE ha adoptado una solución intermedia que no consiste ni en un sistema de compensación y liquidación completamente centralizado, ni en uno completamente descentralizado. La información es intercambiada bilateralmente entre las partes implicadas sin un intercambio físico. La compensación es realizada de manera centralizada por la Sociedad Española de Sistemas de Pago (Iberpay) y, si no existen discrepancias, la liquidación es realizada también de manera centralizada, en las cuentas mantenidas en el SLBE, en el Banco de España.

Los documentos ya no se intercambian físicamente, sino sólo sus datos relevantes. Así, las líneas de telecomunicación son el principal canal de los participantes para transmitirse, a través del software común, la información necesaria entre ellos y con Iberpay, lo que permite una rápida compensación de las operaciones.

Cada transacción se procesa en su subsistema respectivo, por lo que se obtiene un saldo neto para cada par de entidades en cada uno de los subsistemas. Estos saldos bilaterales se comunican a Iberpay.

Propuestas de ADICAE para la participación de SNCE en la mejora de la seguridad de los medios de pago

- El SNCE cuenta con una tecnología fiable y segura, que según cita la página web de Iberpay garantiza la confidencialidad de las operaciones, supone un bajo coste para las entidades participantes y cuenta con un software altamente especializado. Sin embargo, las entidades bancarias no están obligadas a verificar la autenticidad de la operación o documento que se trata de compensar.

- Desde **ADICAE** pensamos que es la primera medida de cara a la seguridad del usuario, que las entidades deberían establecer. En este sentido proponemos que el SNCE e Iberpay empleen la capacidad tecnológica instalada para implantar un sistema que logre autenticar que el firmante del cheque es realmente quien lo ha emitido.

Otros medios de pago: Cheque, letra de cambio, pagaré y giro postal

Aunque estos tipos de medios de pago siguen siendo utilizados y pueden ser objetivo de fraude, éste no es tan generalizado ya que los delincuentes buscan el máximo beneficio y optimizan sus esfuerzos en medios de pago mucho más utilizados y generalizados (tarjetas y banca electrónica, fundamentalmente).

El cheque

Un cheque es un título de crédito en el que la persona que está autorizada para extraer dinero de una cuenta, extiende a otra persona una autorización para retirar una determinada cantidad de dinero de su cuenta, prescindiendo de la presencia del titular de la cuenta bancaria.

Tipos de cheques

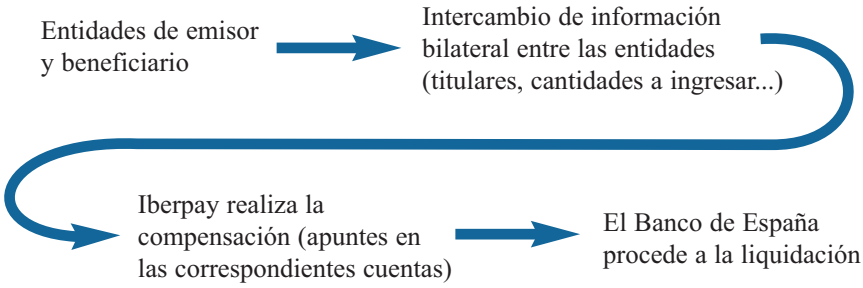
- **Al portador**
- **Nominativo**
- **De caja**
- **Certificado**
- **Cruzado**
- **De Viajero**
- **Para abono en cuenta**
- **De ventanilla**

¿Cuál es la operativa que rige la liquidación de un cheque?

El Sistema Nacional de Compensación Electrónica, SNCE, es el sistema que permite el intercambio, la compensación y la liquidación de los cheques.

En concreto es el Subsistema de compensación de cheques de la SNCE el encargado. En este subsistema se interrelacionan diferentes agentes: las entidades bancarias de beneficiario y ordenate, Iberpay (Sociedad Española de Sistemas de Pago S.A) y el Banco de España.

Subsistema de compensación de cheques de la SNCE



Propuestas de ADICAE
Mejoras técnicas en los cheques para erradicar el fraude

- Durante los plazos establecidos de validez del cheque (15 días a partir de su fecha de emisión,para el caso de operaciones nacionales), el cheque no puede ser revocado, por lo que aunque el banco pagador recibiese instrucciones de su cliente y librador del cheque para que denegase el pago, esta orden no surtiría efecto y el cheque debería ser atendido. **ADICAE** propone que esta operativa desaparezca y que si tanto ordenante como beneficiario están de acuerdo en revocar el cheque puedan hacerlo; puesto que ambos han podido ser víctima del engaño de un tercero.

- Proponemos que desaparezcan los cheques al portador, salvo los empleados en promociones comerciales. Se buscaría la implantación generalizada de un cheque que fuese nominativo y certificado, es decir, que fuese a nombre de un destinatario y que el beneficiario pudiese asegurarse de que el documento cuenta con los fondos suficientes para ser pagado por el banco.

- Imponer en la operativa bancaria que se entienda que, salvo que se indique lo contrario, toda persona a la que han pagado con un cheque que no tiene fondos, ha solicitado al banco levantar “protesto“ . Se trata de una indicación que el banco hace en el cheque señalando que no se hizo el pago. Con esta indicación podrá cobrarle a la persona que expidió el cheque la cantidad que ahí se establezca más la indemnización que de acuerdo a la Ley no puede ser superior al importe del cheque.

Pagaré

Documento que contiene la promesa incondicional de una persona de que pagará una suma determinada de dinero a una segunda persona (beneficiario). A diferencia del cheque, en el momento de su emisión queda determinado el momento a partir del cual se podrá hacer efectivo su cobro.

¿Cuál es la operativa que rige la liquidación de los pagarés?

Al igual que en el caso de los cheques, el Sistema Nacional de Compensación Electrónica, SNCE, es el sistema que permite el intercambio, la compensación y la liquidación de los pagarés.
En concreto es el Subsistema de compensación de efectos de la SNCE el encargado. En este subsistema se interrelacionan diferentes agentes: las entidades bancarias de beneficiario y ordenate, Iberpay (Sociedad Española de Sistemas de Pago S.A) y el Banco de España.

Letra de cambio

Es una orden escrita de una persona (girador) a otra (girado) para que pague una determinada cantidad de dinero en un tiempo futuro (deter- minado o determinable) a un tercero(beneficiario).

Giro postal

Modalidad de pago que consiste en el envío de dinero, por parte de una persona o empresa, a través del servicio de correos. Puede realizarse de manera ordinaria (de 3 a 5 días) o de manera inmediata.

Características

- Puede enviarse el dinero dentro del territorio nacional y en el extranjero.
- El importe mínimo de un giro es de 0,10 euro.
- La entrega se efectúa a domicilio.
- Permite la posibilidad de incluir un escrito privado de hasta 140 caracteres.

Clases de giros

Existen dos tipos de giro postal que se diferencian básicamente en el plazo de ejecución de la entrega.

- Giro ordinario: se realiza en un plazo de 3 a 5 días dentro del territorio nacional, mientras que en el extranjero dependerá del país receptor del envío.
- Giro inmediato: son los que se realizan prácticamente en el acto.

Nuevas fórmulas y métodos para pagar ¿son seguros?

Nuevas fórmulas y métodos para pagar ¿son seguros?

El chip en las tarjetas ¿expuesto al fraude o solución definitiva?

Mucho se ha hablado acerca de la banda magnética en las tarjetas tradicionales y el gran paso en cuanto a seguridad que supone la implantación de la tecnología del "chip" en la operativa con este medio de pago. Para superar falsas creencias sobre la presunta invulnerabilidad del sistema chip, que por cierto todavía no se ha implantado en España de forma efectiva, conviene tener en cuenta una serie de cuestiones técnicas.

Mientras que la banda magnética como hemos visto antes, es un sistema que no encripta el PIN ni los datos de la tarjeta introducidos por el titular, el chip sí. Sin embargo, esto no es una garantía total, ya que existe la posibilidad de alterar este proceso de generación del pin.

Este tipo de tarjetas son las pertenecientes al sistema EMV (Europay MasterCard VISA) introducen un estándar de calidad con circuito integrado, que se basan en la criptografía, son las llamadas "tarjetas inteligentes" que están reemplazando a las tarjetas de banda magnética. Dicho sistema se pretende imponer en su totalidad y sustituir al actual de tarjetas de banda electrónica.

De este tipo de tarjetas debemos distinguir varias clases:

- Tarjetas con circuito integrado de memoria.
- Tarjetas con circuito integrado con microprocesador, son las llamadas "tarjetas inteligentes" en las que se distinguen dos tipos:
  - De contacto
  - Sin contacto

Las tarjetas con **circuito integrado de memoria** no son tarjetas que sirvan como medio de pago, simplemente son tarjetas que almacenan datos.

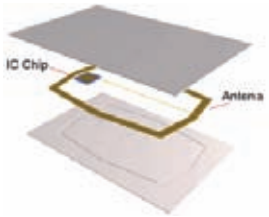
Las tarjetas con **circuito integrado con microprocesador** funcionan de la siguiente manera, al introducirlas en un lector de tarjetas se activan y permiten la transferencia de información entre el lector y la tarjeta, mediante un contacto metálico o sin él, con una lectura láser.

Los datos anuncian una lenta implantación que favorece poco a los consumidores

Las entidades financieras realizarán la migración progresiva de sus tarjetas a EMV según su propio calendario y objetivos, dentro del marco establecido por el EPC (en castellano, Consejo Europeo de Pagos) para SEPA (2008-2010). Según las cifras de la Comisión de Seguimiento del Plan Español de Migración a la SEPA, a finales del tercer trimestre de 2007, el 1,7% de las tarjetas, el 82% de los cajeros y el 64% de los TPV ya se habían adaptado al sistema EMV. De momento el porcentaje de tarjetas migradas aún es bajo; este motivo es justificado por las entidades financieras aduciendo el alto coste que supone la implantación de este nuevo sistema. Esperemos que además del retraso en esta implantación no se repercutan los gastos de la implantación de toda esta nueva infraestructura en el ususario en forma de aumento de comisiones.

Funcionamiento técnico de las tarjetas con chip

Para ello, toda comunicación es iniciada siempre por un dispositivo externo, esto quiere decir que la tarjeta nunca transmite información sin que se haya producido antes una petición externa. De tal manera que, cada vez que se inserta una tarjeta en el terminal lector, sus contactos se conectan a los del terminal y éste procede a activarlos eléctricamente. A continuación, la tarjeta inicia un reset de encendido y envía una respuesta llamada ATR (Answer To Reset) hacia el terminal.



Esta respuesta contiene información referente a cómo ha de ser la comunicación tarjeta-lector, estructura de los datos intercambiados, protocolo de transmisión, etc. Una vez que el lector interpreta el ATR procede a enviar la primera instrucción. La tarjeta procesa la orden y genera una respuesta que es enviada hacia el terminal. El intercambio de instrucciones y respuestas acaba una vez que la tarjeta es desactivada.

Este chip con microprocesador, permite que si por ejemplo, se desean actualizar datos en una tarjeta, con solo conectar el chip al sistema con el que se desea hacer un intercambio de información, se puede actualizar automáticamente, esto significa que en la próxima transacción de cada tarjeta se va a poder actualizar información sin cambiar de tarjeta.

El funcionamiento de las tarjetas inteligentes **de contacto** es sencillo, ya que una vez insertada la tarjeta en el lector, hace que el contacto del chip con los conectores eléctricos de este, trasmitan los datos oportunos en doble vía, del lector al chip y viceversa.

Sin embargo, las tarjetas inteligentes **sin contacto** tienen un funcionamiento más complejo, porque se necesitan unos lectores especiales que transmiten información por radiofrecuencia a la antena que va conectada al chip, para guardar así la información requerida. De la misma forma los lectores de este tipo de tarjeta, funcionan sin necesidad de que el lector tenga un contacto directo con esta.

Este tipo de tarjeta es especial para aplicaciones donde la velocidad de la transacción es de importancia y donde el desgaste de la tarjeta es un factor importante. La operativa es muy sencilla, al acercar la tarjeta a un terminal específico, se transfieren los datos del usuario, mediante un sistema de ondas. De este modo el consumidor no tendrá que firmar ni teclear ningún número secreto (PIN) al realizar una compra.

La tecnología chip aplicada a los monederos electrónicos

Nacimiento del binomio chip-monedero

En 2001 comenzó a ser utilizada en Japón la tarjeta Suica, con tecnología de radiofrecuencia, para hacer pagos en los trenes. Su uso se extendió rápidamente. En Japón el fenómeno se ha generalizado y no sólo hay lectores en la entrada de las estaciones de tren; hay más de 100.000 restaurantes y quioscos, 45.000 supermercados y 80.000 máquinas de bebidas que aceptan este tipo de pago.

La tecnología y la forma en que se ha implantado en Japón, desde hace unos años, en Europa también se empieza a ver en las grandes capitales.En España, las tarjetas sin contacto, sin necesidad de firma ni de PIN, también se están popularizando en pagos de transporte urbano. Así en el caso de pérdida o robo, el consumidor sólo verá comprometida hasta una cantidad muy limitada. El fenómeno de fraude en este tipo de medio de pago y su posible afección al consumidor son mucho más reducidos.

Funcionamiento técnico del monedero electrónico

El sistema del monedero electrónico opera con tarjetas inteligentes que tienen un microchip, éste, al hacer contacto con los lectores de los dispositivos que, para tal fin, tienen instalados los establecimientos comerciales, realiza las transferencias del dinero contenido en la tarjeta.

El microchip está programado para funcionar como una microcomputadora electrónica que lleva a cabo procesos de pagos sólo con insertar la tarjeta inteligente en el lector para tarjetas, además, tiene programado un código de seguridad que permite que las transferencias se realicen bajo complejos sistemas de seguridad, tanto para el establecimiento como para el usuario, ya que todo esto proporciona que ésta se utilice de manera personalizada y segura.

Los negocios que aceptan este sistema de pago, tienen instalada una terminal lectora de tarjetas, donde se inserta el monedero electrónico. Una pantalla en la terminal despliega el importe total de la compra y muestra que la operación de pago con la tarjeta se está realizando.
Tan pronto como se comprueba que el usuario o comprador tuvo suficiente efectivo en su tarjeta, la pantalla de la terminal mostrará, en un parpadeo, que la transacción está completada. El dinero exacto del monto de la compra pasó de la tarjeta del usuario, al lector de la tarjeta instalado en la terminal del negocio.

En cuanto a la seguridad para los establecimientos que aceptan este sistema de pago, existe la posibilidad de asegurar electrónicamente la terminal lectora de la tarjeta, de forma que sólo personal autorizado pueda desactivar el seguro mediante una clave equivalente a un Número de Identificación Personal (PIN).

Implantación del Sistema EMV y primeros fraudes

El 31 de diciembre de 2010 la totalidad de tarjetas electrónicas de banda magnética deben haber migrado al sistema EMV (Europay MasterCard VISA), que lleva el nombre de las tres compañías que han desarrollado el proyecto, y que consiste en una tarjeta con chip que autentica pagos mediante tarjeta de crédito o débito.

Esta tarjeta busca mayor seguridad en las transacciones entre tarjetas y terminales, pero este sistema no es la panacea, el fraude sigue existiendo, y ya se han detectado los primeros casos de fraude con este tipo de tarjetas.

Seguridad en las tarjetas, pros y contras

No hay manera de garantizar la seguridad, porque no existe un sistema seguro al 100%, en ello coinciden todos los expertos. El sistema de tarjetas inteligentes es "teóricamente" el que ofrece un mayor grado de seguridad. Además, por su capacidad interna, es capaz de soportar procesos criptográficos muy complejos. Esta capacidad de la que hablamos se debe a:

- **Encriptación de la información:** consiste en transformar la información a un lenguaje cifrado mientras se hace la transferencia de información, para que sea desencriptada y leída, solo y exclusivamente por terminales autorizados sin permitir intrusos en la transacción. La técnica de cifrado se basa en un algoritmo de cifrado y una clave, de tal forma que se requieren ambos para generar el texto cifrado. Para descifrar se requieren un algoritmo de descifrado y una clave de descifrado.

- **Petición de una clave segura (PIN):** El PIN es un número secreto que va almacenado en un fichero protegido y que es solicitado al usuario para acceder a este tipo de ficheros protegidos. Cuando el usuario lo introduce y el programa se lo pasa a la operación que va a abrir el fichero en cuestión el sistema valida que el PIN sea correcto para dar acceso al fichero.

- **Firmas digitales:** método criptográfico que asocia la identidad de una persona o de un equipo informático al mensaje o documento. En función del tipo de firma, puede, además, asegurar la integridad del documento o mensaje.

Por el contrario, el contenido de la banda magnética, por la tecnología que implica, puede ser leído y, aunque no es sencillo, puede ser manipulado por personas con conocimiento y medios adecuados.

Vulnerabilidad de tarjetas tradicionales (banda magnética)

Las tarjetas de crédito son un clásico ejemplo de un sistema de autenticación doble, ya que se combina un elemento físico que es necesario poseer (la tarjeta de plástico con su banda magnética) con un elemento que teóricamente sólo conoce el titular de la tarjeta de crédito (el PIN, un código numérico habitualmente de cuatro caracteres) que físicamente no reside en ningún sitio. Para poder utilizar la tarjeta de crédito en un cajero automático es necesario disponer de estos dos elementos al mismo tiempo.

Obtener "el plástico", la tarjeta, es una tarea relativamente simple. Son un elemento de libre distribución y comercialización. Falsificar la banda magnética también es una operación no demasiado complicada.

Lo que ya no es tan fácil obtener o identificar es el PIN que el usuario ha seleccionado para la tarjeta de crédito. En teoría, la única forma de identificar este PIN es obligando al titular de la tarjeta a que lo revele utilizando técnicas de fuerza. Para identificar el PIN asociado a la tarjeta son necesarios, de promedio, unos 5.000 intentos.
El estudio realizado ("Decimalisation table attacks for PIN cracking") demuestra que en realidad, una persona con los conocimientos adecuados de los mecanismos de seguridad utilizados y acceso a los sistemas criptográficos que se utilizan en los bancos, únicamente necesita un máximo de 15 intentos para identificar cualquier código PIN de cualquier tarjeta de crédito.

La vulnerabilidad del sistema, se encuentra en los dispositivos hardware utilizados para la realización de las operaciones criptográficas. Estos sistemas criptográficos realizan la validación del PIN realizando un cifrado de los dígitos introducidos, utilizando una clave secreta.

Del resultado de la operación de cifrado se extraen una serie de dígitos, expresados en base hexadecimal*. Como el PIN de la tarjeta utiliza únicamente números de base decimal, se hace necesaria la conversión.

** Sistema hexadecimal: En el sistema hexadecimal los números se representan con dieciséis símbolos: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E y F. Se utilizan los caracteres A, B, C, D, E y F representando las cantidades decimales 10, 11, 12, 13, 14 y 15 respectivamente, porque no hay dígitos mayores que 9 en el sistema decimal. El valor de cada uno de estos símbolos depende, como es lógico, de su posición, que se calcula mediante potencias de base 16.*

La conversión de hexadecimal a decimal no se realiza de forma matemática, sino que se aplica una tabla de conversión, donde se expresa la conversión a realizar para cada dígito hexadecimal.

Ejemplo de tabla de conversión de sistema hexadecimal a decimal

Sistema hexadecimal	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Sistema decimal	9	8	7	6	5	4	3	2	1	0	9	8	7	6	5	4

Utilizando esta tabla, el valor hexadecimal 67F4 se convertiría en el valor decimal 3245. Este seria, en definitiva el PIN que debería cotejarse para determinar si la operación debe realizarse o no.

Por tanto, un empleado del banco con acceso al sistema dispone de la capacidad de manipular las tablas de conversión para determinar los dígitos que forman el PIN. Por ejemplo, utilizando esta tabla de conversión de sistema hexadecimal a decimal

Sistema hexadecimal	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Sistema decimal	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0

Con el código PIN 0000 es posible identificar si el PIN contiene el número 7.

Es en este punto donde se encuentra la vulnerabilidad del protocolo. Estas tablas de conversión no son un valor sensible, sino que es posible facilitar una tabla de conversión arbitraria, conjuntamente con el número de cuenta y el PIN, en el momento de solicitar al sistema criptográfico la validación de la información.

Por tanto, básicamente lo que demuestra el estudio, una vez más, es que utilizar como medida de seguridad el desconocimiento ("security by obscurity") no es efectivo, especialmente cuando se hace referencia a cuestiones relacionadas con la criptografía.

Un problema de este tipo, que requiere una situación muy específica para poder ser utilizado, probablemente hubiera pasado más o menos desapercibido. De hecho, como se deduce de lo publicado anteriormente, las únicas personas que podrían aprovecharse de esta vulnerabilidad para obtener los PIN de las tarjetas de crédito son algunos empleados de los bancos que disponen del acceso necesario a los sistemas criptográficos.

Un problema de seguridad que hasta ahora ha quedado sin resolver es el de la comunicación entre la tarjeta y el lector. Algunas tarjetas se utilizan sobre redes de comunicaciones como Internet en las que se pueden producir escuchas de información confidencial en las que se obtiene la información suficiente para suplantar al legítimo usuario.
Para que esto no suceda, existe un protocolo criptográfico que permite demostrar la identidad de un interlocutor sin que un espía obtenga información que le permita suplantarlo en el futuro. Es el llamado ZKPI, (Zero-knowledge proof identity) que obvia este problema impidiendo un ataque tan simple como escuchar las comunicaciones cuando se está ejecutando el protocolo de demostración de identidad.

Otro de los problemas es el de la autenticación, consistente en asegurar de forma fiable la identidad del interlocutor. La tarjeta tiene que estar segura de que el lector con el que trata o el expendedor de dinero electrónico del que extrae dinero son de fiar y a su vez los lectores y los sistemas centrales de las aplicaciones financieras tienen que asegurarse que están tratando con una tarjeta válida. Por eso la criptografía busca resolver tres problemas básicos: confidencialidad, que la información no sea accesible a un usuario no autorizado; integridad, que la información no sea modificada sin autorización; y autenticación, que se reconozca de forma fiable la identidad del interlocutor. En 2003 se presentó un estudio "Decimalisation table attacks for PIN cracking", de la Universidad de Cambridge que demuestra la vulnerabilidad de los sistemas de seguridad utilizados por los cajeros automáticos para la validación de los PIN asociados a las tarjetas de crédito.

Primeros fraudes en el sistema EMV

Queda constatado que el sistema EMV ofrece mayor seguridad, pero no ofrece seguridad absoluta. Ya en el Reino Unido han aparecido los primeros casos de fraude con este tipo de tarjetas. Los delincuentes no han atacado el sistema de seguridad de la tarjeta, sino lo que han hecho ha sido modificar los terminales de venta de estas tarjetas.

Una vez modificados, estos terminales se introdujeron en el mercado, siendo adquiridos por muchos comercios , con lo que el nivel de diseminación de terminales trucados era muy amplio. ¿En qué consistía esta manipulación? Han permitido el fraude en tres **pasos:**

1º Los terminales adulterados permitían **copiar los datos de tarjeta y el PIN** introducido antes de que el propio terminal pudiera cifrar la información.

2º Conseguidos los datos, éstos se sometían a **cifrado,** empleando llaves criptográficas propiedad de los atacantes, para almacenarlos en un buffer (ubicación de la memoria en una computadura o instrumento digital reservada para el almacenamiento temporal de información digital) existente en el propio terminal modificado.

3º Para finalizar, se dotó a los terminales de facultad para **enviar los datos almacenados en el buffer a servidores remotos.** Estos servidores remotos, localizados en Pakistán, donde una vez recibidas las tramas se descifraban los datos capturados para clonar tarjetas, con el agravante de disponer del PIN.

Este proceso denota una gran especialización, y por tanto, es de prever que los impactos producidos también sean muy altos. Muchos expertos no dudan en calificar el montaje como, posiblemente, el más complejo conocido en la triste historia del fraude relacionado con clonación de tarjetas.

Alguna posible solución a estos primeros fraudes con el sistema EMV podría pasar por endurecer el control de seguridad en el proceso de fabricación de estos terminales. También vendría bien dotar a los terminales de mecanismos de detección de manipulación.

El comercio electrónico: una puerta abierta hacia el fraude

La utilización de Internet por usuarios del mundo entero no ha dejado indiferente a empresas que han aprovechado el aumento de la utilización de la red de redes para comercializar sus productos, más si cabe en época de crisis, ya que internet permite obtener precios más baratos y una mayor variedad de servicios.

Esto también ha supuesto una nueva oportunidad de negocio al sector financiero y a empresas proveedoras de medios de pago. Es necesario que entren en juego los novedosos medios de pago distintos al efectivo. En este sentido, los agentes que intervienen y posibilitan el comercio electrónico no debe actuar como espectador pasivo y procurar medios y fórmulas de pago seguras.

Requisitos de seguridad en los medios de pago on-line

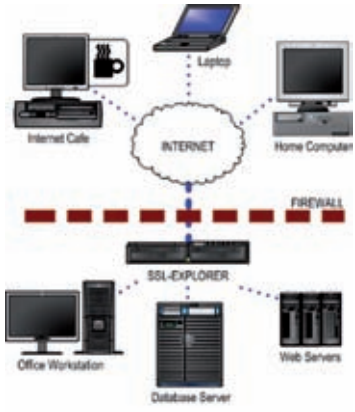
Los expertos establecen 4 requisitos para que una transacción comercial por Internet se considere segura:

- **Autenticación:** Identificación de los participantes en la transacción. Todos deben estar perfectamente identificados (el cliente, el comerciante y los bancos, emisor y adquiriente) para evitar el principal fraude: la utilización ilícita de las tarjetas de crédito.
- **Integridad:** El sistema debe de asegurar la integridad de la información que se intercambia entre los agentes del sistema y no se produzca una modificación de la misma en el tránsito. Para garantizar dicha integridad se usan códigos de autenticación de mensajes (MACs), funciones resumen y firmas digitales.
- **Confidencialidad:** Los datos intercambiados durante una transacción de pago deben ser ocultos salvo para los agentes implicados en la transacción. Ninguna persona ajena a la transacción debe tener acceso a las informaciones intercambiadas. Seria importante que el vendedor ni el banco tuviesen acceso a esos datos de la transacción. Esto normalmente se garantiza con el cifrado de datos.
- **No repudio:** Ni el emisor ni el receptor pueden negar haber solicitado un pago o una autorización de pago. El sistema debe generar recibos que impidan que alguno de los intervinientes en la transacción niegue haber participado en ella.

Protocolos de seguridad en comercio electrónico

Puesto que el comercio electrónico es a distancia, para hacer cumplir estos cuatro requisitos anteriormente citados, se han creado los protocolos de seguridad. Hay que destacar entre los más habituales SSL (Secure Sockets Layer), S-HTTP (Secure HTTP) y SET (Secure Electronic Transaction). SSL está diseñado para mantener comunicaciones seguras en internet, aunque SSL se usa primariamente con aplicaciones para la web. Por el contrario , S-HTTP está dirigido a proporcionar autentificación y preservar el carácter privado de las aplicaciones, mientras que SET va un paso más allá y proporciona seguridad a las transacciones de comercio electrónico.

SSL (Secure Sockets Layer)



El protocolo SSL se basa en la utilización de un sistema de cifrado que emplea un algoritmo (clave pública / clave privada) que utiliza una clave de seguridad de 128 bits de longitud, y que solo conocen la máquina del usuario conectado y el servidor que brinda la conexión. Estas claves permiten la encriptación de los datos para que nadie que no las tenga pueda leer su contenido. Esto significa que cualquier tipo de información que se transmita desde un servidor seguro (que utiliza SSL) y utilizando un navegador con soporte a tecnología SSL (ya prácticamente todos los más comunes en sus versiones más recientes), viajará a través de Internet a salvo de que el mismo pueda ser rastreado, copiado y descifrado por algún usuario que no sea el perteneciente a la comunicación originalmente establecida.

Los certificados SSL son expedidos por una Autoridad Certificadora (CA), quienes no son sino proveedores autorizados expresamente para ello (VeriSign, Thawte, GeoTrust, RapidSSL). Los certificados SSL contienen datos como: nombre de la empresa cliente (para quien es generado el certificado en cuestión), un numero serial propio del certificado, fecha de expiración (del certificado), y una llave pública que permite encriptar la información.

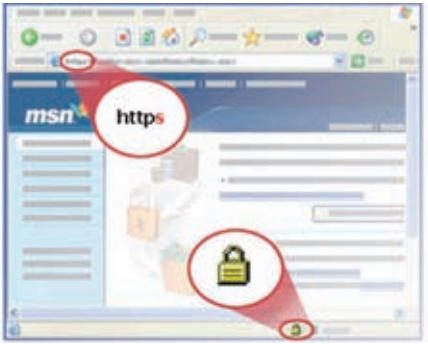
Atención

¿Cómo sabemos si un web cuenta con protección bajo un certificado SSL?

Esto puede verse a simple vista en todos los principales navegadores. Lo primero es el prefijo HTTP de la dirección URL de la pagina web, cambia a HTTPS (que significa HTTP seguro), lo segundo es que en alguna parte de la ventana del navegador (ello depende de que navegador utilice), se visualiza un icono con forma de candado; el mismo al darle click abre una ventana con todos los datos del certificado SSL en cuestión, y los datos de la entidad CA que genero este certificado.

Peligros y fraudes en el protocolo SSL

El protocolo SSL, utilizado en muchas páginas web (como bancos y sitios de comercio electrónico) puede ser vulnerado, tal y como ha demostrado un investigador de seguridad. SSLStrip es una herramienta que permite al delincuente realizar un ataque "man-in-the-middle" (hombre en medio) engañando al usuario para hacerlo creer que se encuentra en un sitio de Internet con cifrado SSL (HTTPS). En realidad sus datos se están transmitiendo sin cifrado alguno (HTTP), pero la cosa no para ahí, SSLStrip también permite engañar el servidor HTTP, haciéndolo pensar que el cifrado ha sido anulado pero en realidad el sitio sigue como si todavía utilizara SSL. Para probar la efectividad del ataque, este investigador se hizo pasar por un atacante y consiguió 117 cuentas de correo electrónico, 16 números de tarjetas de crédito, 7 contraseñas de PayPal y otras 300 cuentas de acceso seguro a diversas páginas web en 24 horas. Entre las páginas web comprometidas se encontraban Paypal, LinkedIn, Hotmail y Gmail.



Carencias del protocolo SSL

1. Por un lado, **SSL** ofrece un canal seguro para el envío de números de tarjeta de crédito, pero **carece de capacidad para completar el resto del proceso comercial:** verificar la validez del número de tarjeta recibido, autorizar la transacción con el banco del cliente, y procesar el resto de la operación con el banco adquiriente y emisor.

2. **Sólo garantiza la confidencialidad e integridad de los datos en tránsito,** ni antes ni después. Por lo tanto, si se envían datos personales al servidor, entre ellos el ya citado número de tarjeta de crédito, el número de la seguridad social, el DNI, etc., SSL solamente asegura que mientras viajan desde el navegador hasta el servidor no serán modificados ni espiados. Lo que el servidor haga con ellos, está ya más allá de la competencia de este protocolo. Los datos podrían ser manipulados irresponsablemente o caer en manos de un atacante que asaltara el servidor con éxito.

3. **Permite realizar ataques sobre servidores de comercio creados deficientemente,** para averiguar números de tarjeta reales. Un programa escrito por el hacker va probando números de tarjeta válidos, sin saber si corresponden o no a cuentas reales, realizando compras ficticias en numerosos servidores. Si el número de tarjeta no sirve, el servidor devuelve un error, mientras que si es auténtico, el servidor lo acepta.

   El programa entonces cancela la compra y registra el número averiguado, para seguir adelante con el proceso. De esta forma, el hacker puede hacerse en breve con cientos de números auténticos.

Otras opciones, mejores pero fallidas

Debido a las carencias del protocolo SSL, se desarrolló un protocolo de seguridad especializado en transacciones de comercio electrónico. Se conoce como **SET** (Secure Electronic Transaction).

Fue desarrollado por Visa y MasterCard, con la colaboración de gigantes de la industria del software, como Microsoft, IBM y Netscape. Pero, uno de los grandes inconvenientes de SET es que es un protocolo transaccional orientado a las aplicaciones de comercio electrónico a través de tarjetas de crédito, no admite otra forma de pago.

Además, es un protocolo robusto y que ofrece un alto nivel de seguridad, pero a costa de hacerlo muy pesado, caro y complejo de utilizar, por lo que el desarrollo de su implantación se ha visto frenado, siendo muy poco utilizado y en la actualidad extinguido. Por lo que se sigue utilizando el SSL, con las carencias anteriormente citadas y los problemas de seguridad para los usuarios.

Propuestas ADICAE: es necesario un nuevo protocolo

Todos estos inconvenientes que se acaban de ver convierten al protocolo SSL en una solución deficiente desde el punto de vista del pago electrónico puesto que es un protocolo seguro de propósito general, que no fue diseñado para el comercio en particular. Por lo que es necesaria la implantación de un nuevo protocolo específico para el comercio electrónico que haga seguras las transacciones y comunicaciones en éste. Exige un esfuerzo y compromiso por parte de las empresas que lo utilicen de buscar el mejor protocolo, no pueden conformarse con intentar solucionar el fraude con un sistema que no se ideó para ese fin. Para ello, junto con las empresas especializadas de seguridad especializadas en la creación de protocolos, se deberá buscar un protocolo que evite caer en los errores del pasado y evitar así la complejidad de uso o su coste en la implantación.

El pago por móvil

El pago por móvil es un servicio que permite realizar pagos y otras transacciones bancarias en cualquier situación, y en cualquier momento y lugar.

La operativa consiste en asociar a un teléfono móvil una o varias tarjetas electrónicas emitidas por una entidad financiera. Ello permite recargar la tarjeta de prepago telefónico del propio móvil o el de familiares o amigos, pagar desde el teléfono móvil, las compras por internet, el taxi, hacer donativos, pagar la lotería, etc… así como consultar los saldos y movimientos de sus cuentas, de forma similar a un cajero automático. En cada transacción se permite que el usuario elija pagar con cualquiera de los medios de pago que tiene activados en su cartera y son admitidos por el establecimiento.

Existe una "clave de autorización personal" (PIN) para cada medio de pago, que es gestionada por la entidad emisora, la cual sólo es conocida por el titular. El usuario autoriza cada transacción mediante la introducción del PIN o el código que le indique en cada caso el emisor del medio de pago, siendo equivalente a la firma manuscrita.

El conjunto de tarjetas asociadas, está directamente vinculada a la SIM del teléfono móvil y únicamente se activará con del PIN del medio de pago con el que se desea operar.

Propuestas ADICAE: evitar depender de la red de un solo operador

- **Reserva de batería específica para evitar que el teléfono móvil se apague en medio de la transacción.**
- **Cobertura garantizada de red telefónica al igual que el de emergencias (112).**
- **Bluetooth en caso de no haber cobertura de red de ningún operador.**

La banca on-line

Banca online o Banca en línea es la banca a la que se puede acceder mediante Internet. Pueden ser entidades con sucursales físicas o que sólo operan por Internet o por teléfono. Los sistemas de banca on-line suelen utilizar estos métodos de utilización.

Código de Usuario y clave de acceso (contraseña):
Tienen carácter personal e intransferible y permite al usuario consultar sus cuentas de activo y pasivo. Si desea acceder a operaciones de nivel más avanzado tendrá que contar con una clave de firma.

Básicamente, existen dos **métodos de seguridad posibles para las contraseñas de banca on-line:**

- El sistema PIN/TAN: PIN es una contraseña utilizada para acceder al sistema y el TAN es una contraseña válida únicamente una vez para autentificar transacciones. Los TAN (Número de Autentificación de la Transacción) pueden ser distribuidos de diversas formas, la más comunes consisten en enviar una lista con estos números impresos en una tarjeta al usuario de banca electrónica. No obstante, la forma más segura de utilizar estas claves TAN es cuando se generan por un disposivo externo a disposición del usuario de banca electrónica. Éste es un sistema de autentificación de doble factor, ya que el acceso a la banca electrónica depende de dos condiciones o requisitos (conocer una clave estática y otra dinámica.

- Firma especial para el uso de banca online, donde todas las transacciones son firmadas y encriptadas digitalmente.

Propuestas ADICAE: aplicación de nuevos medios técnicos

■ **Implantación del uso de tarjetas de coordenadas.** Éstas también ofrecen una elevada fiabilidad.Ya se están utilizando por algunas entidades, pero sería recomendable que todas las utilizasen.

■ **Fomento y promoción por parte de los bancos de la utilización de generadores de clave (Token),** dispositivos de seguridad que generan claves numéricas individuales que varían cada cierto tiempo.

Sistema Paypal

Es un sistema de pagos en Internet desarrollado por una empresa del grupo e-Bay (Centro de compras y ventas en Internet). Es por tanto muy utilizado por los clientes de este tipo de subastas y, en general para las transacciones entre particulares.

Es un sistema internacional: está disponible en 44 países y 5 divisas (Euros, Dólares Americanos, Libras Esterlinas, Dólares Canadienses y Yenes Japoneses). Los pagos son instantáneos, no importa donde se encuentre el comprador.

El sistema se basa en realizar los pagos a través del correo electrónico. Para ello, el sistema permite al usuario registrarse una única vez con su cuenta bancaria o tarjeta de crédito y posteriormente ordenar anónimamente abonos con cargo a esa cuenta o tarjeta.

Estos abonos se ordenan simplemente mediante el suministro de una dirección de correo electrónico de la firma o persona que se desea reciba el dinero. Paypal se encarga de avisar al beneficiario enviándole un mensaje por Internet.

El servicio es gratuito para el cliente, mientras que al vendedor se le cobra una comisión por recibir los pagos. Las comisiones se determinan al principio de cada mes sobre el volumen de ventas que el comerciante ha tenido en el mes anterior.

Cupones prepago

También denominados “U-Kash o Paysafecard”, su funcionamiento es muy sencillo. Se basan en crear un doble pago offline-online. Basta con acudir a un punto de venta: oficinas de correos, gasolineras, locutorios, adquirir un cupón por el importe deseado que contiene un código numérico e introducir este código en la web en la que queramos pagar. Son especialmente usados para webs de apuestas deportivas o casinos online, dado su caracter anónimo. Su incoveniente es que han de ser comprados con antelación.

Sistema Safetypay

Es un Sistema facilitador de Pago y Cámara de Compensación entre Consumidores, Establecimientos On-line y Bancos. Proporciona un sistema de pago en la Red, basada en componentes compatibles y estándares con los protocolos de seguridad de los sistemas de los bancos. La ventaja adicional que aporta es el hecho de no tener que ingresar la información financiera del usuario en Internet.

En la transacción intervienen tres partes: Usuarios de comercio electrónico, empresas virtuales afiliadas al sistema y bancos afiliados también al sistema Saftpay. Este hecho limita en gran medida el uso de este medio de pago.

Funcionamiento del sistema:

PRIMER PASO

- El cliente hace el pedido al comercio afiliado y selecciona Saftpay como método de pago
- El cliente selecciona la moneda en la que querrá pagar y la entidad financiera de su banca online.
- La información aparce en pantalla y se envía por e-mail a la entidad bancaria.

SEGUNDO PASO

- El cliente accede a la banca por Internet de su entidad y autoriza el pago.
- La entidad financiera avisa en tiempo real a Saftpay y autoriza el pago
- En ese momento, el comercio autoriza el pedido y le envía la confirmación Saftpay

TERCER PASO

- Se transfieren los fondos de la entidad al comercio

Este sistema ofrece al consumidor mayores garantías de seguridad, sobretodo con los virus y troyanos; sin embargo el consumidor sigue a expensas de las garantías de seguridad que la entidad bancaria le ofrece.

PARTE 3

Tipología técnica de los fraudes en medios de pago

- **El avance del cibercrimen supera las medidas técnicas de seguridad**
- **Fraude en tarjetas**
- **Fraude en datos bancarios**
  Por internet, e-mail, PC, teléfono
- **Otros fraudes en medios de pago**

El avance del cibercrimen supera las medidas técnicas de seguridad

Los términos cibercrimen, ciberdelitos, ciberdelincuencia, se han hecho un hueco entre nuestro vocabulario, lamentablemente sabemos a qué nos referimos cuando se utiliza este término. En pocos años la sociedad ha tenido que aprender a convivir con esta realidad, que hasta hace poco sonaba a cienciaficción.

El concepto de cibercrimen abarca desde el delito económico, como el fraude informático, el robo, la falsificación, el computer hacking, el espionaje informático, la piratería comercial, delitos contra la intimidad, contra la propiedad intelectual, etc, etc.

El medio donde fundamentalmente se mueven estos ciberdelincuentes es Internet, que tiene unas características y elementos muy favorables para la comisión de delitos:

- **Se ofrece un entorno sin fronteras:** El delincuente puede viajar, virtualmente, de un país a otro, adentrándose en otras jurisdicciones, con total libertad, sin necesidad de aduanas, visados, etc, etc.

- **Independencia geográfica:** Desde cualquier lugar del mundo e independientemente desde donde se esté se puede acceder a cualquier lugar de la red con la misma facilidad y velocidad.

- **Independencia del lenguaje:** Con las nuevas tecnologías ya no existe la "frontera" de los idiomas.

- **Permite la comunicación de uno a muchos:** Esto facilita el trabajo al delincuente, que utiliza internet como una tela de araña para que los efectos de su acción se multipliquen y perjudiquen a multitud de personas.

- **Ampliamente utilizado:** En pocos años, internet y sus avances tecnológicos han llegado a casi todos los hogares de los países desarrollados, también en los subdesarrollados el uso se incrementa a pasos agigantados.

- **Falta de identificadores seguros:** Tanto desde la perspectiva de quien remite la información como de quien la recibe. Ambos, en muchas ocasiones carecen de medios fiables para identificar a sus interlocutores.

- **Inexistencia de una autoridad central que controle el acceso a internet:** Este control se puede producir a posteriori, después de que existan indicios de delito, pero no antes.

De ahí que los ciberdelitos difieren de los delitos terrestres en cuatro aspectos:

- **Se comenten fácilmente**
- **Requieren escasos recursos** en relación al perjuicio causado, lo que incita a muchos individuos a adentrarse en este mundo a pesar de no responder a un perfil de delincuente tradicional.
- **Pueden cometerse en una jurisdicción sin estar físicamente** presente en el territorio sometido a la misma.
- En muchas ocasiones **no son claramente ilegales.** Esta indefinición puede proceder de la misma conducta (actos u omisiones no claramente delictivas por no configurar los tipos enumerados en la legislación penal) o de la falta de diligencia o, incluso, de la intencionada falta de regulación de ciertas conductas por parte de Estados interesados en la instalación de paraísos cibernéticos.

Con este panorama que acabamos de describir y debido a los graves peligros, cada vez mayores y más sofisticados a los que se exponen todos y cada uno de los que cada día navegamos por la red, no es de extrañar que el fenómeno del fraude a través de la red esté preocupando a los Estados, y que en los últimos años se hayan creado foros, reuniones de expertos al más alto nivel, organismos internacionales (técnicos y jurídicos) especializados en el tema, etc que tratan de atajar sus efectos.

Tipos de fraudes en medios de pago

Cada año es más patente la proliferación de casos de fraude de bandas criminales organizadas. Su rango de actividades es muy amplio: phishing, código malicioso, tarjetas de crédito, envío de correo no solicitado (spam), estafas (scam), etc. Estas bandas provienen principalmente de tres focos internacionales (Europa del Este, Brasil y Sureste Asiático), aunque luego utilizan recursos por todo el mundo.

El uso de códigos maliciosos y programas informáticos especializados en el robo de información está proliferando de manera preocupante, llegando incluso a dejar en un segundo plano el método fraudulento más utilizado en los últimos tiempos, el phishing. Cada vez más se están utilizando códigos maliciosos para obtener información y beneficio económico ilícitamente. Esto sucede porque el uso de códigos maliciosos implica un grado de dificultad más alto en su diseño, lo que a su vez hace más complicada su detección.

En cuanto al origen de cada uno de estos delitos, Estados Unidos está a la cabeza de los casos de phishing, con un 38% del total, seguido de Turquía, China, México y Alemania, que representaron un 16,2%, 5,4%, 4,7% y 3,9%, respectivamente. Estados Unidos también se sitúa como origen más común tanto en los troyanos como en los redirectores, con un 49,8% y un 51,8% del total,respectivamente. En el caso de los troyanos, le siguen Rusia, con un 7,2%, y Australia, con un 6,9%, mientras que en los delitos de redirección, Alemania ocupa el segundo lugar con un 9,2% del total.

Fraude en tarjetas

Robo u obtención fraudulenta del código PIN

Se trata de una conducta muy habitual efectuada en cajeros automáticos, sobretodo en los instalados en la calle los cuales cuentan con menos medidas de seguridad.

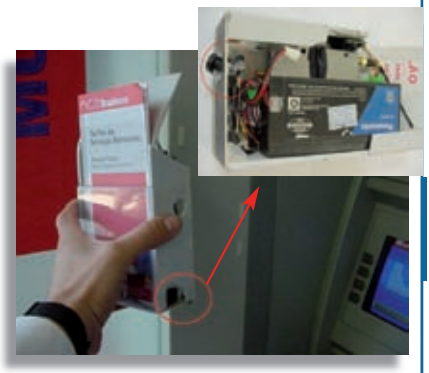
Los "modus operandi" o formas de actuar suelen ser muy variadas, a continuación comentamos las más comunes:

a) Instalar una ranura de tarjeta falsa y una video cámara oculta

- Instalar una vídeo cámara oculta, para grabar la clave secreta de la tarjeta del usuario y una ranura falsa que atrapa la tarjeta del usuario.

- Una vez que el usuario ha sacado dinero del cajero, le es imposible retirar la tarjeta.

- Cuando sale del cajero a pedir ayuda un estafador entra en el mismo y extrae la tarjeta, que podrán utilizar posteriormente con las claves grabadas con la cámara. También se da la variante en la que no se utiliza cámara oculta, pero que se sustituye por un compinche que trata de "ayudar" al usuario desprevenido y de esta forma observa las claves del cliente.



b) La tarjeta queda atrapada en el cajero y un viandante ofrece su ayuda (LAZO LIBANÉS)

- Los timadores introducen el llamado "lazo", que suele ser, la mayoría de las veces, una cinta magnetoscópica, generalmente película de cassettes de vídeo 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. Le facilita su teléfono móvil y le dice que se comunique con la sucursal bancaria para que allí le ayuden. 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.

c) La técnica del despiste del buen samaritano

-Un estafador se sitúa al lado del cliente.

-Cuando éste introduce la tarjeta, el estafador tira un billete al lado del usuario y le dice que se le ha caído.

-Cuando el estafado se agacha, el delincuente saca la tarjeta del cajero y la sustituye por otra diferente. El usuario entonces intenta sacar dinero pero no puede con la tarjeta cambiada; entonces la saca y se va del cajero.

- El estafador pretende ayudarle para ver la clave secreta y posteriormente puede utilizar la tarjeta de crédito para obtener dinero.

d) Obtención del PIN con teclados falsos

En este caso, se produce una alteración física de algunos de los elementos del cajero. Los delicuentes sustituyen el teclado original por uno falso, de forma que la víctima al teclear el número secreto en realidad lo está comunicando a los estafadores. Incluso es posible que sus datos viajen telemáticamente a distancia en ese momento.

Clonación de la banda magnética en cajeros automáticos

La clonación de la banda magnética, para posteriormente cargarnos compras no realizadas por nosotros o extraer dinero de nuestra cuenta puede producirse en muy diversos lugares.

Como hemos comentado en el caso del lazo libanés, los delincuentes colocan una ranura adicional de las tarjetas (del mismo color y material). Esta ranura contiene un lector de tarjeta adicional para copiar la información de la tarjeta. Pero no es éste el único método empleado. El clonado de la banda magnética también puede producirse al pasar la tarjeta por la ranura de identificación de tarjetas a la entrada de los cajeros cerrados.

Un estafador, normalmente perteneciente a una red criminal, se encarga de ocultar un lector de bandas magnéticas en cajeros automáticos con gran afluencia de público. Durante todo el día, los usuarios insertan confiados sus tarjetas de crédito en el cajero sin saber que sus datos están siendo copiados. Por la noche, sólo queda recoger el lector y volcar a un ordenador la información obtenida, con la cual se pueden llegar a clonar un gran número de tarjetas; las cuales emplearán para realizar compras por Internet o robarnos nuestro dinero en diversos cajeros automáticos.

Propuestas ADICAE para frenar el fraude en cajeros automáticos

■ **Cajeros en habitáculos cerrados.** ADICAE propone el establecimiento de la obligación de que todos los cajeros que están a disposición del usuario se encuentren ubicados en un habitáculo cerrado, el cual cuente con cámara de vídeo y sonido; siendo el responsable de esta remodelación el banco o caja al cual pertenezca el cajero.

■ **Sistema de revisión diaria.** Además dichas entidades deben instaurar un sistema de revisión diaria; que compruebe que el cajero no ha sido manipulado con fines fraudulentos.

Skimming/carding

Se trata del clonado de la banda magnética de las tarjetas mediante multitud de técnicas. Suele darse en establecimientos, manipulando TPV (Terminal de Punto de Venta) poco controlados, en especial gasolineras y restaurantes. También es posible que el camarero o dependiente pertenezca a alguna red criminal y cuando vaya a cobrar con la tarjeta al TPV aproveche para clonar la banda magnética de la tarjeta.

Clonado de la banda magnética en establecimientos comerciales

En el caso del duplicado de bandas magnéticas en establecimientos, las redes de delincuencia necesitan a un empleado que trabaje a su vez para ellos. Le ofrecen una determinada cantidad de dinero por cada tarjeta de crédito que pase por el lector de clonado. Entonces ya sólo tienen que esperar a que un cliente decida pagar con su tarjeta de crédito. Con un simple movimiento de muñeca, después de cobrarles, copian la banda magnética con el lector. Una simple operación que dura apenas dos

segundos. La víctima, que ha acudido a un establecimiento de su confianza, jamás sospechará que está siendo víctima de un fraude.
Concluida la jornada de trabajo, el empleado cambia su lector lleno de datos por uno limpio, además de percibir, siempre en mano, el dinero que le ofrece diariamente la banda por el copiado de tarjetas.
Durante una semana, más o menos, la víctima no se percata de que los ladrones le están vaciando la cuenta corriente a base de compras caras en grandes centros comerciales y extracciones en cajeros automáticos.

Algunos estafadores van más allá y abren negocios ficticios que son dados de alta en el Registro Mercantil, para poder solicitar una cuenta corriente en una entidad bancaria y por tanto acceder a un terminal de punto de venta para tarjetas de crédito.
De esta manera pueden utilizar las tarjetas "clonadas" para realizar ingresos en dichas cuentas, pudiendo disponer de ese dinero al día siguiente.

Clonado de la banda magnética en gasolineras y restaurantes

El duplicado de la banda magnética, también suele producirse en este tipo de establecimientos; en los cuales al realizar la compra no tenemos tan controlada la tarjeta como cuando acudimos a caja a pagar.
El método empleado es el mismo; un empleado actúa de manera fraudulenta y coloca un lector de clonado en la ranura por la que pasa la tarjeta cuando realizamos una compra, a cambio de recibir una recompensa por cada tarjeta que consiga clonar.

Clonado de la banda magnética en peajes

La utilización que se hace de las tarjetas de autopista es muy frecuente. Sin embargo en este tipo de tarjetas, resulta muy complejo su control; y es en los nuevos artefactos, como es el caso del Dinamo, Telepeaje o Vía T, donde las posibilidades de utilización fraudulenta aumentan, al no haber un control directo sobre la identidad del usuario.

Otro inconveniente de este tipo de tarjetas es que las tarjetas de crédito se pueden utilizar en los peajes aún cuando han sido canceladas o están caducadas.
Las máquinas de los peajes no tienen medidas de seguridad (no pueden capturar tarjetas) con lo cual no se le puede desproveer al delincuente de su medio de pago.

Fraude en los datos bancarios

Phising

Este delito consiste en la usurpación de las claves de acceso a las cuentas bancarias de un titular con el objeto de robarle su dinero.

El phising paso a paso

El estafador conocido como "phisher", se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo común un correo electrónico, o algún sistema de mensajería instantánea, por ejemplo un mailing masivo a los usuarios de medios de pago mediante mensajes en los que se pretende hacer creer al receptor que su entidad bancaria se pone en contacto con él, solicitándole sus claves de acceso o incluso utilizando también llamadas telefónicas.

También puede sufrirla el usuario al que sustraigan de forma fraudulenta sus claves, mediante cualquier otro sistema. Por ejemplo, mirando en algún recibo extraviado de pago con tarjeta, espiando en su correo, rebuscando en la información no borrada de su antiguo ordenador...Esos números son válidos para comprar por Internet o por teléfono si tienen todos los dígitos y la fecha de caducidad (que también puede calcularse, aunque sea probando). Los ladrones pagan interesantes cantidades por listas de tarjetas válidas conseguidas de este modo.

Originariamente se enviaban aleatoriamente a todos los correos que se pudiese, esperando que por casualidad alguno de los receptores fuese usuario de esa entidad. Actualmente, los estafadores han afinado mucho sus técnicas de forma que pueden incluso detectar cuál es la entidad con la que opera cada usuario y enviarle un correo "personalizado".

Tipos de Phishing

1. Phishing engañoso

Es la forma en la que empezó a perpetrarse el phishing. Se realiza a través de mensajería instantánea y correo electrónico.

Hay acción u omisión del usuario

2. Phishing basado en software malicioso

Este tipo de delito implica la ejecución de un software malicioso en el ordenador de la víctima.

Hay acción u omisión del usuario

3. Phishing mediante introducción de contenidos

Esta modalidad consiste en introducir contenido malicioso dentro de un sitio web legítimo. Dicho contenido puede tener diversas modalidades: redirigir a los visitantes a otra página, instalar algún tipo de malware en el ordenador de los usuarios, etc.

No hay acción u omisión del usuario

4. Phishing mediante la técnica del intercambio

Esta técnica implica el posicionamiento del "phisher" entre el ordenador del usuario y el servidor web legítimo. De este modo el delincuente accede a la información que se transfiere desde el ordenador del usuario atacado al servidor, y viceversa, sin que ninguno de los dos se percaten del ataque.

No hay acción u omisión del usuario

5. Phishing de motor de búsqueda

Los delincuentes crean páginas web para la venta de productos o servicios a precios "ganga" y esperan a que los usuarios visiten las páginas para realizar compras y, por tanto, proporcionen información confidencial o directamente realicen transferencias bancarias.

Si puede haber acción u omisión del usuario

Propuestas ADICAE para frenar la expansión del fenómeno phishing

■ Banca electrónica y direcciones IP

Puesto que los bancos sufren un gran número de ataques y suplantación de identidad para fines fraudulentos; proponemos que cada banco o caja de la opción a sus clientes de suministrarles la dirección IP del ordenador u ordenadores a través de los cuales va a acceder a la banca electrónica. De este modo si las claves de un usuario son obtenidas de manera fraudulenta, no podrán ser usadas en ningún otro ordenador más que en el que haya autorizado el dueño legítimo de la cuenta o tarjeta bancaria. Este sistema requeriría que las entidades desarrollasen un sistema dinámico que permitiese al usuario informar de los cambios de sus direcciones IP de manera activa, lo cual implicaría una inversión por parte de las entidades bancarias.

■ Pregunta secreta

Muchas organizaciones han introducido la característica denominada pregunta secreta, en la que se pregunta información que sólo debe ser conocida por el usuario y la organización. Mediante este sistema se incrementan las medidas de seguridad y se verifica con más seguridad que la persona que está empleando la tarjeta es su dueño.

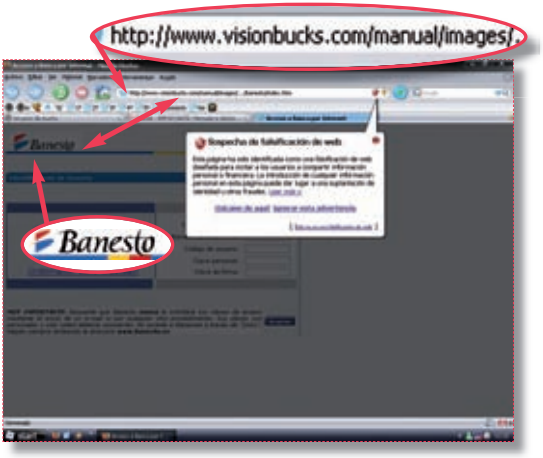
■ Incorporación del método "información de seguimiento en recursos"

Consiste en manipular todos los recursos generados por los servidores web de la entidad (sitios públicos y oficinas virtuales) para incluir una marca digital. De esta forma, la entidad bancaria o los organismos antifraude competentes pueden extraer suficiente información para identificar al pirata.
El resultado de aplicar esta técnica es la identificación del usuario que consiguió las imágenes u otros recursos de la entidad bancaria con el fin de cometer un fraude.

■ Incorporación del método "Seguimiento de Cookies"

Una cookie es un fichero con información que se almacena en el navegador del usuario y que sólo puede ser consultado y modificado por la página web visitada. La utilización de cookies y su seguimiento por parte de las entidades bancarias permite identificar patrones de comportamiento anómalos, tales como el acceso con la misma cookie a distintas cuentas bancarias, las cuales están a nombre de diferentes titulares no relacionados entre sí.

Pharming



El "pharming", un paso más en las técnicas de phising, es otra amenaza un poco más sofisticada y peligrosa, que consiste en manipular las direcciones DNS (Domain Name Server) que utiliza el usuario.

Los servidores DNS son los encargados de conducir a los usuarios a la página que desean ver. Pero a través de esta acción, cuando el usuario teclea en su navegador la dirección de la página a la que quiere acceder, en realidad puede ser enviado a otra creada por el hacker, que tiene el mismo aspecto que la original. Así, el internauta introducirá sus datos confidenciales sin ningún temor, sin saber que los está remitiendo a un delincuente.

¿Cómo se lleva a cabo?

Este fraude puede realizarse de diversas maneras:

- Se puede crear un dominio con nombre muy similar al de la web que se quiere suplantar y se trata de confundir al usuario.
- Se puede crear un link falso que a partir de otras web lleven a la web falsificada.
- Se puede combinar con el phishing añadiéndole el link falso al e-mail fraudulento.

Los piratas intentan conseguir información personal para poder acceder a las cuentas bancarias, robar la identidad o cometer otro tipo de fraudes con el nombre del usuario, de manera que los bancos y otros sitios financieros similares son el objetivo de estos ataques.

El pharming paso a paso

1. El Servidor DNS es interceptado por el "atacante" y tiene como objetivo intervenir el servidor DNS, para poder usarlo en beneficio propio. La principal tarea de un servidor DNS es traducir el nombre de dominio (p.ej. www.nicebank.com) en una dirección IP (p. ej. 194.153.205.26).

2. La dirección de IP del sitio web es cambiada, por ello en lugar de acceder a la web verdadera, se accede a un IP falso.

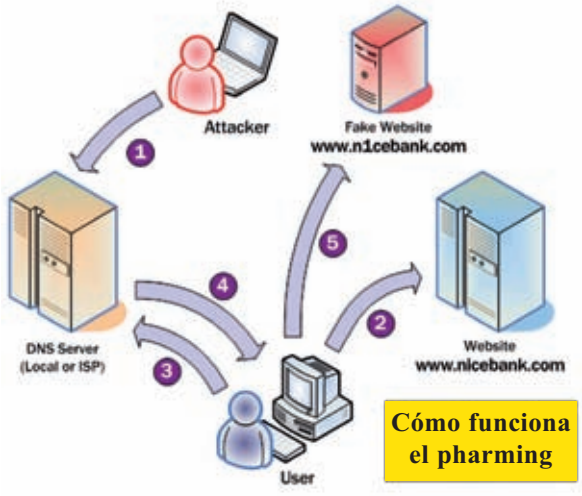
3. El usuario acepta un link para acceder a una dirección Web.

4. El ordenador del usuario " hace una pregunta" al servidor DNS para que se le sirva la dirección de IP del sitio especificado.

5. Pero en este punto el servidor DNS ya estaba interceptado por el "atacante" lo que hace que se le devuelva la dirección de IP del sitio web falso al ordenador del usuario.

6. En el siguiente paso, es el ordenador del usuario, ya manipulado, el que otorga al Usuario una respuesta envenenada y falsa.

7. Finalmente el usuario ha sido manipulado en la visita al sitio web falso pero con apariencia del sitio web original.



Cómo funciona el pharming

Propuestas ADICAE para frenar la expansión del fenómeno pharming

■ **Web únicas.** Protección de las páginas web que ofrecen el servicio de banca a través de Internet y en concreto de sus servicios DNS, para que no puedan ser vulnerados ante un posible ataque. Esta protección puede llevarse a cabo mediante la Utilización de direcciones web identificadas, por parte de los desarrolladores de software y administradores de sistemas de las entidades bancarias. Esta técnica genera direcciones web únicas para cada visita del usuario y recurso solicitado (logos, teclados virtuales, estilos, código…) impidiendo que los recursos sean referenciados posteriormente desde mensajes de correo electrónico u otros sitios web fraudulentos.

Las ventajas de aplicar esta técnica son:

- Los recursos no son utilizables fuera de su entorno.
- Se genera una alerta de seguridad cuando se intenta utilizar un recurso desde fuera de la entidad.
- El recurso solicitado se sustituye por un aviso o imagen que alerta a quien lo visualiza de un intento de fraude.
- El pirata es identificado.

Spoofing

Con esta modalidad de fraude se hace referencia al uso de técnicas de suplantación de identidad generalmente relacionado con usos maliciosos o de investigación.

Existen diferentes tipos dependiendo de la tecnología a la que nos refiramos, como el "IP spoofing" (quizás el más conocido), "ARP spoofing", "DNS spoofing", "Web spoofing" o "e-mail spoofing", aunque en general se puede englobar dentro de spoofing cualquier tecnología de red susceptible de sufrir suplantaciones de identidad.

Se usa para muy diversos fines; principalmente para obtener información del usuario, como sitios web visitados, claves personales, información privada del usuario, etc.

Los ataques de seguridad en las redes a través de técnicas de spoofing ponen en riesgo la privacidad de los usuarios que navegan por Internet así como la integridad de sus datos.

Troyanos

Se le llama troyano o gusano, a un programa malicioso capaz de alojarse en ordenadores y permitir el acceso a usuarios externos, a través de una red local o de Internet, con el fin de recabar información o controlar remotamente a la máquina anfitriona. Un troyano no es en sí un virus, aún cuando teóricamente pueda ser distribuido y funcionar como tal. La diferencia fundamental entre un troyano y un virus consiste en su finalidad. Para que un programa sea un "troyano" sólo tiene que acceder y controlar la máquina anfitriona sin ser advertido, normalmente bajo una apariencia inocua. Al contrario que un virus, que es un huésped destructivo, el troyano no necesariamente provoca daños porque no es su objetivo.

Suele ser un programa alojado dentro de una aplicación, una imagen, un archivo de música u otro elemento de apariencia inocente, que se instala en el sistema al ejecutar el archivo que lo contiene.

¿Cuál es su objetivo?

Habitualmente se utiliza para espiar, usando la técnica para instalar un software de acceso remoto que permite monitorizar lo que el usuario legítimo del ordenador hace (en este caso el troyano es un spyware o programa espía) y, por ejemplo, capturar las pulsaciones del teclado con el fin de obtener contraseñas (cuando un troyano hace esto se le cataloga de “keylogger”) u otra información relevante para causar fraudes.

Tipos de troyanos

Se clasifican según la forma de penetración en los sistemas y el daño que pueden causar. Los ocho tipos principales de troyanos según los efectos que producen son:

- Acceso remoto.
- Envío automático de e-mails.
- Destrucción de datos.
- Troyanos FTP (que añaden o copian datos de la computadora infectada).
- Deshabilitadores de programas de seguridad (antivirus, cortafuegos...).
- Ataque DoS a servidores (denial-of-service) hasta su bloqueo.
- Troyanos URL (Que conectan a la máquina infectada a través de conexiones de módem, normalmente de alto coste).
- Destructor de memoria: Empieza a destruir memoria mientras se envía o se pone en una conversación.

Propuestas ADICAE para frenar la expansión de los troyanos

■ **Mecanismos de seguridad y vigilancia de los contenidos en la red**. Desde ADICAE proponemos la creación de un organismo dedicado a la inspección de las páginas web de descarga de programas y de documentos capaz de detectar páginas o archivos que alojen troyanos, así como otros virus.

Estas autoridades otorgarían una serie de distintivos o tendrían un listado de páginas web inspeccionadas y seguras, lo que mejoraría la confianza de los usuarios.

■ **Antivirus actualizados.** También entendemos que debería facilitarse el acceso de la ciudadanía a antivirus actualizados que permitan eliminar estas y otras amenazas.

Vishing

Este fraude tiene unas características muy similares al phising, pero en vez de enviar e-mails se realizan llamadas telefónicas por Internet solicitando los números de las tarjetas de crédito, claves secretas, etc.

¿En qué consiste?

El criminal configura un “war dialing” (técnica que consiste en hacer llamadas a una serie de números de teléfono automáticamente con el fin de encontrar módems conectados y permitiendo la conexión con algún otro ordenador) para llamar a números telefónicos en una determinada región.

1. Cuando la llamada es contestada, suena una grabación y alerta al "consumidor" de que su tarjeta de crédito está siendo utilizada de forma fraudulenta y que éste debe llamar al número que sigue inmediatamente. El número puede ser un número gratuito falseado para la compañía financiera que se pretende representar.

2. Cuando la víctima llama a este número, es contestada por una voz computerizada que le indica al "cliente" que su cuenta necesita ser verificada y le requiere que ingrese los 16 dígitos de su tarjeta de crédito.

3. Cuando la persona provee la información de su tarjeta de crédito, el “visher” tiene toda la información necesaria para realizar cargos fraudulentos a la tarjeta de la víctima.

4. La llamada puede ser también utilizada para obtener detalles adicionales como el PIN de seguridad, la fecha de expiración, el número de cuenta u otra información importante.

Propuestas ADICAE para frenar la expansión del fenómeno vishing

■ **Campañas informativas.** Debido a la dificultad de perseguir este tipo de delitos por la vía policial, la mejor vía para frenar este fraude es emprender acciones divulgativas que pongan en conocimiento de la población este tipo de prácticas. Por ello, ADICAE propone que sean los cuerpos de seguridad del Estado junto a las Asociaciones de Consumidores los que promuevan este tipo de campañas.

■ **Regulación del buen uso.** Asimismo la erradicación de este fraude pasa por la regulación de Internet y la vigilancia, por parte de las autoridades competentes, de su buen uso.

Smishing

Es una variante del phising. La operativa de este fraude es muy similar a la del phishing convencional, pero en este caso mediante mensajes de texto (SMS).

¿En qué consiste?

El usuario recibe mensajes de texto que le inducen a llamar a líneas de tarificación adicional o realizar transferencias bancarias con distintos reclamos.

El sistema emisor de estos mensajes de texto o incluso un individuo el cual suele ser un spammer; que intentará suplantar la identidad de alguna persona conocida entre nuestros contactos o incluso una empresa de confianza.

Las víctimas reciben un mensaje SMS indicando que se han suscrito a un servicio de citas on-line (u otros) y que se les cargará el servicio a su factura telefónica. También ofrecen un enlace para que desde el propio teléfono se pueda acceder al sitio web y dar de baja esta suscripción, si así lo desea. Mucha gente se puede sentir alarmada y con la intención de cancelar dicha supuesta suscripción, accede a dicho enlace. A partir de ese momento la víctima se sitúa donde el atacante quería y queda expuesto a la descarga involuntaria de un troyano o cualquier otro tipo malware, simplemente por el hecho de acceder a dicho enlace.

Otra de las modalidades que se practica es que se envían mensajes explicando que el banco le ha cargado en su cuenta una fuerte suma de dinero para la que no tiene fondos. Al llamar se encuentra con los mismos tipos de conversaciones grabadas, que sutilmente hacen que el estafado proporcione los datos de su cuenta.

Propuestas ADICAE para frenar la expansión del fenómeno smishing

■ **Información y red de alertas de los operadores.** Puesto que este fraude se realiza a través de teléfonos móviles, las compañías de telefonía deberían encabezar acciones informativas sobre este fenómeno que llevasen a su reducción y posterior desaparición. Las campañas que emprenderían podrían consistir en el envío al teléfono móvil de sus clientes de mensajes que informen sobre este hecho así como el establecimiento de una red de alertas en sus páginas web que informase de los intentos de smishing que se están produciendo, para prevenir a la población.

Otros fraudes en medios de pago

Otros fraudes en medios de pago

Fraude en Paypal, mobipay y otros

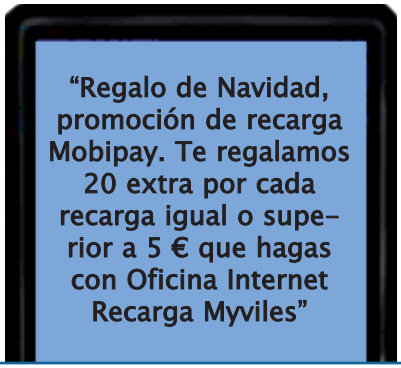
El uso de los nuevos sistemas de pago como Paypal o Mobipay no termina de afianzarse en los pagos en Europa. Uno de los principales motivos por los que no termina de cuajar entre los consumidores es la desconfianza y el miedo al fraude. Aunque en principio estos sistemas se han creado con objeto de garantizar unas transacciones seguras en la Red, los estafadores ya han visto en estos sistemas su blanco para cometer estafas.

Los delitos cometidos consisten en la suplantación de la identidad de las empresas Paypal o Mobipay, enviando a los usuarios de estos sistemas e incluso indiscriminadamente, correos fraudulentos de phishing.

En el caso de los fraudes con suplantación de la entidad Paypal, los correos se hacen pasar por un representante de Paypal, informando de que debe renovar su contraseña o de lo contrario le sería suspendida la cuenta. Se incluye un link a una web falsa, el cual aparentemente te redirige a Paypal pero al colocar el cursor encima se observa que el link redirige a otra web, supuestamente fraudulenta.

En el caso de la suplantación de la empresa Mobipay los ganchos empleados suelen ser promociones:

Como vemos el texto emplea un lenguaje burdo e incluso presenta faltas ortográficas. Al igual que en el anterior caso comentado, el correo incluye un link a una página web falsa con objeto de obtener los datos y claves de la cuenta bancar.



Fraude de los empleados

Este tipo de fraude no suele ser muy común, encontramos únicamente casos aislados. Consiste en que empleados de entidades bancarias, empresas, etc, que a su vez pertenecen a bandas organizadas de delincuentes o "hackers" que sustraen datos de clientes, por ejemplo sus claves secretas, y posteriormente los usan para cometer un fraude.

Cartas nigerianas

En los últimos años están muy en boga los correos difundidos mediante cadenas (cada persona se los envía a sus contactos) pidiendo ayuda para personas enfermas, animales abandonados y otros fines que apelan a la sensibilidad del receptor. No obstante, en numerosas ocasiones se trata de un timo como cualquiera de los antes mencionados.

¿En qué consisten?

Consiste en el envío de correos electrónicos que informan de que el receptor ha ganado la lotería o un sorteo, o piden ayuda para evadir capitales ofreciendo una cuantiosa recompensa. En realidad, se intenta engañar al internauta, al que posteriormente se le pedirá dinero para pagar tasas fronterizas, impuestos, sobornos a funcionarios, etc., como exigencia para obtener la recompensa (que, por supuesto, nunca llegará).

¿Es posible recuperar el dinero sustraído?

A pesar de no ser técnicamente muy complejo, se trata de uno de los fraudes que más daño causa a las personas que son víctimas del mismo. Además, es muy difícil recuperar el dinero estafado ya que usualmente se envía por giros postales a países con escasa seguridad jurídica donde ya se pierde la vista del dinero sustraído.

¿Qué es el "Scam"?

Se trata de una estafa que combina el phising con las cartas nigerianas. En primer lugar, los estafadores ofrecen trabajos con alta remuneración por foros u otros lugares visitados por los internautas, solicitándoles su nombre y cuenta corriente para contratarlos. Posteriormente se obtienen las claves de otros usuarios por el phising y se realizan transferencias al "mulero", que cree que está contratado para gestión de cobros y que deberá enviar las cantidades recibidas por medio de giros a otros países, quedándose una pequeña cantidad en concepto de comisión.

Propuestas ADICAE para frenar la expansión del fraude de los empleados y las cartas nigerianas

■ **Fraude de los empleados:** Las entidades bancarias deben asegurar que los datos y claves bancarias de sus clientes están a buen recaudo y no son transferidas a terceros; por lo que el acceso a las bases de datos de los usuarios debe estar restringido y muy controlado.

ADICAE propone establecer la imposición a los responsables de los bancos y cajas de un sistema de acceso regulado para los trabajadores del banco y toda persona autorizada a disponer de estos datos. El sistema se basaría en la generación de claves distintas y únicas para cada uno de los trabajadores. Esta clave podrá ser usada tan sólo en los tres minutos posteriores a su generación y quedará constancia de su empleo. De este modo, al haber tanta regulación y vigilancia será imposible realizar un fraude sin que el estafador sea detectado.

■ **Cartas nigerianas:** La mejor arma para combatir este fraude es la formación del usuario de Internet. ADICAE, como Asociación de Consumidores, preocupada por el fraude en los nuevos medios de pago, cree necesario que la Comisión Europea encabece una campaña de difusión de este y otros fraudes en los cuales la participación del estafado es necesaria para cometer el delito.

Timos con cheques, letras de cambio y pagarés

Hay muchos tipos de fraudes de cheques falsos, así como letras y pagarés: pero todo comienza cuando alguien le da un cheque que parece real o un giro de dinero y le pide que envíe de vuelta dinero en efectivo a alguna parte. Es falso, y también lo es la historia de la persona, pero que puede tardar semanas en descubrirse. Posteriormente su banco le solicita el dinero. El hecho de que usted pueda obtener el efectivo no significa que el cheque o giro de dinero sea bueno. Al final, usted es el responsable por los cheques o giros de dinero que deposite o canjee.

Domiciliaciones fraudulentas

Consiste en el cargo a nuestra cuenta de pagos periódicos por gastos que no son realizados o servicios que no son contratados. Estas han podido ser realizadas obteniendo nuestros datos mediante algunos de los fraudes anteriormente comentados (fraude de los empleados, phishing...). Si no revisamos periódicamente nuestra libreta podemos ser víctimas de este tipo de fraude durante mucho tiempo, ya que las domiciliaciones se producen de forma periódica. Si detectamos que nos pasan gastos que no hemos realizado, deberemos dar parte a nuestro banco para cancelar el cobro y denegar futuros pagos, diciendo expresamente al empleado de la sucursal que no nos los carguen de aquí en adelante.

Consecuencias de las transferencias fallidas o deficientes

La falta de realización de una transferencia dará lugar a una obligación de reembolso a favor del ordenante y a cargo de la entidad a la que éste ordenó la ejecución de aquella. El importe de ese reembolso está limitado en el caso de las transferencias transfronteriza hasta un total de 12.500 euros. El reembolso está compuesto por el importe de la transferencia, más el de los gastos que el ordenante hubiere abonado y el correspondiente interés legal. El reembolso deberá tener como presupuesto una solicitud formal del ordenante que, como es lógico, solo podrá presentarse una vez que se hubiere agotado el plazo convencional o normativo previsto para la ejecución de la transferencia que se reconoce al ordenante, se impone la obligación de llevar a cabo ese reembolso en el plazo de 14 días contados a partir de la fecha de la solicitud.

PARTE 4

Conclusiones y propuestas

- Conclusiones sobre el estado actual del fraude en medios de pago en España y la Unión Europea

- Propuestas técnicas para acabar con el fraude y sus consecuencias

Conclusiones sobre el estado actual del fraude en medios de pago en España y la Unión Europea

A la vista de la información recogida en este Catálogo podemos ver como la seguridad en los diferentes medios de pago está evolucionando, cada vez se invierten más recursos, tiempo y dinero. El resultado son nuevas medidas y protocolos de seguridad más sofisticados, aparentemente impenetrables y que dejan a las anteriores medidas en la Edad de Piedra. Pero todo es un espejismo temporal, cada vez que sale una nueva medida, lanzada a los cuatro vientos por sus creadores como la definitiva, la absoluta, la que va a acabar con el fraude, vemos como en un breve período de tiempo los delincuentes son capaces de encontrar errores y lagunas en este nuevo invento.

Ya hemos visto cómo diferentes sistemas, medidas o innovaciones en materia de seguridad aparentemente robustos y eficaces han fracasado. ¿A qué se debe? Fundamentalmente a tres **motivos** que van estrechamente unidos:

- En primer lugar, el **coste de implantación,** puesto que lamentablemente hay que tener en cuenta no solo lo seguro que es un sistema, sino también que sea rentable tanto para la empresa que invierte en él como para sus usuarios, puesto que éstos también soportarán el coste de esta infraestructura.

- En segundo lugar, **la generalización de su uso,** es vital que para que una una nueva medida de seguridad se generalice se imponga a las anteriores y quede demostrado que es mucho más eficaz, sino terminará por desaparecer en un breve espacio de tiempo.

- Por último, el nivel de seguridad, **conseguir un altísimo nivel de seguridad no es suficiente,** los usuarios deberán encontrarlo cómodo y de fácil utilización.

Experiencias anteriores han demostrado que un elevado nivel de seguridad suponía un coste de implantación y mantenimiento demasiado alto, además de ser muy complejo de manejar para los usuarios.

A los impedimentos que encuentran la propia industria en la investigación e innovación de medidas de seguridad hay que sumar la postura generalizada de las entidades financiera, muy opacas a la hora de revelar si sufren los efectos del fraude en los medios de pago. Son escasas las noticias, datos referentes a este tema o casos que salen a la luz suministrados directamente por las entidades financieras. Según éstas "sus clientes no sufren a penas fraude a la hora de utilizar sus medios de pago o el servicio de banca electrónica". Estas declaraciones no cuadran con las noticias que salen en los medios de comunicación, casi a diario, de nuevos tipos de fraude o detención de bandas organizadas que ganan con esta actividad cientos de millones de euros. La siguiente cita extraída del Dictamen del Comité Económico y Social Europeo sobre el tema "La lucha contra el fraude y la falsificación de los medios de pago distintos del efectivo" (2009/C 100/04), recoge con claridad esta idea:

> *"El Comité Económico y Social Europeo se lamenta de que las iniciativas emprendidas hasta la fecha para prevenir y luchar contra el fraude y la falsificación de medios de pago distintos del efectivo no hayan resultado suficientes para atajar la difusión de este fenómeno. Como ya subrayó la Comisión en el plan de acción 2004-2007, aunque se ha mejorado y reforzado el marco jurídico comunitario todavía no se ha desarrollado plenamente ni el intercambio de información entre las entidades públicas y privadas, ni la cooperación eficaz entre las autoridades competentes de los Estados miembros. La Comisión ha determinado que el principal obstáculo para lograr la aplicación eficaz de un sistema de prevención en la lucha contra el fraude reside en la dificultad de intercambiar datos sobre los ámbitos de actuación fraudulenta o de riesgo dentro de la Unión Europea. Para garantizar una acción preventiva eficaz, parece necesario aumentar las modalidades de intercambio de información sobre los ámbitos de actuación fraudulenta mediante una mejora de los canales de cooperación entre las autoridades competentes de los Estados miembros".*

Desde luego negar el fraude no es la mejor medida para combatirlo. Son varias las propuestas de solución, iniciativas o medidas que se han puesto en marcha desde diferentes Estados, de manera unilateral, bilateral o multilateral, normalmente a través de instituciones o foros creados con tal intención, pero como podemos comprobar el fraude no se ve frenado, sino que va aumentando, previendo un futuro bastante desesperanzador

Propuestas técnicas para acabar con el fraude y sus consecuencias

Como ya hemos visto anteriormente la generalización del uso de una medida de seguridad es vital para su implantación, la posibilidad de utilizar estos instrumentos en prácticamente todo el mundo exige que estos medios de pago sean eficaces, fáciles de usar, estén ampliamente aceptados, sean fiables y disponibles con un coste relativamente reducido. Dado que el nivel de eficacia depende de su seguridad, es vital garantizar el máximo nivel de seguridad técnica viable desde el punto de vista económico. Quizás la existencia de un marco regulador armonizado en el ámbito de la Unión Europea permitiría a los proveedores de los servicios racionalizar las infraestructuras y los servicios de pago, y a los usuarios beneficiarse de una mayor libertad de elección y un nivel elevado de protección. A parte de esta pequeña propuesta normativa, que sería un posible origen, a continuación nos vamos a centrar exclusivamente en propuestas técnicas que entendemos que irían en beneficio de la seguridad y protección de los ususarios.

Propuesta en utilización de tarjetas

La seguridad en las tarjetas electrónicas va a sufrir un gran espaldarazo con la implantación del chip (Sistema EMV) a partir de finales de 2010 para todas las tarjetas electrónicas en el territorio de la Unión Europea. Según los fabricantes y distribuidores de tarjetas este nuevo sistema es eficaz, pero ya se están empezando a advertir los primeros casos de fraude con tarjetas de chip. Por ello, la industria en materia de seguridad no debe relajarse. Desde **ADICAE** proponemos la implantación de nuevas medidas o la generalización de algunas medidas que de momento no han tenido mucho éxito pero que consideramos que pueden ser eficaces:

- **Mecanismos de autodefensa en cajeros automáticos.** Es decir, que los programas informáticos implantados en la gestión de cajeros automáticos cuenten con mecanismos de autodefensa que delate cualquier movimiento de fondos extraño, ya sea por el lugar en el que se realiza la extracción, la frecuencia de las operaciones o la

cuantía de las mismas. Estos mecanismos de intervención o autodefensa reducen los efectos de una posible manipulación de terminales así como el empleo de tarjetas clonadas.

- **Utilización del teléfono móvil como un segundo canal para autenticar y validar el pago**. El usuario de la tarjeta a través de su móvil recibiría un mensaje para autorizar la operación.

Propuestas en comercio electrónico

Cualquier tipo de empresa que ofrece sus servicios y bienes a través de Internet, sitios web de subastas, e incluso las Administraciones públicas, deben prestar a sus usuarios las máximas garantías de seguridad cuando operan en internet. Por lo que sería recomendable la imposición de tres ideas o propuestas generales para toda aquella empresa o servicio público que opere a través de internet con medios de pago:

Propuestas generales

1. **Incidir en la seguridad como aspecto fundamental para la imagen de negocio o de servicio público.** La confianza es esencial para el usuario que paga a través de internet. Es normal que quien esté estableciendo una relación comercial quiera estar seguro de hacerlo con quien verdaderamente dice serlo.

2. **Considerar los recursos destinados a proteger la seguridad de los sistemas de información como una inversión, no como un gasto.** Dado que la seguridad es un aspecto crítico para cualquier organización, es necesario tratarlo como un fenómeno global, que trasciende todos los procedimientos, rutinas y actuaciones de la empresa.

3. **Acciones preventivas-formativas.** Sería necesario que quien acceda a este tipo de servicios tenga la oportunidad, si no conoce bien el sistema, de informarse y formarse. Por ello sería necesario varias medidas que no suponen gastos excesivos, pero que redundan en la formación del cliente o usuario:

   • Ofrecer un **servicio de atención-asistencia telefónica gratuita durante las 24 horas,** donde el usuario pueda resolver todas sus dudas relacionadas con la seguridad y el funcionamiento del sistema de pago. Esta información debe facilitarse tanto antes

(de manera preventiva) como después, si el cliente a sufrido o cree haber sufrido un fraude (de manera reactiva).

• Contar con un apartado bien visible en la **web con información** general donde se contengan consejos y pautas para el buen uso del medio de pago. A su vez, otro apartado en el que vengan indicaciones del procedimiento de pago (sus fases, medidas de seguridad adoptadas, datos necesarios para poder realizar el pago con éxito, etc).

Propuestas técnicas

1. **La obligación de solicitar el código CVV2**. El código CVV2 (Card Verification Value) es un código de seguridad elaborado por las compañías de las tarjetas. Con este mecanismo de autenticación se identifica la posesión de la tarjeta empleada para el pago en las transacciones realizadas a través de la Red. Este código se debe introducir en el momento de la transacción económica por Internet para verificar que la tarjeta de crédito está en manos de su propietario, introduciendo un nivel de seguridad adicional a las transacciones realizadas.

El formato de estos códigos es variable. Por ejemplo, los códigos CVV2 (Visa) y CVC2 (MasterCard) tienen 3 dígitos mientras que las tarjetas de crédito American Express tienen el código CID de 4 dígitos.

2. **Indicadores de nivel de fraude.** Consistiría en la introducción de un sistema inteligente que permita al usuario conocer, en función de los datos requeridos para una determinada operación, el nivel de riesgo que conllevaría su interceptación maliciosa antes de realizar

dicha operación, advirtiéndole de la conveniencia de asegurarse que la realiza en un entorno seguro. De cara al prestador del servicio a través de la Red, un sistema inteligente de prevención del fraude puede basarse en la generación de avisos basados en resultados anormales en el proceso de validación de datos de una operación. Por ejemplo, sucesivos intentos de validación de datos sobre un mismo número de tarjeta de crédito variando su fecha de caducidad o el código CVV2 puede ser síntoma de un intento de uso fraudulento de dicha tarjeta y la operación podría quedar suspendida hasta comprobar que no se está haciendo un uso ilícito de la misma.

3. **Exigencia a las paginas de comercio a través de la red de que ofrezcan la posibilidad al usuario de utilizar D.N.I. Electrónico.** Las autoridades deberían exigir a toda página web que comercie a través de la web ofrecer la alternativa de, a parte de un sistema común, la utilización del DNI electrónico. Esto daría más prestigio y calidad del servicio a la propia empresa. La utilización de este en operaciones de pago por medio de la red posibilitaría una mayor seguridad para el usuario y el comerciante, puesto que es un sistema de autenticación mucho más fuerte.

4. **Instauración de tarjetas de crédito virtuales como medio de pago generalizado en vez de las tarjetas tradicionales.** Estas tarjetas en realidad son números que se solicitan a la entidad financiera.

Este número se introduce en los formularios de pago cuando se realiza alguna compra por internet o por teléfono. Son de prepago, por lo que se debe cargar previamente transfiriendo dinero desde una cuenta corriente o desde otra tarjeta de crédito. Se puede cargar el dinero que se desee, por lo que el propio usuario limita el riesgo en caso de fraude. Las hay que tienen una duración limitada, de forma que sólo sirven para un periodo determinado, cancelándose una vez transcurrido este vencimiento, medida también muy útil contra el fraude.

5. **Utilización del teléfono móvil como garantía para una segunda validación.** La validación puede hacerse primero de la identidad (quien paga dice ser quien es, el titular de la tarjeta) y segundo del pago (solo el dueño de la tarjeta puede recibir y confirmar la operación con su móvil). Por lo que tener acceso a dos claves que proceden de canales diferentes obstaculizaría notablemente la labor del delincuente.

Todas estas medidas y otras muchas más, deben procurar que la seguridad a nivel tecnológico no se vuelva en contra de un uso dinámico y fácil de internet. El pago de una forma más seguro no puede suponer pérdida de tiempo, un aumento de complejidad y esfuerzo por parte del usuario. El usuario nunca estará dispuesto a perder comodidad y rapidez, algo que siempre ha caracterizado a internet.

Propuestas en banca electrónica

Son muchos los clientes tradicionales que querrían operar a través del servicio de banca por internet de su banco o caja, pero el alto nivel de desconfianza, de inseguridad que les crea provoca que prefieran ir físicamente a su sucursal. De ahí que , las propuestas generales para comercio electrónico sean igualmente aplicables para este servicio que ofrecen las entidades financieras.

Propuestas técnicas

1. **Que las propias entidades financieras suministrasen a sus clientes DVDs, Cds o dispositivo de memoria USB,** que permitiesen “arrancar” el ordenador desde éstos sin necesidad de

instalar ningún programa y sin que en esa sesión se utilizase ningún programa del propio ordenador, con lo que se evitarían todos los posibles virus, troyanos, etc y la influencia de estos.

2. **Implementación de reglas lógicas y de comportamiento del usuario.** Estas reglas y los "motores de comportamiento", se basan en la memorización de las pautas de conducta del usuario, permitiendo establecer alarmas de riesgo ante posibles casos de fraude. Según los expertos es un sistema de protección de un reducido coste, tanto económico como de funcionamiento.

3. **Instauración obligatoria de avisos a móviles mediante mensajes cortos (sms).** Esta medida permite una autenticación a través de dos canales diferentes y con una doble confirmación. Sobre todo a la hora de pagar con una tarjeta asociada a la cuenta o realizar una transferencia.

4. **Tarjetas de coordenadas.** Éstas también ofrecen una elevada fiabilidad. Éstas ya se están utilizando por algunas entidades, pero sería recomendable que todas la utilizasen.

5. **Protección de las páginas web que ofrecen el servicio de banca a través de internet y en concreto de sus servicios DNS**, para que no puedan ser vulnerados ante un posible ataque.

6. **Fomento y promoción por parte de los bancos de la utilización de generadores de clave (Token)**, dispositivos de seguridad que generan claves numéricas individuales que varían cada cierto tiempo.

Bibliografía

- World Payments Report 2008.Capgemini, RBS and EFMA.
- Consumers in Europe: Facts and Figures on services of general interest. 2007 Edition. Eurostat, European Commission.
- Informe de fraude online de 2007 y primer semestre de 2008. S21sec.
- Estudio sobre comercio electrónico B2C 2008. Observatorio Nacional de las Telecomunicaciones y la S.I.(ONTSI)
- La sociedad en red 2007. Informe anual. Observatorio Nacional de las Telecomunicaciones y la S.I.(ONTSI)
- European Financial Integration Report, 2008.
- El sistema Nacional de Compensación Eletronica (Segunda edición). Antonio Rosas Cervantes.Servicio de Estudios del Banco de España. 1995.
- Informe del Sistema Nacional de Compensación Electrónica – SNCE (mayo de 2009).
- Los cibercrímenes en el espacio de libertad, seguridad y justicia. Antonio Pedro Rodríguez Bernal. 2006.
- Informe anual 2006 del Banco de Italia. 2007.
- Decimalisation table attacks for PIN cracking. Mike Bond, Piotr Zielinski. University of Cambridge. Computer Laboratory. 2003.
- Estudio sobre usuarios y entidades públicas y privadas afectadas por la práctica fraudulenta conocida como phishing. Octubre de 2007. Instituto Nacional de Tecnologías de la Comunicación (INTECO).
- Impositores y Usuarios, nº74 (Verano 2007). Dossier “El Euro de los medios de pago”, pp. 19-23
- Global Phishing Survey: Domain Name Use and Trends in 2007. Mayo 2008. APWG (Anti Phishing World Group).
- Dictamen del Comité Económico y Social Europeo sobre el tema “La lucha contra el fraude y la falsificación de los medios de pago distintos del efectivo. Publicado el 30 de abril de 2009 en el Diario Oficial de la Unión Europea.

LAS ENTIDADES FINANCIERAS TAMBIÉN DEBEN IMPLICARSE EN LA LUCHA CONTRA EL FRAUDE

¡¡RECLAMA ANTE TU BANCO O CAJA!!

Tus derechos están en juego

SEDES DE ADICAE

Servicios Centrales ADICAE
C/ Gavín, 12 local 50001 **Zaragoza**
Tfno. 976 390060 - Fax 976 390199
aicar.adicae@adicae.net

Madrid
Embajadores, 135 1º C int.- 28045 **Madrid**
Tfno. 91 5400513 Fax 91 5390023

Catalunya
c/ Entença, 30 entlo. 1º - 08015 **Barcelona**
Tfno. 93 3425044 Fax 93 3425045

Comunidad Valenciana
Av. Pérez Galdós, 97 pta.1 - 46018 **Valencia**
Tfno. 96 3540101 Fax 96 3540106

c/ Aparicio, 5 entlo. 5 - 03003 **Alicante**
Tfno. 96 5926583

Galicia
Avda. Gral. Sanjurjo, 119 -1º dcha
15006 **A Coruña**
Tfno. 981 153969 Fax 881 927603

Castilla y León
c/ Caridad, 1 - 2ºC - 47001 **Valladolid**
Tfno/Fax. 983 373173

Extremadura
c/ Camilo José Cela, 1 3º - 06800 **Mérida**
Tfno/Fax. 924 387468

c/ Gómez Becerra, 25 3º - 10001 **Cáceres**
Tfno/Fax. 927 626336

Andalucía
Av. Eduardo Dato, 85 1ºB - 41005 **Sevilla**
Tfno/Fax. 954 652434

c/ Salvador Noriega, 7 entreplanta dcha
29006 **Málaga**
Tfno/Fax. 952 088955

... o pregunte por nuestras delegaciones en otras provincias

Edita:

ADICAE
Asociación de usuarios de Bancos, Cajas y seguros

Colabora:

Programa de Gestión de la Prevención, Preparación y Gestión del Terrorismo y otros Riesgos relativos a la Seguridad
Comisión Europea, Dirección General de Justicia, Libertad y Seguridad