



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

3^{er} trimestre de 2010



Edición: Enero 2011

El “Estudio sobre el fraude a través de Internet (3^{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 (dirección)

Cristina Gutiérrez Borge (coordinación)

Susana de la Fuente Rodríguez

Laura García Pérez

Eduardo Álvarez Alonso

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

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 Accesibilidad > Formación > Manuales y Guías de la página <http://www.inteco.es>

ÍNDICE

PUNTOS CLAVE	4
I Seguridad y fraude online	4
1 INTRODUCCIÓN Y OBJETIVOS	6
1.1 Presentación	6
1.2 Estudio sobre el fraude a través de Internet	8
1. DISEÑO METODOLÓGICO	9
1.3 Universo	9
1.4 Tamaño y distribución muestral	9
1.5 Captura de información y trabajo de campo	11
1.6 Error muestral	14
2 SEGURIDAD Y FRAUDE ONLINE	15
2.1 Intento de fraude y manifestaciones	15
2.2 Forma adoptada por el remitente origen de la comunicación sospechosa de ser fraudulenta	18
2.3 Impacto económico del fraude	19
2.4 Fraude y malware	22
2.5 Influencia del intento de fraude en los hábitos relacionados con la banca a través de Internet y el comercio electrónico	24
3 CONCLUSIONES Y RECOMENDACIONES	29
3.1 Conclusiones del análisis	29
3.2 Recomendaciones	30
ÍNDICE DE GRÁFICOS	32
ÍNDICE DE TABLAS	33

PUNTOS CLAVE

El Observatorio de la Seguridad de la Información publica el *Estudio sobre el fraude a través de Internet (3^{er} trimestre de 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 julio a septiembre de 2010. Durante este tiempo se han realizado 3.538 encuestas y 8.836 análisis online a los 7.351 equipos que componen el panel.

Se exponen a continuación los puntos clave del estudio.

I Seguridad y fraude online

En el tercer trimestre de 2010, un 53,1% de los usuarios de Internet españoles declara haber sufrido alguna situación de intento de fraude (no consumado) a través de Internet o del teléfono móvil. En ambos casos, los atacantes utilizan diferentes técnicas de ingeniería social para intentar consumir una estafa.

A través de la Red, los usuarios reciben en mayor proporción peticiones para visitar alguna página web sospechosa (un 33,2%), seguidas de la recepción de emails ofertando un servicio no solicitado (un 27,3%), una oferta de trabajo falsa (un 24,2%) o un correo electrónico solicitando claves de usuario (un 18,4%).

Con respecto al intento de fraude mediante el teléfono móvil, un 8% de los encuestados declara haber recibido mensajes cortos de texto ofertando un servicio no requerido. Menos numerosas son las incidencias que tienen que ver con la solicitud de las claves de usuario a través del teléfono móvil, tanto a través de una llamada (3,6%) como a través de un SMS (1,9%).

Los atacantes adoptan la forma de supuestas entidades bancarias o financieras (un 43,2%) y páginas web de compra-venta online (38,7%).

Los usuarios que sufren perjuicio económico debido a un intento de fraude en el 3^{er} trimestre de 2010 son minoritarios (el 5,1%), frente a un 94,9% que declara no haber percibido ningún impacto en su economía. Dentro del primer grupo, se analiza el importe defraudado, teniendo en cuenta que 400 euros es la cuantía que la Ley establece para distinguir entre falta y delito. En los casos en los que el fraude llega a consumarse, la cuantía económica es pequeña: inferior a 400 euros en el 80,6% de los casos y por debajo de 100 euros en el 42,8%. Ello a pesar de que este trimestre hayan aumentado las víctimas que han perdido más de 400 euros.

El escaneo de los equipos arroja en septiembre de 2010 el dato de un 38,7% de equipos que alojan troyanos, categoría de malware que en ocasiones es utilizada para el robo de información y por tanto, efectiva para el fraude. A su vez, los troyanos bancarios están presentes en el 7% de los equipos y el rogueware¹ en un 5,8%. La evolución histórica muestra un incremento en la proporción de equipos que alojan troyanos, alcanzando valores máximos en la serie, superiores al 38%. En el caso de los troyanos bancarios, parece confirmarse la estabilidad de la tendencia, mientras que el rogue malware se incrementa con respecto al trimestre anterior (primer periodo en el que se analiza), acercándose a los valores actuales de los troyanos bancarios.

Los usuarios muestran un buen nivel de confianza en Internet como medio para realizar compras y transacciones bancarias. Los internautas que han sido víctimas de intento de fraude y/o han sufrido perjuicio económico declaran mayor fidelidad (58,6% en las operaciones bancarias en Internet y un 51% en la compra-venta online) que los que no lo han sido (con un 51,1% y un 44,5% respectivamente).

Para cerrar el presente informe, los usuarios son fieles a sus hábitos de compra y banca electrónica tras haber sido víctimas de intento de fraude. Un 81,9% de los encuestados declara no cambiar sus hábitos de comercio electrónico. Y con respecto a la banca a través de Internet, el porcentaje de usuarios que no modifican sus hábitos se sitúa en un 88,5%. Esta tendencia es constante en el tiempo.

¹ 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.

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 5ª entrega del mismo.

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

Se muestra también la influencia del intento de fraude en la modificación de los hábitos de los usuarios a la hora de utilizar el comercio electrónico y la banca en línea y la e-confianza que les genera estos hábitos tras sufrir un intento de fraude.

1. DISEÑO METODOLÓGICO

El *Estudio sobre el fraude a través de Internet (3er 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. En la actualidad el panel está compuesto por 7.351 hogares con conexión a Internet repartidos por todo el territorio nacional. 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.

1.3 Universo

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

1.4 Tamaño y distribución muestral

La afijación muestral responde a un modelo polietápico:

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

- Muestreo por cuotas de tamaño del hogar, edad, sexo, actividad laboral y tamaño del hábitat².

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
2 ^o trimestre 2010	3.519
3 ^{er} trimestre 2010	3.538

Fuente: INTECO

² Estas cuotas se han obtenido de datos representativos a nivel nacional de usuarios de Internet mayores de 15 años que se conectan más de una vez al mes desde el hogar facilitados por Red.es, entidad pública empresarial del Ministerio de Industria, Turismo y Comercio. (Las TIC en los hogares españoles: 26ª oleada octubre-diciembre 2009)

Tabla 2: Número de equipos escaneados mensualmente

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

Fuente: INTECO

1.5 Captura de información y trabajo de campo

El trabajo de campo ha sido realizado entre julio y septiembre 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 goodware³ demostraron ser altamente paranoicos.*
- b. *Eliminación de ciertas soluciones que comparten firmas, para sólo considerar un motor con el mismo conjunto de firmas.*
- c. *Creación de un subconjunto de motores. Se han tomado los 11 antivirus más reputados (con mejor tasa de detección frente a especímenes detectados por más de 10 antivirus) para crear un subconjunto de productos que será referenciado como motores necesariamente exigidos. De este modo, para que un fichero sea marcado como malware, deberá ser detectado por 5 productos de los 46 considerados y, además, al menos uno de ellos deberá ser alguno de estos 11 motores exigidos.*

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

INTECO mantiene una base de datos de software de fabricantes confiables y de freeware⁴ y shareware⁵ 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.

³ Software y ficheros legítimos, archivos inocuos.

⁴ Software gratuito.

⁵ Software de descarga gratuita pero limitado en funcionalidad o tiempo de uso.

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

Eliminación de detecciones concretas y corrección de categorías incorrectamente determinadas

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

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

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

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

1.6 Error muestral

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

Tabla 3: Errores muestrales de las encuestas (%)

Período	Tamaño muestral	Error muestral
1 ^{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	$\pm 1,66\%$
2 ^o trimestre 2010	3.519	$\pm 1,68\%$
3 ^{er} trimestre 2010	3.538	$\pm 1,68\%$

Fuente: INTECO

2 SEGURIDAD Y FRAUDE ONLINE

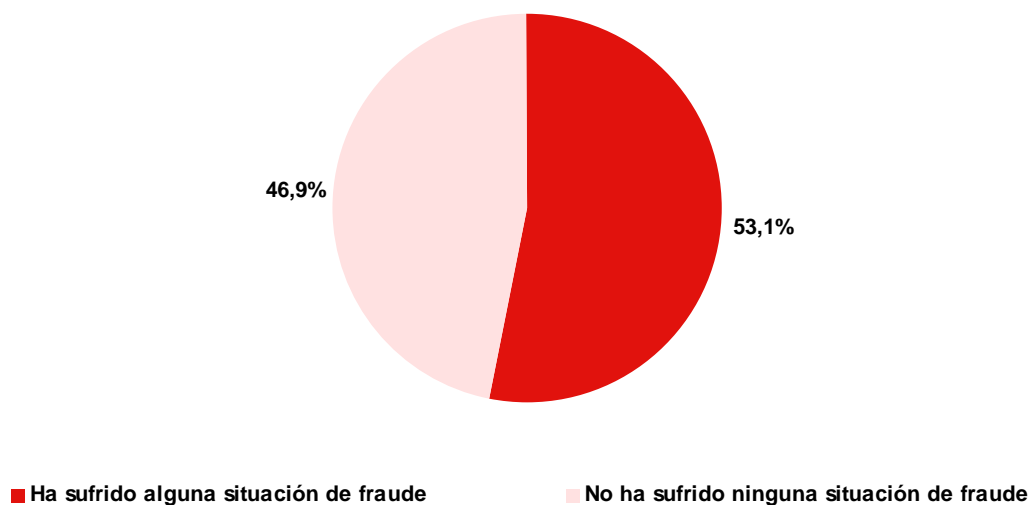
2.1 Intento de fraude y manifestaciones

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.

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 tercer trimestre de 2010, algo más de la mitad de los usuarios encuestados (53,1%) ha sido víctima de alguna situación de este tipo, mientras que el 46,9% no ha percibido incidencia alguna.

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=3.538 en 3T10)

Fuente: INTECO

En segundo lugar se muestra la incidencia que perciben los usuarios de situaciones de fraude a través de Internet. La perspectiva evolutiva de los valores se puede apreciar en el Gráfico 2.

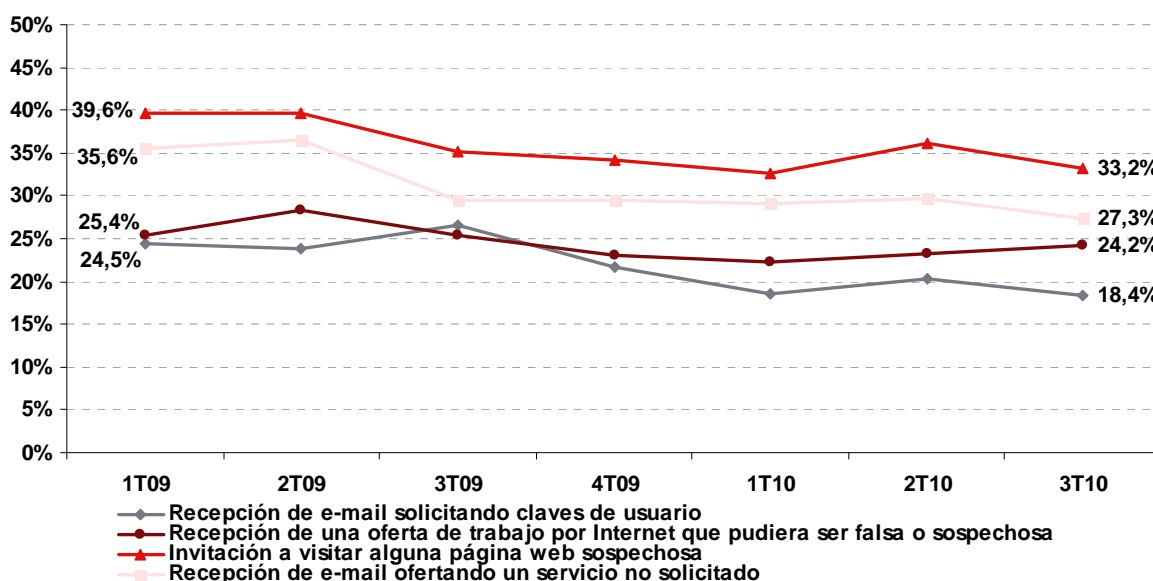
En los últimos tres meses, las invitaciones para visitar alguna página web sospechosa son las incidencias de intento de fraude (no consumado) más declaradas por los encuestados (un 33,2% así lo declara), seguidas de la recepción de correos electrónicos ofertando servicios no solicitados (un 27,3%) y la recepción de ofertas de trabajo falsas

(un 24,2%). Por último, un 18,4% de los internautas declara haber recibido un correo electrónico solicitando claves de usuario.

Atendiendo a la evolución de los datos, se aprecia que la tendencia general a lo largo de la serie es de signo negativo. Con respecto al trimestre anterior, en el que hubo un ligero incremento en todos los valores, en el tercer trimestre de 2010 únicamente la recepción de una oferta de trabajo a través de Internet registra una leve subida (1 punto porcentual). El resto de valores experimentan descensos, destacando en este sentido la invitación a visitar alguna página web sospechosa, con 3,1 puntos porcentuales menos que en el trimestre anterior.

Estos descensos pueden estar relacionados con una importante operación contra el spam que tuvo lugar durante el periodo analizado en este informe. A mediados de septiembre, las operaciones de spamit.com fueron cerradas. Se trata de un grupo muy conocido que trabajaba con spammers y botnets para proporcionar las infraestructuras y recursos necesarios para gestionar las ganancias de los negocios publicitados. Por tanto, se trataba de un sistema underground que, asociado con los spammers, conseguía gestionar los negocios anunciados en correos basura. En concreto spamit.com era responsable de gran parte de los conocidos anuncios de "Canadian Pharmacy", esto es, farmacias que venden sin receta y a precios bajos productos como Viagra, Xanax, etc. La desaparición de spamit.com 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.

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=3.538 en 3T10)

Fuente: INTECO

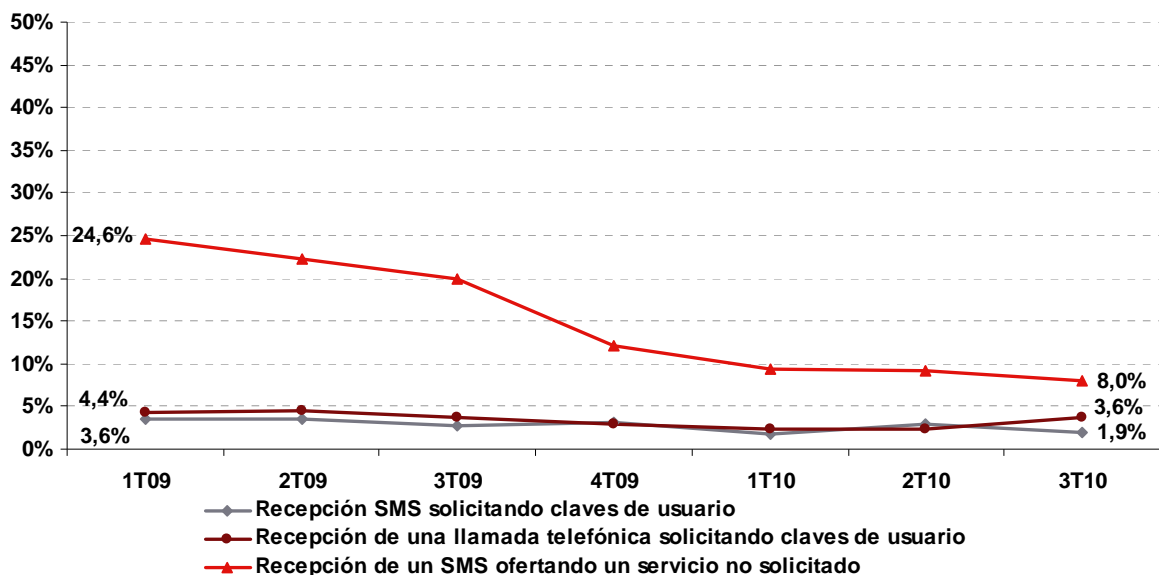
A continuación se estudia la incidencia de situaciones de fraude declarada por los encuestados, en este caso a través del teléfono móvil, presentándose en el Gráfico 3 la evolución de los valores.

Un 8% de los encuestados ha recibido mensajes cortos de texto ofertando servicios no solicitados. Con valores más reducidos, los usuarios declaran ser los destinatarios de comunicaciones que solicitan sus claves de usuario, bien a través de una llamada telefónica (un 3,6%), bien a través de un mensaje de texto (1,9%).

Desde el primer trimestre de 2009 se observa, en general, un descenso continuado en todos los valores. La caída más acusada (16,6 puntos porcentuales) se produce en el caso de la recepción de un SMS ofertando servicios no solicitados, mientras que el resto de casos, las bajadas son más moderadas a lo largo del tiempo.

Como se señalaba en el *Informe sobre el fraude a través de Internet* del 2º trimestre 2010, el gasto que supone para el atacante la realización de llamadas telefónicas o el envío de mensajes de texto puede ser el motivo para que la incidencia de situaciones de intento de fraude a través del teléfono móvil sea menor. No obstante, la generalización de servicios de comunicaciones móviles a través de Internet, o servicios de VoIP, más baratos o gratuitos, puede alterar el signo de esta tendencia.

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=3.538 en 3T10)

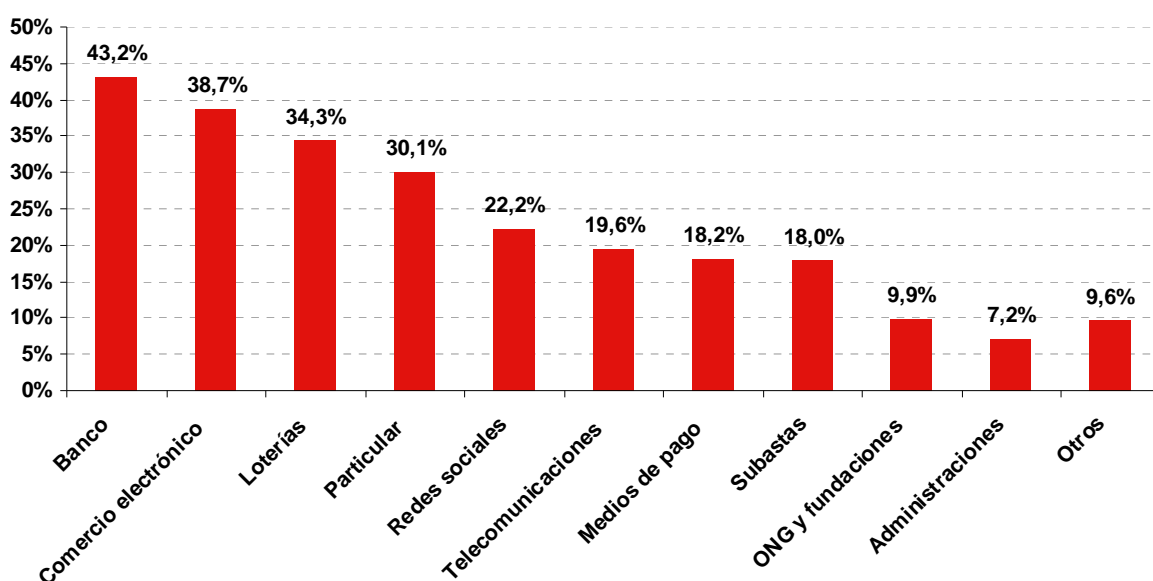
Fuente: INTECO

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

Como muestra el Gráfico 4, los atacantes intentan defraudar a través de comunicaciones sospechosas que simulan proceder de diferentes remitentes. En el trimestre actual, la banca online (43,2%) y comercio electrónico (38,7%) son las principales “máscaras” utilizadas.

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 1º trimestre de 2010, señala al sector financiero y a los servicios de pago como principales objetivos de los ciberestafadores⁶

Gráfico 4: Formas adoptadas por el remitente de la comunicación sospechosa de ser fraudulenta⁷ (%)



Base: Usuarios que han sufrido algún intento de fraude (n=1.905)

Fuente: INTECO

El análisis de la evolución de las formas adoptadas por el remitente de la comunicación sospechosa de ser fraudulenta (Tabla 4) 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.

⁶ Anti-Phishing Working Group (APWG) (2010). Disponible en: http://www.antiphishing.org/reports/apwg_report_Q1_2010.pdf.

⁷ 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.

En cuanto al resto de formatos utilizados, este trimestre sigue incrementándose el porcentaje de comunicaciones en las que el atacante se presenta como particular con algún pretexto de contacto con la víctima, con un 30,1%. Esta forma ha experimentado la mayor subida desde el primer trimestre de 2009, cuando el dato se situaba en el 11,9%.

Por último, destaca igualmente el incremento experimentado por la forma “Otros”, de 3,1 puntos porcentuales con respecto al 2º trimestre de 2010 y de 6,5 puntos desde el inicio de la serie. Este incremento puede ser debido a la constante búsqueda de nuevas fórmulas por parte de los atacantes.

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

Forma adoptada ⁸	1T 2009	2T 2009	3T 2009	4T 2009	1T 2010	2T 2010	3T 2010
Banco	37,5	39,0	44,4	43,1	39,9	41,8	43,2
Comercio electrónico	31,9	35,8	29,3	41,9	43,9	42,2	38,7
Loterías	35,5	38,4	33,7	39,0	37,2	36,4	34,3
Particular	11,9	11,4	11,2	23,8	25,7	29,3	30,1
Redes sociales	23,9	24,1	20,7	21,3	23,9	23,7	22,2
Telecomunicaciones	25,0	23,8	21,8	21,4	21,3	19,7	19,6
Medios de pago	15,0	17,0	18,6	23,1	21,1	21,7	18,2
Subastas	17,9	19,2	16,5	20,9	19,2	17,1	18,0
ONG y fundaciones	6,4	7,4	6,5	8,3	7,9	9,0	9,9
Administraciones	3,5	3,8	6,4	9,1	6,2	8,1	7,2
Otros	3,1	3,9	3,3	5,1	7,7	6,5	9,6

Fuente: INTECO

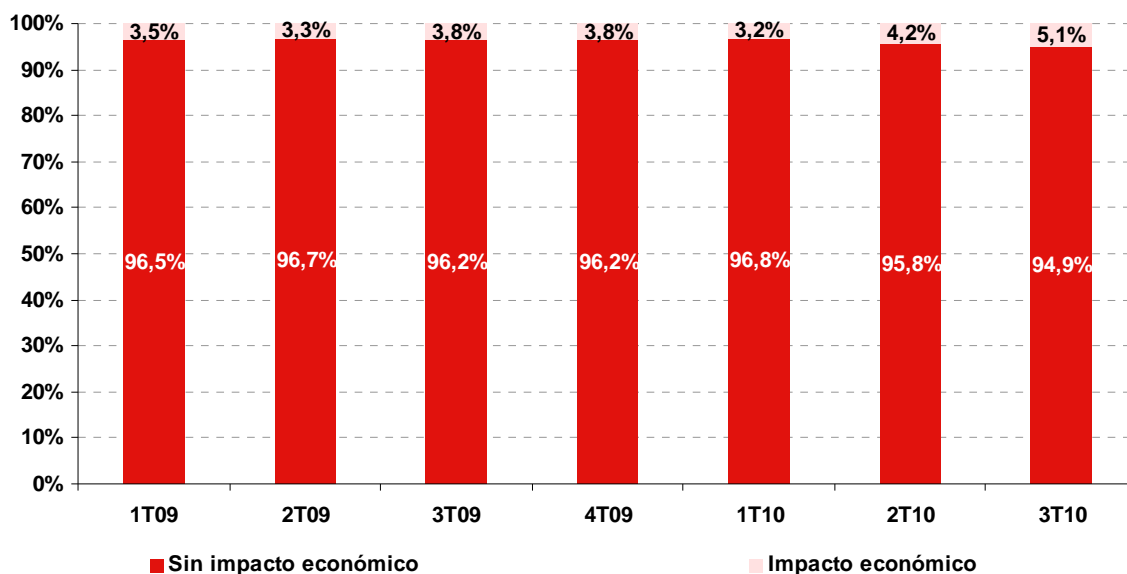
2.3 Impacto económico del fraude

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

El Gráfico 5 muestra el fraude con impacto económico efectivo para el usuario, con los datos de los últimos siete trimestres. En el tercer trimestre de 2010, el 94,9% de los usuarios declara no haber sufrido perjuicio económico a consecuencia de un intento de fraude, frente a un 5,1% que sí han tenido impacto pecuniario. A pesar de haberse incrementado ligeramente el porcentaje de los que han sufrido una pérdida económica (1,9 puntos porcentuales desde el primer trimestre de 2010), la evolución presenta datos muy estables a lo largo de la serie.

⁸ Aparece sombreada la principal forma adoptada para cada trimestre.

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



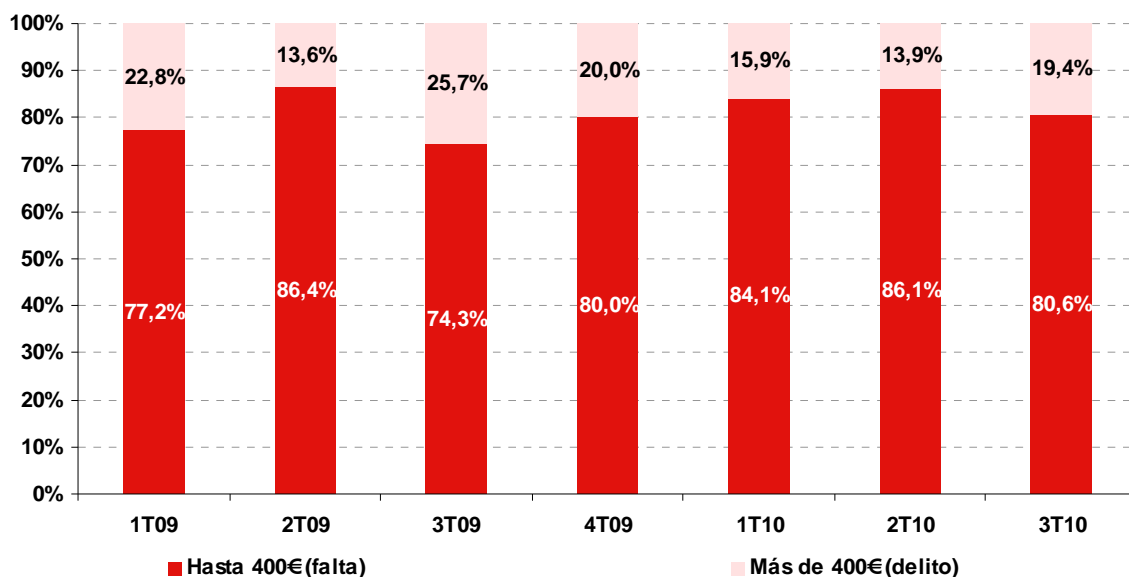
Base: Total usuarios (n=3.538 en 3T10)

Fuente: INTECO

En cuanto a la cuantía defraudada, en este trimestre el 80,6% de los que han sufrido fraude con perjuicio económico declara que la cantidad afectada es inferior a 400 euros, mientras que el 19,4% ha perdido una cantidad superior a esa cifra. Esta cantidad de referencia es la establecida por la Ley como límite a la hora de considerar falta (menos de 400 euros) o delito (más de 400 euros).

La evolución muestra valores relativamente estables, siendo mayoría los usuarios cuya cuantía defraudada es pequeña (datos por encima del 75% a lo largo de los trimestres). Ello a pesar de que en el último trimestre hayan aumentado las víctimas que han perdido una cantidad superior a 400 euros.

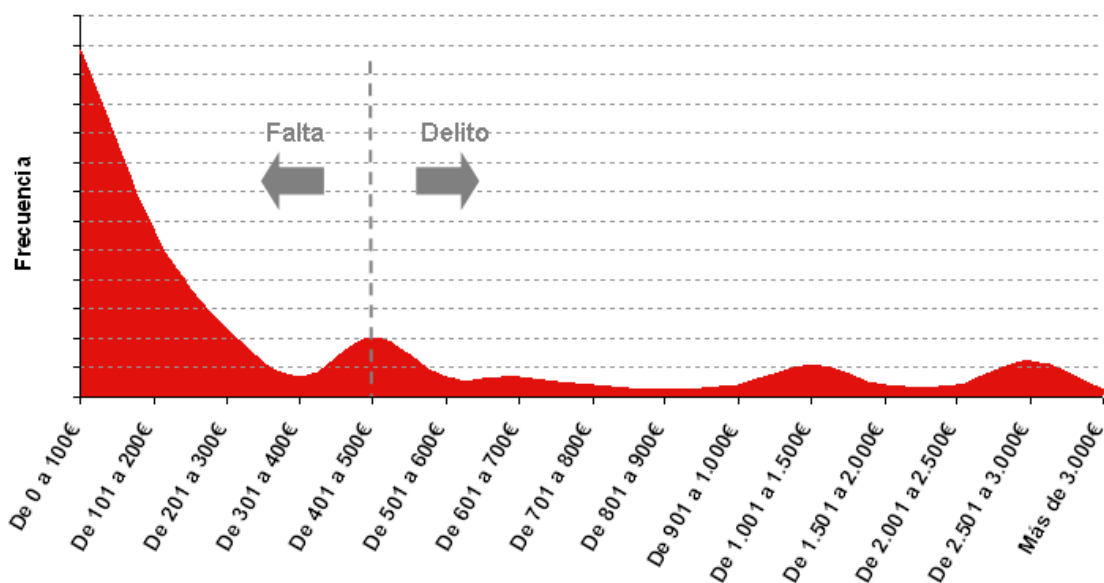
Gráfico 6: Evolución de la cuantía económica derivada del fraude (%)



Base: Usuarios que han sufrido perjuicio económico como consecuencia de un fraude online (n=138 en 3T10)
Fuente: INTECO

Atendiendo a la distribución del importe defraudado, en el tercer trimestre de 2010 casi dos de cada tres usuarios afectados (de un total de 138) declaran que la cantidad estafada era inferior a los 200 euros y un 42,8% que este importe está por debajo de los 100 euros.

Gráfico 7: Distribución del importe defraudado en el 3T 2010



Base: Usuarios que han sufrido perjuicio económico como consecuencia de un fraude online (n=138)
Fuente: INTECO

2.4 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 online⁹.

Para realizar el estudio, se han considerado las siguientes familias de troyanos bancarios más populares que efectúan ataques dirigidos contra entidades bancarias¹⁰.

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

- 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

⁹ Fuente: glosario técnico PANDA SECURITY.

¹⁰ 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.

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.

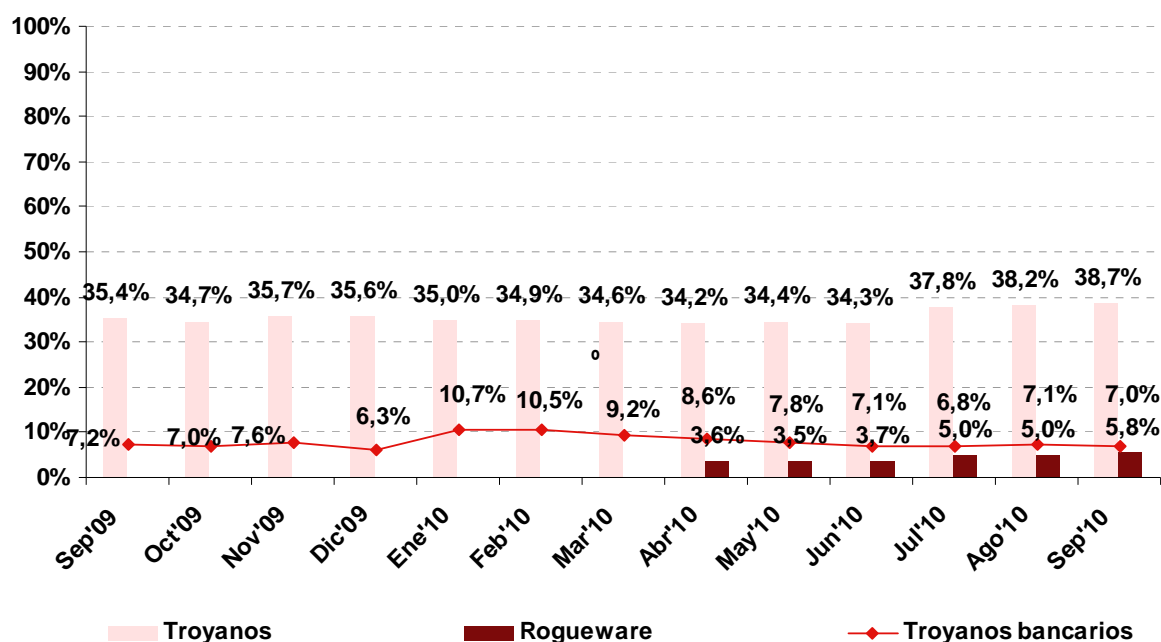
Como muestra el Gráfico 8, en septiembre de 2010 un 38,7% de los equipos analizados alojan troyanos, un 7% alojan troyanos bancarios y un 5,8% sufre una infección por rogueware.

Atendiendo a la evolución histórica de los valores, la tendencia de equipos que alojan troyanos (no específicamente dedicados al robo de credenciales bancarias) se muestra bastante estable en el tiempo.

En el caso de los equipos infectados por troyanos bancarios, parece confirmarse de nuevo la constancia en los valores (un 7% en septiembre de 2010), tras el repunte experimentado a principios de 2010, cuando alcanzó el 10,7%.

En el segundo trimestre que incluye el análisis de los equipos que alojan rogueware se observa un ligero incremento de los valores con respecto a los registrados en los tres meses anteriores (en junio de 2010 este dato era un 3,7%, frente al 5,8% del último mes analizado).

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



Fuente: INTECO

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

En el Gráfico 9 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.

De los siete comportamientos señalados, los cuatro primeros son adoptados mayoritariamente por los usuarios, con valores superiores al 75% en todos los casos y sin apreciarse diferencias relevantes entre aquellos que han sufrido pérdidas económicas y los que no.

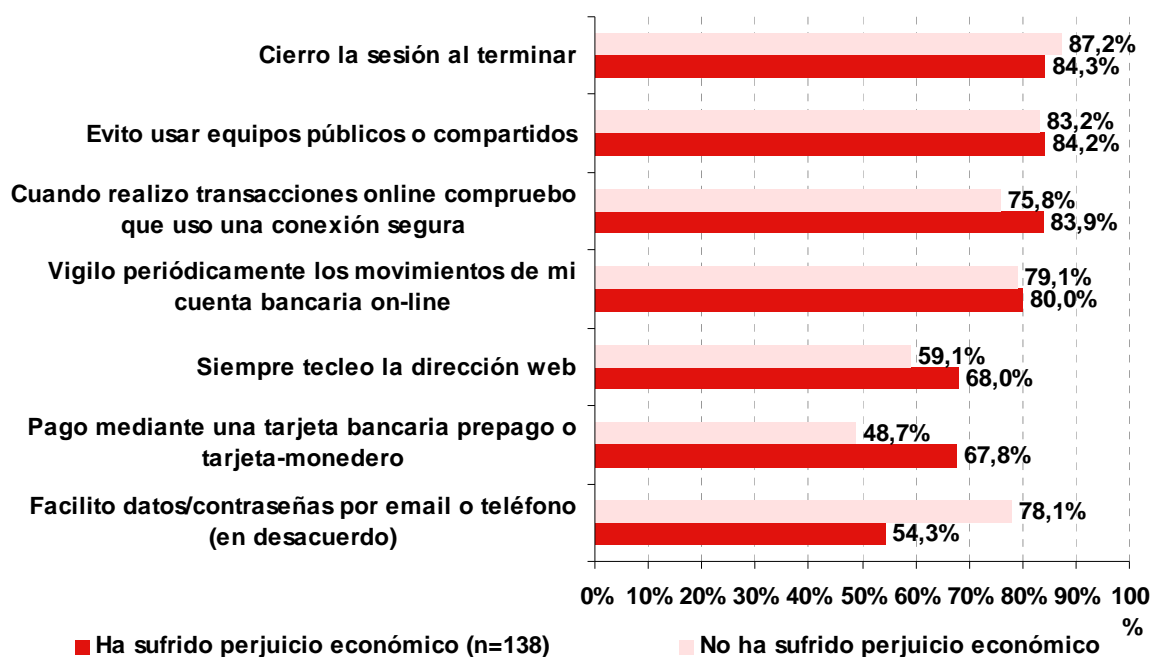
En cuanto a los tres últimos hábitos de la relación, estos son menos adoptados en términos generales. Se observa cómo algunos de estos comportamientos prudentes han sido adoptados en mayor medida por los usuarios que han sido estafados, y otros en cambio, por aquellos que no. En este sentido, cabe señalar:

- Siempre tecleo la dirección web: este hábito prudente es más seguido por los usuarios que declaran haber sufrido perjuicio económico el 68%, frente al 59,1% de los que no.
- Pago mediante tarjeta bancaria prepago o tarjeta-monedero: de los usuarios que registraron pérdidas a consecuencia del fraude, el 67,8% utiliza estos medios de pago, frente al 48,7% de los usuarios que no tuvieron ese impacto en su

economía. Tanto en este caso como en el anterior, haber sido víctima de un perjuicio económico implica mayor prudencia a la hora de utilizar servicios de banca online o comercio electrónico.

- Facilito datos/contraseñas por email o teléfono (en desacuerdo): un 78,1% de los que no han experimentado pérdidas económicas declaran estar en desacuerdo con esta afirmación, frente a un 54,3% de los que sí. En este caso, no se cumple la misma relación que en los dos anteriores y son los encuestados que no han sufrido perjuicio económico quienes adoptan este hábito mayoritariamente.

Gráfico 9: 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=3.248)

Fuente: INTECO

En el Gráfico 10 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.

Los usuarios muestran un buen nivel de confianza en Internet como medio para realizar compras y transferencias bancarias.

- Un 58,6% de los usuarios que han sufrido intento de fraude confían mucho o bastante en las operaciones bancarias en Internet y un 51% en las compras online con tarjeta de crédito.

- En el caso de los que no han sido víctimas, un 51,1% deposita mucha y bastante confianza en la banca en línea y un 44,5% en la compra-venta en la Red.

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

Gráfico 10: Nivel de confianza entre los usuarios que han sido víctima de intento de fraude y/o haber sufrido perjuicio económico y los que no (%)



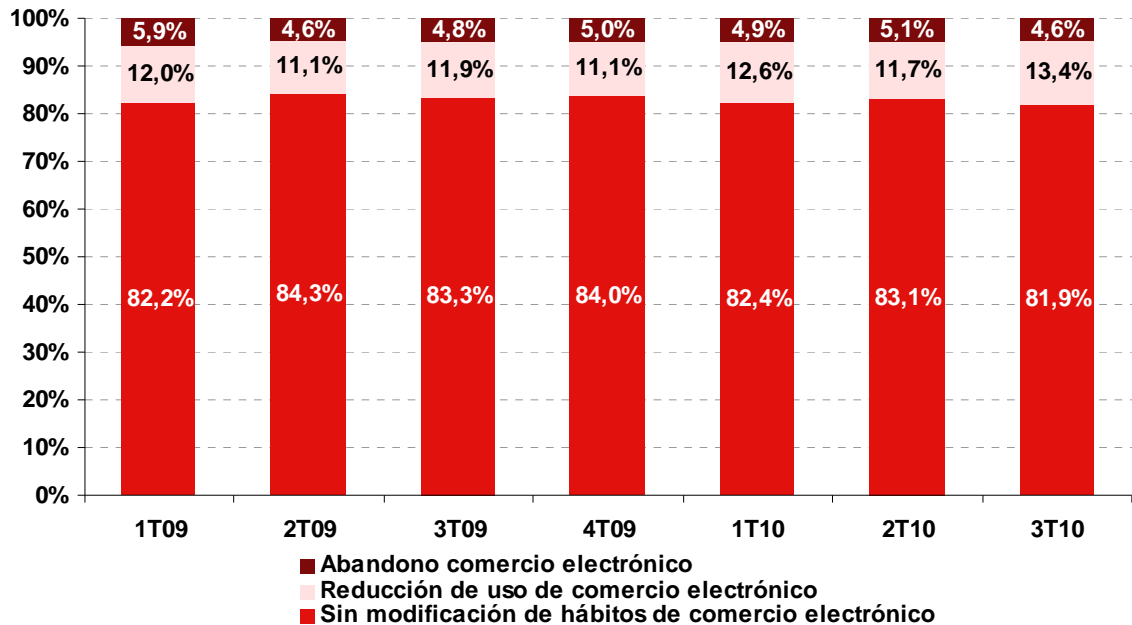
Base: Usuarios que utilizan comercio electrónico y/o banca en línea (n=3.248)

Fuente: INTECO

Atendiendo al Gráfico 11 se observa que los usuarios que sufren un intento de fraude (no consumado) apenas modifican sus hábitos de comercio electrónico. Más en detalle, un 81,9% no modifican el uso, frente a un 4,6% que abandonan esta actividad y un 13,4% que lo reducen.

Estos valores se muestran muy estables en el tiempo, lo que puede ser debido a que lo han interiorizando de tal forma que no abandonan su uso.

Gráfico 11: Modificación de hábitos de comercio electrónico tras sufrir intento (no consumado) de fraude (%)



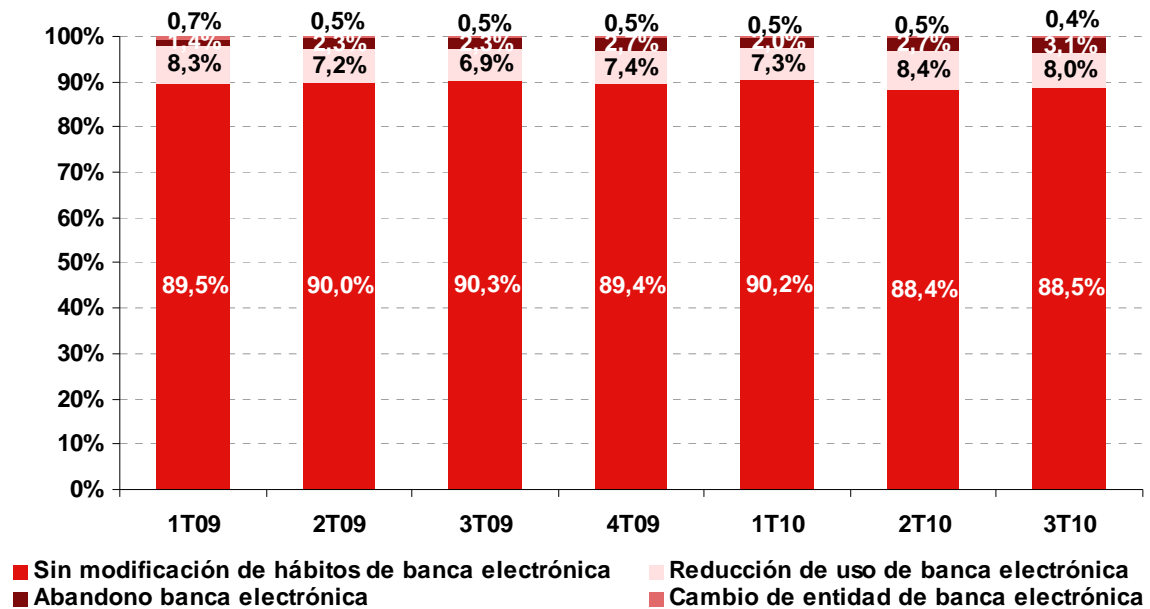
Base: Usuarios que han sufrido algún intento de fraude y/o un perjuicio económico (n=1.928)

Fuente: INTECO

En el caso de los servicios bancarios online, se aprecia incluso una fidelización mayor que en el caso anterior: un 88,5% de los usuarios que sufren intento de fraude no modifican el uso de estos servicios. Dentro de los que declaran algún tipo de reacción ante una incidencia, un 8% reducen el uso, un 3,1% lo abandona y un 0,4% elige cambiar la entidad de banca electrónica.

Los valores, al igual que en el caso anterior, muestran bastante constancia en su evolución.

Gráfico 12: 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=1.928)

Fuente: INTECO

3 CONCLUSIONES Y RECOMENDACIONES

3.1 Conclusiones del análisis

Algo más de la mitad de los internautas declara haber sido víctima de intento (no consumado) de fraude a través de Internet o a través del teléfono en los últimos tres meses mediante diversas técnicas de ingeniería social.

La incidencia de situaciones de intento (no consumado) a través del teléfono móvil es proporcionalmente menor a la de las realizadas a través del correo electrónico, según la percepción de los usuarios. Sin embargo, la generalización de servicios de comunicaciones móviles a través de Internet, o servicios de VoIP, más baratos o gratuitos frente a la telefonía móvil convencional, puede alterar el signo de esta tendencia.

Tras haber introducido en el estudio el trimestre pasado del tipo de troyano conocido como rogueware, las primeras impresiones dan a entender que supone una amenaza al alza, acumulando dos puntos porcentuales de detección en los últimos tres meses.

Una vez más, el análisis pone de manifiesto que los usuarios de Internet españoles no pierden la confianza depositada en la banca y la compra-venta a través de Internet tras sufrir un intento de fraude. El fraude online es más una “barrera de entrada” para los no usuarios que un “impulso de salida” para los usuarios de servicios telemáticos. Resulta especialmente interesante la elevada fidelización por la banca online, a pesar de ser la principal forma adoptada por los atacantes.

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

Los usuarios de Internet perciben que los correos que les resultan sospechosos de enmascarar fraude provienen principalmente de supuestos bancos y entidades financieras. Los atacantes están constantemente buscando nuevas fórmulas para contactar con sus víctimas.

¿Cuánto impacto económico ha causado el fraude?

En el tercer 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 €. Por primera vez desde el primer trimestre de 2009 se supera la barrera del 5% en el porcentaje de usuarios afectados económicamente.

¿Qué datos ofrecen los análisis empíricos?

Los escaneos realizados a través de la herramienta iScan indican que durante este trimestre repunta la proporción de equipos que alojan troyanos, hasta el 38,7% en septiembre de 2010.

Atendiendo a la tipología de troyanos, el porcentaje de troyanos bancarios mantiene la estabilidad de los últimos meses (un 7% en septiembre de 2010), mientras que asciende el del rogueware (un 5,8% en el mismo mes).

¿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 siempre es sinónimo de pérdida de confianza y, en este sentido, los usuarios cada vez muestran más respaldo a los medios online. Un 58,6% 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 51% en el caso de las compras por Internet utilizando la tarjeta de crédito.

Por último, a pesar de haber sufrido un intento de fraude, los hábitos de los usuarios apenas se modifican 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.

3.2 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: Incidencia declarada de situaciones de intento (no consumado) de fraude a través de Internet o telefónico en los últimos 3 meses (%)	15
Gráfico 2: Evolución de la incidencia declarada de situaciones de intento (no consumado) de fraude a través de Internet en los últimos 3 meses (%)	16
Gráfico 3: Evolución de la incidencia declarada de situaciones de intento (no consumado) de fraude a través del teléfono móvil en los últimos 3 meses (%).....	17
Gráfico 4: Formas adoptadas por el remitente de la comunicación sospechosa de ser fraudulenta (%)	18
Gráfico 5: Evolución del fraude con impacto económico para el usuario (%)	20
Gráfico 6: Evolución de la cuantía económica derivada del fraude (%)	21
Gráfico 7: Distribución del importe defraudado en el 3T 2010	21
Gráfico 8: Evolución de equipos que alojan troyanos bancarios y rogueware (%).....	24
Gráfico 9: 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 (%)	25
Gráfico 10: Nivel de confianza entre los usuarios que han sido víctima de intento de fraude y/o haber sufrido perjuicio económico y los que no (%)	26
Gráfico 11: Modificación de hábitos de comercio electrónico tras sufrir intento (no consumado) de fraude (%)	27
Gráfico 12: Modificación de hábitos de banca electrónica tras sufrir intento (no consumado) de fraude (%)	28

ÍNDICE DE TABLAS

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



Instituto Nacional
de Tecnologías
de la Comunicación

<http://www.inteco.es>



<http://observatorio.inteco.es>



Canal Twitter del Observatorio de la Seguridad de la Información:

<http://twitter.com/ObservaINTECO>



Blog del Observatorio de la Seguridad de la Información:

<http://www.inteco.es/blog/Seguridad/Observatorio/BlogSeguridad/>



observatorio@inteco.es