



GOBIERNO
DE ESPAÑA

MINISTERIO
DE INDUSTRIA, TURISMO
Y COMERCIO

plan
avanza2.0



Instituto Nacional
de Tecnologías
de la Comunicación

Estudio sobre el fraude a través de Internet

1^{er} trimestre de 2010



Edición: Agosto 2010

El “Estudio sobre el fraude a través de Internet (1^{er} 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

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. 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 [HAccesibilidad > Formación > Manuales y GuíasH](#) 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
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	18
3.4 Fraude y malware	20
3.5 Influencia del intento de fraude en los hábitos relacionados con la banca a través de Internet y el comercio electrónico	21
4 CONCLUSIONES Y RECOMENDACIONES	26
4.1 Conclusiones del análisis	26
4.2 Recomendaciones	27
ÍNDICE DE GRÁFICOS	29
ÍNDICE DE TABLAS	30

PUNTOS CLAVE

El Observatorio de la Seguridad de la Información publica el *Estudio sobre el fraude a través de Internet (1^{er} 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 online proporciona datos acerca de la incidencia de malware específico para la comisión de fraude.

El período analizado en este documento abarca desde enero a marzo de 2010. Durante este tiempo se han realizado 3.599 encuestas y un total de 11.854 análisis de seguridad en los equipos panelistas, llevados a cabo con periodicidad mensual.

Se exponen a continuación los puntos clave del estudio.

I Seguridad y fraude online

Los intentos de fraude basados en técnicas de ingeniería social a través de la Red y a través del teléfono móvil son diversos.

En el 1^{er} trimestre de 2010 la invitación a través de correo electrónico a visitar una página web sospechosa es la mayor incidencia de intento de fraude declarada por los usuarios, con un 32,6%. En segundo lugar se encuentra la recepción de un e-mail ofertando un servicio no solicitado (29,1%).

A través de los teléfonos móviles también pueden darse intentos de fraude a través de mensajes cortos o llamadas telefónicas. Así un 9,4% afirma haber recibido un SMS ofertando un servicio no solicitado.

En el análisis interanual de estas incidencias de intento de fraude (tanto a través de Internet como del teléfono móvil) se observa que la invitación a través de un correo electrónico para visitar alguna página web sospechosa ha aumentado con respecto al 1^{er} trimestre de 2008, pasando de un 29,4% en 2008 a un 32,6% en 2010. Lo contrario ocurre en el caso de la recepción de un SMS ofertando un servicio no solicitado que desciende considerablemente desde el 1^{er} trimestre de 2008 en el que se situaba en un 23,2% para acabar en un 9,4% en los tres primeros meses de 2010.

La forma adoptada preferida por los atacantes para realizar la comunicación sospechosa de fraude es a través de páginas que simulan compras o ventas a través de Internet. Un 43,9% de los usuarios así lo declaran en el 1^{er} trimestre de 2010. Además, casi un 40%

de las comunicaciones sospechosas simulaban ser una entidad bancaria, seguidos muy de cerca por las páginas de loterías, casinos y juegos online.

Analizando la evolución interanual, el banco, que en 2008 y 2009 se posicionaba como la principal forma adoptada por el remitente de la comunicación sospechosa de ser fraudulenta se ha situado en segundo lugar en 2010, por debajo de las páginas de comercio electrónico o compraventa online que han aumentado 25,9 puntos porcentuales desde el 1^{er} trimestre de 2008.

Este trimestre se alcanza un mínimo anual en el número de usuarios que han sufrido un impacto económico a consecuencia de algún tipo de fraude a través de Internet. Sólo un 3,2% de los usuarios afirma haber sufrido un perjuicio económico en los últimos 3 meses.

En el caso de los usuarios que han sufrido un perjuicio económico en el 1^{er} trimestre de 2010, un porcentaje muy elevado (84,1%) ha perdido menos de 400 € a consecuencia de la estafa.

Los datos procedentes de los análisis empíricos muestran el porcentaje de código malicioso catalogado como troyanos así como la proporción de troyanos bancarios que se encuentran en los equipos de los hogares españoles. En marzo de 2010, un 9,2% de los equipos analizados aloja algún tipo de troyano bancario, frente al 34,6% que alojan troyanos.

Haber sido víctima de intento de fraude y/o haber sufrido un perjuicio económico influye a la hora de llevar a cabo hábitos prudentes relacionados con la banca en línea y el comercio electrónico. El hábito prudente de no facilitar datos/contraseñas por correo electrónico o teléfono es el que presenta mayor diferencia entre los que han sido víctima y los que no. Un 55,8% de los que han sufrido un intento de fraude y/o un perjuicio económico lo hacen frente a un 44,6% de aquellos que no lo han sufrido.

La confianza depositada en la realización de procesos telemáticos no se ve afectada por el hecho de que el usuario haya sido víctima de intento de fraude. De entre los internautas que han sufrido un intento de fraude y/o un perjuicio económico, un 45,9% y un 38% declara, respectivamente, que realizar operaciones bancarias y compras a través de Internet les genera mucha/bastante confianza.

Finalmente, un porcentaje considerable afirma no haber modificado sus hábitos en la compra online (82,4%) y en la banca a través de Internet (90,2%), tras sufrir un intento de fraude.

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 (1^{er} trimestre de 2010)* 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.

Este informe constituye la segunda entrega de una serie de informes trimestrales. Esta serie comenzó con un análisis anual de 2009 del fraude a través de Internet. Mediante esta nueva entrega se pueden visualizar los resultados de 2009 junto con el 1^{er} trimestre de 2010.

El documento 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 es 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.

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.

2 DISEÑO METODOLÓGICO

El *Estudio sobre el fraude a través de Internet (1^{er} 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 5.212 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 hábitat¹.

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 ^{er} trimestre 2009	3.563
2 ^o trimestre 2009	3.521
3 ^{er} trimestre 2009	3.540
4 ^o trimestre 2009	3.640
1 ^{er} trimestre 2010	3.599

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
Ene'10	4.079
Feb'10	3.751
Mar'10	4.024

Fuente: INTECO

¹ 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: 25ª oleada julio-septiembre 2009)

2.3 Captura de información y trabajo de campo

El trabajo de campo ha sido realizado entre enero y marzo 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 goodware² demostraron ser altamente paranoicos.*

² Software y ficheros legítimos, archivos inocuos.

- 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 freeware³ y shareware⁴ 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).

³ Software gratuito.

⁴ Software de descarga gratuita pero limitado en funcionalidad o tiempo de uso.

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.

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 ^{er} trimestre 2009	3.563	$\pm 1,68\%$
2 ^o trimestre 2009	3.521	$\pm 1,68\%$
3 ^{er} trimestre 2009	3.540	$\pm 1,68\%$
4 ^o trimestre 2009	3.640	$\pm 1,66\%$
1 ^{er} trimestre 2010	3.599	$\pm 1,66\%$

Fuente: INTECO

3 SEGURIDAD Y FRAUDE ONLINE

3.1 Intento de fraude y manifestaciones

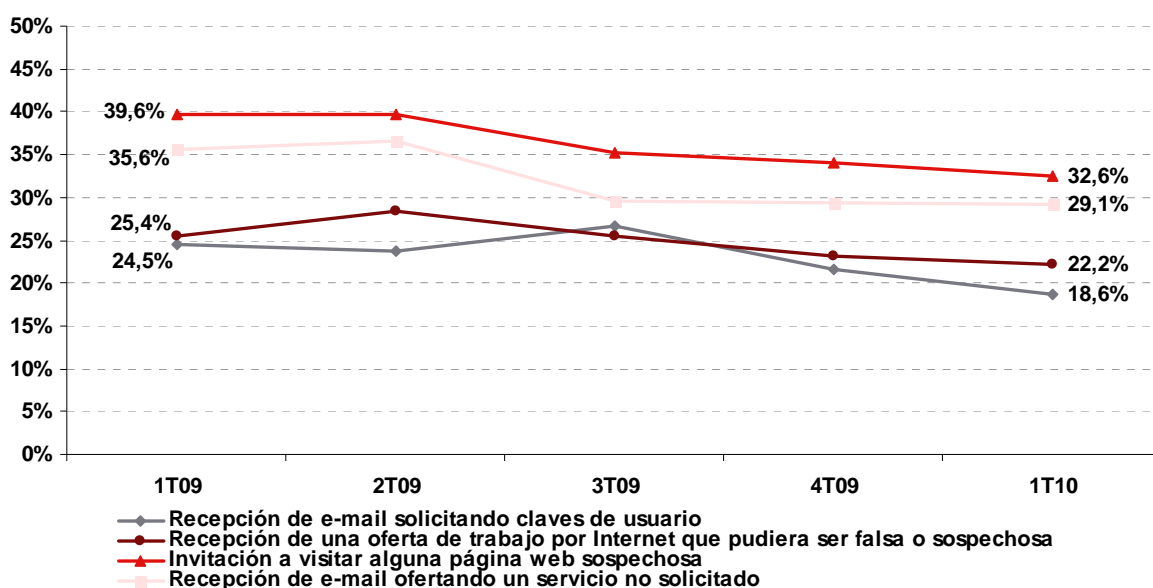
El análisis comienza con la evolución de la incidencia de situaciones de fraude basado en técnicas de ingeniería social a través de la Red (Gráfico 1) entre los usuarios de Internet españoles.

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.

En el 1^{er} trimestre de 2010 la mayor incidencia declarada por los usuarios es haber recibido invitaciones a través de correo electrónico a visitar una página web sospechosa (32,6%) seguido de la recepción de un email ofertando un servicio no solicitado (29,1%), una oferta de trabajo por Internet que pudiese ser falsa o sospechosa (22,2%) y un email solicitando claves de usuario (18,6%).

Al analizar la evolución desde el 1^{er} trimestre de 2009, la incidencia que más desciende es la de la invitación a visitar alguna página web sospechosa. Pasando de un 39,6% a comienzos del año 2009 a un 32,6% en el mismo período de 2010.

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=3.599 en 1T10)

Fuente: INTECO

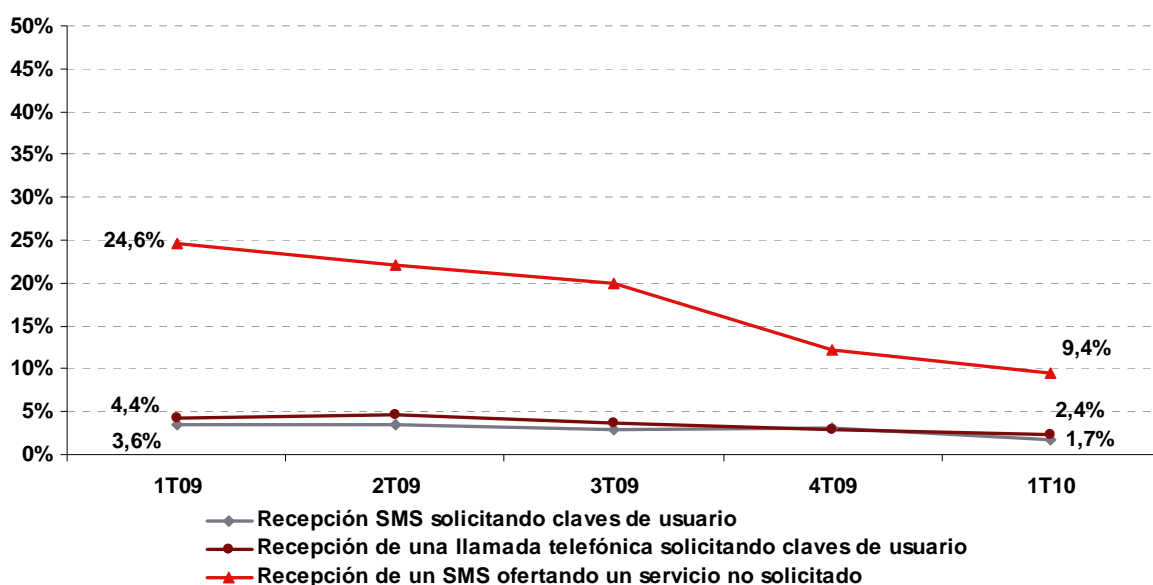
En el Gráfico 2 se aprecia que en los teléfonos móviles también pueden darse intentos de fraude a través de mensajes cortos o llamadas telefónicas. No obstante, no es el medio

más usado por los atacantes debido a su coste (comparado, por ejemplo, con el envío masivo de correo basura).

La recepción de SMS ofertando un servicio no solicitado se sitúa en un 9,4% en este trimestre. La petición de claves de usuario es otra incidencia declarada que se da a través del teléfono móvil. Un 2,4% señala haber recibido una llamada solicitándolas y un 1,7% si se la petición se realiza a través de un SMS.

El descenso más pronunciado a lo largo de los 5 trimestres analizados se evidencia en el porcentaje de usuarios que dice haber recibido un SMS ofertando un servicio no solicitado. Un 9,4% de usuarios lo afirma en el 1^{er} trimestre de 2010 frente al 24,6% a comienzos del año anterior. Los atacantes parecen no tener preferencia por esta vía de publicidad no solicitada, y parece estar siendo abandonada progresivamente.

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=3.599 en 1T10)

Fuente: INTECO

A continuación, se analiza la variación interanual que ha sufrido la incidencia declarada de situaciones de intento (no consumado) de fraude a través de Internet y a través del teléfono móvil comparando el 1^{er} trimestre de 2008, 2009 y 2010.

Todas las situaciones han sufrido un descenso desde comienzos de 2008, exceptuando la recepción de un e-mail ofertando un servicio no solicitado y la invitación a visitar alguna página web sospechosa, que aumentan un 5,1 y 3,2 puntos porcentuales respectivamente en el 1^{er} trimestre de 2010.

En el caso de las incidencias de intento de fraude a través del teléfono móvil, el mayor descenso lo efectúa la recepción de un SMS ofertando un servicio no solicitado, con un retroceso de 13,8 puntos porcentuales.

Tabla 4: Evolución interanual de la incidencia declarada de situaciones de intento (no consumado) de fraude (%)

	1T 2008	1T 2009	1T 2010
A través de Internet			
Invitación a visitar alguna página web sospechosa	29,4	39,6	32,6
Recepción de e-mail ofertando un servicio no solicitado	24,0	35,6	29,1
Recepción de una oferta de trabajo por Internet que pudiera ser falsa o sospechosa	25,2	25,4	22,2
Recepción de e-mail solicitando claves de usuario	25,5	24,5	18,6
A través del teléfono móvil			
Recepción de un SMS ofertando un servicio no solicitado	23,2	24,6	9,4
Recepción de una llamada telefónica solicitando claves de usuario	<i>n.d.</i>	4,4	2,4
Recepción SMS solicitando claves de usuario	3,3	3,6	1,7

Fuente: INTECO

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

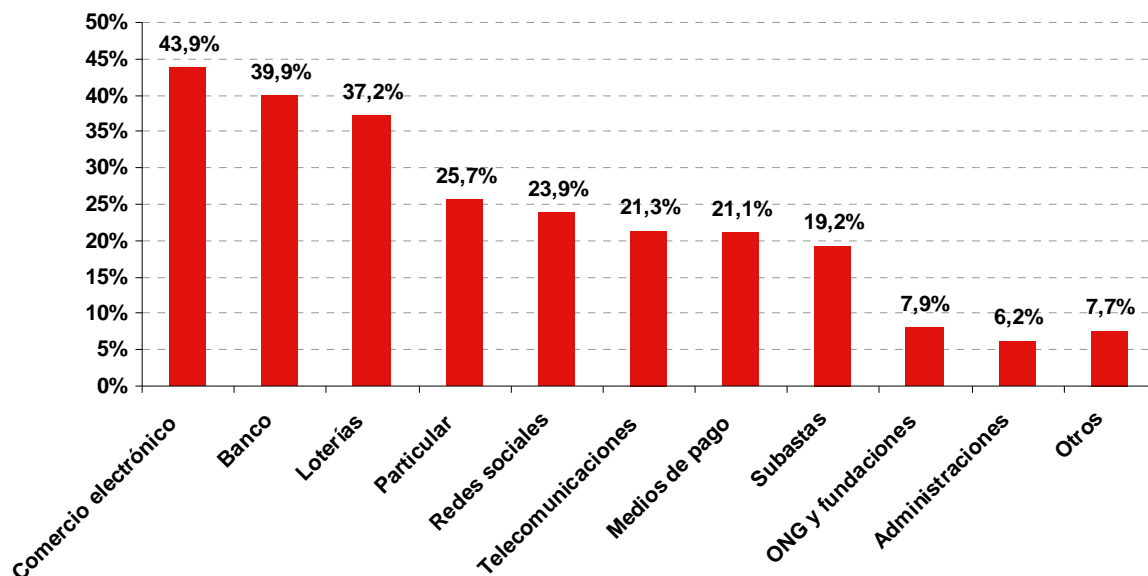
Las formas adoptadas por el atacante que intenta defraudar a través de una comunicación sospechosa son diversas (Gráfico 3). En la mayoría de las ocasiones, el atacante suplanta entidades reputadas (como bancos o ONGs) para generar confianza en la víctima, o simplemente, anuncia estafas en forma de lotería y subastas ilegales a las que invita a participar.

En el 1^{er} trimestre de 2010 la forma favorita adoptada por los atacantes para realizar la comunicación sospechosa de fraude es la de compras online o *e-commerce* (43,9%). Casi un 40% de las comunicaciones sospechosas simulaban ser una entidad bancaria, seguidos muy de cerca por las páginas de loterías, casinos y juegos online.

Según los datos proporcionados por el *Anti-Phishing Working Group* (APWG) a nivel mundial, en el 4^o trimestre de 2009, un 39% de los ataques se dirigían al sector financiero y un 33% a servicios de pago⁵.

⁵ Anti-Phishing Working Group (APWG) (2009). Disponible en: http://www.antiphishing.org/reports/apwg_report_Q4_2009.pdf.

Gráfico 3: Formas adoptadas por el remitente de la comunicación sospechosa de ser fraudulenta ⁶ (%)



Base: Usuarios que han sufrido algún intento de fraude (n= 1.878)

Fuente: INTECO

En la Tabla 5 se observa cómo el banco, que en 2008 y 2009 se posicionaba como la principal forma adoptada por el remitente de la comunicación sospechosa de ser fraudulenta, se ha situado en segundo lugar en 2010, por debajo del comercio electrónico. El comercio electrónico ha experimentado un aumento de 25,9 puntos porcentuales desde el 1^{er} trimestre de 2008.

Las redes sociales han experimentado un aumento de 13,9 puntos desde 2008, manteniéndose constante el valor durante 2009 y 2010.

Las páginas de subastas online también han ido en aumento aunque de manera más progresiva, pasando de un 13,3% de usuarios que las declaraban como las remitentes de la comunicación sospechosa en el 1^{er} trimestre de 2008, a un 17,9% en 2009 y a un 19,2% en 2010.

En el caso de tratarse de Organismos de la Administración Pública, el valor se ha mantenido constante desde 2008, con un ligero retroceso en 2009 y posterior recuperación hasta situarse en un 6,2% el 1^{er} trimestre de 2010.

⁶ 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.

Tabla 5: Evolución interanual de las formas adoptadas por el remitente de la comunicación sospechosa de ser fraudulenta (%)

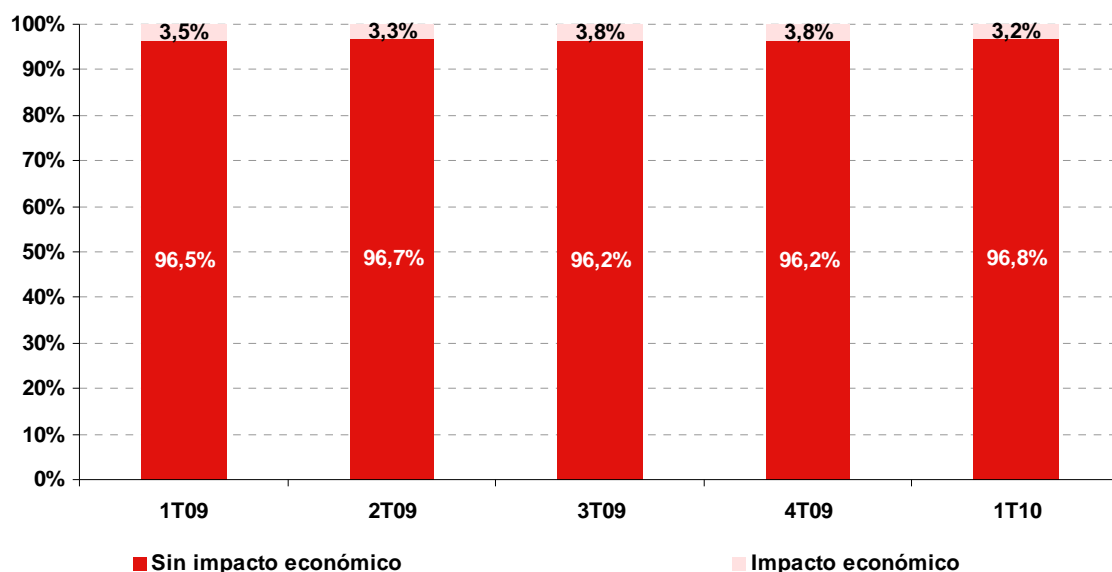
	1T 2008	1T 2009	1T 2010
e-Commerce	18,0	31,9	43,9
Banco	25,5	37,5	39,9
Loterías	n.d.	35,5	37,2
Particular	n.d.	11,9	25,7
Redes sociales	10,0	23,9	23,9
Telecomunicaciones	n.d.	25,0	21,3
Medios de pago	n.d.	15,0	21,1
Subastas	13,3	17,9	19,2
ONG y fundaciones	n.d.	6,4	7,9
Administraciones	6,6	3,5	6,2
Otros	6,0	3,1	7,7

Fuente: INTECO

3.3 Impacto económico del fraude

Este trimestre se alcanza un mínimo anual en el número de usuarios que han sufrido un impacto económico a consecuencia de algún tipo de fraude a través de Internet. Sólo un 3,2% de los usuarios afirma haber sufrido un perjuicio económico en los últimos 3 meses, el dato más bajo declarado por los encuestados desde el 1^{er} trimestre de 2009.

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



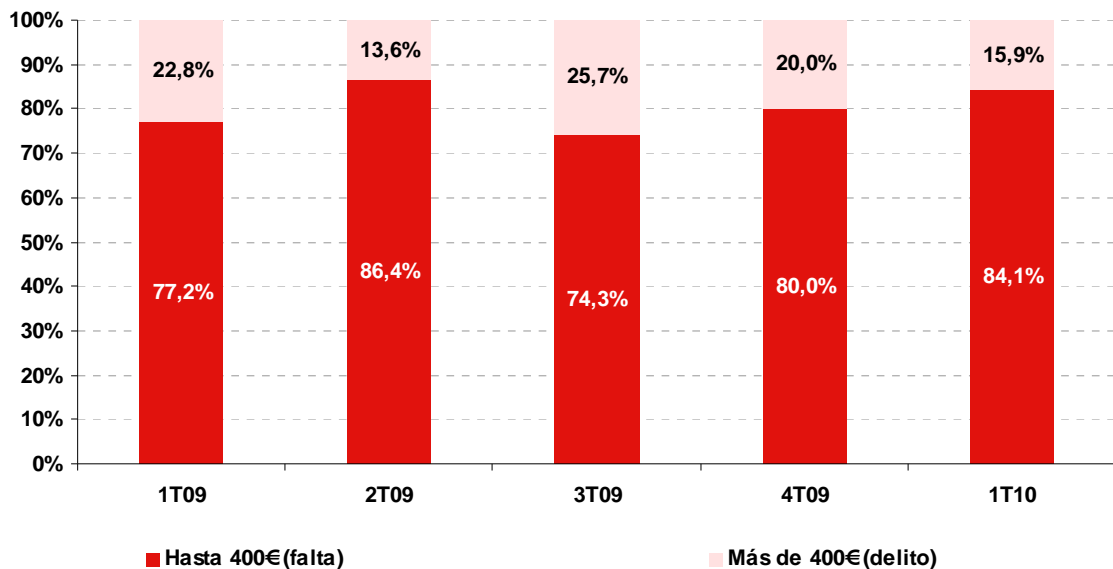
Base: Total usuarios (n=3.599 en 1T10)

Fuente: INTECO

De forma también positiva, en el caso de los usuarios que han sufrido un perjuicio económico en el 1^{er} trimestre de 2010, un porcentaje muy elevado (84,1%) ha perdido

menos de 400 € a consecuencia de la estafa. Si el fraude con perjuicio económico no asciende de éste límite no es considerado delito sino falta y el tratamiento jurídico (en el caso en el que los atacantes fueran detenidos) sería mucho más leve.

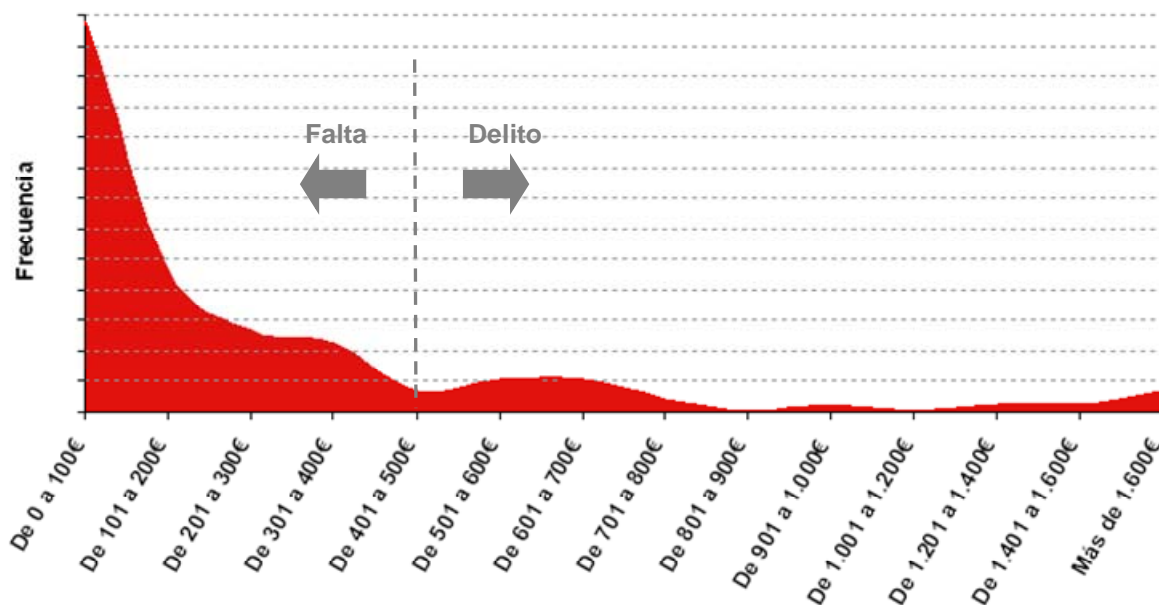
Gráfico 5: Evolución de la cuantía económica derivada del fraude (%)



Base: Usuarios que han sufrido perjuicio económico como consecuencia de un fraude online (n=132 en 1T10)
Fuente: INTECO

La distribución del importe defraudado revela que la mayoría de usuarios (111) han perdido hasta 400 €. De ellos, más de la mitad (64) se encuentran en el intervalo de menos de 100 €.

Gráfico 6: Distribución del importe defraudado en el 1T 2010



Base: Usuarios que han sufrido perjuicio económico como consecuencia de un fraude online (n=132)

Fuente: INTECO

3.4 Fraude y malware

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 bancarios⁷ 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 bancarias⁸.

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

Cabe recordar, para interpretar correctamente las cifras, que los equipos que alojan malware bancario no necesariamente terminan experimentando una situación de fraude. Para que un fraude se consuma deben concurrir las siguientes circunstancias: en primer lugar, el equipo del usuario ha de estar infectado por este tipo de troyano; además, el

⁷ Programas maliciosos, que utilizando diversas técnicas, roban información confidencial a los clientes de banca y/o plataformas de pago online ([Glosario técnico PANDA SECURITY](#))

⁸ 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.

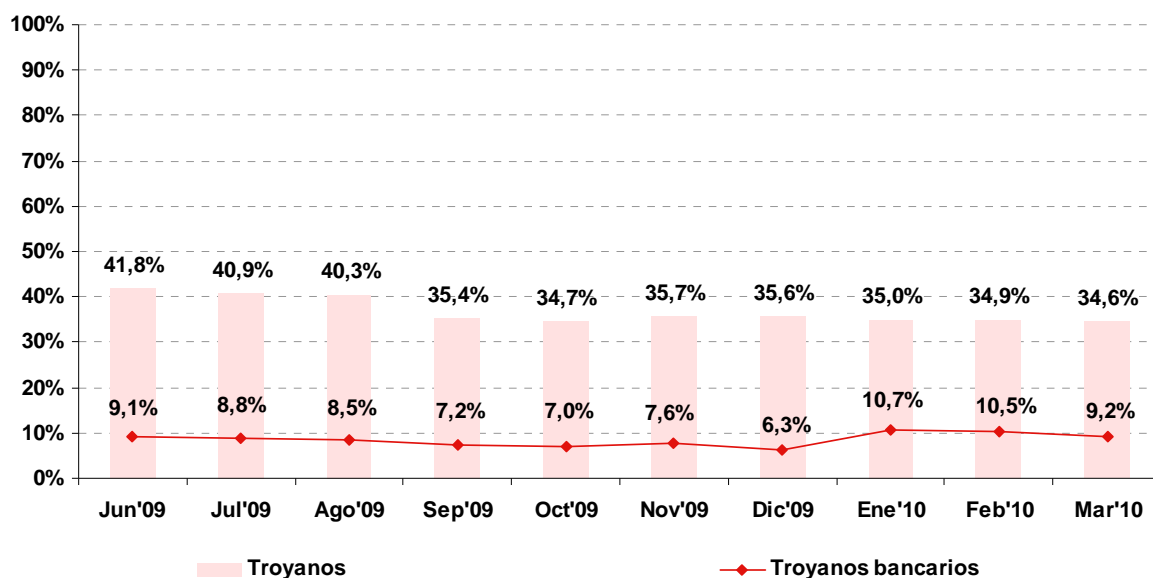
espécimen que infectó la máquina ha de atacar a la entidad bancaria con la que opera el usuario; por último, el ciudadano ha de iniciar sesión en su espacio de banca electrónica y rellenar los datos adicionales que se le soliciten.

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.

El Gráfico 7 muestra cómo en marzo de 2010 un 9,2% de los equipos analizados aloja algún tipo de troyano bancario, frente al 34,6% que alojan troyanos.

Se rompe el descenso de la infección de troyanos bancarios, que alcanzó su mínimo en diciembre de 2009. Sin embargo, los equipos que alojan troyanos (no específicamente dedicados al robo de credenciales bancarias) desciende, lo que consolida una tendencia a la baja que viene observándose desde hace varios meses.

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



Fuente: INTECO

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

Se analiza a continuación los hábitos prudentes relacionados con la banca y el comercio a través de la Red, comparando los resultados entre los usuarios que no han sido víctimas de intento fraude y/o perjuicio económico y los que sí lo han sido.

¿Influye en los hábitos prudentes de los encuestados haber sufrido un intento de fraude y/o haber sufrido perjuicio económico?

En el Gráfico 8 se puede observar cómo los usuarios que han sido víctima de fraude y/o perjuicio económico son más prudentes en todos los hábitos relacionados con la banca en línea y el comercio electrónico. Cabe señalar que en todos los hábitos existen diferencias, aunque en algunos casos éstas no son muy elevadas.

El mayor contraste (11,6 puntos de diferencia) la presenta el hábito prudente de no facilitar datos/contraseñas por correo electrónico o teléfono cuando su banco se lo pide. Un 55,8% de los encuestados que han sido víctimas de intento de fraude y/o perjuicio económico lo declaran frente a un 44,2% de usuarios que no ha vivido situación de fraude.

El hábito prudente de evitar usar equipos públicos o compartidos (cibercafés, estaciones, aeropuertos,...) es realizado por un 55,4% de los que han sufrido un intento de fraude y/o un perjuicio económico y por un 44,6% de aquellos que no lo han sufrido.

Gráfico 8: 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 (%)



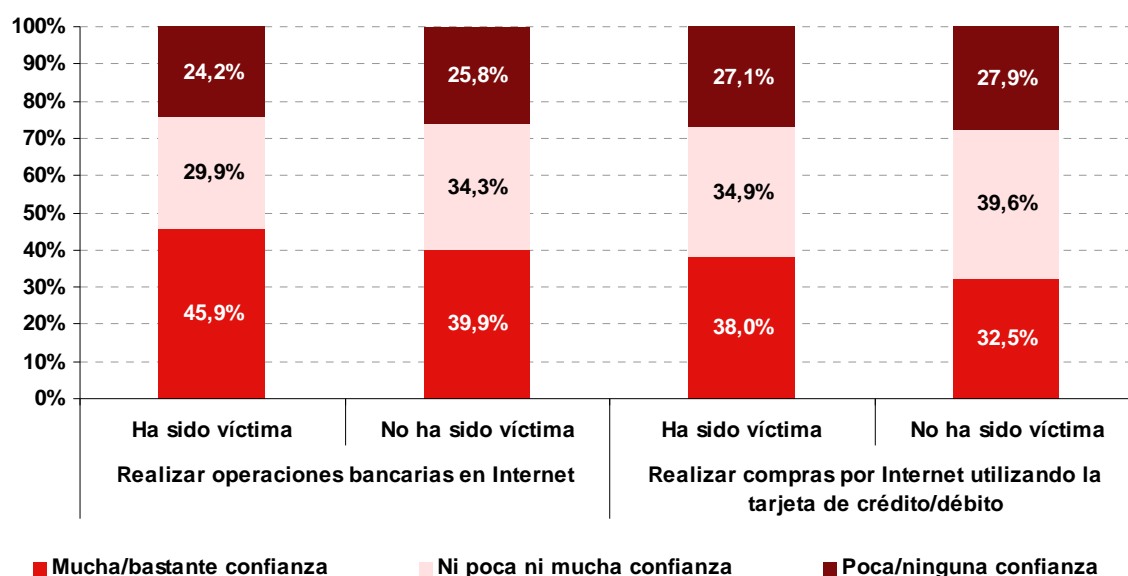
Base: Usuarios que utilizan comercio electrónico y/o banca en línea (n=3.302)

Fuente: INTECO

También es significativo el análisis de la confianza depositada en realizar operaciones bancarias y compras por Internet, comparando aquellos encuestados que han sido víctimas de intento de fraude y/o han sufrido perjuicio económico con los que no los han sufrido.

El hecho de haber sido víctima de intento de fraude no afecta negativamente al nivel de confianza. Se observa en el Gráfico 9 que haber sufrido un intento de fraude y/o haber sufrido perjuicio económico no influye a la hora de depositar confianza en procedimientos telemáticos como operaciones bancarias en Internet y compras a través de la Red utilizando la tarjeta de crédito/débito.

Gráfico 9: 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=3.302)

Fuente: INTECO

Un 45,9% confía mucho y bastante en realizar operaciones bancarias y un 38% en realizar compras online a pesar de haber sido víctima de fraude y/o haber sufrido perjuicio económico.

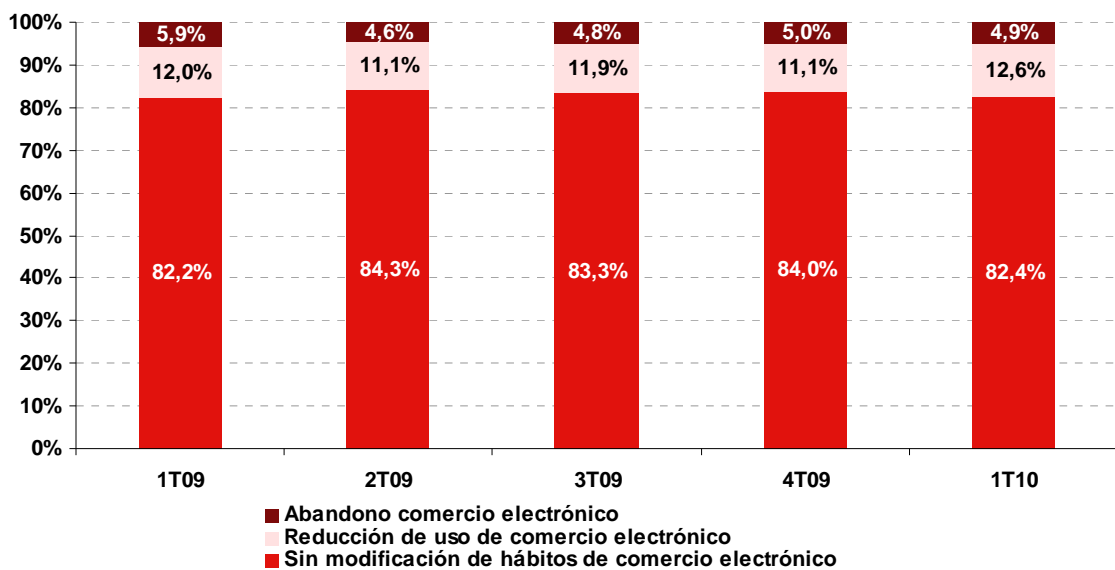
Lo fraudes (o intentos de fraude) sufridos ¿frenan el avance en el uso de las nuevas tecnologías y servicios online disponibles en la Red? Se analizan a continuación los posibles cambios de hábitos de comercio electrónico (Gráfico 10) y banca electrónica (

Gráfico 11) que puede adoptar un usuario tras sufrir un intento de fraude.

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. Los usuarios entienden que la compra online y la banca electrónica son servicios que no merecen ser abandonados por intentos de fraude (que quizás consideran aislados). También da una idea de lo arraigado de estos comportamientos en la Sociedad de la Información.

Un porcentaje considerable (82,4%) afirma no haber modificado sus hábitos en la compra online tras sufrir un intento de fraude. Sube ligeramente, sin embargo, el porcentaje de usuarios que afirma reducir el número de compras (hasta un 12,6%), y se mantiene estable los usuarios que abandonan el hábito de compra online, en torno al 5%.

Gráfico 10: Modificación de hábitos de comercio electrónico tras sufrir intento (no consumado) de fraude (%)

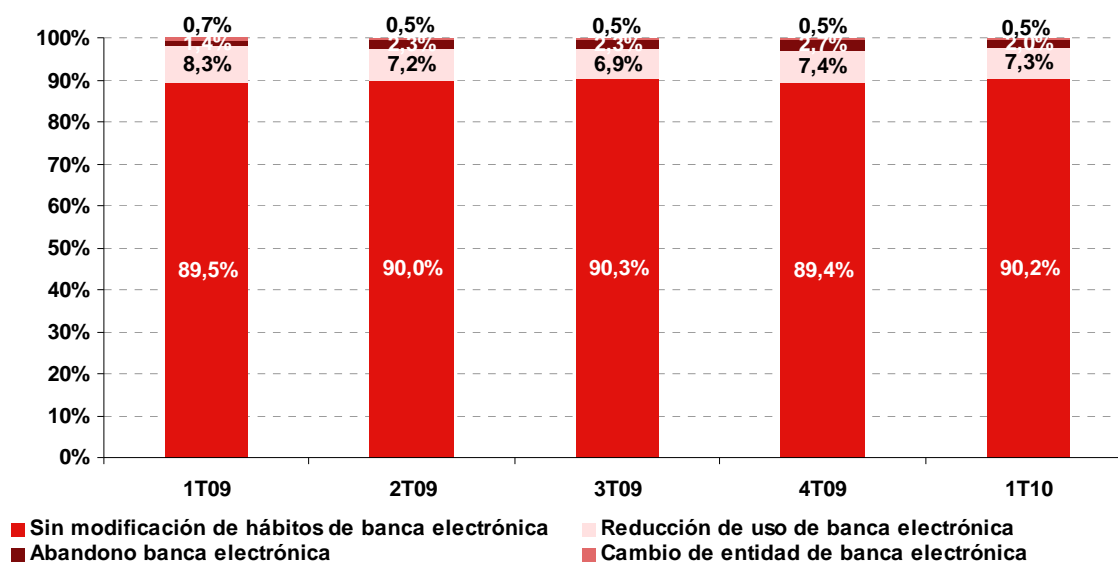


Base: Usuarios que han sufrido algún intento de fraude y/o un perjuicio económico (n=1.908)

Fuente: INTECO

Con respecto a la banca online, los usuarios muestran un comportamiento parecido, un 90,2% de los encuestados declara no modificar sus hábitos de banca electrónica después de sufrir un intento de fraude.

Gráfico 11: 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=1.908)

Fuente: INTECO

La evolución interanual muestra un incremento de los usuarios que no modifican sus hábitos ni en el comercio electrónico ni en la banca a través de Internet. El mayor aumento se da entre el 1^{er} trimestre de 2008 y el de 2009, para estabilizarse en 2010.

Así, el porcentaje de usuarios que no modifica sus hábitos de compra a través de la Red pasa de un 77,9% en 2008 a un 82,4% en 2010, y en el caso de la banca a través de Internet los datos se sitúan en un 81% en 2008 para elevarse a un 90,2% en 2010.

Tabla 6: Evolución interanual de la modificación de hábitos tras sufrir intento (no consumado) de fraude (%)

	1T 2008	1T 2009	1T 2010
Modificación de hábitos de comercio electrónico			
No he modificado en absoluto mis hábitos de compra online	77,9	82,2	82,4
He reducido mis compras online	13,6	12,0	12,6
Ha motivado que deje de realizar compras online	8,5	5,9	4,9
Modificación de hábitos de banca electrónica			
No he modificado en absoluto mi uso de banca online	81,0	89,5	90,2
He reducido el uso de banca online	10,9	8,3	7,3
Ha motivado que deje de usar servicios de banca online	7,2	1,4	2,0
Ha motivado un cambio de banco online	1,0	0,7	0,5

Fuente: INTECO

4 CONCLUSIONES Y RECOMENDACIONES

4.1 Conclusiones del análisis

La incidencia de situaciones de fraude basado en técnicas de ingeniería social a través de la Red y a través del teléfono móvil sigue descendiendo en el 1^{er} trimestre de 2010. Alcanzan todas las situaciones el mínimo porcentaje declarado desde comienzos del año 2009.

La evolución interanual (comparando los datos de 2008, 2009 y 2010) presenta una realidad análoga a la trimestral. Todas las incidencias declaradas de situaciones de intento (no consumado) de fraude han descendido, exceptuando la invitación a visitar alguna página web sospechosa y la recepción de un e-mail ofertando un servicio no solicitado, siendo la que mayor bajada presenta la recepción de un SMS ofertando un servicio no solicitado.

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

Es a través de páginas que simulan compras o ventas a través de Internet como los atacantes, en el 1^{er} trimestre de 2010, se encubren para realizar comunicaciones sospechosas de fraude, siendo esta técnica la más señalada por los encuestados. Hasta este trimestre, eran los bancos los que acaparaban el mayor porcentaje de usuarios que declaraban que la comunicación sospechosa se llevaba a cabo mediante estas entidades.

Este cambio puede responder a un aumento de usuarios españoles que utilizan el comercio electrónico unido a que cada vez son más las recomendaciones e indicaciones para evitar el tipo de fraude a través de la suplantación de bancos y entidades financieras.

¿Cuánto impacto económico ha causado el fraude?

El número de usuarios que han sufrido impacto económico causado como consecuencia de una situación de fraude experimenta, el 1^{er} trimestre de 2010, un mínimo anual. Sólo un 3,2% de los encuestados declaran haber sufrido pérdidas económicas. De entre los que han sufrido estas pérdidas el mayor número de usuarios se sitúa en la franja económica de menos de 400 €.

¿Qué influencia ha tenido el intento de fraude en los hábitos y la e-confianza relacionados con la banca a través de Internet y el comercio electrónico?

Los hábitos prudentes relacionados con el comercio electrónico y la banca en línea de los encuestados diferenciando entre los que han sufrido un intento de fraude y/o perjuicio

económico y los que no lo han sufrido muestran diferencias a favor de los usuarios que han sido víctimas de intento de fraude y/o de perjuicio económico. El mayor contraste lo presenta el hábito prudente de no facilitar datos/contraseñas por correo electrónico o teléfono cuando su banco se lo pide. Un 55,8% de los encuestados que han sido víctimas de intento de fraude y/o perjuicio económico lo declaran frente a un 44,2% de usuarios que no ha vivido situación de fraude.

Por otro lado, haber sufrido un intento de fraude y/o haber sufrido perjuicio económico no influye negativamente a la hora de depositar confianza en procedimientos telemáticos como operaciones bancarias en Internet y compras a través de la Red utilizando la tarjeta de crédito/débito.

Y por último, 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. Los usuarios entienden estos servicios no merecen ser abandonados por intentos de fraude que consideran aislados en su mayor parte.

4.2 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. 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.

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 (%)	14
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 (%).....	15
Gráfico 3: 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 (%)	19
Gráfico 6: Distribución del importe defraudado en el 1T 2010	20
Gráfico 7: Evolución de equipos que alojan troyanos bancarios (%)	21
Gráfico 8: 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 (%)	22
Gráfico 9: Nivel de confianza entre los usuarios que han sido víctima de intento de fraude y/o haber sufrido perjuicio económico y los que no(%)	23
Gráfico 10: Modificación de hábitos de comercio electrónico tras sufrir intento (no consumado) de fraude (%)	24
Gráfico 11: Modificación de hábitos de banca electrónica tras sufrir intento (no consumado) de fraude (%)	25

ÍNDICE DE TABLAS

Tabla 1: Tamaños muestrales para las encuestas	10
Tabla 2: Número de equipos escaneados mensualmente	10
Tabla 3: Errores muestrales de las encuestas (%).....	13
Tabla 4: Evolución interanual de la incidencia declarada de situaciones de intento (no consumado) de fraude (%)	16
Tabla 5: Evolución interanual de las formas adoptadas por el remitente de la comunicación sospechosa de ser fraudulenta (%).....	18
Tabla 6: Evolución interanual de la modificación de hábitos tras sufrir intento (no consumado) de fraude (%)	25



Instituto Nacional
de Tecnologías
de la Comunicación

<http://www.inteco.es>

<http://observatorio.inteco.es>