GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

plan avanza2

INTECO
Instituto Nacional de Tecnologías de la Comunicación

Estudio sobre el fraude a través de Internet

Informe anual 2010 (6ª oleada)

OBSERVATORIO DE LA **SEGURIDAD** DE LA **INFORMACIÓN**

Edición: Junio 2011

El "Estudio sobre el fraude a través de Internet (Informe anual 2010)" ha sido elaborado por el siguiente equipo de trabajo del Observatorio de la Seguridad de la Información de INTECO:

Pablo Pérez San-José (dirección)

Cristina Gutiérrez Borge (coordinación)

Eduardo Álvarez Alonso

Susana de la Fuente Rodríguez

Laura García Pérez

Correo electrónico del Observatorio de la Seguridad de la Información: ***observatorio@inteco.es***

ÍNDICE

PUNTOS CLAVE

El Observatorio de la Seguridad de la Información publica el *Estudio sobre el fraude a través de Internet (informe anual 2010)*. La metodología utilizada para la realización del informe incluye 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 estudio 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 octubre a diciembre de 2010. Durante este tiempo se han realizado **3.571 encuestas y 8.578 análisis online** a los equipos que componen el panel. Además, siendo este el informe que cierra el año, ofrece un análisis evolutivo a lo largo de todo 2010, haciendo una comparativa con los datos de 2009.

Entre los principales resultados y conclusiones del estudio, cabe destacar que en el cuarto trimestre de 2010, un 53,1% de los usuarios de Internet españoles declaran haber sido víctimas de un intento (no necesariamente consumado) de fraude en los últimos tres meses. Los atacantes utilizan técnicas de ingeniería social para consumar sus estafas por dos vías: bien a través de Internet, bien por medio del teléfono móvil.

En el análisis de las situaciones potencialmente fraudulentas ocurridas a los usuarios cuando navegan en la Red, destacan la recepción de invitaciones para visitar alguna página web sospechosa (34,4%) y de correos electrónicos que ofertan servicios no solicitados (25,9%). En menor proporción, son los destinatarios de ofertas de trabajo sospechosas de ser falsas (21,1%) y de correos electrónicos solicitando claves de usuario (19,9%).

Por lo que respecta a los intentos de fraude a través del teléfono móvil, los usuarios declaran recibir mensajes cortos de texto ofertando un servicio no requerido (11,1%) y, con menor frecuencia, la solicitud de claves de usuario, bien a través de una llamada telefónica (2,7%), bien a través de un mensaje de texto (2,2%).

Las formas que con mayor frecuencia adoptan los remitentes de las comunicaciones sospechosas de ser fraudulentas son las entidades bancarias (42,7%), las páginas de compra-venta online (39%) y las loterías (35,7%).

En el periodo analizado en el informe, el 95,2% de los internautas españoles afirma no haber sufrido en los últimos tres meses un perjuicio económico como consecuencia de un fraude electrónico, mientras que un 4,8% sí han sufrido pérdida. De estos últimos, la cuantía defraudada es inferior a 400 euros en la mayoría de los casos (84,3%), es decir, la mayoría de los atacantes no sobrepasa la barrera económica marcada por el Código Penal, que determina la consideración de la estafa como delito (en lugar de falta, si la cantidad defraudada es inferior a los 400 euros).

En diciembre de 2010, el análisis empírico de los equipos muestra que un 39,8% de los equipos aloja algún tipo de troyano, un 6,8% alojan troyanos bancarios (código malicioso destinado a interceptar credenciales de banca electrónica de entidades concretas) y un 5,8% sufre una infección por rogueware (o falsos antivirus). El porcentaje de troyanos bancarios se ha reducido a lo largo de 2010 en casi 4 puntos porcentuales.

Los usuarios se muestran fieles en la utilización de servicios de compra online y de banca electrónica, aun cuando han sido víctimas de un intento de fraude (no necesariamente consumado).

En el último trimestre de 2010, un 81,8% de los internautas que ha sufrido un incidente de este tipo en la utilización de servicios de comercio electrónico no modifican sus hábitos, frente a un 5% que abandonan esta actividad y un 13,1% que reducen su utilización.

Por último, también es mayoritario el porcentaje de usuarios de servicios de banca en línea que no modifica sus hábitos tras ser víctimas de un intento de fraude (87,8%), teniendo el resto de comportamientos un carácter minoritario: reducción de uso (8,9%), abandono en el uso de estos servicios (2,9%) y cambio de entidad de banca online (0,5%).

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 6ª entrega del mismo.

El análisis recoge datos empíricos obtenidos a través de iScan, que 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 si el intento de fraude influye en la modificación de los hábitos de uso de comercio electrónico y banca en línea. También se analiza la e-confianza que les genera estos hábitos tras sufrir un intento de fraude. Las conclusiones, en este caso, se basan en datos procedentes de la encuesta.

2. DISEÑO METODOLÓGICO

El *Estudio sobre el fraude a través de Internet (informe anual 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. Sobre los miembros del panel se aplican dos técnicas diferenciadas, que permiten obtener dos tipos diferentes de información:

- Encuestas online a usuarios españoles de Internet mayores de 15 años con acceso frecuente desde el hogar, llevadas a cabo con una periodicidad trimestral. Los datos extraídos de las encuestas permiten obtener la percepción sobre la incidencia de prácticas constitutivas de fraude y su posible relevancia económica, así como el nivel de e-confianza de los ciudadanos tras sufrir un intento de fraude.

- Análisis online del nivel de seguridad real de los equipos informáticos existentes en los hogares, realizados mensualmente. Para ello, se utiliza el software iScan, desarrollado por INTECO, que analiza los sistemas y las incidencias de seguridad en los equipos gracias a la utilización conjunta de 46 motores antivirus. Este software se instala en los equipos y los analiza, detectando todo el malware residente en los mismos y recogiendo además datos del sistema operativo, de su estado de actualización y de las herramientas de seguridad instaladas. El programa informático remite esta información a INTECO, que la trata de manera anónima y agregada.

2.1. Universo

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

2.2. Tamaño y distribución muestral

La afijación muestral responde a un modelo polietápico:

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

- Muestreo por cuotas de tamaño del hogar, edad, sexo, actividad laboral y tamaño del hábitat[1].

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

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
1er trimestre 2009	3.563
2º trimestre 2009	3.521
3er trimestre 2009	3.540
4º trimestre 2009	3.640
1er trimestre 2010	3.599
2º trimestre 2010	3.519
3er trimestre 2010	3.538
4º trimestre 2010	3.571

Fuente: INTECO

Tabla 2: Número de equipos escaneados mensualmente

Período	Equipos escaneados	Período	Equipos escaneados
Ene'09	5.649	Ene'10	4.079
Feb'09	4.325	Feb'10	3.751
Mar'09	4.695	Mar'10	4.024
Abr'09	4.954	Abr'10	3.746
May'09	4.677	May'10	3.499
Jun'09	4.293	Jun'10	3.279
Jul'09	3.971	Jul'10	3.337
Ago'09	3.677	Ago'10	2.716
Sep'09	4.520	Sep'10	2.783
Oct'09	4.294	Oct'10	3.232
Nov'09	4.039	Nov'10	2.742
Dic'09	4.452	Dic'10	2.604

Fuente: INTECO

2.3. Captura de información y trabajo de campo

El trabajo de campo ha sido realizado entre octubre y diciembre 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*[2] *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*

[2] Software y ficheros legítimos, archivos inocuos.

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[3] y shareware[4] confirmado como inocuo. Todos los ejemplares que siguen siendo detectados tras las dos primeras capas de filtrado son comparados con esta base de datos para eliminar más falsos positivos.

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

Eliminación de detecciones concretas y corrección de categorías incorrectamente determinadas

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

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

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

En cualquier caso, a pesar de la fortaleza de la herramienta iScan y de las medidas adoptadas por INTECO para mitigar la incidencia de falsos positivos, se debe puntualizar que existen otras limitaciones intrínsecas a la metodología empleada que hacen que el análisis no sea infalible. Por ello, a pesar del rigor y robustez del análisis, los datos que el

[3] Software gratuito.
[4] Software de descarga gratuita pero limitado en funcionalidad o tiempo de uso.

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 ±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
1er trimestre 2009	3.563	±1,68%
2º trimestre 2009	3.521	±1,68%
3er trimestre 2009	3.540	±1,68%
4º trimestre 2009	3.640	±1,66%
1er trimestre 2010	3.599	±1,66%
2º trimestre 2010	3.519	±1,68%
3er trimestre 2010	3.538	±1,68%
4º trimestre 2010	3.571	±1,68%

Fuente: INTECO

3. SEGURIDAD Y FRAUDE ONLINE

3.1. Intento de fraude y manifestaciones

En primer lugar se analiza la incidencia declarada de situaciones de fraude a través de Internet o del teléfono móvil en los últimos tres meses, representada en el Gráfico 1.

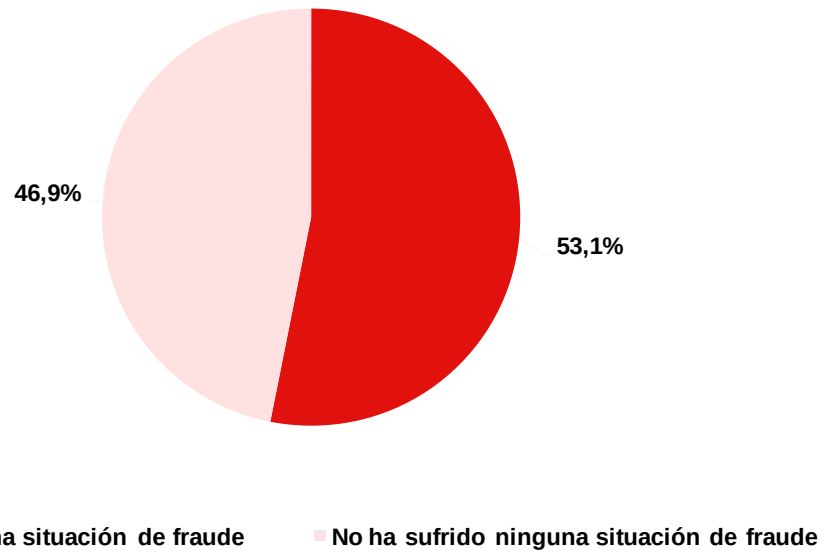
Para la interpretación correcta de los datos, es necesario realizar dos puntualizaciones previas:

- En primer lugar, los datos proporcionados en ambos gráficos están basados en las respuestas a la encuesta aplicada al panel de usuarios de Internet españoles, ofreciendo por tanto la perspectiva del ciudadano.

- En segundo lugar, no debe entenderse que las personas que afirman haber experimentado alguna de las situaciones analizadas son efectivamente víctimas de fraude. Se habla, por tanto, de intento de fraude y no de fraude consumado.

En el cuarto trimestre de 2010, son ligeramente más numerosos los usuarios que declaran haber sido víctimas de un intento de fraude (53,1%) que quienes dicen que no han percibido incidencia alguna (46,9%). Se mantienen los valores registrados en el trimestre anterior.

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=3.571 en 4T10) *Fuente: INTECO*

En segundo lugar, el Gráfico 2 muestra la evolución a lo largo de 2010 de la incidencia de situaciones de fraude a través de Internet, en base a las declaraciones de los usuarios.

En el último trimestre del año, las incidencias de intento de fraude (no consumado) que más perciben los encuestados son las invitaciones para visitar alguna página web sospechosa (declarado por un 34,4% de usuarios) y la recepción de e-mails ofertando servicios no solicitados (un 25,9%). Por detrás de estas se sitúan la recepción de ofertas de trabajo falsas (un 21,1%) y de correos electrónicos solicitando claves de usuario (19,9%).

Atendiendo a la evolución anual de los datos, se aprecia que la tendencia es bastante estable. Las incidencias que registran un incremento en sus valores son la invitación para visitar alguna página web sospechosa (1,8 puntos porcentuales con respecto al valor de principios de año), y la recepción de e-mails solicitando claves de usuario (1,3 puntos porcentuales).

El resto de valores experimentan descensos al final de la serie, destacando en este sentido la caída en la segunda mitad del año en la recepción de correos electrónicos ofertando servicios no solicitados, con un balance anual de 3,2 puntos porcentuales menos que a comienzos de 2010. La recepción de ofertas de trabajo falsas ha registrado una caída de 3,1 puntos porcentuales en el último trimestre del año, después de tres trimestres de ascensos continuados en los valores.

La explicación a estos descensos puede estar relacionada con una serie de acontecimientos registrados en la segunda mitad del año.

- En primer lugar, en septiembre se produjo el cierre de uno de los principales grupos que gestionaban los negocios publicitarios anunciados en correos basura, Spamit.com, lo que hizo que los valores generales de spam durante la segunda mitad de septiembre fuesen mucho más bajos que los habituales, mientras los atacantes se reabastecían con nuevas infraestructuras.

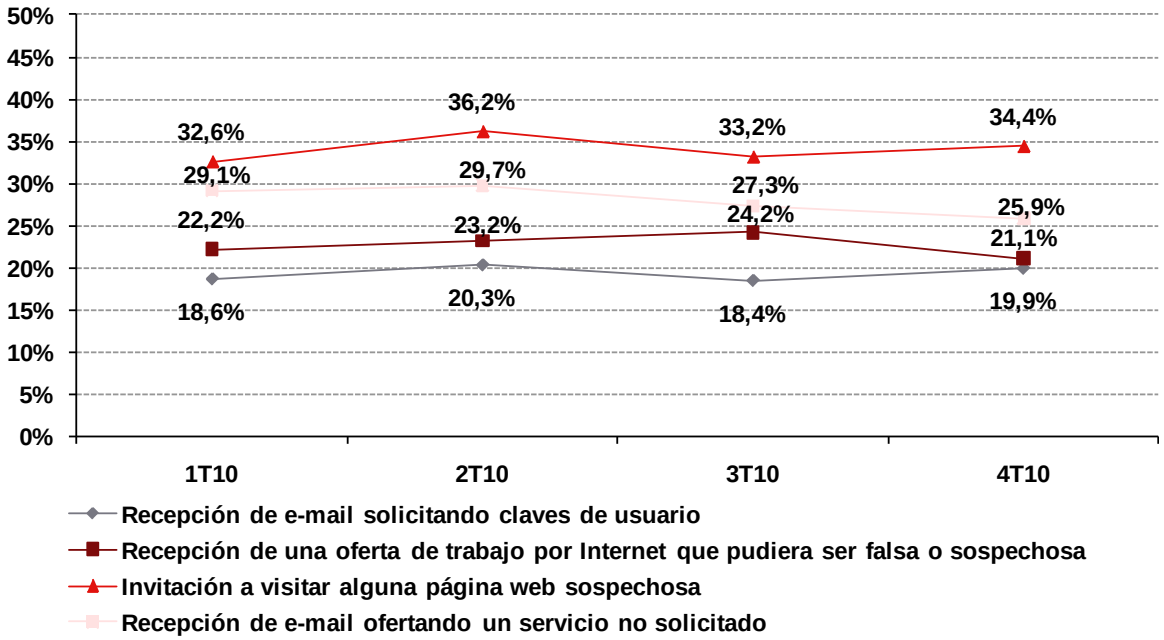
- Otro factor ha sido la inclusión de la firma Zbot[5] a la MSRT (*Malicious Software Removal Tool*) de Microsoft, en octubre de 2010. De los más de 1.300.000 sistemas limpiados, se encontró Zbot en uno de cada cinco. Esta acción supuso que, en apenas unos días, se convirtiera en el troyano más eliminado.

- Por último, se apunta a las redes sociales como Facebook y Twitter como el nuevo objetivo de los spammers: aproximadamente el 4% de los abonados a Twitter son en realidad programas para enviar correo no deseado y más del 15%

[5] Zeus (Zbot) es uno de los tipos de botnets más activos y con más usuarios infectados.

de los mensajes con enlaces que circulan por Facebook son spam. Los spammers han concluido que la efectividad del correo basura es menor que el impacto que pueden obtener a través de redes sociales[6].

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=3.571 en 4T10) *Fuente: INTECO*

A continuación, el Gráfico 3 recoge la evolución de la incidencia de situaciones de fraude, en este caso a través del teléfono móvil, en base a la percepción de los usuarios encuestados.

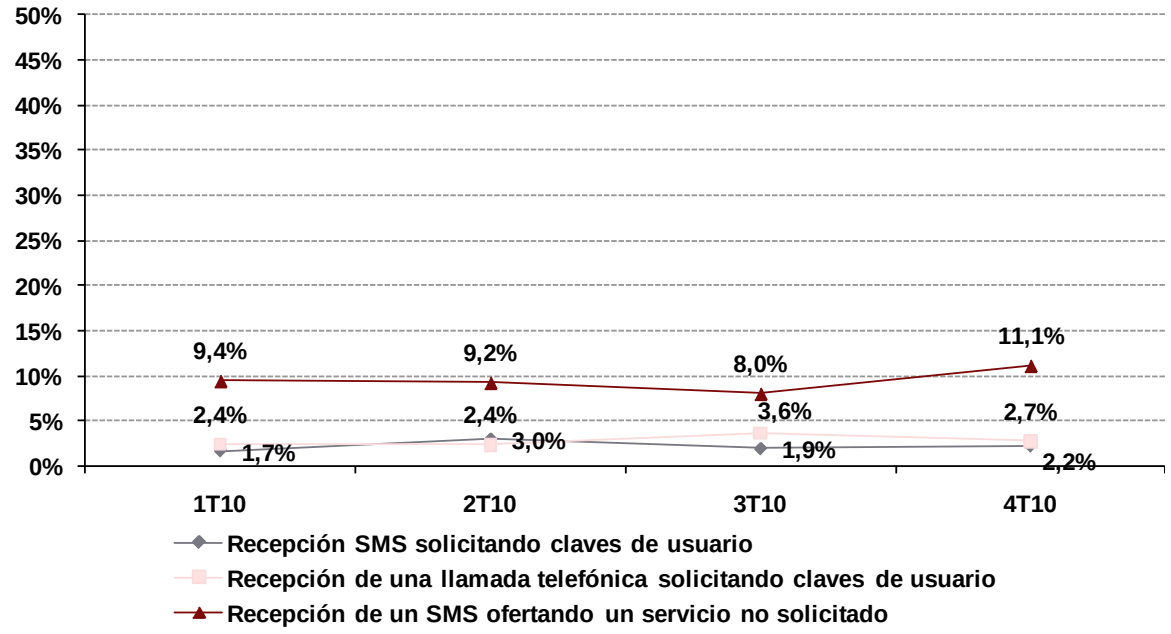
La recepción de mensajes cortos de texto ofertando servicios no solicitados es la situación más declarada (11,1%). A mayor distancia se sitúan las que tienen que ver con la solicitud de claves de usuario, bien a través de una llamada telefónica (un 2,7%), bien a través de un mensaje de texto (2,2%).

Si bien se observa una tendencia constante a lo largo de 2010, destaca el pico registrado en la recepción de SMS ofertando servicios no solicitados en el último trimestre, que supone un incremento de 1,7 puntos porcentuales desde el comienzo del año y 3,1 puntos porcentuales con respecto al trimestre anterior, en el que se registraba el mínimo histórico en los valores (8%).

[6] Fuente: *El envío de 'spam' se reduce el 75% en seis meses.* Disponible en: http://www.elpais.com/articulo/Pantallas/envio/spam/reduce/75/meses/elpepirtv/20110115elpepirtv_2/Tes.

En el resto de casos, las variaciones son más moderadas a lo largo del tiempo.

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=3.571 en 4T10) *Fuente: INTECO*

Por último, se incluye a continuación la Tabla 4, en la que se comparan los datos del último trimestre analizado, frente a los registrados a finales de 2009. En general, la evolución de la incidencia de situaciones de fraude es de signo negativo, tanto si se producen a través de la Red como del teléfono móvil, salvo en la invitación a visitar una página web sospechosa y en la recepción de una llamada telefónica solicitando claves de usuario, situaciones cuyos valores son similares a los del año anterior.

Hasta el momento, los niveles de incidencia de situaciones de intento de fraude a través del teléfono móvil son menores. Frente al gasto que supone para el atacante la realización de llamadas telefónicas o el envío de mensajes de texto a través de este dispositivo, los servicios de voz a través de Internet (VoIP) son más baratos o gratuitos. Sin embargo, las principales empresas del sector de la seguridad de la información señalan como una de las principales tendencias para los próximos años el incremento de ataques a través de dispositivos móviles con conexión a Internet (smartphones, blackberries, etc.), mediante la combinación de técnicas de ingeniería social con ataques

técnicos a los principales sistemas operativos (Android, Symbian, Windows Mobile, IOs, etc.) que buscan, en última instancia, un beneficio económico de la víctima[7].

Tabla 4: Evolución de la incidencia declarada de situaciones de intento (no consumado) de fraude entre 2009 y 2010 (%)

Incidencia declarada de situaciones de intento (no consumado) de fraude (%)		2009	2010	Evolución
A través de Internet	Recepción de e-mail solicitando claves de usuario	21,6%	19,9%	▼
	Recepción de una oferta de trabajo por Internet que pudiera ser falsa o sospechosa	23,1%	21,1%	▼
	Invitación a visitar alguna página web sospechosa	34,1%	34,4%	▶
	Recepción de e-mail ofertando un servicio no solicitado	29,4%	25,9%	▼
A través de correo electrónico	Recepción SMS solicitando claves de usuario	3,1%	2,2%	▼
	Recepción de una llamada telefónica solicitando claves de usuario	2,9%	2,7%	▶
	Recepción de un SMS ofertando un servicio no solicitado	12,2%	11,1%	▼

Fuente: INTECO

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

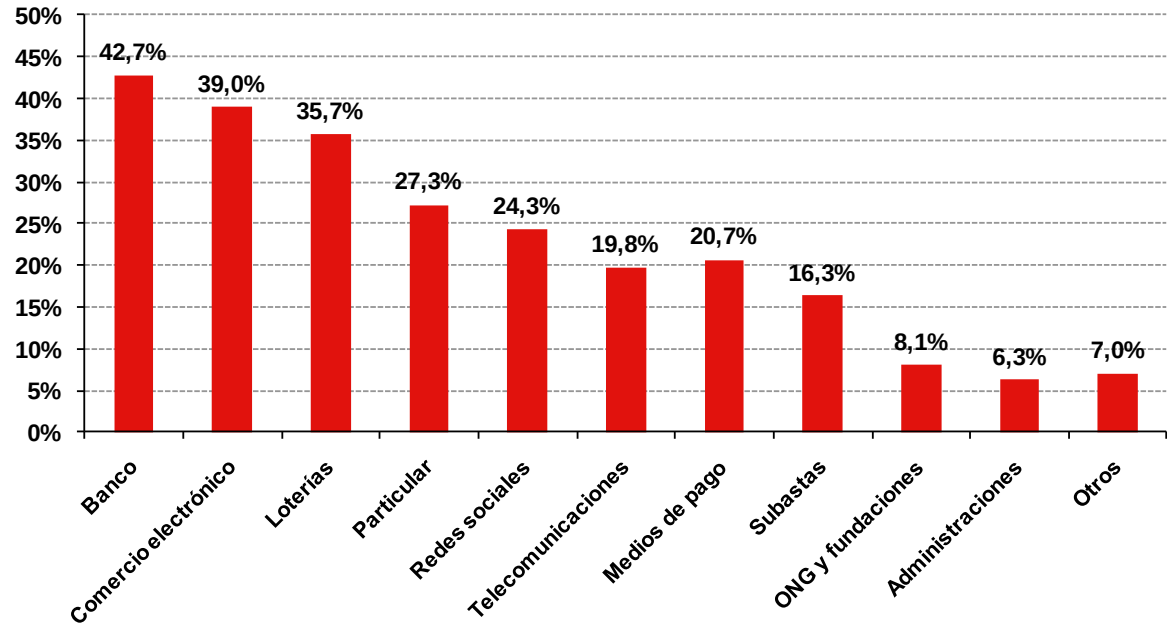
Los atacantes intentan defraudar a través de comunicaciones sospechosas que simulan proceder de diferentes remitentes, como muestra el Gráfico 4. En el cuarto trimestre de 2010, la banca online (42,7%) el comercio electrónico (39,0%) y las loterías (35,7%), son los principales sectores afectados por este tipo de estafa.

Estos datos están en línea con los publicados por el *Anti-Phishing Working Group* (APGW), organización dedicada a estudiar el fenómeno del phishing a nivel mundial. APGW en su informe del 2º trimestre de 2010 (último informe disponible en el que analiza la forma adoptada por el atacante), señala al sector financiero y a los servicios de pago como principales objetivos de los ciberestafadores[8].

[7] Fuente: *Informe anual de fraude online y cibercrimen 2010*. **S21sec**. 2011. Disponible en: http://www.s21sec.com/default.aspx

[8] Fuente: *Phishing Activity Trends Report. 2nd Quarter 2010*. **Anti Phishing Working Group**. 2011. Disponible en: http://www.antiphishing.org/reports/apwg_report_q2_2010.pdf

Gráfico 4: Formas adoptadas por el remitente de la comunicación sospechosa de ser fraudulenta[9] (%)



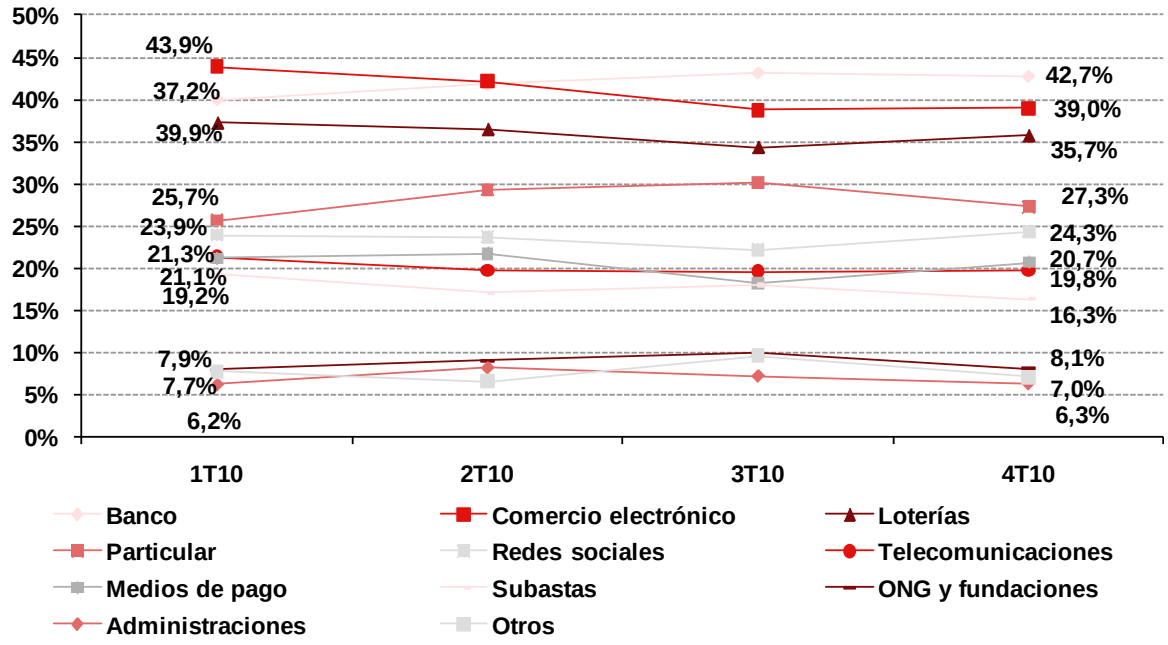
Base: Usuarios que han sufrido algún intento de fraude (n=1.938) *Fuente: INTECO*

El análisis de la evolución anual de las formas adoptadas por el remitente de la comunicación sospechosa de ser fraudulenta (Gráfico 5) muestra que los bancos y entidades financieras vuelven a la primera posición tras un primer semestre de 2010 en el que el e-comercio era la principal forma adoptada. La tercera posición sigue siendo para las loterías, con valores que se reducen paulatinamente a lo largo de la serie (desde el 39,9% en el primer trimestre hasta el 35,7% registrado en el último).

Destaca, en el cuarto lugar, los ascensos en el segundo y tercer trimestre de las comunicaciones promovidas aparentemente por particulares, con valores cercanos al 30%, tendencia que no se confirma en el último trimestre. En cuanto al resto de formatos utilizados, la evolución se muestra muy estable.

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

Gráfico 5: Evolución de las formas adoptadas por el remitente de la comunicación sospechosa de ser fraudulenta[10] en 2010 (%)



Base: Usuarios que han sufrido algún intento de fraude (n=1.938) *Fuente: INTECO*

Por último, al cotejar los datos del último trimestre analizado con los del mismo periodo de 2009, se observa que las mayores subidas se producen en los formatos de remitente que simulan ser particulares (con un incremento de 3,5 puntos porcentuales) y redes sociales (3 puntos porcentuales). Los valores que experimentan los mayores descensos son las subastas (4,6 puntos porcentuales menos) y las loterías (3,3 puntos).

[10] Ver Nota al Pie 9.

Tabla 5: Evolución de las formas adoptadas por el remitente de la comunicación sospechosa de ser fraudulenta entre 2009 y 2010 (%)

Forma adoptada	4T 2009	4T2010	Evolución
Banco	**43,1**	**42,7**	▶
Comercio electrónico	41,9	39,0	▼
Loterías	39,0	35,7	▼
Particular	23,8	27,3	▲
Redes sociales	21,3	24,3	▲
Telecomunicaciones	21,4	19,8	▼
Medios de pago	23,1	20,7	▼
Subastas	20,9	16,3	▼
ONG y fundaciones	8,3	8,1	▶
Administraciones	9,1	6,3	▼
Otros	5,1	7,0	▲

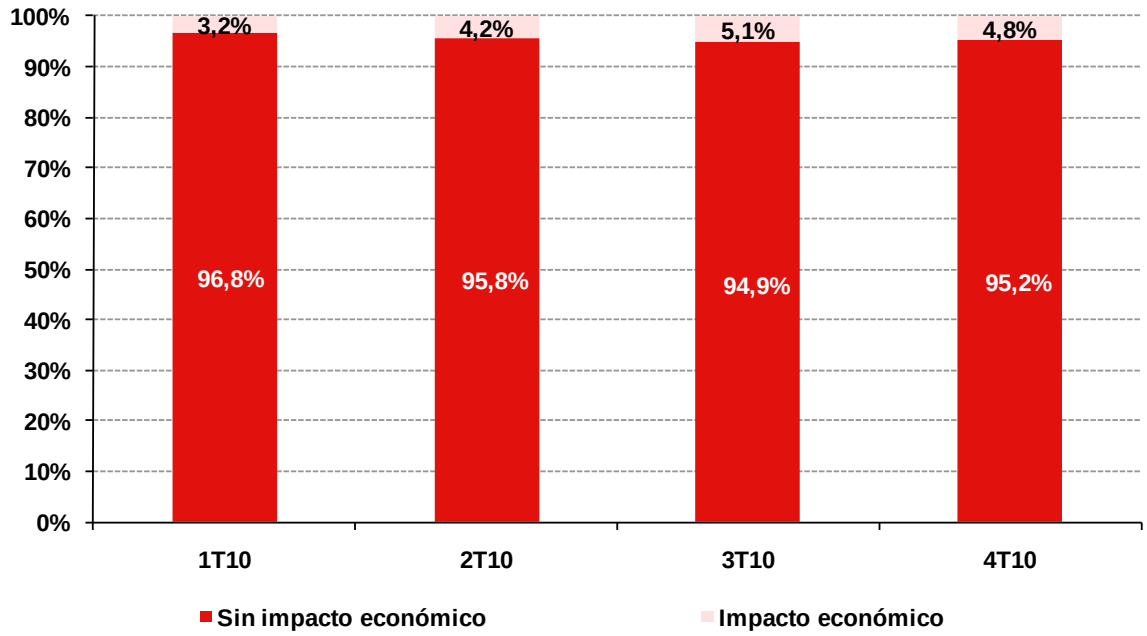
Fuente: INTECO

3.3. Impacto económico del fraude

Se estudia a continuación el impacto económico provocado por los intentos de fraude a través de la Red o del teléfono móvil, en términos de perjuicio económico efectivo y cuantía del mismo.

En el cuatro trimestre de 2010, el 95,2% de los internautas españoles afirma no haber sufrido en los últimos tres meses un perjuicio económico como consecuencia de un fraude online, mientras que un 4,8% sí han sufrido pérdida. A pesar del ligero incremento experimentado en los dos últimos trimestres de 2010, la evolución presenta datos muy estables a lo largo de la serie.

Gráfico 6: Evolución del fraude con impacto económico para el usuario (%)

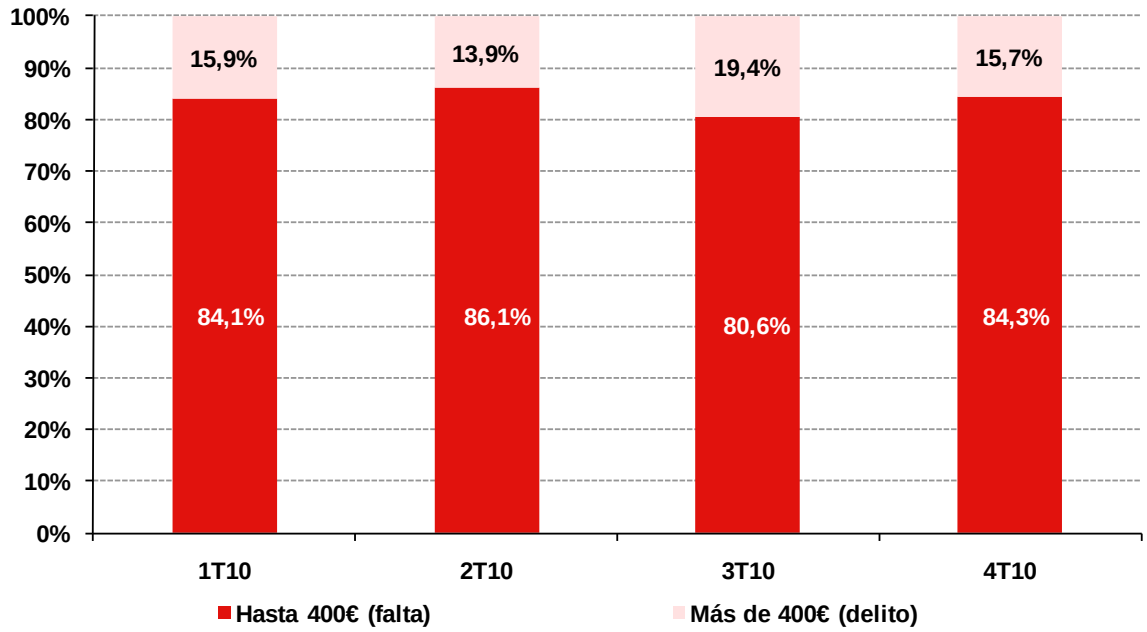


Base: Total usuarios (n=3.571 en 4T10) *Fuente: INTECO*

El Código Penal español establece en 400€ el límite entre lo que se considera falta (si es igual o inferior a esa cantidad) y delito (si es superior). En el trimestre analizado, el 84,3% de los que han sufrido fraude con perjuicio económico declara que la cantidad afectada es inferior a 400 euros, mientras que el 15,7% ha perdido una cantidad superior a esa cifra.

La tendencia a lo largo de 2010 es bastante estable, con mayoría de incidencias de fraude declaradas que corresponderían a faltas (datos por encima del 80% en todos los trimestres).

Gráfico 7: Evolución de la cuantía económica derivada del fraude (%)



Base: Usuarios que han sufrido perjuicio económico como consecuencia de un fraude online (n=128 en 4T10)
Fuente: INTECO

El análisis de la evolución entre 2009 y 2010 muestra que los datos del impacto económico de las estafas online son similares en ambos años, mientras que en el caso de la cuantía defraudada, aumenta la proporción de estafas reportadas por un valor inferior a 400€ (4,3 puntos porcentuales en el último año), no constitutivas de delito según la Ley.

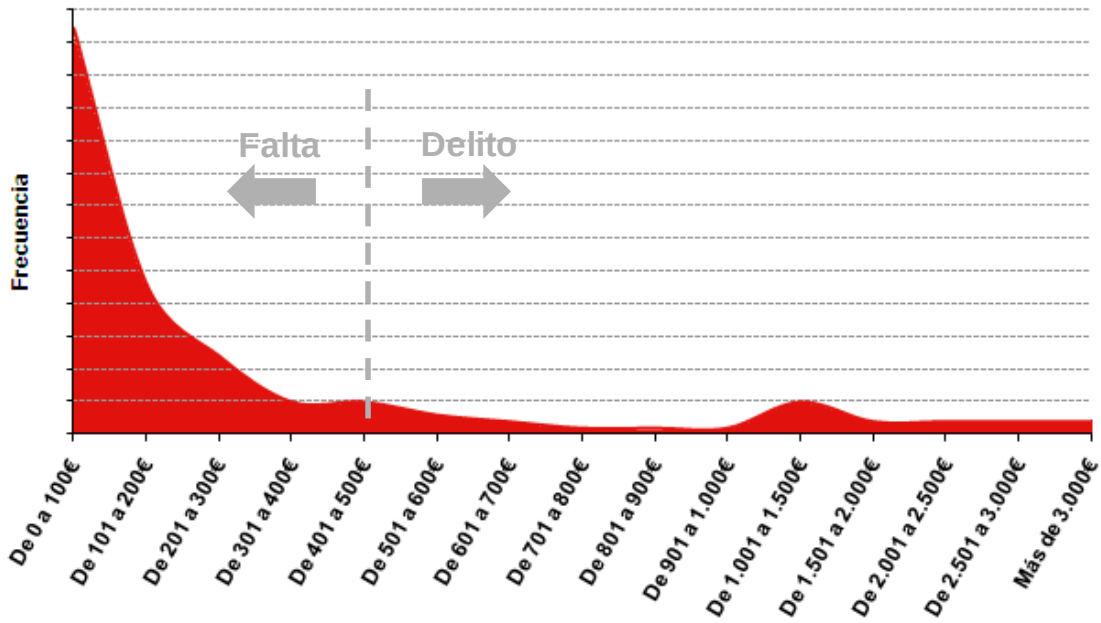
Tabla 6: Evolución del impacto económico del fraude entre 2009 y 2010 (%)

Impacto económico del fraude (%)		2009	2010	Evolución
Impacto económico	Sin impacto económico	96,2%	95,2%	▶
	Con impacto económico	3,8%	4,8%	▶
Cuantía económica	Hasta 400 € (falta)	80,0%	84,3%	▲
	Más de 400 € (delitos)	20,0%	15,7%	▼

Fuente: INTECO

Para completar esta parte del análisis, en el cuarto trimestre de 2010 dos de cada 3 usuarios afectados (de un total de 128) declaran que la cantidad estafada era inferior a los 200 euros. Asimismo, destaca que el porcentaje de usuarios que declaran haber sufrido una estafa en la franja comprendida entre 401 y 500 € es el mismo que entre 1.001 y 1.500 €.

Gráfico 8: Distribución del importe defraudado en el 4T 2010



Base: Usuarios que han sufrido perjuicio económico como consecuencia de un fraude online (n=128)
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 malware catalogado como troyano, así como la proporción de troyanos bancarios y rogueware que se encuentran en los equipos de los hogares españoles.

1) Los troyanos bancarios son programas maliciosos que, utilizando diversas técnicas, roban información confidencial a los clientes de banca y/o plataformas de pago online[11].

   Para realizar el estudio, se han considerado las siguientes familias de troyanos bancarios más populares que efectúan ataques dirigidos contra entidades bancarias[12].

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

[11] Fuente: glosario técnico PANDA SECURITY.

[12] 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.

2) A partir del segundo trimestre de 2010 se ha incluido en el análisis de los troyanos la tipología rogueware. El rogueware 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.

   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. Así, 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. Del mismo modo, para que se produzca efectivamente el fraude por rogueware, 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.

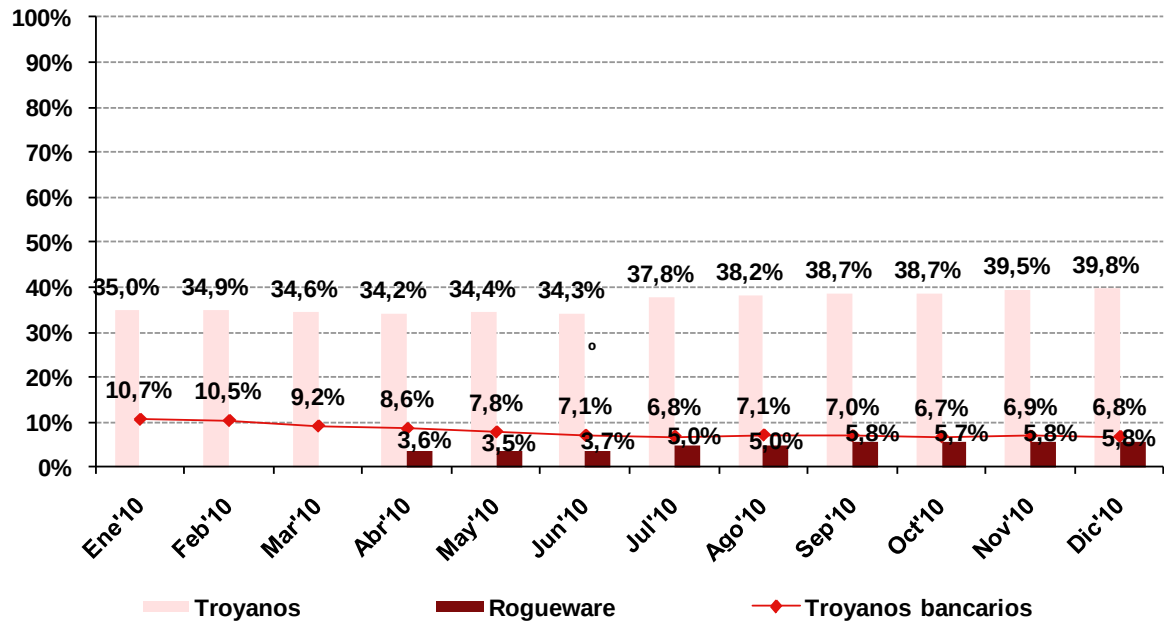
Como muestra el Gráfico 9, en diciembre de 2010 un 39,8% de los equipos analizados alojan troyanos, un 6,8% alojan troyanos bancarios y un 5,8% sufre una infección por rogueware.

Atendiendo a la evolución histórica de los valores, la tendencia de equipos que alojan troyanos (no específicamente dedicados al robo de credenciales bancarias) en la primera mitad del año es muy constante, si bien en la segunda mitad de 2010 se observa un ligero incremento en los valores, por lo que, en el conjunto del año, la subida es de casi 5 puntos porcentuales.

En el caso de los equipos infectados por troyanos bancarios, la tendencia se caracteriza por un descenso leve pero continuado en los valores, desde un 10,7% de infecciones en enero de 2010 hasta un 6,8% en el último mes del año.

Las infecciones por rogueware se mantienen en los mismos niveles que en septiembre de 2010 (5,8%). Desde el primer mes que incluyó el análisis de los equipos que alojaban rogueware (abril de 2010), se ha producido un incremento de 2,2 puntos porcentuales.

Gráfico 9: Evolución de equipos que alojan troyanos bancarios y rogueware (%)



Fuente: INTECO

Teniendo en cuenta el valor alcanzado en diciembre de 2009, un año después el porcentaje de equipos infectados por troyanos se ha incrementado en 4,2 puntos porcentuales. Este comportamiento está en línea con la información proporcionada desde la industria de seguridad, que caracteriza el año 2010 como un punto de inflexión en la seguridad de la información con respecto a años anteriores.

Con respecto a 2009, en 2010 todavía no se aprecian grandes cambios en las infecciones, pero durante el mismo aparecen nuevos factores que implicarán que 2011 sea un año en el que el número, la complejidad y la gravedad de los incidentes de seguridad crecerá: combinaciones de malware dirigidas al sector financiero, falsa sensación de seguridad por parte de los usuarios al utilizar redes sociales, coexistencia de mafias organizadas de ciberatacantes y hackers jóvenes con motivaciones temerarias

(los llamados *script-kiddies*), nuevos orígenes de los ataques (Europa del Este, Latinoamérica), etc[13].

Tabla 7: Evolución de equipos que alojan troyanos bancarios y rogueware entre 2009 y 2010 (%)

Equipos que alojan troyanos bancarios y rogueware (%)	2009	2010	Evolución
Troyanos	35,6%	39,8%	▲
Rogueware	n.d.	5,8%	
Troyanos bancarios	6,3%	6,8%	▶

Fuente: INTECO

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

En el Gráfico 10 se analizan los hábitos prudentes relacionados con la banca y el comercio a través de la Red, comparando los resultados entre los usuarios que no han sufrido perjuicio económico derivado de fraude y los que sí.

Los usuarios que han sufrido pérdidas económicas adoptan mayoritariamente hábitos como cerrar la sesión al terminar (87,1%), comprobar del uso de conexiones seguras en las transacciones online (78,3%), evitar la utilización de equipos públicos o compartidos (76,3%) y vigilar periódicamente los movimientos de la cuenta bancaria online (73,5%).

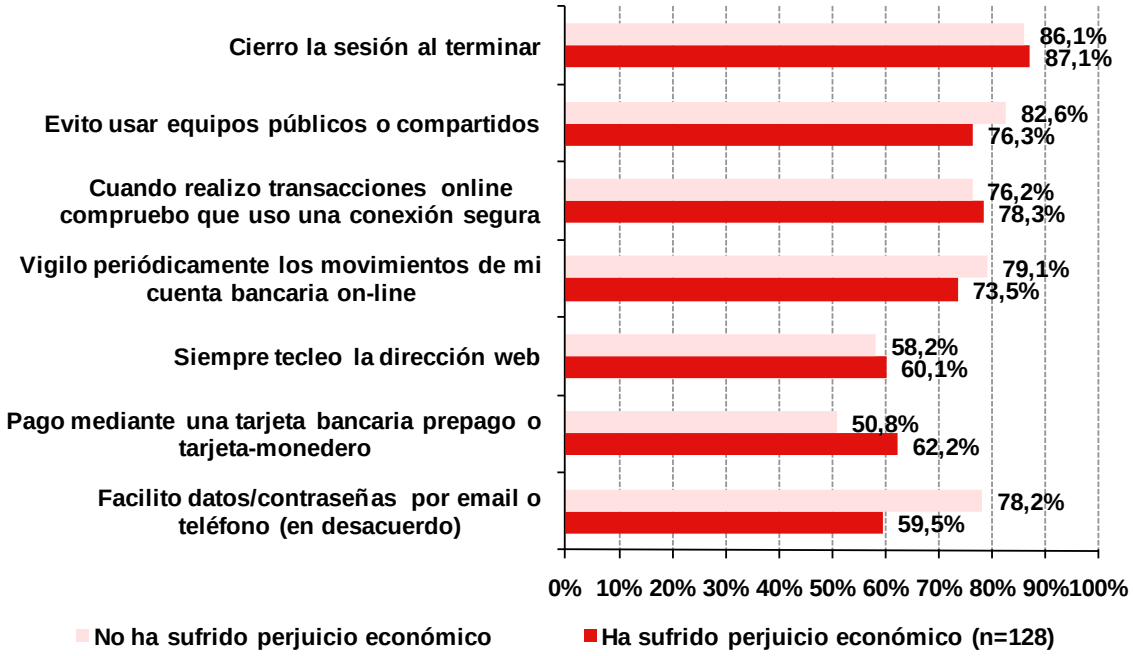
Por su parte, aquellos usuarios que declaran no haber registrado una pérdida derivada de fraude realizan en mayor medida los siguientes comportamientos prudentes: cierro sesión al terminar (86,1%), evito usar equipos públicos o compartidos (82,6%), vigilo los movimientos de mi cuenta en línea (79,1%), facilito datos/contraseñas por email o teléfono (en desacuerdo) (78,2%) y compruebo que la conexión es segura al realizar operaciones en línea (76,2%).

En general, no existen diferencias relevantes en la adopción de hábitos prudentes entre aquellos que han tenido un impacto en su economía y los que no. La mayor diferencia se observa en la afirmación *Facilito datos/contraseñas por email o teléfono (en desacuerdo),* más adoptada por los usuarios que no han sufrido perjuicio económico (78,2%) que por los que sí lo han tenido (59,5%). Destaca también la diferencia en el hábito *Pago mediante una tarjeta bancaria prepago o tarjeta-monedero*, en este caso realizado en

[13] Ver nota al pie 7.

mayor medida por los usuarios que declaran perjuicio económico (62,2%), que los que no (50,8%).

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=3.289) *Fuente: INTECO*

En el Gráfico 11 se representa 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.

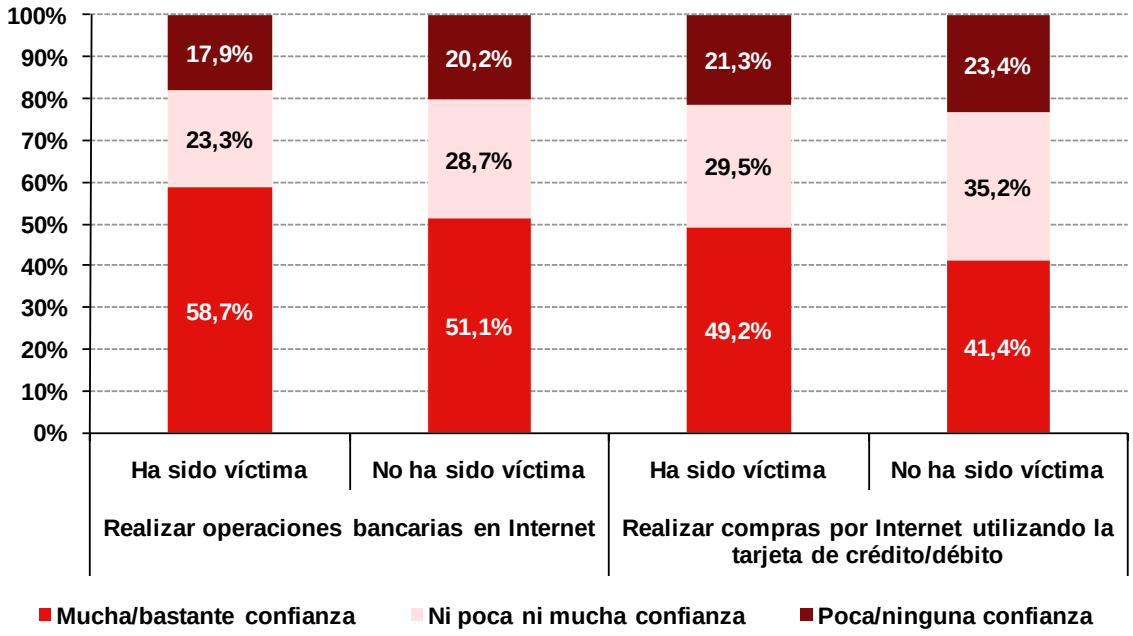
En el cuarto trimestre de 2010, los usuarios muestran un buen nivel de confianza en Internet como medio para realizar compras y transferencias bancarias.

- Un 58,7% de quienes han sido víctimas de un intento de fraude confían mucho o bastante en las operaciones bancarias en Internet y un 49,2% en las compras online con tarjeta de crédito/débito.

- En el caso de los que no han sufrido un intento de ataque fraudulento, un 51,1% deposita mucha y bastante confianza en la banca en línea y un 41,4% en la compra-venta en la Red.

La mayor confianza de los usuarios del primer grupo puede deberse a que estos son navegantes más “intensivos” y por tanto usan más estos servicios y sufren más intentos de fraude.

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 (%)

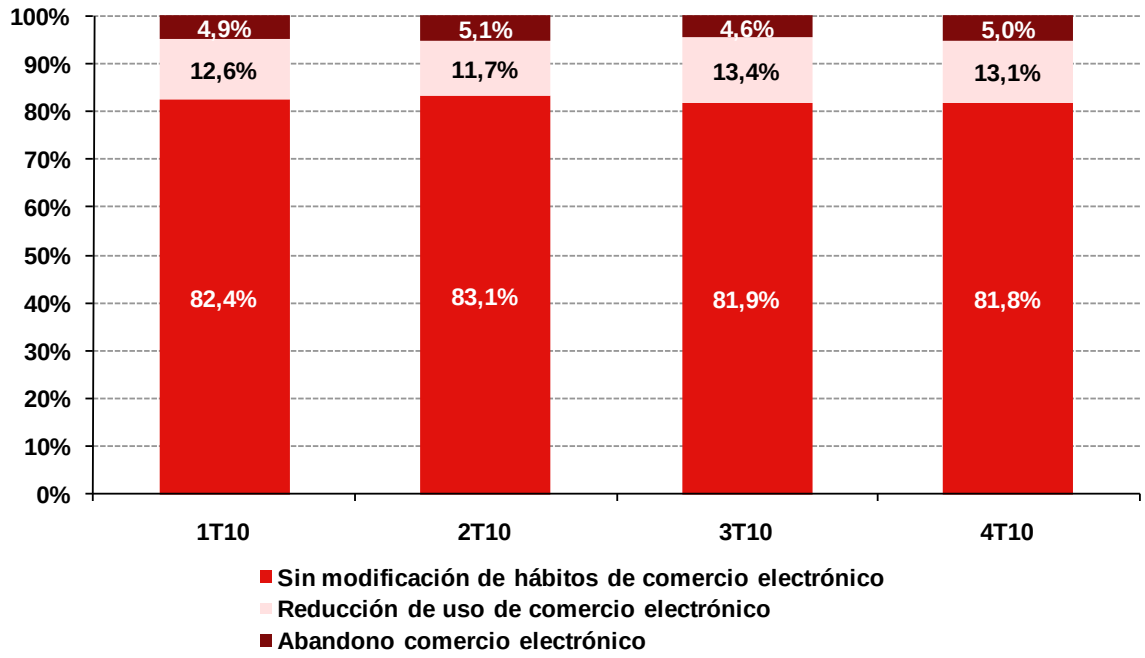


Base: Usuarios que utilizan comercio electrónico y/o banca en línea (n=3.289) *Fuente: INTECO*

En el caso de la utilización de servicios de comercio electrónico, los usuarios que sufren un intento de fraude (no consumado) muestran fidelidad en sus hábitos después de sufrir el incidente. Un 81,8% no modifican el uso, frente a un 5% que abandonan esta actividad y un 13,1% que reducen su utilización.

Los valores a lo largo de 2010 se muestran muy estables, lo que puede deberse a que los usuarios, a pesar de ser víctimas de situaciones de fraude, consideran estos servicios online como imprescindibles, por lo que no abandonan su uso.

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



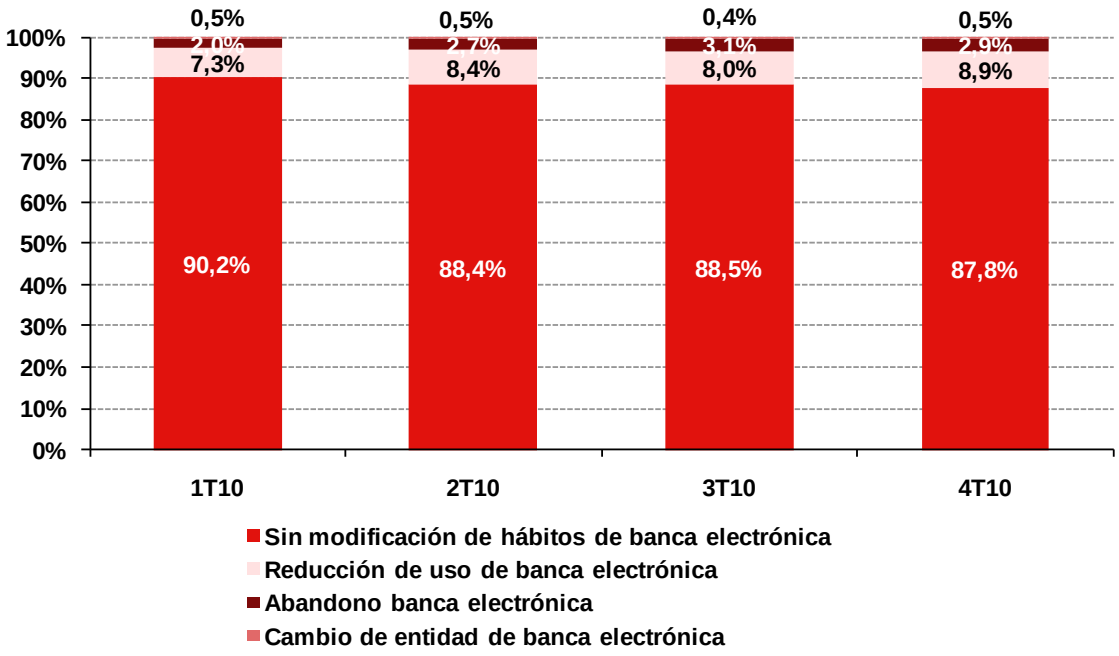
Base: Usuarios que han sufrido algún intento de fraude y/o un perjuicio económico (n=1.950)

Fuente: INTECO

Los comportamientos son muy similares en el caso de los servicios bancarios online. De los usuarios que son víctimas de una situación de este tipo, sólo un 2,9% abandona la utilización de estos servicios después del incidente y un 0,5% cambia de entidad de banca online. Frente a estos usuarios, un 87,8% no modifican el uso de estos servicios y un 8,9% reducen su uso.

En este caso los valores también muestran bastante constancia en su evolución.

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=1.950)

Fuente: INTECO

Por último, se incluye la Tabla 8 relativa a la comparación de los datos obtenidos a finales de 2009 y en el mismo periodo de 2010. En el último año, destaca la reducción en 2,2 puntos porcentuales en la proporción de usuarios que no modifican sus hábitos de comercio electrónico tras sufrir un incidente de fraude (no consumado), mientras que se incrementa casi en la misma medida aquellos que reducen su uso (2 puntos porcentuales). Esta situación es muy similar a la experimentada en la utilización de servicios de banca online tras ser víctima de un intento de fraude.

Tabla 8: Evolución de la modificación de hábitos tras sufrir un intento (no consumado) de fraude entre 2009 y 2010 (%)

Modificación de hábitos tras sufrir un intento (no consumado) de fraude (%)		2009	2010	Evolución
Comercio electrónico	Sin modificación de hábitos	84,0%	81,8%	▼
	Reducción del uso	11,1%	13,1%	▲
	Abandono	5,0%	5,0%	▶
Banca electrónica	Sin modificación de hábitos	89,4%	87,8%	▼
	Reducción del uso	7,4%	8,9%	▲
	Abandono	2,7%	2,9%	▶
	Cambio de entidad de banca electrónica	0,5%	0,5%	▶

Fuente: INTECO

4. CONCLUSIONES Y RECOMENDACIONES

4.1. Conclusiones del análisis

En el último trimestre de 2010, así como en el conjunto anual, los internautas que afirman haber sido víctima de intento (no necesariamente consumado) de fraude online en los últimos tres meses superan ligeramente a los que niegan haber sufrido una estafa de este tipo.

Los atacantes utilizan diversas técnicas de ingeniería social para cometer fraude, mayoritariamente a través de la Red, aunque con previsiones de una incidencia cada vez mayor en el teléfono móvil. Esto se debe a la gran extensión de dispositivos móviles con conexión a la Red en el último año y el consiguiente abaratamiento del coste de las comunicaciones de la telefonía móvil convencional.

Los análisis empíricos muestran que 4 de cada 10 equipos sufren una infección por troyanos al cierre de 2010. Los datos muestran una mayor incidencia en la segunda mitad del año, dato que está en línea con la información proporcionada por la industria de seguridad[14], que caracteriza el año 2010 como un punto de inflexión en la seguridad de la información, a partir del cual los ataques conocidos hasta el momento van a intensificarse en número y, sobre todo, en complejidad y gravedad.

El tipo de troyanos específicamente dirigido al robo de credenciales bancarias ha mostrado una tendencia decreciente a lo largo del año, hasta terminar en mínimos históricos. En cambio, en el segundo trimestre de 2010 se incorporó al análisis el tipo de troyano conocido como rogueware y la evolución que ha experimentado en los últimos nueve meses apunta a que puede ser una amenaza al alza de cara a 2011.

Trimestre tras trimestre, los usuarios reafirman la confianza que depositan en los servicios de banca online y comercio electrónico, aun cuando hayan sufrido un intento de fraude. Resulta especialmente interesante la elevada fidelización por la banca online, a pesar de ser la principal "máscara" adoptada por los ciberestafadores en sus comunicaciones.

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

Las entidades bancarias y los servicios de comercio electrónico son los principales remitentes de los correos sospechosos de ser fraudulentos. Esto puede deberse, tal vez, a que estas entidades son las que más confianza ofrecen a los usuarios, y por eso los

[14] Fuente: *Informe anual de fraude online y cibercrimen 2010*. S21sec. 2011. Disponible en: http://www.s21sec.com/default.aspx

atacantes perfeccionan los ataquen a través de estos canales para que resulten más creíbles para las víctimas.

¿Cuánto impacto económico ha causado el fraude?

En el último trimestre de 2010, casi dos de cada tres usuarios que ha sufrido un impacto económico como consecuencia de un intento de fraude afirman que la cantidad estaba por debajo de los 200 €. A pesar del repunte experimentado en el tercer trimestre del año en la proporción de usuarios afectados económicamente, en el que se supera la barrera del 5%, el último dato del año vuelve a estar por debajo de ese umbral.

¿Qué datos ofrecen los análisis empíricos?

Los escaneos realizados a través de la herramienta iScan indican que en la segunda mitad de 2010 se observa un ligero incremento en los valores, hasta alcanzar en diciembre el porcentaje de 39,8% de equipos infectados por troyanos. En el conjunto del año, la subida es de casi 5 puntos porcentuales.

Atendiendo a la tipología de troyanos, el porcentaje de troyanos bancarios confirma una tendencia de descenso paulatino (3,9 puntos porcentuales menos que a comienzos del año, hasta un 6,8% en diciembre de 2010), mientras que asciende la proporción de equipos que alojan rogueware (de un 3,6% en abril a un 5,8% en el último mes del año). Este incremento puede deberse a que los atacantes están obteniendo un importante rédito al crear este tipo de malware y que esto les lleva a su producción masiva, mejorando las muestras.

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

Haber sufrido un intento de fraude no es sinónimo de pérdida de confianza y, en este sentido, los usuarios cada vez muestran más respaldo a los servicios en línea. Un 58,7% de los usuarios que han sido víctimas de fraude declaran que realizar operaciones bancarias en Internet les genera mucha y bastante confianza y el porcentaje alcanza un 49,2% en el caso de las compras por Internet utilizando la tarjeta de crédito/débito. Aquellos que no han sufrido un incidente de este tipo muestran valores de confianza ligeramente inferiores a los anteriores.

Por último, los hábitos de los usuarios apenas se modifican tras haber sufrido un intento de fraude y, tanto en el caso de la realización de operaciones bancarias online como en el caso de la compra y venta a través de la Red, la gran mayoría de los usuarios no abandonan estos servicios, con valores muy similares a los de trimestres anteriores.

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

ÍNDICE DE TABLAS

INTECO

Instituto Nacional
de Tecnologías
de la Comunicación

http://www.inteco.es

OBSERVATORIO INTECO

http://observatorio.inteco.es

	ObservaINTECO en Facebook		ObservaINTECO en Twitter
BLOG	Blog de ObservaINTECO		ObservaINTECO en Youtube
	ObservaINTECO en Scribd		ObservatINTECO en SlideShare
	Contenidos RSS		observatorio@inteco.es