



GOBIERNO  
DE ESPAÑA

MINISTERIO  
DE INDUSTRIA, TURISMO  
Y COMERCIO

PLAN  
AVANZA2010



Instituto Nacional  
de Tecnologías  
de la Comunicación

# Estudio sobre el fraude a través de Internet

Informe anual 2009



**Edición: Junio 2010**

*El “Estudio sobre el fraude a través de Internet” ha sido elaborado por el siguiente equipo de trabajo del Observatorio de la Seguridad de la Información de INTECO:*

*Pablo Pérez San-José (Coordinador)*

*Susana de la Fuente Rodríguez*

*Laura García Pérez*

*Cristina Gutiérrez Borge*

*Javier Rey Perille*

*INTECO quiere señalar la participación en la realización del trabajo de campo e investigación de este estudio de:*

**SIGMADOS**



La presente publicación pertenece al **Instituto Nacional de Tecnologías de la Comunicación (INTECO)** y está bajo una licencia Reconocimiento-No comercial 2.5 España de Creative Commons, y por ello esta permitido copiar, distribuir y comunicar públicamente esta obra bajo las condiciones siguientes:

- Reconocimiento: El contenido de este informe se puede reproducir total o parcialmente por terceros, citando su procedencia y haciendo referencia expresa tanto a INTECO como a su sitio web: [www.inteco.es](http://www.inteco.es). Dicho reconocimiento no podrá en ningún caso sugerir que INTECO presta apoyo a dicho tercero o apoya el uso que hace de su obra.
- Uso No Comercial: El material original y los trabajos derivados pueden ser distribuidos, copiados y exhibidos mientras su uso no tenga fines comerciales.

Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso de INTECO como titular de los derechos de autor. Nada en esta licencia menoscaba o restringe los derechos morales de INTECO. <http://creativecommons.org/licenses/by-nc/2.5/es/>

El presente documento cumple con las condiciones de accesibilidad del formato PDF (Portable Document Format). Así, se trata de un documento estructurado y etiquetado, provisto de alternativas a todo elemento no textual, marcado de idioma y orden de lectura adecuado.

Para ampliar información sobre la construcción de documentos PDF accesibles puede consultar la guía disponible en la sección Accesibilidad > Formación > Manuales y Guías de la página <http://www.inteco.es>

## ÍNDICE

---

PUNTOS CLAVE .....	4
Seguridad y fraude online .....	4
1 INTRODUCCIÓN Y OBJETIVOS .....	6
1.1 Presentación .....	6
1.1.1 Instituto Nacional de Tecnologías de la Comunicación. ....	6
1.1.2 Observatorio de la Seguridad de la Información.....	7
1.2 Estudio sobre el fraude a través de Internet .....	8
2 DISEÑO METODOLÓGICO .....	9
2.1 Universo.....	9
2.2 Tamaño y distribución muestral .....	9
2.3 Captura de información y trabajo de campo .....	11
2.4 Error muestral .....	13
3 SEGURIDAD Y FRAUDE ONLINE.....	14
3.1 Intento de fraude y manifestaciones .....	14
3.2 Forma adoptada por el remitente origen de la comunicación sospechosa de ser fraudulenta .....	16
3.3 Impacto económico del fraude.....	17
3.4 Fraude y malware .....	19
3.5 Influencia del intento de fraude en la modificación de hábitos .....	21
4 CONCLUSIONES Y RECOMENDACIONES .....	23
ÍNDICE DE GRÁFICOS.....	25

## PUNTOS CLAVE

---

El Observatorio de la Seguridad de la Información publica el *Estudio sobre el fraude a través de Internet (informe anual 2009)*. Para elaborar el análisis se han realizado encuestas periódicas a usuarios de Internet y análisis online de equipos de hogares españoles.

El informe permite realizar, con una perspectiva evolutiva, un diagnóstico de la incidencia de situaciones que podrían crear intentos de fraude entre los usuarios de Internet, y el impacto que las mismas han ejercido, tanto a nivel económico como en cuanto al cambio en los hábitos de uso de servicios de banca o compra electrónica. El análisis online proporciona datos acerca de la incidencia de malware específico para la comisión de fraude.

El período analizado en este documento abarca todo el año 2009. Durante este tiempo se han realizado 14.264 encuestas en 4 tomas de datos y un total de 57.832 análisis de seguridad en los equipos panelistas, llevados a cabo con periodicidad mensual.

Se ofrece, por tanto, un análisis evolutivo a lo largo de los 4 trimestres de 2009.

Se exponen a continuación los puntos clave del estudio.

### Seguridad y fraude online

El 34,1% de los usuarios de Internet españoles declara, en el cuarto trimestre de 2009 (39,6% a principios de año), haber recibido alguna petición de visitar páginas web sospechosas en los 3 meses previos a la realización de la encuesta. Por detrás de ella, el 29,4% (35,6% en el primer trimestre) afirman haber recibido e-mails ofertando servicios no solicitados.

Los casos de ofertas de trabajo potencialmente falsas o sospechosas y la recepción de un e-mail solicitando las claves de usuario son más infrecuentes, y son declarados por un 23,1% y 21,6% de los usuarios, respectivamente. Ambos porcentajes han descendido a lo largo de 2009.

En el análisis de los intentos de fraude a través del teléfono móvil, las frecuencias resultan mínimas comparadas con los casos en Internet: la recepción de SMS ofertando servicios no solicitados, que alcanzaba a un 24,6% de usuarios en el primer trimestre del año, desciende bruscamente hasta el 12,2% en el cuarto trimestre. Menos numerosas aún son las incidencias que tienen que ver con la solicitud de las claves de usuario a través del teléfono móvil a finales de año, tanto a través de una llamada (2,9%) como a través de un SMS (3,1%).

En las formas adoptadas por el remitente de la comunicación sospechosa de ser fraudulenta destacan los bancos o entidades financieras que, aumentando a lo largo de 2009, se sitúan en un 43,1% en el último trimestre.

El porcentaje de usuarios que declara haber sufrido algún perjuicio económico debido a un fraude a través de Internet o telefónico es muy escaso (3,8% en el último trimestre de 2009), concentrándose la distribución del importe defraudado por debajo de los 400 € (límite que establece la ley para diferenciar entre falta y delito).

El análisis empírico de los equipos muestra que, a finales de 2009, un 6,3% aloja algún tipo de troyano bancario (código malicioso destinado a interceptar credenciales de banca electrónica de entidades concretas), del total de 35,6% que alojan algún tipo de troyanos. El porcentaje de este tipo de código malicioso ha descendido un 2,8% desde que se comenzó a analizar este dato (junio de 2009).

El hecho de haber sufrido un intento de fraude (no necesariamente consumado) no influye significativamente en los hábitos de uso de compra y banca electrónica.

Un 84,0% de los usuarios declara en el cuarto trimestre de 2009 que no ha modificado en absoluto sus hábitos de compra en Internet tras haber sufrido un intento de fraude. Un 11,1% reconoce haber reducido sus compras y sólo un 5% afirma abiertamente haber dejado de utilizar los servicios de comercio electrónico.

En el caso de la banca a través de Internet un 89,4% no ha realizado ninguna modificación en sus hábitos de banca electrónica, un 7,4% ha reducido su uso, un 2,7% declara haber abandonado el servicio y un 0,5% haber cambiado de entidad con la que operar a través de la Red.

.

# 1 INTRODUCCIÓN Y OBJETIVOS

---

## 1.1 Presentación

### 1.1.1 Instituto Nacional de Tecnologías de la Comunicación

El Instituto Nacional de Tecnologías de la Comunicación, S.A. (INTECO), es una sociedad estatal adscrita al Ministerio de Industria, Turismo y Comercio a través de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información.

INTECO es un centro de desarrollo de carácter innovador y de interés público de ámbito nacional que se orienta a la aportación de valor, a la industria y a los usuarios, y a la difusión de las nuevas tecnologías de la información y la comunicación (TIC) en España, en clara sintonía con Europa.

Su objetivo fundamental es servir como instrumento para desarrollar la Sociedad de la Información, con actividades propias en el ámbito de la innovación y el desarrollo de proyectos asociados a las TIC, basándose en tres pilares fundamentales: la investigación aplicada, la prestación de servicios y la formación.

La misión de INTECO es aportar valor e innovación a los ciudadanos, a las PYMES, a las Administraciones Públicas y al sector de las tecnologías de la información, a través del desarrollo de proyectos que contribuyan a reforzar la confianza en los servicios de la Sociedad de la Información en nuestro país, promoviendo además una línea de participación internacional.

Para ello, INTECO desarrolla actuaciones en las siguientes líneas:

- **Seguridad Tecnológica:** INTECO está comprometido con la promoción de servicios de la Sociedad de la Información cada vez más seguros, que protejan los datos personales de los interesados, su intimidad, la integridad de su información y eviten ataques que pongan en riesgo los servicios prestados. Y por supuesto que garanticen un cumplimiento estricto de la normativa legal en materia de TIC. Para ello coordina distintas iniciativas públicas en torno a la seguridad de las TIC, que se materializan en la prestación de servicios por parte del Observatorio de la Seguridad de la Información, el Centro de Respuesta a Incidentes de Seguridad en Tecnologías de la Información (INTECO-CERT) con su Centro Demostrador de Tecnologías de Seguridad, y la Oficina de Seguridad del Internauta, de los que se benefician ciudadanos, PYMES, Administraciones Públicas y el sector tecnológico.
- **Accesibilidad:** INTECO promueve servicios de la Sociedad de la Información más accesibles, que supriman las barreras de exclusión, cualquiera que sea la dificultad o carencia técnica, formativa, etc., incluso discapacidad, que tengan sus

usuarios. Y que faciliten la integración progresiva de todos los colectivos de usuarios, de modo que todos ellos puedan beneficiarse de las oportunidades que ofrece la Sociedad de la Información. Asimismo desarrolla proyectos en el ámbito de la accesibilidad orientados a garantizar el derecho de ciudadanos y empresas a relacionarse electrónicamente con las AA.PP.

- **Calidad TIC:** INTECO promueve unos servicios de la Sociedad de la Información que cada vez sean de mayor calidad, que garanticen unos adecuados niveles de servicio, lo cual se traduce en una mayor robustez de aplicaciones y sistemas, un compromiso en la disponibilidad y los tiempos de respuesta, un adecuado soporte para los usuarios, una información precisa y clara sobre la evolución de las funcionalidades de los servicios, y en resumen, servicios cada vez mejores. En esta línea impulsa la competitividad de la industria del Software a través de la promoción de la mejora de la calidad y la certificación de las empresas y profesionales de la ingeniería del software.
- **Formación:** la formación es un factor determinante para la atracción de talento y para la mejora de la competitividad de las empresas. Por ello, INTECO impulsa la formación de universitarios y profesionales en las tecnologías más demandadas por la industria.

### 1.1.2 Observatorio de la Seguridad de la Información

El Observatorio de la Seguridad de la Información se inserta dentro de la línea estratégica de actuación de INTECO en materia de Seguridad Tecnológica. Nace con el objetivo de describir de manera detallada y sistemática el nivel de seguridad y confianza en la Sociedad de la Información y de generar conocimiento especializado en la materia. De este modo, se encuentra al servicio de los ciudadanos, las empresas y las administraciones públicas españolas para describir, analizar, asesorar y difundir la cultura de la seguridad de la información y la e-confianza.

El Observatorio ha diseñado un Plan de Actividades y Estudios con el objeto de producir conocimiento especializado y útil en materia de seguridad por parte de INTECO, así como de elaborar recomendaciones y propuestas que definan tendencias válidas para la toma de decisiones futuras por parte de los poderes públicos.

Dentro de este plan de acción se realizan labores de investigación, análisis, estudio, asesoramiento y divulgación que atenderán, entre otras, a las siguientes estrategias:

- Elaboración de estudios e informes propios en materia de seguridad de las Tecnologías de la Información y la Comunicación, con especial énfasis en la Seguridad en Internet.

- Seguimiento de los principales indicadores y políticas públicas relacionadas con la seguridad de la información y la confianza en el ámbito nacional e internacional.
- Generación de una base de datos que permita el análisis y evaluación de la seguridad y la confianza con una perspectiva temporal.
- Impulso de proyectos de investigación en materia de seguridad TIC.
- Difusión de estudios e informes publicados por otras entidades y organismos nacionales e internacionales, así como de información sobre la actualidad nacional y europea en materia de la seguridad y confianza en la Sociedad de la Información.
- Asesoramiento a las Administraciones Públicas en materia de seguridad de la información y confianza, así como el apoyo a la elaboración, seguimiento y evaluación de políticas públicas en este ámbito.

## 1.2 Estudio sobre el fraude a través de Internet

El *Estudio sobre el fraude a través de Internet* permite analizar de manera evolutiva los intentos de fraude a través de la Red que han sufrido los usuarios a lo largo de 2009, las formas adoptadas por el remitente origen de la comunicación sospechosa de ser fraudulenta y como consecuencia, el impacto económico sufrido.

Este informe sigue la línea iniciada con otras publicaciones del Observatorio de la Seguridad de la Información, [Estudio sobre usuarios y profesionales de entidades públicas y privadas afectados por la práctica fraudulenta conocida como phishing](#) y [Estudio sobre el fraude a través de Internet](#). En esta ocasión no se trata de un análisis tan exhaustivo como los estudios anteriores, si no que se trata de una actualización de los datos de usuarios basados en encuestas y análisis remotos de sus equipos. Este estudio es el primero de una serie de informes trimestrales.

Mediante datos empíricos obtenidos a través de iScan, se analiza la incidencia de malware específico para la comisión de fraude. Se muestran los resultados de ordenadores que contienen código malicioso destinado a interceptar credenciales de banca a través de Internet.

Por último, se señala también la influencia del intento de fraude en la modificación de los hábitos de los usuarios a la hora de utilizar el comercio electrónico y la banca en línea.

## 2 DISEÑO METODOLÓGICO

---

El *Estudio sobre el fraude a través de Internet (informe anual 2009)* se realiza a partir de panel online dedicado compuesto por hogares con conexión a Internet repartidos por todo el territorio nacional.

El panel posibilita la realización de lecturas periódicas del fenómeno del fraude y ofrecer, y por tanto, una perspectiva evolutiva de la situación. El tamaño del panel se mantiene siempre por encima de los 3.000 hogares (en la actualidad el panel está compuesto por 5.752 hogares) y el análisis del mismo lo conforman dos técnicas diferenciadas:

- Encuestas online a usuarios españoles de Internet mayores de 15 años con acceso frecuente desde el hogar, llevadas a cabo con una periodicidad trimestral. Los datos extraídos de las encuestas permiten obtener la percepción sobre la incidencia de prácticas constitutivas de fraude y su posible relevancia económica, así como el nivel de e-confianza de los ciudadanos tras sufrir un intento de fraude.
- Análisis online del nivel de seguridad real de los equipos informáticos existentes en los hogares, realizados mensualmente. Para ello, se utiliza el software iScan, desarrollado por INTECO, que analiza los sistemas y las incidencias de seguridad en los equipos gracias a la utilización conjunta de 46 motores antivirus. Este software se instala en los equipos y los analiza, detectando todo el malware residente en los mismos y recogiendo además datos del sistema operativo, de su estado de actualización y de las herramientas de seguridad instaladas. El programa informático remite esta información a INTECO, que la trata de manera anónima y agregada.

### 2.1 Universo

Usuarios españoles de Internet mayores de 15 años con acceso frecuente a Internet desde el hogar. Para delimitar con mayor precisión el concepto de usuario, se exige una conexión a Internet desde el hogar de, al menos, una vez al mes.

### 2.2 Tamaño y distribución muestral

La afijación muestral responde a un modelo polietápico:

- Estratificación por Comunidades Autónomas para garantizar un mínimo de sujetos en cada una de ellas.

- Muestreo por cuotas de tamaño del hogar, edad, sexo, actividad laboral y tamaño del hábitat<sup>1</sup>.

Dado que la periodicidad de extracción de datos es diferente (trimestral en el caso de las encuestas y mensual en el de los escaneos) y que las bases consideradas no son idénticas (por ejemplo, pueden existir hogares en que se realice el análisis online pero no la encuesta, o viceversa), se presentan de forma independiente: la Tabla 1 presenta el tamaño de la muestra correspondiente a la encuesta y la Tabla 2 indica el número de equipos escaneados correspondiente a los análisis de seguridad de los equipos.

**Tabla 1: Tamaños muestrales para las encuestas**

Período	Tamaño muestral
1 <sup>er</sup> trimestre 2009	3.563
2 <sup>o</sup> trimestre 2009	3.521
3 <sup>er</sup> trimestre 2009	3.540
4 <sup>o</sup> trimestre 2009	3.640

Fuente: INTECO

**Tabla 2: Número de equipos escaneados mensualmente**

Período	Equipos escaneados
Ene'09	5.649
Feb'09	4.325
Mar'09	4.695
Abr'09	4.954
May'09	4.677
Jun'09	4.293
Jul'09	3.971
Ago'09	3.677
Sep'09	4.520
Oct'09	4.294
Nov'09	4.039
Dic'09	4.452

Fuente: INTECO

<sup>1</sup> Estas cuotas se han obtenido de datos representativos a nivel nacional de usuarios de Internet mayores de 15 años que se conectan más de una vez al mes desde el hogar facilitados por Red.es, entidad pública empresarial del Ministerio de Industria, Comercio y Turismo. ("Las TIC en los hogares españoles: 25<sup>a</sup> oleada julio-septiembre 2009")

### 2.3 Captura de información y trabajo de campo

El trabajo de campo ha sido realizado entre enero y diciembre de 2009 mediante entrevistas online y análisis de equipos informáticos a partir de un panel de usuarios de Internet.

El análisis de equipos informáticos se realiza con la herramienta **iScan** (INTECO Scanner). Esta herramienta es un software multiplataforma desarrollado por INTECO, que se entrega a los panelistas con el fin de que lo instalen en sus ordenadores. iScan utiliza 46 motores antivirus. Este software analiza mensualmente los equipos de los panelistas, detectando el malware específico para la comisión de fraude residente en los mismos.

El programa informático remite esta información a INTECO, que la trata de manera anónima y agregada. A lo largo de todo el proceso se cumple estrictamente con la normativa vigente en materia de protección de datos de carácter personal.

El escaneo de iScan no da información sobre si un determinado código malicioso se encuentra activo en el sistema. Podría darse el caso de que un sistema aloja malware pero no se encuentra infectado. Imagínese, por ejemplo, que un investigador tiene un directorio con código malicioso para estudiar, su equipo sería catalogado por iScan como infectado pero dichas muestras nunca se habrían ejecutado en el sistema y por tanto no estaría infectado. Esto también ocurriría si un antivirus detecta un código malicioso y lo mueve a una carpeta de cuarentena sin ofuscarlo.

Con el fin de reducir el impacto de los falsos positivos se aplican una serie de filtros, que se explican a continuación:

#### Eliminación y ponderación de soluciones antivirus

- a. *Eliminación de productos antivirus de perímetro que tras pruebas con grandes cantidades de malware y goodware<sup>2</sup> demostraron ser altamente paranoicos.*
- b. *Eliminación de ciertas soluciones que comparten firmas, para sólo considerar un motor con el mismo conjunto de firmas.*
- c. *Creación de un subconjunto de motores. Se han tomado los 11 antivirus más reputados (con mejor tasa de detección frente a especímenes detectados por más de 10 antivirus) para crear un subconjunto de productos que será referenciado como motores necesariamente exigidos. De este modo, para que un fichero sea marcado como malware, deberá ser detectado por 5 productos de los 46 considerados y, además, al menos uno de ellos deberá ser alguno de estos 11 motores exigidos.*

<sup>2</sup> Software y ficheros legítimos, archivos inocuos.

### Contraste con bases de datos de software conocido y de ficheros inocuos

INTECO mantiene una base de datos de software de fabricantes confiables y de freeware<sup>3</sup> y shareware<sup>4</sup> confirmado como inocuo. Todos los ejemplares que siguen siendo detectados tras las dos primeras capas de filtrado son comparados con esta base de datos para eliminar más falsos positivos.

De igual forma, los ficheros son contrastados con la estadounidense National Software Reference Library del NIST (National Institute of Standards and Technology), base de datos de software conocido. Si se detectase que alguno de los ficheros señalados por iScan está en dicha base de datos y no forma parte de un kit de hacking o cracking, el archivo no será considerado como malicioso.

### Eliminación de detecciones concretas y corrección de categorías incorrectamente determinadas

Se elimina toda detección de la familia “Annihilator” porque se trata del nombre que emplean algunos antivirus para detectar (erróneamente) los ficheros legítimos del antivirus Panda. Las detecciones “WinVNC” y “VNCView” también son suprimidas pues designan una herramienta de gestión remota de equipos que -muy probablemente- puede haber sido instalada deliberadamente por el usuario.

Todos estos filtros son mejoras importantes de cara a la fiabilidad del estudio, pero no eliminan por completo la problemática de los falsos positivos (una problemática inherente a la industria antivirus).

Por otro lado, al exigir más condiciones de cara a marcar un fichero como malware, también se puede elevar la tasa de falsos negativos. Se trata de un compromiso entre capacidad de detección (utilización de varios antivirus) y detecciones incorrectas (falsos positivos).

En cualquier caso, a pesar de la fortaleza de la herramienta iScan y de las medidas adoptadas por INTECO para mitigar la incidencia de falsos positivos, se debe puntualizar que existen otras limitaciones intrínsecas a la metodología empleada que hacen que el análisis no sea infalible. Por ello, a pesar del rigor y robustez del análisis, los datos que el informe ofrece cuentan con un margen de error que da una perspectiva de los problemas actuales a los que se enfrenta la industria de seguridad a la hora de desarrollar sus programas antivirus.

---

<sup>3</sup> Software gratuito.

<sup>4</sup> Software de descarga gratuita pero limitado en funcionalidad o tiempo de uso.

## 2.4 Error muestral

De acuerdo con los criterios del muestreo aleatorio simple para variables dicotómicas en las que  $p=q=0,5$  y para un nivel de confianza del 95,5%, se establece un error muestral inferior a  $\pm 1,7\%$  en cada uno de los períodos analizados, tal y como se recoge en la siguiente tabla.

**Tabla 3: Errores muestrales de las encuestas (%)**

Período	Tamaño muestral	Error muestral
1 <sup>er</sup> trimestre 2009	3.563	$\pm 1,68\%$
2 <sup>o</sup> trimestre 2009	3.521	$\pm 1,68\%$
3 <sup>er</sup> trimestre 2009	3.540	$\pm 1,68\%$
4 <sup>o</sup> trimestre 2009	3.640	$\pm 1,66\%$

*Fuente: INTECO*

## 3 SEGURIDAD Y FRAUDE ONLINE

---

### 3.1 Intento de fraude y manifestaciones

En primer lugar se analiza la evolución de la incidencia de situaciones de fraude basado en técnicas de ingeniería social a través de Internet (Gráfico 1) y a través del teléfono móvil (Gráfico 2) entre los usuarios de Internet españoles.

Para la interpretación correcta de los datos, es necesario realizar dos puntualizaciones previas:

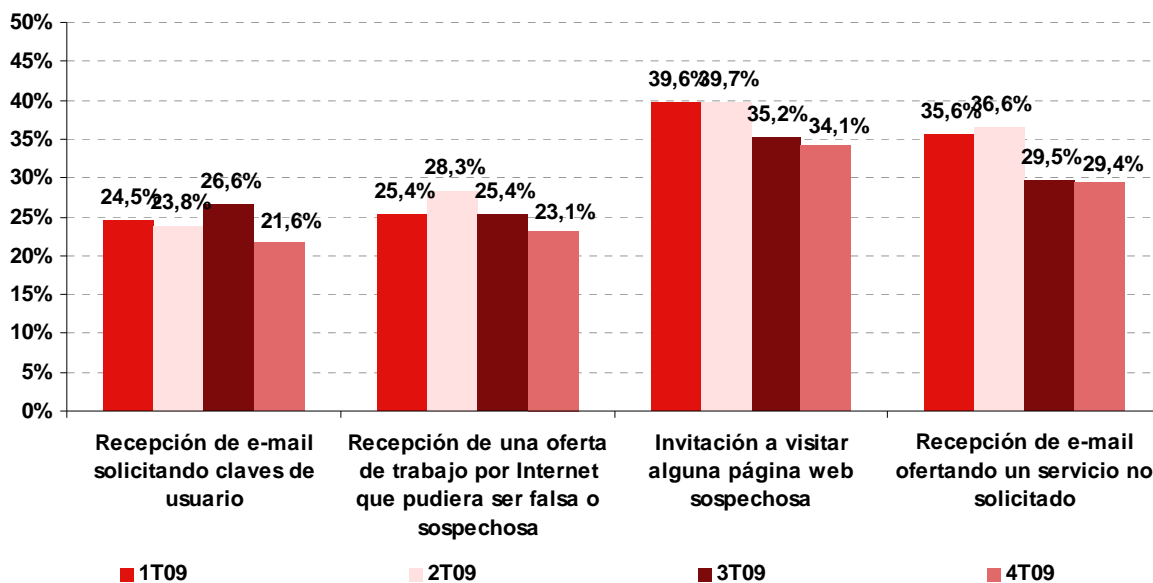
- En primer lugar, los datos proporcionados en ambos gráficos están basados en las respuestas proporcionados por el panel de usuarios de Internet españoles, ofreciendo por tanto la perspectiva del ciudadano.
- En segundo lugar, no debe entenderse que las personas que afirman haber experimentado alguna de las situaciones analizadas son efectivamente víctimas de fraude. Se podría hablar, por tanto, de intento de fraude, pero no de fraude consumado.

Las dos incidencias declaradas con mayor frecuencia a lo largo de 2009 son haber recibido alguna petición de visitar páginas web sospechosas en los 3 meses previos a la realización de la encuesta, pasando de un 39,6% en el primer trimestre del año a 34,1% en el último, y haber recibido e-mails ofertando servicios no solicitados con un 35,6% a comienzos de 2009 y 29,4% a finales de año.

El correo basura ofertando servicios o los correos que incitan a visitar una página web (bien sea para redirigir a las tiendas online, bien para intentar infectar el equipo) son amenazas que se realizan en Internet desde hace años, y siguen siendo de las más populares (sin perder efectividad) debido al bajo coste y relativamente alto índice de éxito para los atacantes.

Los casos de ofertas de trabajo potencialmente falsas o sospechosas (usadas para captar personas que muevan el dinero robado de phishings y troyanos) y la recepción de un e-mail solicitando las claves de usuario son más infrecuentes, y son declarados por un 23,1% y 21,6% de los usuarios, respectivamente. La especificación del malware en el robo de contraseñas de banca online y el relativo éxito del phishing son circunstancias que explican la necesidad de los atacantes de mover el dinero robado y, por tanto, de captar a personas incautas para realizar estas operaciones ilegales a través de ese tipo de correos.

**Gráfico 1: Evolución de la incidencia declarada de situaciones de intento (no consumado) de fraude a través de Internet en los últimos 3 meses (%)**



Base: Total usuarios (n=3.640 en 4T09)

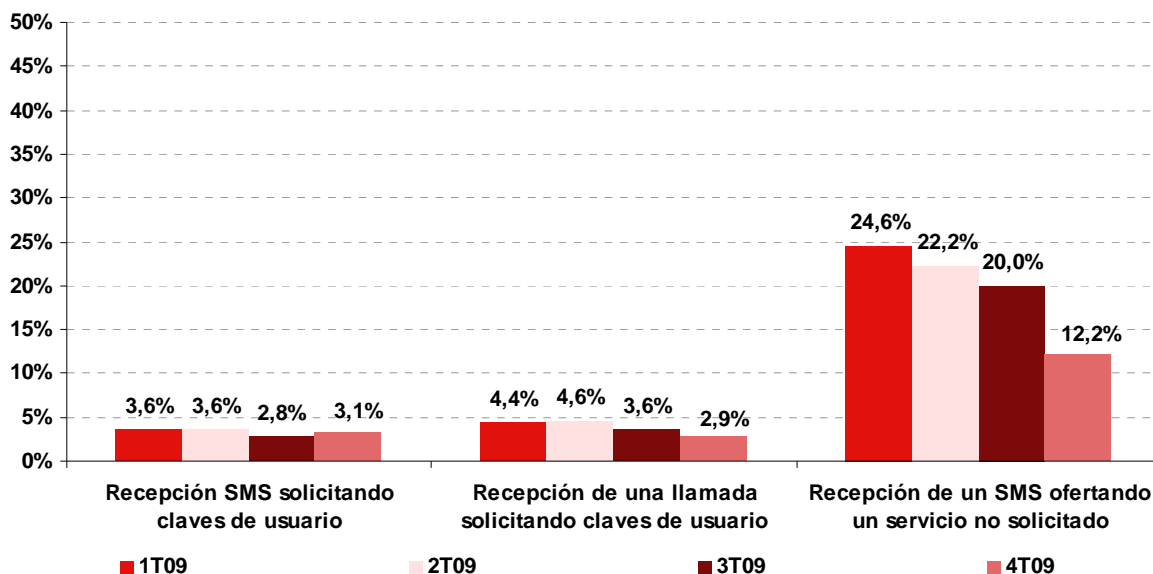
Fuente: INTECO

El teléfono móvil, aunque omnipresente, no resulta todavía un objetivo prioritario para los atacantes. Así lo muestra el Gráfico 2, que demuestra que las frecuencias de intento de fraude e incidencias resultan mínimas comparadas con los casos en Internet.

La recepción de SMS ofertando servicios no solicitados, que alcanzó a un 24,6% de usuarios en el primer trimestre del año, desciende bruscamente hasta el 12,2% en el cuarto trimestre de 2009. El mayor coste del envío de SMS frente al envío de correos electrónicos puede explicar esta tendencia.

Menos numerosas son las incidencias que tienen que ver con la solicitud de las claves de usuario a través del teléfono móvil, tanto a través de una llamada (2,9%) como a través de un SMS (3,1%).

**Gráfico 2: Evolución de la incidencia declarada de situaciones de intento (no consumado) de fraude a través del teléfono móvil en los últimos 3 meses (%)**



Base: Total usuarios (n=3.640 en 4T09)

Fuente: INTECO

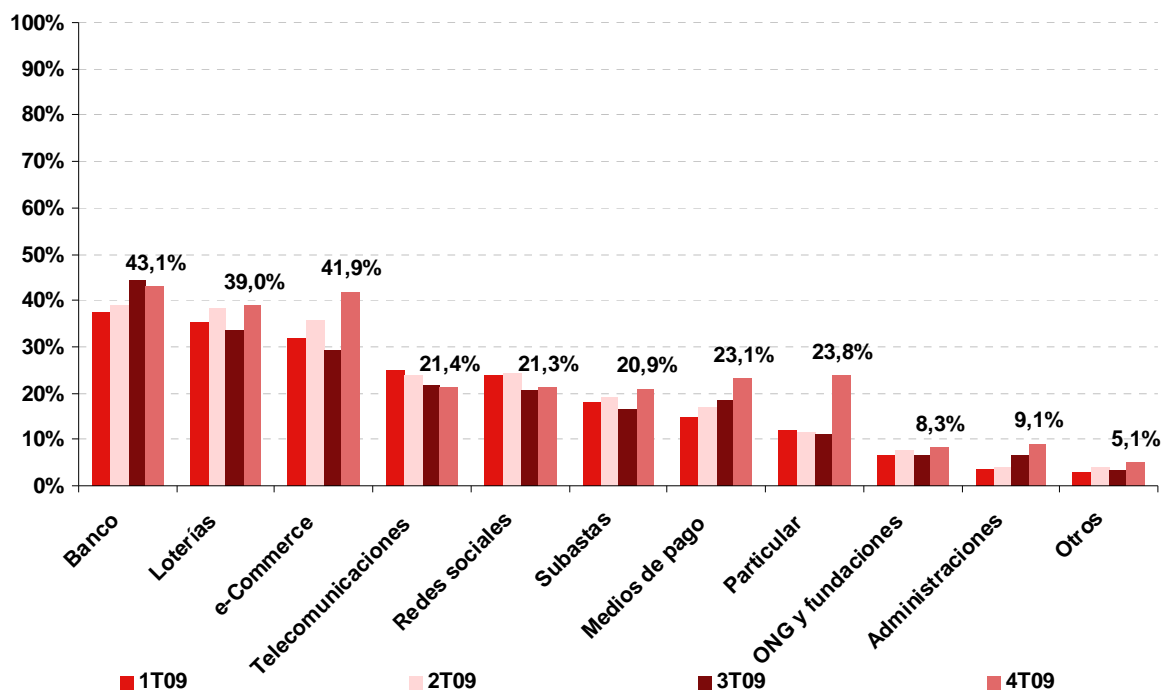
### 3.2 Forma adoptada por el remitente origen de la comunicación sospechosa de ser fraudulenta

En el Gráfico 3 se muestran las respuestas de los panelistas a la pregunta: *¿qué tipo de entidad sospechosa decía ser la que solicitaba sus claves/datos?*

Aunque el sector más afectado sigue siendo el bancario (con un 43,1% de los usuarios que afirmaron haber recibido comunicaciones fraudulentas de un supuesto banco), se aprecia en el último trimestre de 2009 una importante subida del phishing basado en el comercio electrónico. Pasa de un 31,9% a comienzos de año a un 41,9% en el último trimestre. Igualmente suben las estafas que se hacen pasar por casinos o juegos online (39%) y subastas (sube tres puntos desde comienzos de año hasta situarse en 20,9).

Además de la subida del phishing basado en el comercio electrónico y de los fraudes simulando medios de pago, cabe destacar también la importante subida los intentos de estafa que decían provenir de un particular (sube hasta un 23,8%). Es difícil determinar qué tipo de fraude se esconde bajo este tipo, pero puede tratarse de estafas también relacionadas con los casos de ofertas de trabajo potencialmente falsas o sospechosas usadas para captar personas que muevan el dinero robado de phishings y troyanos. En muchas ocasiones, en este tipo de correos, se presentan como particulares que ofrecen contratos privados o colaboraciones.

**Gráfico 3: Evolución de las formas adoptadas por el remitente de la comunicación sospechosa de ser fraudulenta <sup>5</sup> (%)**



Base: Usuarios que han sufrido algún intento de fraude (n=1.937 en 4T09)

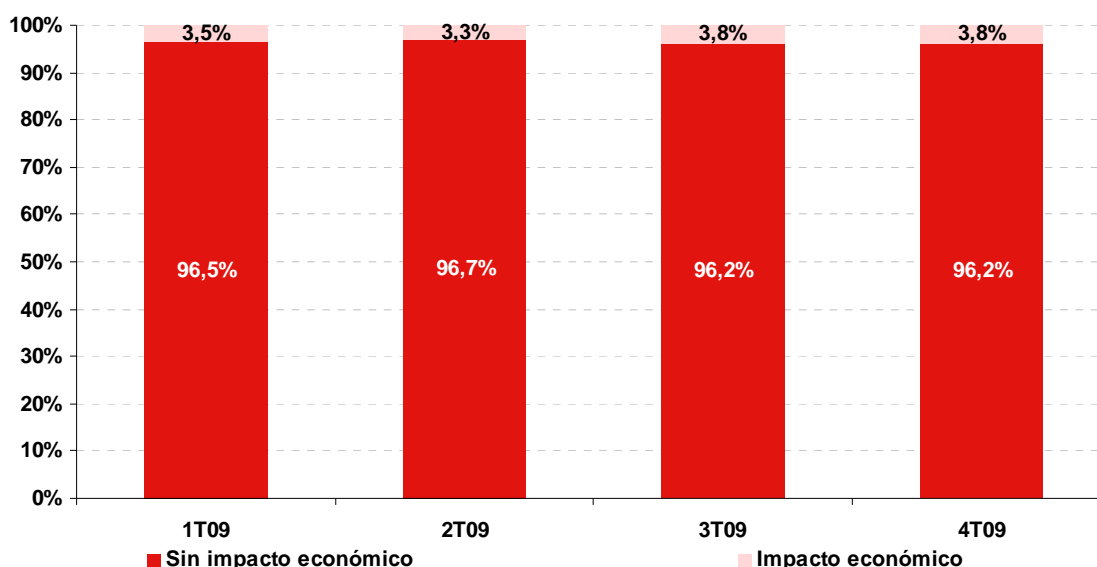
Fuente: INTECO

### 3.3 Impacto económico del fraude

En el cuarto trimestre de 2009 el 96,2% de los usuarios de Internet españoles afirma no haber sufrido una pérdida económica como consecuencia de un fraude electrónico en los últimos 3 meses. El dato se mantiene estable durante el año. La incidencia de fraude con perjuicio económico se mantiene constante entre el 3,5% y el 3,8%.

<sup>5</sup> Los literales utilizados en el cuestionario son los siguientes: Banco o entidades financieras, Páginas de comercio electrónico o compraventa online, Entidades de medios de pago (tarjetas de crédito, PayPal, etc.), Redes sociales, páginas de contactos, Organismos de la Administración Pública, Operadores de telecomunicaciones (telefonía fija, móvil, Internet), Organizaciones sin ánimo de lucro (ONGs, fundaciones, museos, etc.), Páginas de subastas online, Páginas de loterías, casinos o juegos online, Un particular, Otros.

**Gráfico 4: Evolución del fraude con impacto económico para el usuario (%)**

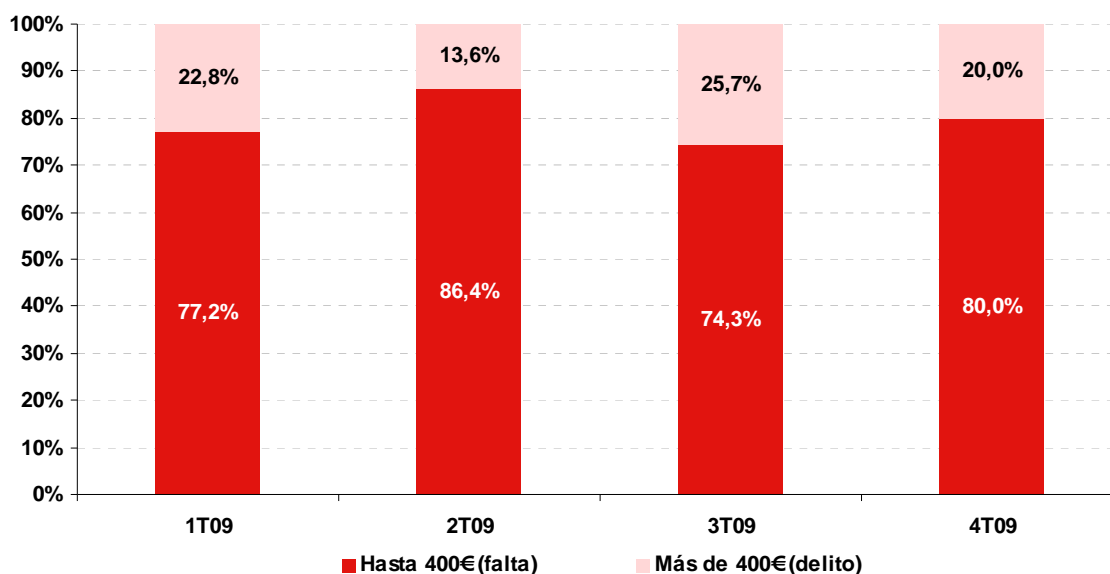


Base: Total usuarios (n=3.640 en 4T09)

Fuente: INTECO

El Código Penal español establece en 400 € el límite entre lo que se considera falta y delito. La distinción es relevante, y afecta a la severidad de la pena a aplicar al estafador (más grave en el caso de un delito que de una falta). En el 4º trimestre de 2009, el 80% de los usuarios que sufrieron una pérdida económica reportó menos de 400 € (en el 1º trimestre de 2009 este porcentaje era de 77,2%).

**Gráfico 5: Evolución de la cuantía económica derivada del fraude (%)**

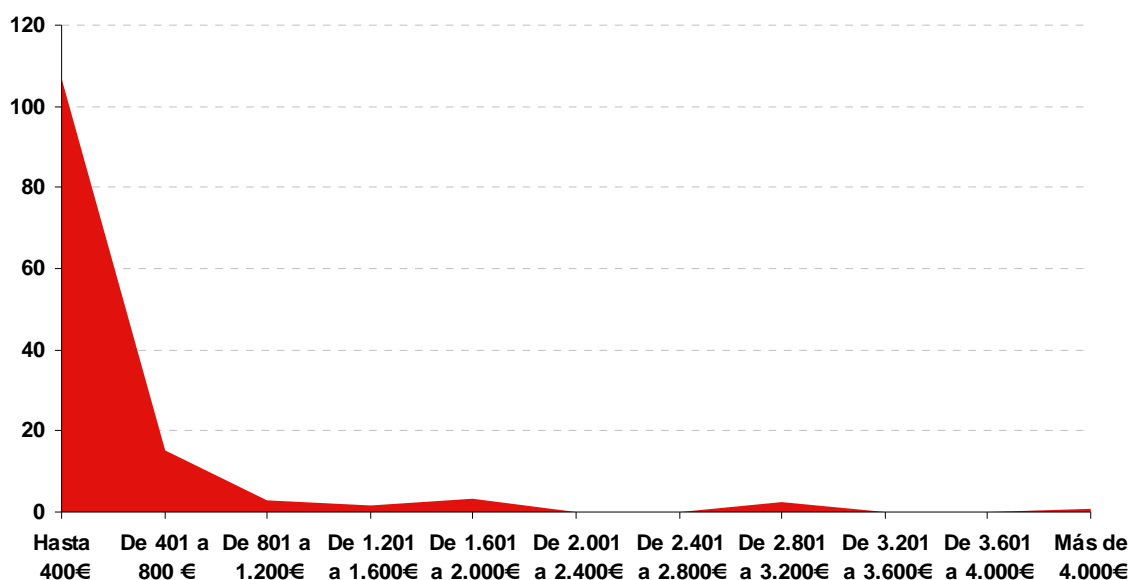


Base: Usuarios que han sufrido perjuicio económico como consecuencia de un fraude online (n=139 en 4T09)

Fuente: INTECO

Se muestra en el Gráfico 6 la distribución de la frecuencia del importe defraudado para el 4º trimestre de 2009. Se aprecia que la mayor agrupación de usuarios se encuentra en el límite inferior de la distribución (menos de 400 €).

**Gráfico 6: Distribución del importe defraudado en el 4T 2009 (frecuencia)**



Base: Usuarios que han sufrido perjuicio económico como consecuencia de un fraude online (n=139)

Fuente: INTECO

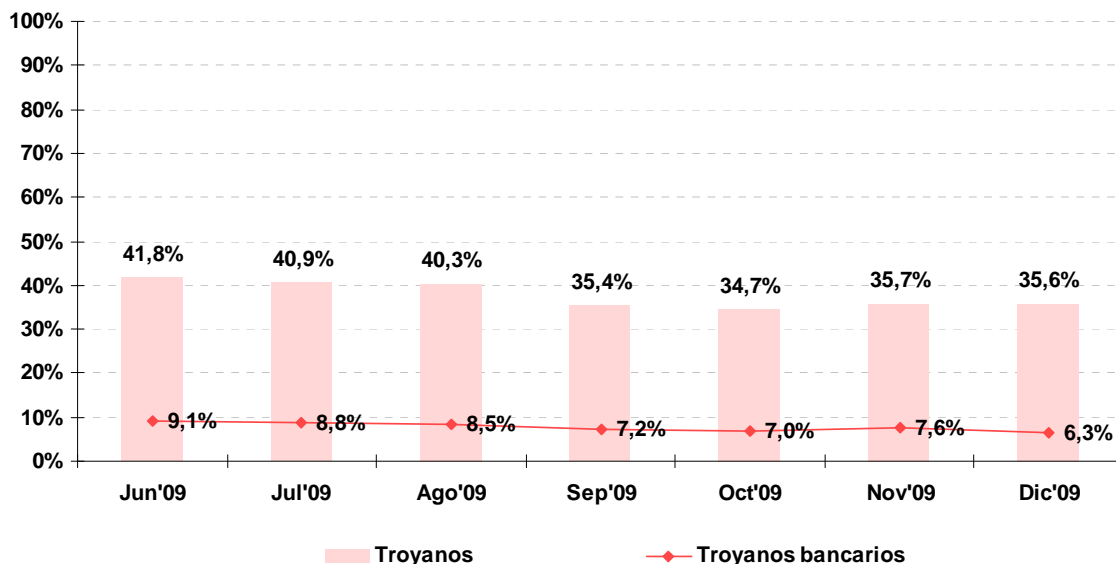
### 3.4 Fraude y malware

Se analiza a continuación la incidencia de malware específico para la comisión de fraude: ordenadores que contienen código malicioso destinado a interceptar credenciales de banca electrónica de entidades concretas. Para ello se han identificado los equipos que contienen código malicioso de alguna familia de troyanos bancarios que usa un archivo de configuración o estructura de datos en donde aparece explícitamente algún banco concreto referenciado.

Estos datos proceden de los datos empíricos obtenidos a través de iScan.

En diciembre de 2009, un 6,3% de los equipos analizados aloja algún tipo de troyano bancario, del total de 35,6% que alojan algún tipo de troyanos.

**Gráfico 7: Evolución de equipos que alojan troyanos bancarios (%)**



Fuente: INTECO

Se han considerado las familias de troyanos bancarios más populares que efectúan ataques dirigidos contra entidades bancarias<sup>6</sup>. Son las siguientes:

*bancos, bank, banker, silentbanker, zbot, sinowal, torpig, fraud, zeus, infostealer, ambler, stealer, yessim, yaludle, banload, bankpatch, multibanker, nethell, chromeinject, goldun, banspy, bancodoor y bancodo.*

A la hora de interpretar los datos, es necesario aclarar que los equipos que alojan malware bancario no necesariamente terminan en una situación de fraude. Para que un fraude se produzca se han de dar tres circunstancias:

- 1) El equipo del usuario ha de estar infectado por este tipo de troyanos.
- 2) El espécimen que infectó la máquina del usuario ha de atacar a la entidad bancaria con la que opera el usuario.
- 3) El usuario ha de iniciar sesión en su espacio de banca electrónica y rellenar los datos adicionales que se le soliciten.

<sup>6</sup> Existen otras familias de troyanos que pueden emplearse para cometer fraude aunque éste no sea su cometido primordial o único. Por ejemplo, los capturadores genéricos de teclas en ocasiones pueden ser utilizados para capturar credenciales bancarias. De igual forma, los troyanos tradicionales de puerta trasera permiten hacer capturas de pantalla remotas y ver lo que el usuario escribe. Así, podrían ser empleados por un atacante para interceptar credenciales de servicios de banca o pagos online. Estas familias no se están considerando en el análisis.

### 3.5 Influencia del intento de fraude en la modificación de hábitos

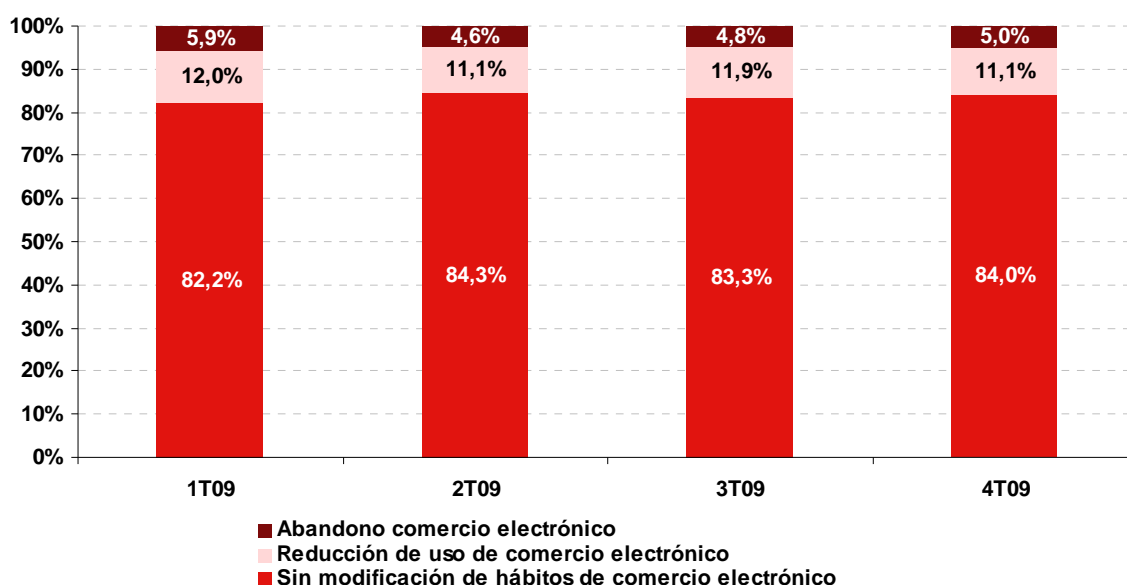
En este epígrafe se intenta averiguar si el hecho de haber sufrido un intento (no necesariamente consumado) de fraude influye de algún modo en los hábitos de la víctima. Se analiza el posible impacto en hábitos de comercio electrónico (Gráfico 8) y banca electrónica (Gráfico 9), ofreciendo una perspectiva evolutiva a lo largo de 2009.

Una vez más, la conclusión es que el haber sufrido un intento de fraude no influye significativamente en los hábitos de uso de compra y banca electrónica.

Un 84,0% de los usuarios declara en el cuarto trimestre de 2009 que no ha modificado en absoluto sus hábitos de compra en Internet tras haber sufrido un intento de fraude. Un 11,1% reconoce haber reducido sus compras y sólo un 5% afirma abiertamente haber dejado de utilizar los servicios de comercio electrónico.

Los datos son muy similares a los de trimestres anteriores.

**Gráfico 8: Modificación de hábitos de comercio electrónico tras sufrir intento (no consumado) de fraude (%)**

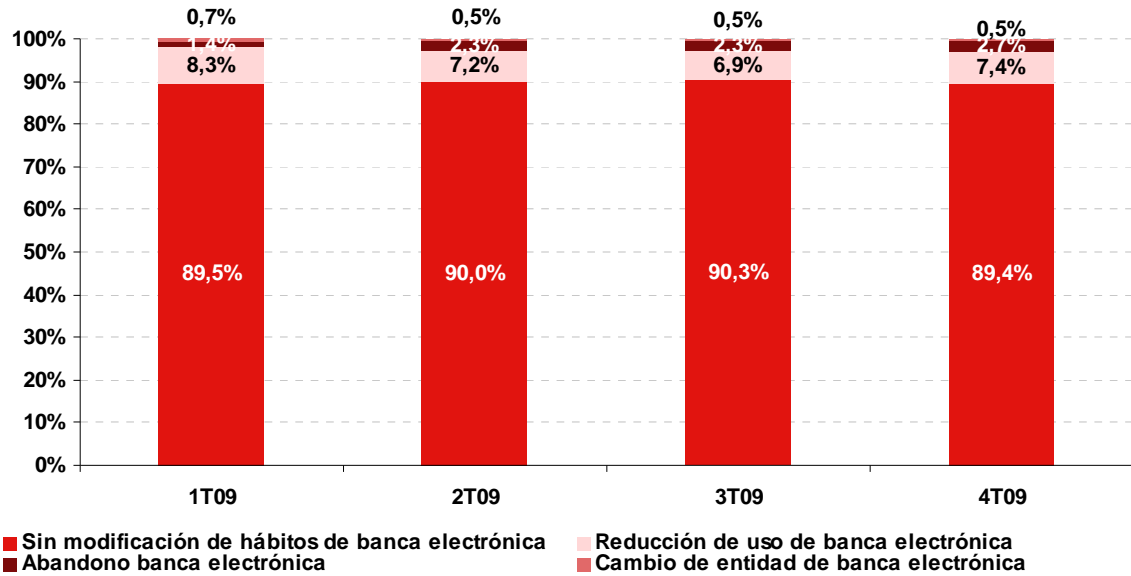


Base: Usuarios que han sufrido algún intento de fraude y/o un perjuicio económico (n=1.968 en 4T09)

Fuente: INTECO

En banca electrónica, el usuario no modifica en absoluto el uso que hace del servicio tras sufrir un intento de fraude en un 89,4%. Un 7,4% reduce su uso y un 0,5% cambia de banco. Sólo un 2,7% reconoce dejar de usar la banca online.

**Gráfico 9: Modificación de hábitos de banca electrónica tras sufrir intento (no consumado) de fraude (%)**



Base: Usuarios que han sufrido algún intento de fraude y/o un perjuicio económico (n=1.968 en 4T09)

Fuente: INTECO

## 4 CONCLUSIONES Y RECOMENDACIONES

---

La evolución de la incidencia declarada de situaciones de intento (no consumado) de fraude en los últimos tres meses muestra que las técnicas de ingeniería social a través de Internet son mayoritarias si se comparan con aquellas relacionadas con el teléfono móvil.

La proporción de usuarios que creen haber recibido un intento de fraude, aunque no haya llegado a consumarse (en términos de impacto económico), en la mayoría de los casos ha disminuido a lo largo del año 2009. En el cuarto trimestre la incidencia declarada por mayor número de usuarios de Internet fue la invitación a visitar alguna página web sospechosa, seguida de la recepción de un e-mail ofertando un servicio no solicitado.

A la hora de destacar el mayor descenso en las incidencias declaradas, es la recepción de un SMS ofertando un servicio no solicitado la que experimenta una mayor reducción, pasando del 24,6% a comienzos de año 2009 a 12,2% en el cuarto trimestre.

### ¿Qué tipo de entidad adoptaba el remitente?

Son, durante todo el año 2009, los bancos o las entidades financieras las formas adoptadas en mayor medida por el remitente origen de la comunicación sospechosa de ser fraudulenta. Esto se debe, tal vez, a la mayor confianza que ofrece este tipo de instituciones a los usuarios.

### ¿Han sufrido los usuarios un perjuicio económico debido al fraude?

La evolución del fraude sin impacto económico se mantiene estable a lo largo del año, entre el 96,5% y el 96,2%. Entre la base de usuarios que sí han sufrido perjuicio económico como consecuencia de un fraude a través de Internet o telefónico en el último trimestre de 2009, la distribución del importe defraudado se concentra en menos de 400 €.

### ¿Ha habido cambios en los hábitos de los usuarios como consecuencia del intento de fraude?

La principal conclusión que se puede extraer del análisis es que los usuarios no manifiestan modificaciones a la hora de realizar operaciones de comercio electrónico o banca a través de Internet después de haber sufrido algún intento de fraude y/o un perjuicio económico.

Tanto en el comercio electrónico como en la banca en línea más del 80% de los usuarios declaran no haber realizado modificaciones en sus hábitos.

Para ayudar a no ser víctima de intento de fraude a través de Internet o telefónico, a continuación se recogen unas recomendaciones generales:

- Utilizar cuentas de usuario con permisos limitados.
- Utilizar contraseñas seguras.
- No enviar información personal o financiera a través del correo electrónico.
- Limitar la información personal que se proporciona en las redes sociales.
- Usar programas de seguridad en los equipos en los que se realicen operaciones a través de Internet.
- Tener precaución a la hora de descargar o abrir archivos adjuntos.
- Mantenerse informado sobre cuestiones de seguridad informática, conocer los riesgos y las principales amenazas de las que protegerse.

La colaboración de los usuarios a la hora de evidenciar un intento de fraude es primordial para poder interceptarlos a tiempo y poder localizar lugares desde donde se publican páginas, se emiten mensajes fraudulentos o donde se reciben los datos capturados.

Para facilitar esta colaboración, la [Oficina Seguridad del Internauta](#) (OSI) pone a disposición del usuario el formulario de [alta de incidentes](#), desde donde se puede indicar las entidades afectadas y toda la información disponible sobre el caso de fraude, y el teléfono de asistencia 901 111 121.

Por último, en caso de haber sido víctima de un fraude, es conveniente poner inmediatamente la denuncia correspondiente, para lo que el usuario puede ponerse en contacto con:

- El [Cuerpo Nacional de Policía](#), a través de la Comisaría General de la Policía Judicial, dispone de la [Brigada de Investigación Tecnológica](#) (BIT) para combatir la delincuencia que utiliza los medios que proporcionan las nuevas Tecnologías de la Información y se puede contactar con ella a través del correo electrónico Buzón de delitos tecnológicos de la policía: [delitos.tecnologicos@policia.es](mailto:delitos.tecnologicos@policia.es). La presentación de la denuncia se puede realizar a través del teléfono: 902 102 112, [página web](#) o en cualquier [comisaría](#).
- La [Guardia Civil](#) cuenta con el [Grupo de Delitos Telemáticos](#) (GDT) de la Unidad Central Operativa (UCO), con el que se puede contactar a través de la [sección colabora](#) de su página web o del correo electrónico: [delitostelematicos@guardiacivil.org](mailto:delitostelematicos@guardiacivil.org).

## ÍNDICE DE GRÁFICOS

---

Gráfico 1: Evolución de la incidencia declarada de situaciones de intento (no consumado) de fraude a través de Internet en los últimos 3 meses (%) .....	15
Gráfico 2: Evolución de la incidencia declarada de situaciones de intento (no consumado) de fraude a través del teléfono móvil en los últimos 3 meses (%).....	16
Gráfico 3: Evolución de las formas adoptadas por el remitente de la comunicación sospechosa de ser fraudulenta (%).....	17
Gráfico 4: Evolución del fraude con impacto económico para el usuario (%) .....	18
Gráfico 5: Evolución de la cuantía económica derivada del fraude (%) .....	18
Gráfico 6: Distribución del importe defraudado en el 4T 2009 (frecuencia) .....	19
Gráfico 7: Evolución de equipos que alojan troyanos bancarios (%) .....	20
Gráfico 8: Modificación de hábitos de comercio electrónico tras sufrir intento (no consumado) de fraude (%) .....	21
Gráfico 9: Modificación de hábitos de banca electrónica tras sufrir intento (no consumado) de fraude (%).....	22



Instituto Nacional  
de Tecnologías  
de la Comunicación

<http://www.inteco.es>

<http://observatorio.inteco.es>