

# Estudio sobre el fraude a través de Internet

2º trimestre de 2010



**Edición: Noviembre 2010**

*El “Estudio sobre el fraude a través de Internet (2º trimestre de 2010)” 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*

*Eduardo Álvarez Alonso*

*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
I    Seguridad y fraude online .....	4
1    INTRODUCCIÓN Y OBJETIVOS .....	6
1.1    Presentación .....	6
1.2    Estudio sobre el fraude a través de Internet .....	8
1.    DISEÑO METODOLÓGICO .....	9
1.3    Universo .....	9
1.4    Tamaño y distribución muestral .....	9
1.5    Captura de información y trabajo de campo .....	11
1.6    Error muestral .....	14
2    SEGURIDAD Y FRAUDE ONLINE .....	15
2.1    Intento de fraude y manifestaciones .....	15
2.2    Forma adoptada por el remitente origen de la comunicación sospechosa de ser fraudulenta .....	17
2.3    Impacto económico del fraude .....	19
2.4    Fraude y malware .....	21
2.5    Influencia del intento de fraude en los hábitos relacionados con la banca a través de Internet y el comercio electrónico .....	24
3    CONCLUSIONES Y RECOMENDACIONES .....	28
1.2.    Conclusiones del análisis .....	28
1.3.    Recomendaciones .....	29
ÍNDICE DE GRÁFICOS .....	31
ÍNDICE DE TABLAS .....	32

## PUNTOS CLAVE

---

El Observatorio de la Seguridad de la Información publica el *Estudio sobre el fraude a través de Internet (2º trimestre de 2010)*. Para elaborar el informe se han realizado encuestas a usuarios de Internet y análisis online de equipos de hogares españoles.

El informe permite realizar un diagnóstico de la incidencia de situaciones que podrían crear intentos de fraude entre los usuarios de Internet. Asimismo, analiza el impacto que estas situaciones han tenido a nivel económico y la influencia que han ejercido en los hábitos relacionados con la banca a través de Internet y el comercio electrónico. El análisis muestra también la diferencia existente entre los usuarios que han sufrido intento de fraude y los que no a la hora de depositar su confianza en la realización de operaciones bancarias a través de Internet y compras online.

El análisis online proporciona datos acerca de la incidencia de malware específico para la comisión de fraude.

El período analizado en este documento abarca los meses de abril a junio de 2010. Durante este tiempo se han realizado 3.519 encuestas y 10.524 análisis online llevados a cabo con periodicidad mensual a los 4.500 equipos que componen el panel.

Se exponen a continuación los puntos clave del estudio.

### I Seguridad y fraude online

La incidencia de situaciones de intento (no consumado) de fraude a través de Internet o telefónico en los últimos 3 meses es declarada por el 54,8% de los usuarios. Los atacantes utilizan diferentes técnicas de ingeniería social para intentar consumir una estafa de fraude ya sea a través de Internet o mediante el teléfono móvil.

En el 2º trimestre de 2010 un 36,2% de los usuarios recibe peticiones de visitar alguna página web sospechosa, seguido de un 29,7% que recibe emails ofertando un servicio no solicitado, un 23,2% asegura haber recibido una oferta de trabajo falsa y un 20,3% ha sido víctima de intento de phishing (recepción de un correo electrónico solicitando claves de usuario).

Con respecto al intento de fraude mediante el teléfono móvil un 9,2% de los usuarios declara haber recibido mensajes cortos de texto ofertando un servicio no requerido. 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 un SMS (3%) como a través de una llamada (2,4%).

Las formas adoptadas por el atacante que intenta defraudar a través de una comunicación sospechosa son variadas. En este trimestre, las compras online son el

reclamo más adoptado por los atacantes, con un 42,2%, seguido de intentos de fraude en forma de banca en línea con un 41,8%.

Un 95,8% declara no haber sufrido perjuicio económico debido a un intento de fraude en el 2º trimestre de 2010. Este valor sigue la tendencia de los trimestres anteriores. Entre los usuarios que aseguran haber sido víctimas de pérdidas económicas, la cuantía defraudada se ha mantenido relativamente estable a lo largo de los períodos analizados. En este trimestre el 86,1% de los que han sufrido fraude con perjuicio económico declara haber perdido una cantidad menor a 400 euros, y un 13,9% más de 400 euros.

El análisis del malware específico para la comisión de fraude muestra que en el último mes analizado (junio de 2010) el porcentaje de troyanos se sitúa en un 34,3% y el de troyanos bancarios en un 7,1%. Los equipos que alojan troyanos, aunque ha descendido desde el comienzo del análisis (julio 2009) se mantienen estables a lo largo de 2010. La cifra de troyanos bancarios después de experimentar un aumento en los primeros meses del año, vuelve a tomar valores en torno al 7% - 9%.

El porcentaje de rogeware detectado en los últimos tres meses es significativo, aunque inferior al de troyanos bancarios. En este segundo trimestre de 2010, primero en el que se introduce el análisis de esta categoría de malware, se observa que el rogeware está presente en un 3,6% de los equipos.

Los datos muestran que haber sufrido un intento de fraude no influye en la confianza. Un 37,1% de los usuarios que han sido víctimas de fraude declaran que realizar compras por Internet utilizando la tarjeta de crédito les genera mucha y bastante confianza y el porcentaje se eleva a 45,9% en el caso de las operaciones bancarias en Internet.

Entre los que no han sido víctimas de fraude los porcentajes son, aunque menos elevados, muy similares. Un 34,4% deposita mucha y bastante confianza en las compras a través de Internet y un 41,3% en las operaciones bancarias online.

Y por último, una vez más, los usuarios no modifican sus hábitos relacionados con los servicios telemáticos a través de la Red tras haber sido víctima de intento de fraude. Un 83,1% de los encuestados declara no cambiar sus hábitos de comercio electrónico. Y con respecto a la banca a través de Internet, el porcentaje de usuarios que no modifican sus hábitos se sitúa en un 88,4%.

# 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, las formas adoptadas por el remitente origen de la comunicación sospechosa de ser fraudulenta y como consecuencia, el impacto económico sufrido. El presente informe constituye la 3ª entrega del mismo.

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.

Se muestra 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 y la e-confianza que les genera estos hábitos tras sufrir un intento de fraude.

## 1. DISEÑO METODOLÓGICO

---

El *Estudio sobre el fraude a través de Internet (2º trimestre de 2010)* se realiza a partir del 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 ofrece, 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 4.500 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.

### 1.3 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.

### 1.4 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
1 <sup>er</sup> trimestre 2010	3.599
2 <sup>o</sup> trimestre 2010	3.519

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, Turismo y Comercio. (Las TIC en los hogares españoles: 26ª oleada octubre-diciembre 2009)

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
Ene'10	4.079
Feb'10	3.751
Mar'10	4.024
Abr'10	3.746
May'10	3.499
Jun'10	3.279

Fuente: INTECO

### 1.5 Captura de información y trabajo de campo

El trabajo de campo ha sido realizado entre abril y junio de 2010 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.

La herramienta de INTECO tiene como piedra angular una base de datos de más de 25 millones de archivos detectados por, al menos, uno de esos 46 antivirus. Esta base de datos está en constante crecimiento.

iScan compara todos los archivos de un sistema con la base de datos. Si el análisis detecta el archivo con 5 ó más antivirus, el fichero se considera potencialmente malicioso.

El uso de 46 antivirus asegura una mayor tasa de detección, pues ante las nuevas amenazas de carácter altamente indetectable es difícil que un espécimen escape a todos los motores.

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.*

#### 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*

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

<sup>3</sup> Software gratuito.

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

*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.

## 1.6 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	$\pm 1,66\%$
1 <sup>er</sup> trimestre 2010	3.599	$\pm 1,66\%$
2 <sup>o</sup> trimestre 2010	3.519	$\pm 1,68\%$

Fuente: INTECO

## 2 SEGURIDAD Y FRAUDE ONLINE

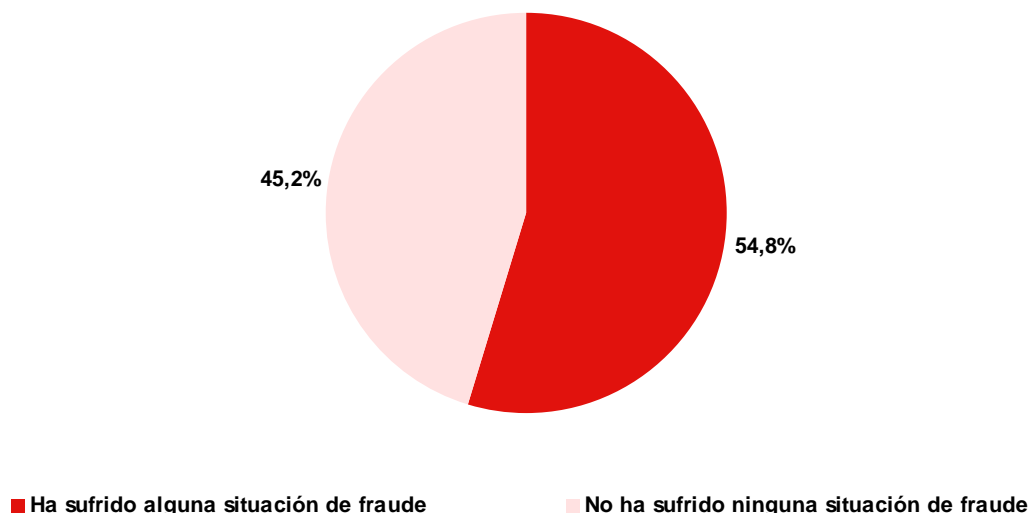
### 2.1 Intento de fraude y manifestaciones

El análisis comienza con la incidencia declarada de situaciones de intento (no consumado) de fraude a través de Internet o telefónico en los últimos tres meses (Gráfico 1).

Estos datos están basados en las respuestas dadas por los propios usuarios, y por tanto, sujetos a su percepción. En este sentido, es importante tener en cuenta que se analiza el intento de fraude, no de fraude consumado.

Más de la mitad de los usuarios (54,8%) ha sufrido, en el 2º trimestre de 2010, alguna situación de intento de fraude frente a un 45,2% que declara no haber sido víctima.

**Gráfico 1: Incidencia declarada de situaciones de intento (no consumado) de fraude a través de Internet o telefónico en los últimos 3 meses (%)**



Base: Total usuarios (n=3.519 en 2T10)

Fuente: INTECO

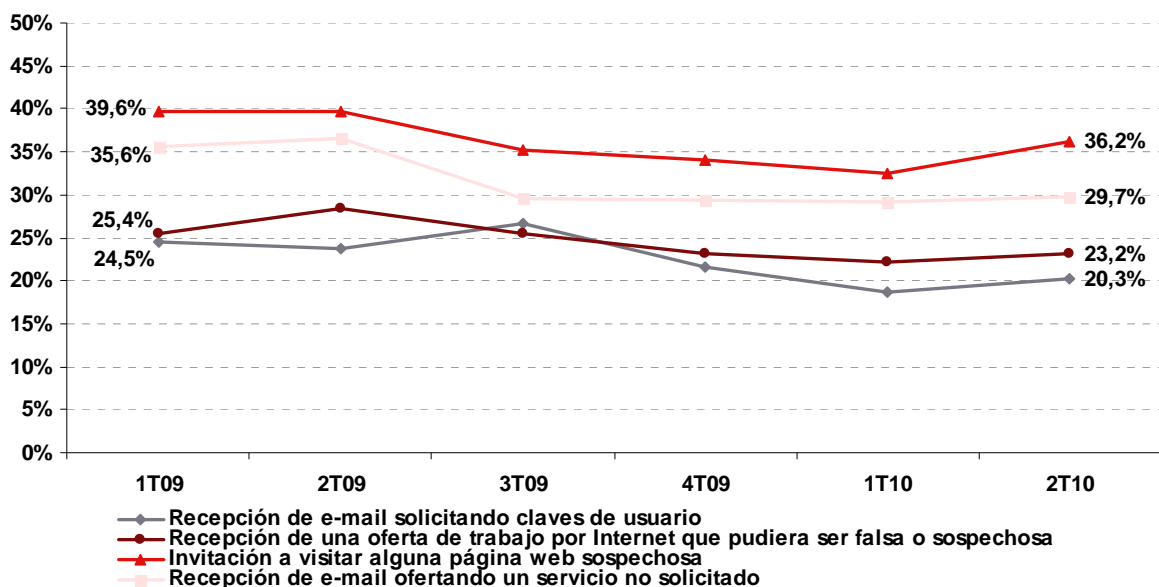
A continuación se muestra la evolución de la incidencia de situaciones de fraude basado en técnicas de ingeniería social a través de la Red (Gráfico 2) entre los usuarios de Internet españoles.

En el 2º trimestre de 2010 un 36,2% recibe peticiones de visitar alguna página web sospechosa, seguido de un 29,7% que recibe emails ofertando un servicio no solicitado, un 23,2% asegura haber recibido una oferta de trabajo falsa y un 20,3% ha sido víctima de intento de phishing (recepción de un correo electrónico solicitando claves de usuario).

Los envíos de correos electrónicos para que el receptor visite una página web sospechosa es sin duda una de las técnicas más usadas por los spammers y creadores de malware para intentar consumir una estafa, ofrecer publicidad fraudulenta a la víctima, o directamente infectar al usuario. Esto último se consigue habitualmente aprovechando vulnerabilidades del navegador. Si no se mantiene el programa para navegar actualizado, puede ocurrir que, con solo visitar una página web, un atacante llegue a instalar algún tipo de malware en el sistema.

Todas las situaciones de intento (no consumado) de fraude a través de Internet han descendido desde el 1<sup>er</sup> trimestre de 2009 (período en el que se comenzó la serie). El descenso más pronunciado (5,9 puntos) lo protagoniza la recepción de un correo electrónico ofertando un servicio no solicitado.

**Gráfico 2: 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=3.519 en 2T10)

Fuente: INTECO

En el siguiente gráfico, se estudia la evolución de las incidencias declaradas de intento de fraude, pero en un escenario diferente: el teléfono móvil.

Un 9,2% de los usuarios declara haber recibido mensajes cortos de texto ofertando un servicio no requerido.

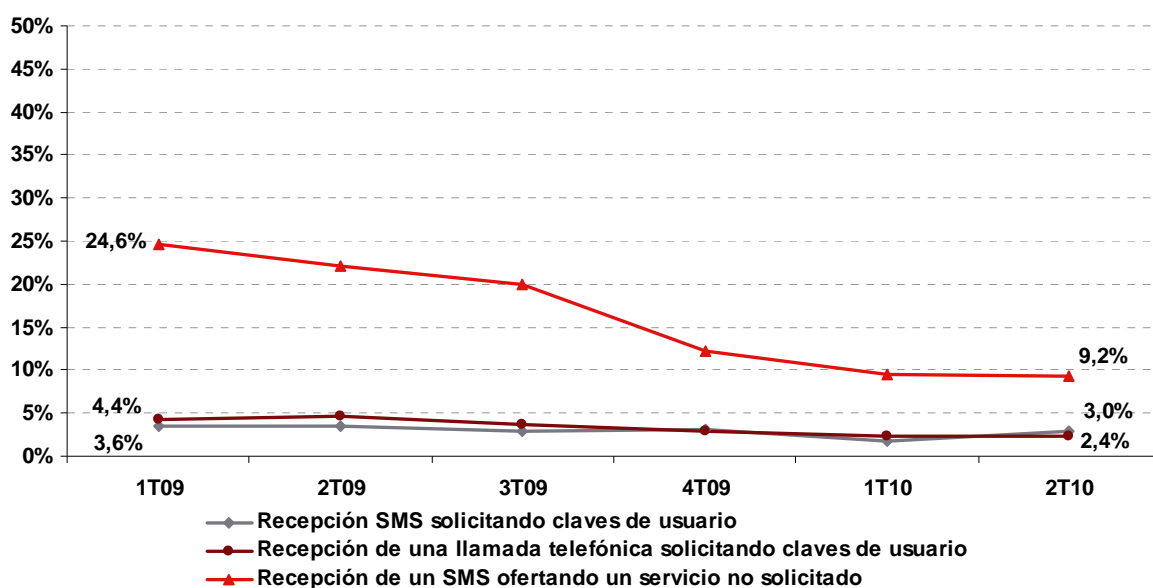
Menos numerosas son las incidencias que tienen que ver con la solicitud de las claves de usuario a través del teléfono móvil, tanto a través de un SMS (3%) como a través de una llamada (2,4%).

Si se compara con el 1<sup>er</sup> trimestre de 2009, la recepción de un SMS ofertando un servicio no solicitado desciende 15,4 puntos porcentuales. Esto puede deberse al coste que han de afrontar los anunciantes a través de este método; comparado con el coste, cercano a nulo, que tiene un correo electrónico.

Las incidencias relacionadas con la solicitud de claves de usuario tanto a través de SMS como a través de llamadas telefónicas se mantienen relativamente estables desde el 1<sup>er</sup> trimestre de 2009 hasta este 2<sup>o</sup> trimestre de 2010, en torno al 2 – 4%.

Este tipo de amenazas que incluyen mensajes cortos o llamadas telefónicas, son menos comunes debido al gasto derivado para el atacante. Existe la posibilidad de que a medida que las comunicaciones móviles se abaraten gracias a servicios de VoIP, los ataques de este tipo se intensifiquen.

**Gráfico 3: 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=3.519 en 2T10)

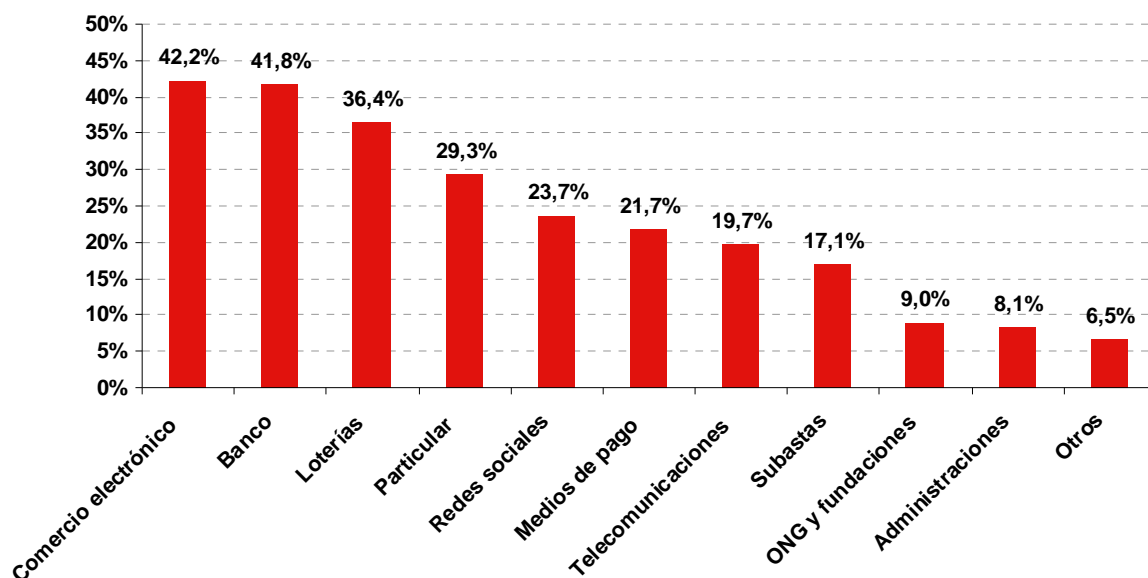
Fuente: INTECO

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

Las formas adoptadas por el atacante que intenta defraudar a través de una comunicación sospechosa son diversas (Gráfico 3). En este trimestre, las compras online son el reclamo más adoptado por los atacantes, con un 42,2%, seguido de intentos de fraude en forma de banca online con un 41,8%.

Según los datos<sup>5</sup> más actuales ofrecidos por el *Anti-Phishing Working Group* (APWG) a nivel mundial, en el primer trimestre de 2010, un 37% de los ataques se dirigían a servicios de pago, seguido de un 35,9% que eran destinados al sector financiero.

**Gráfico 4: Formas adoptadas por el remitente de la comunicación sospechosa de ser fraudulenta<sup>6</sup> (%)**



Base: Usuarios que han sufrido algún intento de fraude (n=1.903)

Fuente: INTECO

En la comparativa evolutiva realizada en la Tabla 4 se observa cómo el comercio electrónico vuelve a ser en el 2º trimestre de 2010, por segunda vez consecutiva, la principal forma adoptada por el remitente de la comunicación sospechosa de ser fraudulenta, con un 42,2%. Hasta comienzos de 2010 eran los bancos o entidades financieras los que se posicionaban en primer lugar, situándose en un 41,8% en la última toma de datos.

Adoptar la forma de un particular para enviar comunicaciones sospechosas es la que mayor aumento presenta desde comienzos del año pasado. A principios de 2009 este porcentaje se situaba en un 11,9% para ascender a un 29,3% en este último trimestre analizado.

Esto corrobora la tendencia clara que actualmente siguen los atacantes: se presentan como particulares que desean realizar algún negocio con la víctima, o bien como

<sup>5</sup> Anti-Phishing Working Group (APWG) (1st Quarter 2010). Disponible en: [http://www.antiphishing.org/reports/APWG\\_GlobalPhishingSurvey\\_1H2010.pdf](http://www.antiphishing.org/reports/APWG_GlobalPhishingSurvey_1H2010.pdf)

<sup>6</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.

personas con problemas que necesitan ayuda económica. Es posible que este modelo de intento de fraude esté teniendo un éxito relativo y los atacantes lo pongan en práctica de forma mucho más agresiva.

**Tabla 4: Evolución de las formas adoptadas por el remitente de la comunicación sospechosa de ser fraudulenta (%)**

Forma adoptada <sup>7</sup>	1T 2009	2T 2009	3T 2009	4T 2009	1T 2010	2T 2010
Comercio electrónico	31,9	35,8	29,3	41,9	<b>43,9</b>	<b>42,2</b>
Banco	<b>37,5</b>	<b>39,0</b>	<b>44,4</b>	<b>43,1</b>	39,9	41,8
Loterías	35,5	38,4	33,7	39,0	37,2	36,4
Particular	11,9	11,4	11,2	23,8	25,7	29,3
Redes sociales	23,9	24,1	20,7	21,3	23,9	23,7
Medios de pago	15,0	17,0	18,6	23,1	21,1	21,7
Telecomunicaciones	25,0	23,8	21,8	21,4	21,3	19,7
Subastas	17,9	19,2	16,5	20,9	19,2	17,1
ONG y fundaciones	6,4	7,4	6,5	8,3	7,9	9,0
Administraciones	3,5	3,8	6,4	9,1	6,2	8,1
Otros	3,1	3,9	3,3	5,1	7,7	6,5

Fuente: INTECO

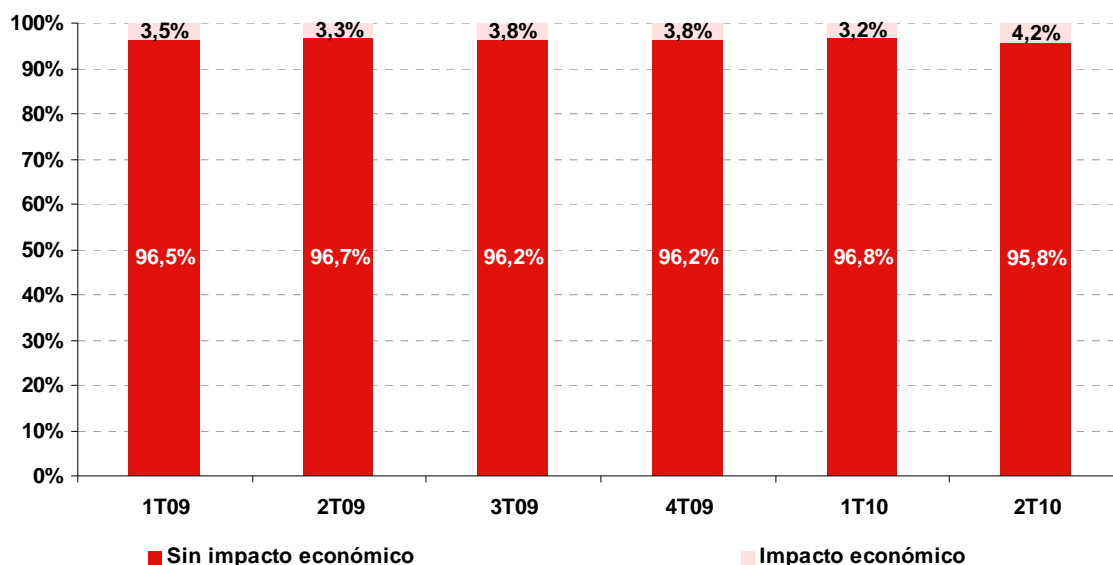
### 2.3 Impacto económico del fraude

Se analiza aquí el impacto económico que ha causado los intentos de fraude a través de Internet o mediante el teléfono móvil, si han causado perjuicio económico y la cuantía del mismo.

En el 2º trimestre de 2010 un 95,8% declara no haber sufrido perjuicio económico debido a un intento de fraude. Este valor sigue la tendencia de los trimestres anteriores.

<sup>7</sup> Aparece sombreada la principal forma adoptada para cada trimestre.

**Gráfico 5: Evolución del fraude con impacto económico para el usuario (%)**

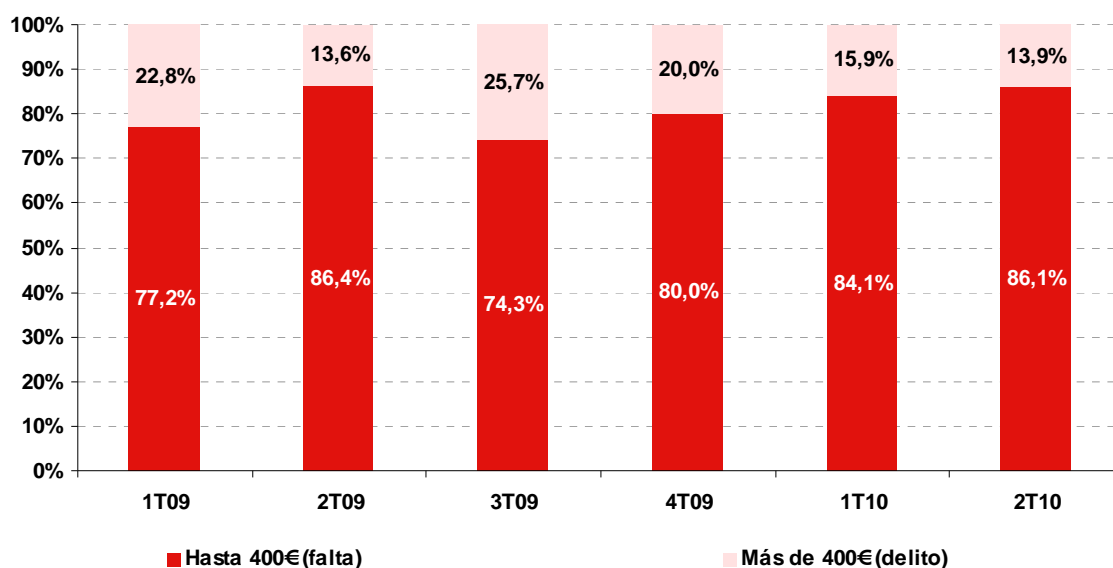


Base: Total usuarios (n=3.519 en 2T10)

Fuente: INTECO

La cuantía defraudada se ha mantenido relativamente estable a lo largo de los períodos analizados. En el 2º trimestre de 2010, el 86,1% de los que han sufrido fraude con perjuicio económico declara haber perdido una cantidad menor a 400 euros, y un 13,9% más de 400 euros. La Ley establece en esta cantidad el límite a la hora de considerar falta (menos de 400 euros) o delito (más de 400 euros).

**Gráfico 6: Evolución de la cuantía económica derivada del fraude (%)**

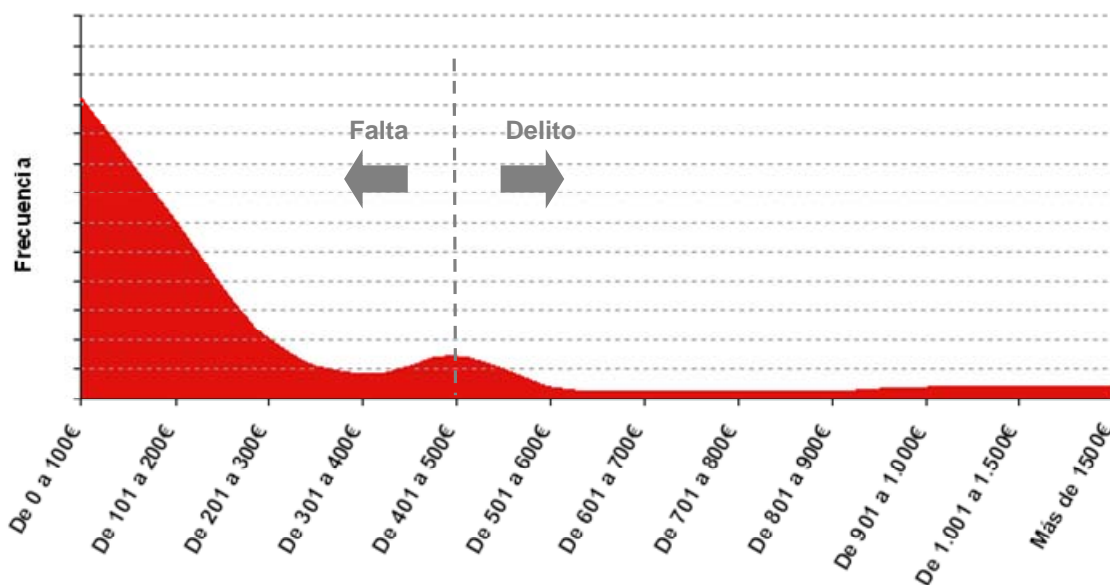


Base: Usuarios que han sufrido perjuicio económico como consecuencia de un fraude online (n=113 en 2T10)

Fuente: INTECO

Atendiendo a la distribución del importe defraudado, se observa que en los últimos tres meses, de los 113 usuarios que declaran haber sufrido perjuicio económico, casi la mitad (51) afirman que la cantidad defraudada estaba por debajo de los 100 €.

**Gráfico 7: Distribución del importe defraudado en el 2T 2010**



Base: Usuarios que han sufrido perjuicio económico como consecuencia de un fraude online (n=113)

Fuente: INTECO

## 2.4 Fraude y malware

En este trimestre se ha introducido una novedad en la tipología del código malicioso analizado. Se ha añadido el tipo rogeware como variante de troyanos.

El rogeware o rogue software es un tipo de malware cuya principal finalidad es hacer creer a la víctima que está infectada por algún tipo de virus, induciendo a pagar una determinada suma de dinero para eliminarlo. El concepto del pago suele ser la compra de un falso antivirus, que resulta en realidad el malware en sí. En los últimos tiempos, este tipo de malware está siendo muy difundido y se están detectando gran cantidad de variantes.

Hasta el momento se analiza la incidencia de troyanos bancarios dentro de la categoría de troyanos, en este trimestre y a partir de ahora, se estudiará el rogeware dentro de esta categoría.

Los datos presentados a continuación proceden de los análisis empíricos obtenidos a través de iScan. Se analiza el porcentaje de código malicioso catalogado como troyanos

así como la proporción de troyanos bancarios<sup>8</sup> que se encuentran en los equipos de los hogares españoles.

Para realizar el estudio, se han considerado las siguientes familias de troyanos bancarios más populares que efectúan ataques dirigidos contra entidades bancarias<sup>9</sup>.

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

En el caso de rogueware, se han considerado las siguientes denominaciones reconocidas:

*Rogue, rogueware, rogue-ware, fakeav, avfake, fakealert, fake-alert, alertfake alert-fake, , FraudLoad, FakeVimes, Fakesecure, Virusalarmpro, Fraudpack, Codecpack, AlertVir, SimulatedVir, WinFixer y XPantivirus.*

Cabe recordar, para interpretar correctamente las cifras, que los equipos que alojan malware bancario o rogueware no necesariamente terminan experimentando una situación de fraude.

Para que un fraude por troyano bancario se consume, deben concurrir las siguientes circunstancias: en primer lugar, el equipo del usuario ha de estar infectado por este tipo de troyano; además, el espécimen que infectó la máquina ha de atacar a la entidad bancaria con la que opera el usuario; por último, el ciudadano ha de iniciar sesión en su espacio de banca electrónica y rellenar los datos adicionales que se le soliciten.

Para que el fraude por rogueware se consume, el usuario debe quedar infectado por ese tipo de troyano y además pagar la licencia del software malicioso.

Muchos equipos pueden pasar meses infectados hasta que se dan todas estas circunstancias, o puede que incluso el usuario nunca opere con su tarjeta o no llegue a rellenar todos los datos extra solicitados por el troyano y por tanto el fraude no sea consumado.

### 1.1.1. Malware

El Gráfico 7 muestra la relación evolutiva entre el porcentaje de equipos que alojan troyanos con respecto a los troyanos bancarios. En el último mes analizado (junio de

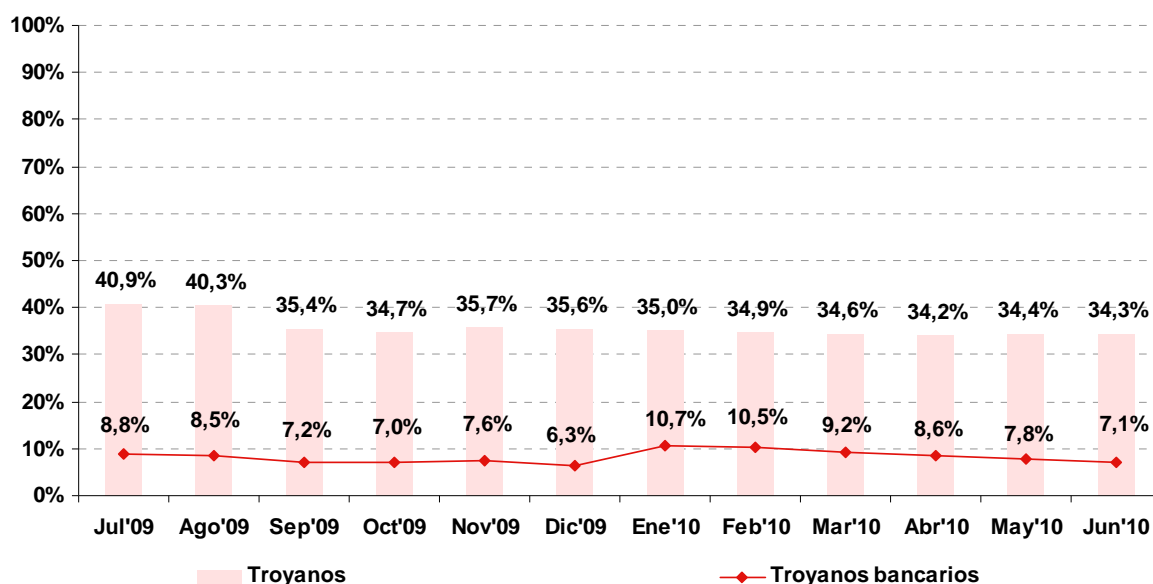
<sup>8</sup> Programas maliciosos, que utilizando diversas técnicas, roban información confidencial a los clientes de banca y/o plataformas de pago online ([Glosario técnico PANDA SECURITY](#))

<sup>9</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.

2010) el porcentaje de troyanos se sitúa en un 34,3% y el de troyanos bancarios en un 7,1%. Los equipos que alojan troyanos, aunque ha descendido desde el comienzo del análisis (julio 2009) se mantienen estables a lo largo de 2010. La cifra de troyanos bancarios después de experimentar un aumento en los primeros meses del año, vuelve a tomar valores en torno al 7%-9%.

El porcentaje de troyanos ha descendido desde comienzos del análisis (julio de 2009) para mantenerse estable durante 2010 cuyo porcentaje se sitúa en un 34,3% en junio de 2010. El número de troyanos bancarios, en cambio, después de experimentar un aumento en el primer trimestre del año vuelve a alcanzar cifras similares .

**Gráfico 8: Evolución de equipos que alojan troyanos bancarios (%)**

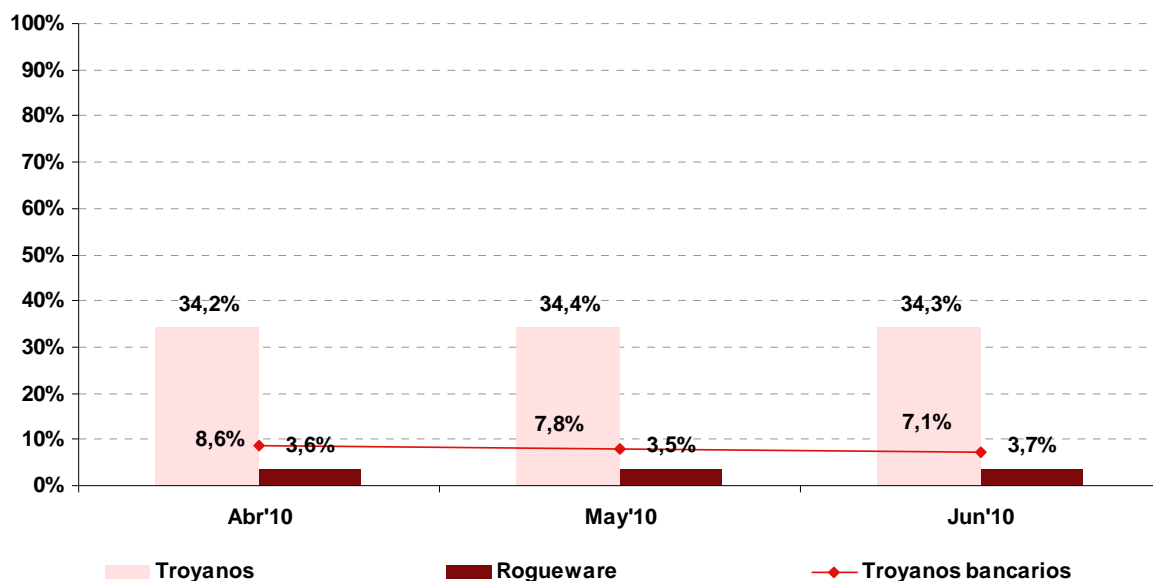


Fuente: INTECO

### 1.1.2. Rogueware

El porcentaje de rogueware detectado en los últimos tres meses es inferior al de troyanos bancarios aunque significativo. En este segundo trimestre de 2010, primero en el que se introduce el análisis de este tipo de troyano, se observa que el rogueware alcanza un 3,7% de los equipos analizados en junio de 2010. En las sucesivas tomas de datos se observará la evolución de este valor.

**Gráfico 9: Equipos que alojan diferente tipología relacionada con el fraude (%)**



Fuente: INTECO

## 2.5 Influencia del intento de fraude en los hábitos relacionados con la banca a través de Internet y el comercio electrónico

¿De que manera influye en los usuarios haber sufrido un intento de fraude y/o haber experimentado perjuicio económico como consecuencia del mismo?

Los resultados ofrecidos a continuación relacionan los hábitos prudentes en la banca y el comercio electrónico con los usuarios que han sufrido perjuicio económico a causa del fraude sufrido y los que no.

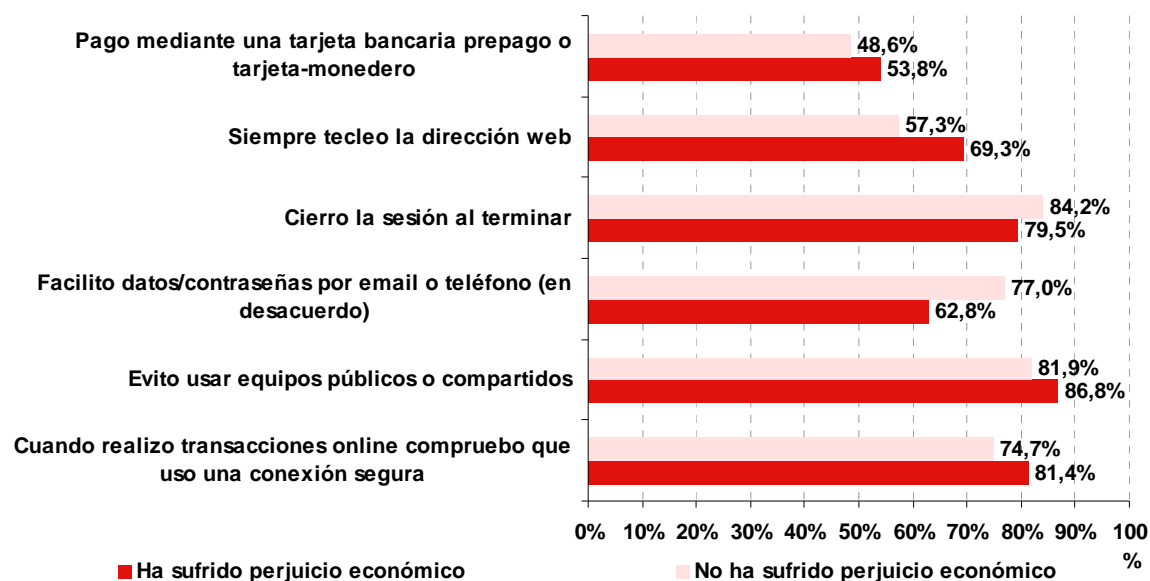
Se observa cómo algunos de los hábitos prudentes han sido adoptados en mayor medida por los usuarios que han sido víctimas de perjuicio económico, y otros en cambio, por aquellos que no han sufrido pérdidas económicas como consecuencia del fraude.

Los hábitos que presentan mayor contraste son:

- Facilito datos/contraseñas por email o teléfono: un 77% de los que no han sufrido perjuicio económico declaran llevar a cabo este hábito prudente. En cuanto a los que no han padecido pérdidas económicas un 62,8% aseguran no facilitar datos/contraseñas por email o teléfono cuando su banco se lo pide.
- Siempre tecleo la dirección web en la barra de direcciones: un 57,3% de los encuestados que declararon no haber sufrido perjuicio económico como consecuencia del fraude teclean en la barra de direcciones la dirección del banco

o web de compraventa on-line. En el caso de aquellos que si que fueron víctimas de perjuicio económico, el porcentaje se eleva a un 69,3%.

**Gráfico 10: Hábitos prudentes relacionados con banca en línea y comercio electrónico entre los usuarios que han sido víctima de perjuicio económico por el fraude sufrido y los que no (%)**



Base: Usuarios que utilizan comercio electrónico y/o banca en línea (n=3.241)

Fuente: INTECO

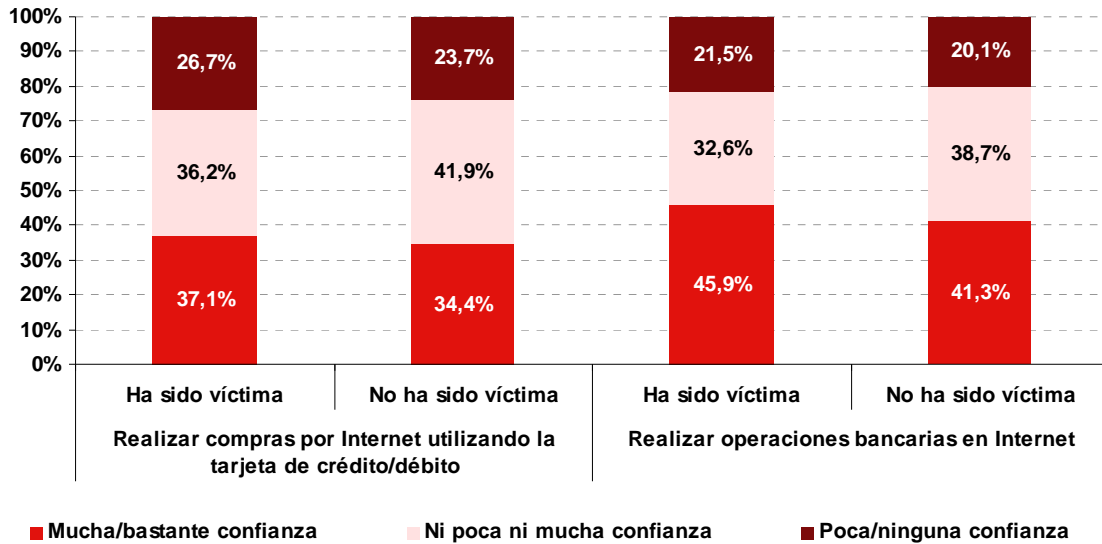
¿Y la confianza depositada en la realización de operaciones telemáticas a través de la Red, varía en función de haber experimentado un intento de fraude y/o haber sufrido un perjuicio económico?

En el Gráfico 11 se analiza el nivel de confianza que les ofrece a los usuarios realizar compras a través de Internet y la banca online, distinguiendo entre aquellos que han sido víctima de intento de fraude y/o han sufrido perjuicio económico y los que no.

Los datos muestran que haber sufrido un intento de fraude no influye en la confianza. Un 37,1% de los usuarios que han sido víctimas de fraude declaran que realizar compras por Internet utilizando la tarjeta de crédito les genera mucha y bastante confianza y el porcentaje se eleva a 45,9% en el caso de las operaciones bancarias en Internet.

Entre los que no han sido víctimas de fraude los porcentajes son, aunque menos elevados, muy similares. Un 34,4% deposita mucha y bastante confianza en las compras a través de Internet y un 41,3% en las operaciones bancarias online.

**Gráfico 11: Nivel de confianza entre los usuarios que han sido víctima de intento de fraude y/o haber sufrido perjuicio económico y los que no (%)**

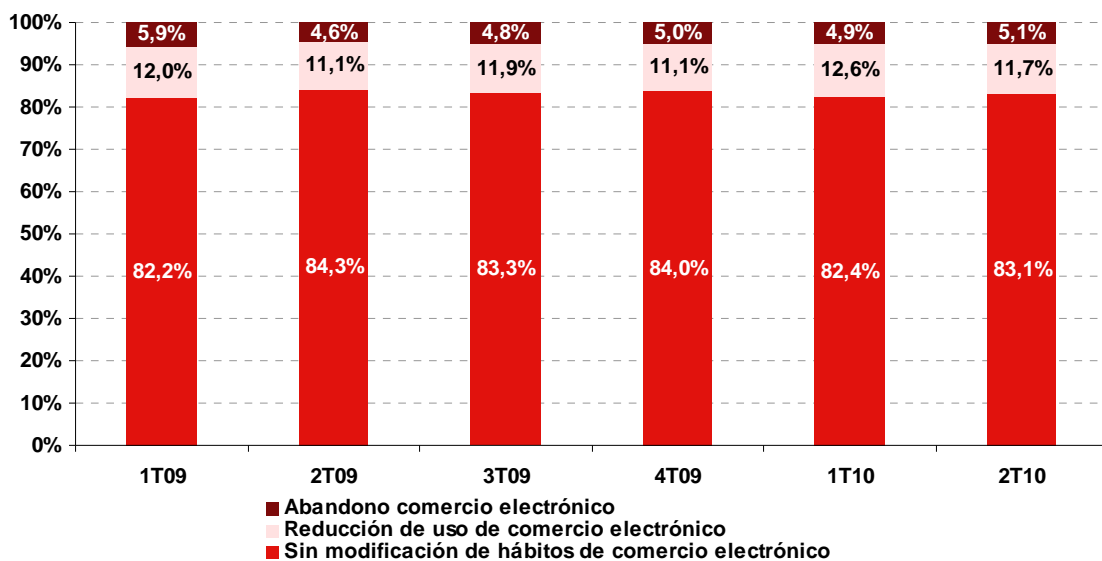


Base: Usuarios que utilizan comercio electrónico y/o banca en línea (n=3.241)

Fuente: INTECO

Los usuarios no abandonan sus hábitos de comercio electrónico tras sufrir intento de fraude. La inmensa mayoría de los encuestados (83,1%) así lo afirman. Un 11,7% reduce su uso y un 5,1% lo abandona. Estos datos se mantienen estables desde el 1<sup>er</sup> trimestre de 2009.

**Gráfico 12: Modificación de hábitos de comercio electrónico tras sufrir intento (no consumado) de fraude (%)**

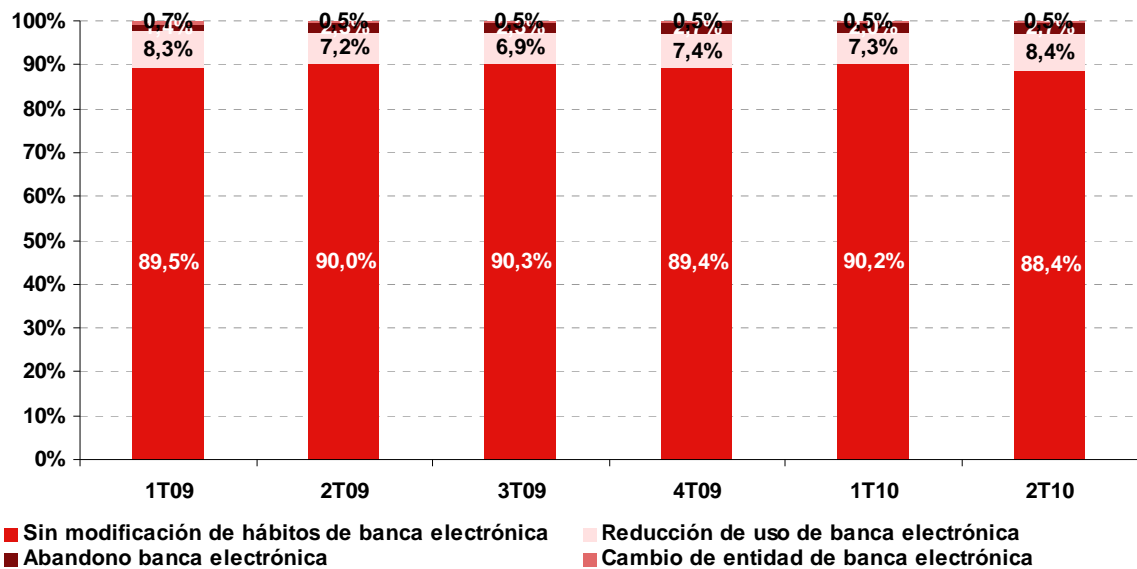


Base: Usuarios que han sufrido algún intento de fraude y/o un perjuicio económico (n=1.921)

Fuente: INTECO

Con respecto a la banca a través de la Red, el porcentaje de usuarios que no modifican sus hábitos se sitúa en un 88,4%. Un 8,4% aseguran que reducen el uso, un 2,7% abandona este servicio y un 0,5% cambia de entidad de banca electrónica. Los serie histórica, al igual que en el comercio electrónico se mantiene constante.

**Gráfico 13: 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=1.921)

Fuente: INTECO

## 3 CONCLUSIONES Y RECOMENDACIONES

---

### 1.2. Conclusiones del análisis

Un 54,8% declara haber sido víctima de intento (no consumado) de fraude a través de Internet o a través del teléfono en los últimos tres meses mediante diversas técnicas de ingeniería social.

Una vez más, el análisis pone de manifiesto que los usuarios no pierden la confianza depositada en la banca y la compra-venta a través de Internet tras sufrir un intento de fraude.

#### **¿Qué forma adopta el remitente origen de la comunicación sospechosa de ser fraudulenta?**

Los atacantes, siguen encubriéndose en páginas que simulan compras o ventas a través de la Red para realizar comunicaciones sospechosas de fraude. Esta es la técnica más señalada por los usuarios en el 2º trimestre de 2010.

#### **¿Cuánto impacto económico ha causado el fraude?**

El porcentaje de usuarios que han sufrido pérdidas económicas como consecuencia de un intento de fraude sigue una tendencia constante de menos del 5% desde el 1º trimestre de 2009. Atendiendo a la cuantía defraudada, en los últimos tres meses, de los 113 usuarios que declaran haber sufrido perjuicio económico, casi la mitad (51) afirman que la cantidad estaba por debajo de los 100 €.

#### **¿Qué datos ofrecen los análisis empíricos?**

En este trimestre se ha introducido una novedad en la tipología del código malicioso analizado. Se ha añadido el tipo rogeware como variante de troyanos que alcanza un valor de 5,3% en este primer análisis.

El porcentaje de troyanos bancarios se mantiene relativamente estable en los últimos meses (7,1% en junio de 2010) y el de troyanos viene experimentando un descenso desde enero de 2010 situándose en un 34,3% en la última toma de datos.

#### **¿Qué influencia ha tenido el intento de fraude en la e-confianza relacionada con la banca a través de Internet y el comercio electrónico?**

Los datos muestran que haber sufrido un intento de fraude no influye en la confianza. Un 37,1% de los usuarios que han sido víctimas de fraude declaran que realizar compras por Internet utilizando la tarjeta de crédito les genera mucha y bastante confianza y el porcentaje se eleva a 45,9% en el caso de las operaciones bancarias en Internet.

Por último, en el análisis de la influencia del intento de fraude en los hábitos relacionados con la banca a través de Internet y el comercio electrónico los usuarios siguen la línea de trimestres anteriores declarando que no modifican sus hábitos a la hora de utilizar estos servicios.

### 1.3. Recomendaciones

A continuación se muestran algunas recomendaciones para evitar ser víctima de intento de fraude a través de Internet o telefónico:

- Utilizar cuentas de usuario con permisos limitados.
- Utilizar contraseñas seguras.
- No enviar información personal o financiera a través del correo electrónico.
- Ser consciente de que los bancos o entidades financieras nunca piden los datos personales por correo electrónico.
- Siempre que el usuario introduzca los datos bancarios en una página web debe cerciorarse de que está utilizando un protocolo seguro (la URL debe comenzar por https en lugar de por http).
- Disponer del navegador de Internet actualizado permite tener los protocolos de seguridad en regla.
- Guardar o imprimir la información cuando se realiza una operación económica a través de la Red.
- 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.
- Disponer de los programas de seguridad actualizados en todo momento.
- A la hora de conectarse a una red pública se debe ser prudente, ya que puede existir cualquier persona conectada capturando las conexiones que pasan por ella.
- 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: Incidencia declarada de situaciones de intento (no consumado) de fraude a través de Internet o telefónico en los últimos 3 meses (%) .....	15
Gráfico 2: Evolución de la incidencia declarada de situaciones de intento (no consumado) de fraude a través de Internet en los últimos 3 meses (%) .....	16
Gráfico 3: Evolución de la incidencia declarada de situaciones de intento (no consumado) de fraude a través del teléfono móvil en los últimos 3 meses (%).....	17
Gráfico 4: Formas adoptadas por el remitente de la comunicación sospechosa de ser fraudulenta (%) .....	18
Gráfico 5: Evolución del fraude con impacto económico para el usuario (%) .....	20
Gráfico 6: Evolución de la cuantía económica derivada del fraude (%) .....	20
Gráfico 7: Distribución del importe defraudado en el 2T 2010 .....	21
Gráfico 8: Evolución de equipos que alojan troyanos bancarios (%) .....	23
Gráfico 9: Comparativa de la tipología de malware relacionada con el fraude en 2T 2010(%).....	24
Gráfico 10: Hábitos prudentes relacionados con banca en línea y comercio electrónico entre los usuarios que han sido víctima de intento de fraude y/o han sufrido perjuicio económico y los que no (%) .....	25
Gráfico 11: Nivel de confianza entre los usuarios que han sido víctima de intento de fraude y/o haber sufrido perjuicio económico y los que no (%) .....	26
Gráfico 12: Modificación de hábitos de comercio electrónico tras sufrir intento (no consumado) de fraude (%) .....	26
Gráfico 13: Modificación de hábitos de banca electrónica tras sufrir intento (no consumado) de fraude (%) .....	27

## ÍNDICE DE TABLAS

---

Tabla 1: Tamaños muestrales para las encuestas .....	10
Tabla 2: Número de equipos escaneados mensualmente .....	11
Tabla 3: Errores muestrales de las encuestas (%).....	14
Tabla 4: Evolución de las formas adoptadas por el remitente de la comunicación sospechosa de ser fraudulenta (%).....	19



Instituto Nacional  
de Tecnologías  
de la Comunicación

<http://www.inteco.es>

<http://observatorio.inteco.es>