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

Evolución 2007 - 2009

INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN

Edición: Diciembre 2009

El "Estudio sobre el fraude a través de Internet" ha sido elaborado por el equipo de trabajo del Observatorio de la Seguridad de la Información y el equipo de trabajo del Centro de Respuesta a Incidentes de Seguridad (INTECO-CERT) del Instituto Nacional de Tecnologías de la Comunicación:

Pablo Pérez San-José (Coordinador equipo Observatorio)

Susana de la Fuente Rodríguez

Laura García Pérez

Marcos Gómez Hidalgo (Coordinador equipo CERT)

Javier Berciano Alonso

Luis Blanco García

Elena García Díez

Manuel Ransán Blanco

Sandra Salán Clares

ÍNDICE

PUNTOS CLAVE

El fraude online se ha desarrollado en paralelo a la expansión de servicios como el comercio a través de Internet y la banca electrónica. El crecimiento del fenómeno, el perjuicio económico que causa a sus víctimas y, sobre todo, la amenaza que puede suponer a la consolidación de la e-confianza, hacen necesario un análisis profundo de la situación.

Por ello INTECO publica este estudio, realizado con el objetivo de conocer la evolución del estado del fraude online para los usuarios de Internet en España y analizar su impacto en el nivel de e-confianza.

Lo novedoso del informe es que ofrece la perspectiva del usuario, ya sea víctima de fraude online o no. Una muestra amplia (32.484 encuestas) y ocho tomas de datos entre 2007 y 2009 aseguran rigor y continuidad a la información. Además, la metodología empleada se basa en la combinación de técnicas subjetivas de percepción (aplicación de encuesta) con medidas objetivas de incidencia basadas en la observación: un total de más de 128.325 análisis de seguridad en los equipos de los panelistas, llevados a cabo con periodicidad mensual, permiten extraer conclusiones sobre el nivel de infección de los equipos españoles.

Se trata, además, de la primera ocasión en que se realiza un ejercicio de esta magnitud por parte de una sociedad dependiente de la Administración.

I El fraude en Internet

- El fraude online es un fenómeno ampliamente extendido a nivel internacional. La evolución del fraude electrónico en el ámbito mundial, según datos ofrecidos por Anti-Phishing Working Group (APWG), muestra una tendencia creciente continuada desde 2005 hasta 2007, año en que se alcanza el máximo histórico de páginas web fraudulentas identificadas mensualmente (cerca de 60.000. A partir de ahí, se invierte la tendencia y empieza a apreciarse un retroceso, tanto en sitios web fraudulentos como en campañas de ataques de phishing. Parece que, desde comienzos de 2009, el phishing ha vuelto a repuntar, situándose en niveles cercanos a los experimentados en 2007. Los últimos meses analizados por el APWG, mayo y junio de 2009, muestran niveles considerables phishing: en mayo se detectaron 45.959 webs fraudulentas y 37.165 campañas de phishing, y en junio 49.084 webs y 35.918 campañas únicas.

- El área de Servicios Reactivos y Operaciones de INTECO-CERT detectó 1.846 casos de phishing en 2008 y 1.959 en los tres primeros trimestres de 2009. Igualmente, identificó 2.191 URLs fraudulentas en 2008 y 1.810 en 2009 (hasta el mes de septiembre). En el ámbito nacional, el volumen de URLs alojadas en

dominios .es fue de 441 en 2008 y de 153 en los tres primeros trimestres de 2009, lo que supone el 20% y 8,5% del total de URLs fraudulentas detectadas. Igualmente baja es la proporción de sitios web fraudulentos alojados en servidores españoles: 134 en 2008 (6,1% sobre el total) y 178 entre enero y septiembre de 2009 (9,8% sobre el total). Los ciberdelincuentes suelen utilizar servidores ajenos, que comprometen explotando vulnerabilidades en alguno de los productos software que utiliza. La reducción del número de URLs alojadas en España se debe conseguir a través de la mejora en los mecanismos de control y actualización de los servicios proporcionados por los servidores.

II Tipología de fraude en Internet

- En sus inicios, el fraude online no era sino una traslación del fraude tradicional al mundo virtual. Así, las técnicas empleadas para cometer fraude representaban la actualización en Internet de los timos tradicionales. Esta dinámica, conocida como ingeniería social, se basa en la explotación de vulnerabilidades sociales (es decir, engaños que buscan aprovecharse de la ingenuidad de la víctima), no tecnológicas, y hasta mediados de 2007 era la manifestación más representativa del fraude online.

- Esta situación ha evolucionado y actualmente los fraudes tienen un componente tecnológico más acentuado, además de mejorar los mecanismos de ingeniería social utilizados. Así, cada vez tiene mayor relevancia el fraude basado en código malicioso o malware y la utilización de ingeniería social más específica para el destinatario. Se trata de ataques más complejos técnicamente, personalizados y organizados, y por todo ello, más difíciles de prevenir, identificar y combatir. Los ciberdelicuentes disponen de estructuras organizativas complejas, que incluyen tareas de reclutamiento de muleros para el blanqueo del capital y un volumen creciente de recursos para la infraestructura técnica de los fraudes electrónicos.

- Lo que parece claro es que cada vez es más amplia la casuística. En este entorno, debemos asegurarnos de disponer de las herramientas y prácticas de seguridad adecuados para hacer frente a estas amenazas. Además debemos ser cautelosos con nuestra información personal ya que se han detectado casos en los que se utiliza esta información personal robada para llevar a cabo otros delitos relacionados con ciertos tipos de fraude o incluso con casos de pornografía infantil.

- En conclusión, el fraude electrónico es cada vez más complejo desde el punto de vista técnico, se lleva a cabo de manera más personalizada a las particularidades del destinatario, y se está profesionalizando en su ejecución.

III Incidencia del fraude online entre los usuarios españoles

- El correo electrónico se posiciona como el canal más empleado para los intentos de fraude, mientras que los SMS y las llamadas directas tienen una incidencia menor. Las mecánicas de fraude más habituales son el enlace a webs fraudulentas, la oferta de productos o servicios no contratados, las ofertas de empleo falsas y la petición de claves a través de correo electrónico.

- En el tercer trimestre de 2009, un 3,8% de los internautas españoles declaran haber sufrido un perjuicio económico consecuencia de una situación de fraude online. En la segunda mitad de 2007 el nivel se encontraba en un 1,7%. La mayor parte de las pérdidas económicas consecuencia del fraude son de escasa cuantía: en un 44,5% de los casos se catalogan como micro-fraudes que no superan los 100 euros.

- La industria más afectada sigue siendo el sector bancario, con un 44,4% de los usuarios que afirmaron haber recibido comunicaciones fraudulentas de un supuesto banco en el 3er trimestre de 2009. Por detrás de las entidades bancarias, las webs de loterías (33,7%), las webs de compras online (29,3%), operadores de telecomunicaciones (21,8%), redes sociales (20,7%) y las páginas de subastas (16,5%) son los sectores más afectados por el fraude electrónico.

- El panorama del malware entre los usuarios españoles se perfila a partir de los siguientes trazos (los datos, extraídos de escaneos de seguridad sobre los equipos, muestran datos reales, no datos basados en percepción): en septiembre de 2009, un 56,2% de los equipos informáticos están infectados con algún tipo de código malicioso; en un 35,4% los equipos alojan troyanos, tipología de malware más relacionada con la comisión de fraude online.

IV Relación entre el fraude y la e-confianza

- El fraude tiene dos consecuencias directas sobre los usuarios: en primer lugar, la ya analizada pérdida económica tangible en caso de que el ciberdelincuente consiga su propósito; en segundo lugar la posible pérdida de confianza que los internautas pueden experimentar tras ser víctimas de una situación de fraude. Este segundo efecto, quizás menos nombrado que el primero, no es en absoluto trivial e incide en el desarrollo y consolidación de la Sociedad de la Información. (Tampoco debe obviarse el hecho de que ciertos tipos de fraude pueden tener otras consecuencias, como la posibilidad de ser detenido por colaboración en blanqueo de dinero, en el caso de los muleros, o el posible riesgo de la integridad física durante el desarrollo de los timos nigerianos. Además, algunas de las vertientes del fraude llegan a tener incluso consecuencias para la integridad física del usuario, como hay constancia en ciertos casos de timos nigerianos que han derivado en secuestros y/o amenazas físicas.)

- El nivel de confianza en Internet para realizar operaciones económicas es alto: aproximadamente 6 de cada 10 usuarios muestran mucha o bastante confianza en la utilización de banca electrónica.

- A pesar de este considerable nivel de confianza en Internet como canal de realización de transacciones económicas, los ciudadanos siguen mostrando más confianza en la utilización del servicio en persona. En cualquier caso se aprecia una tendencia positiva: el porcentaje de ciudadanos que afirma confiar mucho y bastante en las operaciones que implican pagos y transacciones económicas a través de Internet se incrementa trimestre tras trimestre.

- El haber sufrido un intento (no consumado) de fraude no influye significativamente en los hábitos de uso de compra y banca electrónica: tras haber sufrido un intento de fraude, un 83,3% de los usuarios mantiene invariables sus hábitos de compra en Internet y un 90,3%, sus hábitos de banca electrónica.

- Cuando el intento de fraude deriva, efectivamente, en un perjuicio económico, la situación es diferente: en este caso, a pesar de que la respuesta mayoritaria sigue siendo la no modificación de los hábitos de compra y banca electrónica, se aprecia una considerable proporción de usuarios que cambia sus prácticas o incluso abandona el servicio. Las tasas de abandono son ciertamente minoritarias (en torno al 4%), incluso entre los ciudadanos que han experimentado una pérdida económica, y parece que suponen un indicio de que ambos servicios, en especial la banca, se han hecho difícilmente sustituibles entre sus usuarios. Se debe tener en cuenta este indicador, en tanto en cuanto constituye un indicio muy fiable del nivel de e-confianza de la ciudadanía.

En conclusión, el fenómeno del fraude es una realidad a nivel nacional e internacional. A pesar de las dificultades metodológicas para ofrecer una única cifra válida y homogénea, los datos disponibles para la realidad española son coherentes y en línea con las tendencias apuntadas por organismos nacionales e internacionales.

Para combatir el fraude es clave, por un lado, la observancia de pautas de seguridad y la generalización en la adopción de herramientas por parte de los usuarios. Por otra, es necesaria la actuación conjunta de todos los actores implicados: administraciones, empresas de seguridad y sector bancario, entre otros. En la actualidad, se están haciendo esfuerzos decididos en este ámbito, que se deberán potenciar en el futuro de cara a construir un sólido nivel de e-confianza entre la ciudadanía.

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 (INTECO), sociedad estatal promovida por el Ministerio de Industria, Turismo y Comercio, es una plataforma para el desarrollo de la Sociedad del Conocimiento a través de proyectos del ámbito de la innovación y la tecnología.

Su objetivo es doble: por una parte, contribuir a la convergencia de España con Europa en la Sociedad de la Información y, por otra parte, promover el desarrollo regional, enraizando en León un proyecto con vocación global.

La misión de INTECO es impulsar y desarrollar proyectos de innovación relacionados con el sector de las Tecnologías de la Información y la Comunicación (TIC) y en general, en el ámbito de la Sociedad de la Información, que mejoren la posición de España y aporten competitividad, extendiendo sus capacidades tanto al entorno europeo como al latinoamericano. Así, el Instituto tiene la vocación de ser un centro de desarrollo de carácter innovador y de interés público a nivel nacional que constituirá una iniciativa enriquecedora y difusora de las nuevas tecnologías en España en clara sintonía con Europa.

El objeto social de INTECO es la gestión, asesoramiento, promoción y difusión de proyectos tecnológicos en el marco de la Sociedad de la Información. Para ello, INTECO desarrollará actuaciones, al menos, en las líneas estratégicas de Seguridad Tecnológica, Accesibilidad y Calidad del Software.

1.1.2 Observatorio de la Seguridad de la Información

El Observatorio de la Seguridad de la Información (http://observatorio.inteco.es) 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.

1.1.3 INTECO-CERT: Centro de Respuesta a Incidentes de Seguridad

El Centro de Respuesta a Incidentes de Seguridad (INTECO-CERT) (http://cert.inteco.es) se crea a raíz de las iniciativas enmarcadas dentro del Plan Avanza, con el objetivo de dar respuesta a la necesidad de proporcionar apoyo en materia de seguridad informática y seguridad de la información tanto a los ciudadanos como al tejido industrial español.

Integrado en el área de e-Confianza de INTECO proporciona servicios de carácter público asociados a la prevención, información, concienciación y atención, en materia de seguridad de las tecnologías de la información, para la PYME y el ciudadano español.

Está formado por un equipo de profesionales especializados en distintas áreas de la seguridad TIC y ofrece un amplio catálogo de servicios gratuitos:

1) Servicios de información sobre actualidad de la seguridad:
   - Suscripción a boletines, alertas y avisos de seguridad.
   - Difusión de noticias de actualidad y eventos de relevancia.
   - Avisos sobre nuevos virus, vulnerabilidades y fraudes electrónicos.

- Publicación de estadísticas[1].

2) Servicios de formación en seguridad y en la legislación vigente para la PYME y el ciudadano, proporcionando guías, manuales, cursos online y otros recursos.

3) Servicios de protección y prevención, proporcionando un catálogo de útiles gratuitos y actualizaciones de software.

4) Servicios de respuesta y soporte:

   - Gestión y soporte a incidentes de seguridad.
   - Gestión de malware y análisis de muestras en el laboratorio del INTECO-CERT.
   - Colaboración activa en las actividades de lucha contra el fraude electrónico.
   - Asesoría legal relacionada con la seguridad en las tecnologías de la información.
   - Foros de Seguridad.

A través de los servicios y proyectos enmarcados en INTECO-CERT se han establecido diversos mecanismos de cooperación y coordinación con otras entidades de referencia en el sector, tanto a nivel nacional como internacional, con el fin de fomentar la creación de sinergias que permitan mejorar cada uno de los servicios proporcionados.

Fruto de estas iniciativas y otros proyectos realizados por el área de eConfianza, INTECO-CERT es reconocido a nivel nacional, europeo e internacional por diferentes organizaciones como entidad nacional de seguridad del Gobierno de España. Por este motivo, INTECO-CERT es miembro acreditado y reconocido por el FIRST (Forum of Incident Response and Security Teams), el APWG (Antiphishing Working Group), la ENISA (European Network and Information Security Agency), Trusted-Introducer de TERENA y Task Force – CSIRT de TERENA.

Dentro de las tareas realizadas para la gestión del fraude electrónico, cabe resaltar la colaboración con Red.es en el protocolo antifraude para dominios .es, mediante el cuál INTECO-CERT figura como referencia en la recepción de avisos de fraude electrónico alojados bajo dominios .es. Este protocolo pretende facilitar la eliminación de los dominios .es registrados con fines fraudulentos y limitar el tiempo de utilización de dichos dominios con fines fraudulentos.

[1] A través de la web en http://ersi.inteco.es

1.1.3.1 Repositorio de fraude electrónico de INTECO-CERT

Dentro de sus actividades colaborativas, INTECO se ha involucrado activamente en el desarrollo del proyecto SEVEF (Servicio para las Evidencias Electrónicas Financieras), promovido por la Asociación Nacional de Establecimientos Financieros de Crédito. En el lanzamiento de este proyecto se crean dos grupos de trabajo en los que están representadas diversas entidades financieras, el Banco de España, la Agencia Española de Protección de Datos, la Brigada de Investigación Tecnológica del Cuerpo Nacional de Policía, el Grupo de Delitos Telemáticos de la Guardia Civil, la Unidad Técnica Policía Judicial de la Guardia Civil, la Ertzaintza, los Mossos d'Esquadra, la Asociación Nacional de Establecimientos Financieros de Crédito y el propio INTECO.

A partir de los trabajos desarrollados en ambos grupos, INTECO construye el Repositorio de Fraude Electrónico, enmarcado en la plataforma de gestión de fraude electrónico para INTECO-CERT. Esta plataforma permite la gestión de los incidentes de fraude electrónico recibidos en INTECO-CERT, recopilando la información técnica asociada que puede ser consultada posteriormente a través del repositorio de fraude electrónico.

El Repositorio de Fraude Electrónico de INTECO-CERT recoge información estructurada de todos los tipos de fraude a partir de los casos e incidentes detectados detallando la información técnica de los recursos y servicios electrónicos utilizados y/o afectados:

- Correos electrónicos.
- Direcciones web y dominios
- Direcciones IP relacionadas
- Otra información: ingeniería social asociada, comportamiento atacante, peculiaridades del caso, etc.

Mantiene por tanto un histórico de los casos de fraude detectados que puede ser explotado para poder obtener:

- Estadísticas detalladas de los casos detectados.
- Correlación entre recursos y servicios electrónicos presentes en diferentes casos, ataques dirigidos, etc.
- Estudio de la evolución del fraude electrónico en España.
- Detección de nuevas tendencias de fraude.
- Evaluación de la incidencia del fraude en el usuario.

1.1.4 Oficina de Seguridad del Internauta

Dentro de la promoción de diversas actuaciones y políticas públicas en el campo de la seguridad informática llevada a cabo por el Ministerio de Industria, Turismo y Comercio, a través de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, a la que está adscrito el Instituto Nacional de Tecnologías de la Comunicación (INTECO), se encuentra enmarcada la reciente puesta en marcha de la Oficina de Seguridad del Internauta (www.osi.es).

El diseño e implementación de los servicios de la OSI se ha basado en los siguientes criterios y objetivos:

1) Poner a disposición del usuario un punto de referencia cercano y accesible para cualquier aspecto de seguridad informática con atención disponible en un amplio horario y mediante diferentes vías de acceso.

2) Acercar los servicios de seguridad a todos los usuarios a través de una plataforma de comunicación multicanal que responda a las diferentes necesidades: portal web, correo electrónico y atención telefónica.

3) Ofrecer formación y atención en un lenguaje adaptado a todos los públicos de manera que un usuario sin conocimientos técnicos previos pueda adquirir la información básica necesaria para un uso seguro de Internet.

4) Adaptar, mejorar y enriquecer servicios similares que, con una carga técnica superior, desde 2001 se prestan a Pymes y Ciudadanos de forma exitosa por parte de INTECO-CERT.

5) Obtener indicadores adicionales sobre el nivel de la cultura de seguridad de los usuarios que ayuden a perfeccionar los propios servicios de OSI y a detectar posibles nuevas necesidades.

Por todo ello, la OSI se ha definido como un instrumento ágil, flexible e interactivo, que ofrece a los internautas los mejores servicios posibles de información, concienciación, apoyo y asesoramiento, para poder sortear los posibles incidentes de seguridad por los que se puedan ver afectados. La puesta en práctica de estos criterios por parte de INTECO, se ha materializado en un portal web multi-idioma (http://www.osi.es) de fácil acceso y navegación mediante el que se ofrece seguridad en la red en tres pasos:

1) **Conocer los conceptos y amenazas de seguridad.** Con un sencillo test que facilita al usuario la evaluación de sus conocimientos de seguridad informática y un ABC de la seguridad que le acercará a los principales conceptos y amenazas de seguridad en la red.

2) **Cómo protegerse.** Medidas preventivas y consejos para el uso seguro de los diferentes servicios de Internet (navegación, correo electrónico, móviles, redes

P2P, mensajería instantánea, etc.), e información sobre distintas herramientas con las que proteger el ordenador y su conexión a Internet. Asimismo se incluye un servicio diario de alertas de seguridad y servicios de información mediante otros canales como RSS.

3) **Ayuda y soporte para resolver dudas, problemas e incidentes**: En el número 901 111 121, los usuarios pueden contactar con el Servicio de Atención Telefónica de la OSI para un tratamiento directo y personalizado, además de un servicio de Foros y un Asistente de Seguridad On-line para consultar dudas y problemas que son atendidos por un equipo de técnicos especializados.

1.2 Estudio sobre el fraude a través de Internet

1.2.1 Contexto y oportunidad del estudio

El desarrollo de la Sociedad de la Información ha hecho que servicios como la banca electrónica o la realización de compras a través de Internet sean hoy una realidad consolidada. Así, en el tercer trimestre de 2008 (último período analizado por Red.es), cerca del 38% de los usuarios de Internet españoles utilizaban servicios de banca electrónica, y casi el 30% efectuaba compras de viajes o vacaciones a través de Internet. Son resultados del estudio *Evolución de los usos de Internet en España 2009*, entre cuyas conclusiones destaca que *las compras son significativamente más elevadas que hace dos años, lo que demuestra que se está asentando una mayor confianza en la Red para la compra online*[2].

Tan real como el avance de la economía de Internet es la proliferación de amenazas informáticas. En cierto modo intrínseco a las transacciones económicas, existen una serie de situaciones de fraude electrónico que pueden suponer un riesgo para el desarrollo de algunos servicios de Internet de carácter económico.

El origen de estas amenazas electrónicas es, en ocasiones, coincidente al de sus equivalentes en el mundo físico. Así, a la hora de analizar las causas de las situaciones de fraude electrónico se identifica, en primer lugar, lo que se viene denominando ingeniería social: técnicas que, a través del engaño, y explotando las vulnerabilidades "sociales" de la víctima (la persona física, no la máquina), persiguen el lucro del estafador. Pero, además de estas técnicas basadas en el engaño tradicional, existen sofisticadas manifestaciones de malware que, en muchas ocasiones, se encuentran en el origen del ilícito. Programas capaces de suplantar la identidad y robar las claves de acceso son ejemplos de este malware que persigue la comisión de un fraude. No es sencillo aislar el origen último de cada situación fraudulenta y en numerosas ocasiones aparecen distintas causas entrelazadas. Además suele haber un entramado

[2] **Red.es** (2009). *Evolución de los usos de Internet en España 2009.* Disponible en: http://observatorio.red.es/hogares-ciudadanos/articles/id/3650/evolucion-los-usos-internet-espana-2009.html

perfectamente organizado detrás de todas estas actividades delictivas y que cada vez dispone de mayores y mejores recursos para llevarlas a cabo.

Con todo ello, lo cierto es que la proliferación de este tipo de comportamientos, además del evidente perjuicio económico que un fraude puede comportar al usuario, puede suponer un freno en la e-confianza de los usuarios y, en última instancia, podría limitar el desarrollo de la Sociedad de la Información en general, y de los servicios de banca electrónica y comercio electrónico en particular. Esta es la hipótesis de partida del estudio, que se contrastará y analizará en detalle en el capítulo 6.

En este contexto, el presente informe describe, desde la óptica del usuario de Internet, la evolución de las situaciones relacionadas con el fraude electrónico desde 2007 hasta el tercer trimestre de 2009, y el impacto que dichas situaciones han tenido sobre el usuario, tanto a nivel económico como en el grado de e-confianza. La premisa a contrastar es si la existencia de fraude electrónico puede afectar a la confianza de los usuarios en los servicios de Internet, lo cual incidiría en el ritmo de incorporación y desarrollo a la Sociedad de la Información, y en definitiva en el crecimiento económico.

En el momento de elaboración del informe se han identificado diversos estudios publicados que ofrecen la visión de la industria y del sector bancario. Lo novedoso del presente estudio radica en que ofrece la visión de los usuarios de la Red, último eslabón de la cadena sobre el que descansa en última instancia la confianza en la Sociedad de la Información, y en que se trata del primer estudio de esta índole que es llevado a cabo por una sociedad gubernamental.

1.2.2 Objetivos

El objetivo de este Estudio es conocer la evolución del estado del fraude electrónico para los usuarios de Internet en España y analizar su impacto en el nivel de e-confianza. Todo ello, con el fin de sentar una base de conocimiento para la recomendación de acciones que impulsen la seguridad de la información y la e-confianza entre los usuarios de Internet en España.

2 DISEÑO METODOLÓGICO

Para conseguir los objetivos planteados, la ejecución del proyecto ha combinado diferentes metodologías:

- **Búsqueda y análisis documental de informes y estudios** que, por su contenido, metodología o enfoque, enriquecen el proyecto y contribuyen a la consecución de los objetivos perseguidos.

- **Panel online** dedicado compuesto por hogares con conexión a Internet repartidos por todo el territorio nacional. El panel se configura como la metodología idónea para la consecución de los objetivos del proyecto, ya que permite realizar lecturas periódicas del fenómeno del fraude y ofrecer, por tanto, una perspectiva evolutiva de la situación. Para garantizar la robustez de la muestra y conseguir que los errores muestrales se mantengan en niveles inferiores a ± 2,00% para un nivel de confianza del 95,5% (1,96 σ respecto de la μ), el tamaño del panel se mantiene siempre por encima de los 3.000 hogares. Sobre los miembros del panel se aplican, a su vez, 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. Para ello, se utiliza el software iScan[3], 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, del estado de su actualización y de las herramientas de seguridad instaladas. El programa informático remite esta información a INTECO, que la trata de manera anónima y agregada. Sabiendo que en la actualidad buena parte del fraude procede a través de código malicioso que se distribuye a través de la Red, este análisis es determinante a la

[3] El software, propiedad de INTECO, es un programa sencillo e inocuo que permite realizar un análisis exhaustivo en remoto tanto del sistema como de la seguridad de los ordenadores. Todo ello, con absoluta confidencialidad y transparencia. Una explicación detallada de la herramienta se encuentra en el apartado 2.3 Análisis de seguridad de los equipos.

hora de conocer el nivel de riesgo real de los equipos. El análisis del epígrafe 6.4 Fraude y malware se ha realizado a partir de los datos obtenidos de esta forma.

Se analiza la evolución de los datos desde 2007 hasta el tercer trimestre de 2009, agrupando los resultados en ciclos trimestrales (en el caso de las encuestas) o mensuales (en el caso de los análisis online). Así, es posible observar las variaciones de los resultados anualmente, pero también descender al detalle de la evolución trimestral y mensual. Una de las fortalezas del estudio radica en que combina medidas objetivas de incidencia con medidas subjetivas de percepción de seguridad y confianza en la Red.

La novedad del informe radica en que la metodología empleada en el informe permite ofrecer conclusiones sobre incidencia y efectos del fraude desde la perspectiva del usuario, y no de las entidades afectadas o empresas de seguridad. Se trata de la primera vez en España que se identifica un estudio con este enfoque.

Además, también se ha dispuesto de la siguiente información:

- Datos recopilados en INTECO por el área de Servicios Reactivos y Operaciones durante la prestación del servicio de gestión del fraude por el equipo de INTECO-CERT.

- Test de Evaluación[4] existente en el portal de la Oficina de Seguridad del Internauta y que recaba datos estadísticos sobre los conocimientos de seguridad de los internautas que lo realizan. Se dispone de datos de más de 2500 test realizados que proporcionan una aproximación al nivel de conocimiento de los internautas que han accedido a este portal.

2.1 Búsqueda y análisis documental

Esta fase tiene como objetivo analizar contenidos publicados en la materia que puedan enriquecer y orientar el proyecto de investigación.

Se han localizado y seleccionado diversas publicaciones consideradas de relevancia por la metodología empleada, el contenido, las conclusiones y los objetivos perseguidos.

Las referencias consultadas pueden encontrase en el anexo bibliográfico al final de este informe.

[4] Disponible en la dirección web: http://www.osi.es/evaluación

2.2 Panel online dedicado: ficha técnica de la encuesta

2.2.1 Universo

Usuarios españoles de Internet, con acceso frecuente a Internet desde el hogar, mayores de 15 años. 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.

2.2.2 Tamaño y distribución muestral

La extracción de la muestra de usuarios de Internet, se realiza mediante afijación muestral según un modelo polietápico: estratificación por comunidades autónomas para garantizar un mínimo de sujetos en cada una de estas entidades y muestreo por cuotas de tamaño del hogar, edad, sexo, actividad laboral y tamaño del hábitat[5].

La muestra se ha equilibrado al universo en base a los datos poblacionales por CCAA, para el universo descrito anteriormente, y a las variables de cuota, para alcanzar un ajuste más perfecto.

De la muestra se obtienen dos tipos diferentes de información: la proporcionada por los usuarios en las encuestas y la obtenida directamente mediante observación (análisis online de sus equipos). 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, puede haber hogares en que se realice el análisis online pero no la encuesta, o viceversa), se presentan de forma separada: la Tabla 1 describe los tamaños muestrales de la encuesta y la Tabla 2 indica el número de equipos escaneados.

[5] Estas cuotas se han obtenido de datos representativos a nivel nacional de internautas mayores de 15 años que se conectan más de una vez al mes desde el hogar facilitados por Red.es, entidad pública empresarial del Ministerio de Industria, Comercio y Turismo.

Tabla 1: Tamaños muestrales para las encuestas

Período	Tamaño muestral
1er trimestre 2007	3.076
2º trimestre 2007	3.023
3er trimestre 2007	3.021
4º trimestre 2007	3.021
1er trimestre 2008	3.523
2º trimestre 2008	*n.d.*
3er trimestre 2008	*n.d.*
4º trimestre 2008	*n.d.*
1er trimestre 2009	3.563
2º trimestre 2009	3.521
3er trimestre 2009	3.540

Fuente: INTECO

Tabla 2: Número de equipos escaneados mensualmente

Año 2007	Equipos escaneados	Año 2008	Equipos escaneados	Año 2009	Equipos escaneados
Ene'07	2.910	Ene'08	4.659	Ene'09	5.649
Feb'07	2.979	Feb'08	4.450	Feb'09	4.325
Mar'07	2.839	Mar'08	3.893	Mar'09	4.695
Abr'07	4.618	Abr'08	4.102	Abr'09	4.954
May'07	3.389	May'08	4.610	May'09	4.677
Jun'07	3.408	Jun'08	3.889	Jun'09	4.293
Jul'07	3.701	Jul'08	3.187	Jul'09	3.971
Ago'07	3.552	Ago'08	2.793	Ago'09	3.677
Sep'07	3.003	Sep'08	2.617	Sep'09	4.520
Oct'07	4.523	Oct'08	2.421		
Nov'07	3.959	Nov'08	3.661		
Dic'07	3.376	Dic'08	4.286		

Fuente: INTECO

2.2.3 Captura de información, períodos analizados y fecha del trabajo de campo

Las entrevistas se han realizado online a partir de un panel de usuarios de Internet.

El trabajo de campo ha tenido lugar entre 2007 y septiembre de 2009. Los escaneos se realizan con una periodicidad mensual, de forma que existen datos reales de todos y cada uno de los meses comprendidos en el período analizado en el informe. Para las encuestas, se ha intentado aproximar la fecha de toma de datos a los trimestres naturales del año, en base a la siguiente tabla.

Tabla 3: Fecha del trabajo de campo de las encuestas (%)

Período	Fecha del trabajo de campo
1er trimestre 2007	Febrero a abril de 2007
2º trimestre 2007	Mayo a julio de 2007
3er trimestre 2007	Agosto a diciembre de 2007
4º trimestre 2007	Agosto a diciembre de 2007
1er trimestre 2008	Enero a marzo de 2008
2º trimestre 2008	*No disponible*
3er trimestre 2008	*No disponible*
4º trimestre 2008	*No disponible*
1er trimestre 2009	Diciembre de 2008 a febrero de 2009
2º trimestre 2009	Marzo a mayo de 2009
3er trimestre 2009	Junio a septiembre de 2009

Fuente: INTECO

2.2.4 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 ±2,00% en cada uno de los períodos analizados, tal y como se recoge en la siguiente tabla.

Tabla 4: Errores muestrales de las encuestas (%)

Período	Tamaño muestral	Error muestral
1er trimestre 2007	3.076	±1,80%
2º trimestre 2007	3.023	±1,82%
3er trimestre 2007	3.021	±1,82%
4º trimestre 2007	3.021	±1,82%
1er trimestre 2008	3.523	±1,68%
2º trimestre 2008	*n.d.*	*n.d.*
3er trimestre 2008	*n.d.*	*n.d.*
4º trimestre 2008	*n.d.*	*n.d.*
1er trimestre 2009	3.563	±1,68%
2º trimestre 2009	3.521	±1,68%
3er trimestre 2009	3.540	±1,68%

Fuente: INTECO

2.3 Análisis de seguridad de los equipos

Para llevar a cabo los análisis en línea se ha utilizado el programa iScan, una herramienta de análisis de seguridad propiedad de INTECO especializada en la detección de medidas activas de seguridad y, sobre todo, de código malicioso (malware).

En el análisis del malware, iScan detecta las incidencias de seguridad con 46 antivirus distintos con el objetivo de asegurar una mayor tasa de detección (especialmente ante las nuevas amenazas de carácter altamente indetectable). Como contrapunto, precisamente con el objeto de minimizar los falsos positivos[6], se establecen una serie de filtros y controles posteriores:

4) **Filtrado y ponderación de soluciones antivirus.** En la selección de los motores se han tenido en cuenta los siguientes factores:

   a. En el listado de soluciones antimalware utilizadas por iScan se excluyen productos antivirus de perímetro, altamente paranoicos.

   b. Tampoco se consideran algunas soluciones que comparten firmas, para de este modo considerar sólo un motor con el mismo conjunto de firmas.

   c. Se ha identificado un subconjunto con los 11 antivirus más reputados, con mejor tasa de detección frente a especimenes detectados por más de 10 antivirus.

   Para que un archivo sea marcado como malware, éste debe ser detectado por 5 productos de los 46 considerados, teniendo en cuenta que uno de los 5 necesariamente debe pertenecer al subconjunto de los 11 antivirus más reputados.

5) **Verificación manual de un número acotado de ejemplares.** Tras una primera capa de filtrado, se ordenan todos los ficheros detectados en los equipos auditados por tasa de penetración (número de equipos en los que han sido avistados). Los 40 ficheros más avistados se analizan manualmente, con el fin nuevamente de filtrar falsos positivos.

6) **Comparación de los ficheros marcados como maliciosos con bases de datos de software conocido y de ficheros inocuos.** INTECO mantiene una base de datos de software de fabricantes confiables. Todos los ejemplares que siguen siendo detectados tras las dos capas de filtrado anteriores 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*[7] del National Institute of Standards and Technology (NIST). Si se detectase que alguno de los ficheros señalados por iScan está en dicha

[6] Un "falso positivo" es la detección, errónea, de un fichero inocuo como malicioso.

[7] National Institute of Standards and Technology: National Software Reference Library. Disponible en http://www.nsrl.nist.gov

base de datos y no forma parte de un kit de hacking o cracking, el archivo no es considerado como malicioso.

El establecimiento de estos filtros y controles es una medida muy importante de cara a asegurar la fiabilidad del estudio, pero aun así no elimina por completo la problemática de los falsos positivos (una problemática inherente a la industria antivirus), ni la de los falsos negativos.

Asimismo, debe tenerse en cuenta que al comparar todos los ficheros de los equipos inspeccionados con las bases de datos de malware conocido, no es posible detectar ningún especimen desconocido que no se encuentre en dichas librerías. Esto es especialmente acusado en el caso de los gusanos y virus. Los gusanos suelen incluir un motor polimórfico que da lugar a un fichero binariamente distinto en cada replicación del mismo. En consecuencia, es muy difícil que un gusano polimórfico sea detectado, pues muchos de ellos serán únicos para cada infección y por tanto no estarán presentes en la base de datos de malware conocido. El caso de los virus es similar: muchos virus infectan otros archivos, dando lugar a ficheros con nuevas huellas digitales que no están presentes en la base de datos.

Por último, iScan no proporciona información sobre si un determinado código malicioso se encuentra activo en el sistema. Podría darse la posibilidad (ciertamente infrecuente, por otra parte) de un sistema que, aun alojando malware, en realidad no estuviera infectado. Por ejemplo, el caso de un investigador que tuviera un directorio con código malicioso para estudiar, o el caso de que un código malicioso haya sido detectado por un antivirus y movido a una carpeta de cuarentena sin ofuscarlo[8]. Se trata de una situación que no parece muy probable, pero que sería considerado malware por iScan.

En definitiva, a pesar de la fortaleza de la herramienta iScan y de las medidas adoptadas por INTECO para mitigar la incidencia de falsos positivos, existen limitaciones intrínsecas a la metodología empleada que hacen que el análisis no sea infalible. Por ello los datos que se ofrecen, basados en un análisis sólido y robusto, 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.

[8] En informática, la ofuscación consiste en un acto deliberado de realizar un cambio no destructivo, ya sea en el código fuente de un programa informático o código máquina cuando el programa está en forma compilada o binaria, con el fin de que no sea fácil de entender o leer. Es decir, se hace ininteligible específicamente para ocultar su funcionalidad.

3 INCIDENTES DE FRAUDE EN INTERNET A NIVEL MUNDIAL

El fraude a través de Internet es un fenómeno de dimensiones globales. La evolución del fraude electrónico, según datos ofrecidos por *Anti-Phishing Working Group* (APWG), muestra una tendencia creciente continuada desde 2005 hasta 2007, año en que se alcanza el máximo histórico de páginas web fraudulentas identificadas mensualmente (cerca de 60.000. A partir de ahí, se invierte la tendencia y empieza a apreciarse un retroceso, tanto en sitios web fraudulentos como en campañas de ataques de phishing. Parece que, desde comienzos de 2009, el phishing ha vuelto a repuntar, situándose en niveles cercanos a los experimentados en 2007.

En este punto, es importante destacar que la metodología utilizada por el APWG para la extracción de datos se basa en el reporte efectivo de casos recibido a través de las empresas que forman parte de la Asociación. Teniendo en consideración que la APGW es una organización de ámbito mundial que cuenta con más de 3.000 socios de diversos sectores (bancos, empresas privadas, compañías TIC y seguridad, organismos gubernamentales, etc.), se puede considerar que los datos son significativos y en cualquier caso válidos para mostrar tendencias.

No obstante, una de las dificultades metodológicas en la medición del phishing es la existencia de diferentes criterios para su cuantificación. El *Anti-Phishing Working Group considera* dos variables:

- Campañas únicas de phishing (línea roja del gráfico), que el APWG define como cada e-mail dirigido a varios usuarios, apuntando a una misma página web, con un mismo asunto en el correo electrónico.

- Webs únicas de phishing (línea marrón del gráfico), URLs fraudulentas identificadas.

Un análisis del fenómeno basado en el número de sitios web fraudulentos identificados en el mundo permite identificar 3 fases en la evolución del phishing, tal y como se aprecia en el Gráfico 1:

- Fase 1 - Introducción: Durante el año 2005 el número de sitios web fraudulentos se mantuvo constante, en un nivel inferior a los 5.000 casos mensuales.

- Fase 2 - Crecimiento: Los últimos meses de 2005 supusieron el inicio de una tendencia creciente, que caracterizó a todo el año 2006. Así, diciembre de 2006 cerró el año con 28.531 casos identificados. Tras un retroceso experimentado en

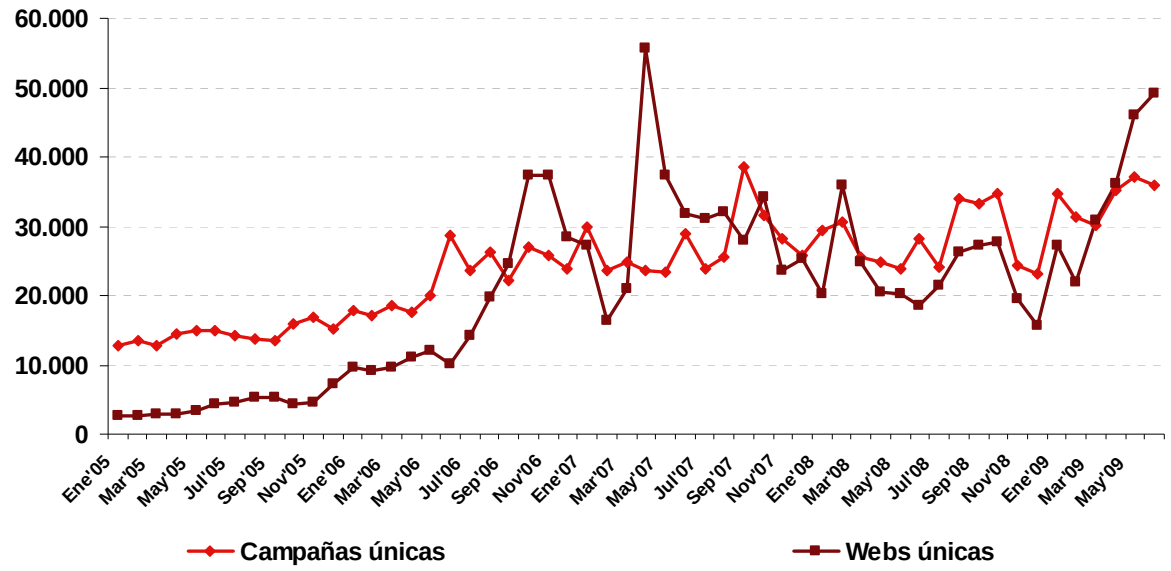
los primeros meses de 2007, abril experimenta un nuevo repunte, que supone el máximo histórico de 55.643 sitios web fraudulentos reportados.

- Fase 3 - Madurez: A partir del pico experimentado en abril de 2007 se inicia una tendencia decreciente que llega hasta diciembre de 2008, si bien es cierto que se producen oscilaciones y repuntes en algunos meses. En cualquier caso, el nivel de sitios web fraudulentos se sitúa en el entorno de los 30.000. Sigue siendo una cifra alta, aunque más moderada que los datos alcanzados en los picos experimentados en 2007. Noviembre y diciembre de 2008 muestran un retroceso importante tanto en el número de webs como de campañas únicas: diciembre de 2008 cerró con 23.187 campañas únicas y 15.709 webs fraudulentas únicas.

En la primera mitad de 2009 se ha experimentado un nuevo repunte del fraude, según la información facilitada por el APWG. Los últimos meses analizados, mayo y junio de 2009, muestran niveles considerablemente altos de phishing, que prácticamente duplican los datos de cierre de 2008. Así, en mayo se detectaron 45.959 webs fraudulentas y 37.165 campañas de phishing, y en junio 49.084 webs y 35.918 campañas únicas.

En cualquier caso, es un hecho que las manifestaciones de fraude electrónico evolucionan y cambian a medida que lo hacen las fórmulas para combatirlas.

Gráfico 1: Evolución del phishing entre 2005 y junio de 2009



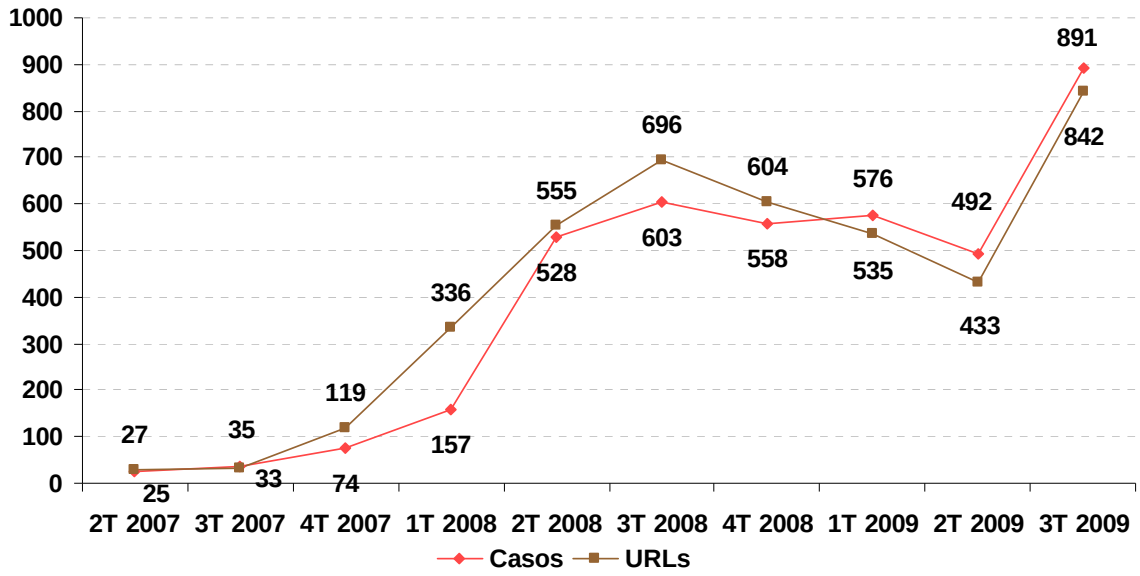
Fuente: Anti-Phishing Working Group (APWG)

4 INCIDENTES DE FRAUDE EN INTERNET EN ESPAÑA

Los datos recabados por el servicio de gestión del fraude de INTECO-CERT proporcionan una fuente adicional al comportamiento del fraude electrónico, circunscribiendo el análisis a la realidad española. El punto de partida de esta información es el 2º trimestre de 2007, momento en el que se comienza a prestar este servicio desde INTECO. (Esto explica el reducido volumen de casos y URLs reportados durante los primeros períodos de análisis, tal y como muestra el Gráfico 2.)

Los datos reflejan un repunte de los casos de fraude gestionados en el tercer trimestre del año 2008, seguido de un paulatino descenso durante los períodos posteriores, hasta el 2º trimestre de 2009. En este momento, parece que se invierte la tendencia y el 3er trimestre alcanza un pico de 891 casos de fraude y 842 URLs fraudulentas.

Gráfico 2: Evolución del fraude en España entre 2007 y 2009



Fuente: INTECO-CERT

Debido al protocolo antifraude en dominios .es, y a los reportes de entidades antifraude y CERTs extranjeros a INTECO de actividades fraudulentas alojadas en dominios .es, se puede analizar la incidencia del fraude en este tipo de dominios. Los datos recabados se ofrecen en el Gráfico 3, donde se analiza el total de URLs fraudulentas, la proporción de ellas que utilizan dominios .es así como las que están alojadas en España.

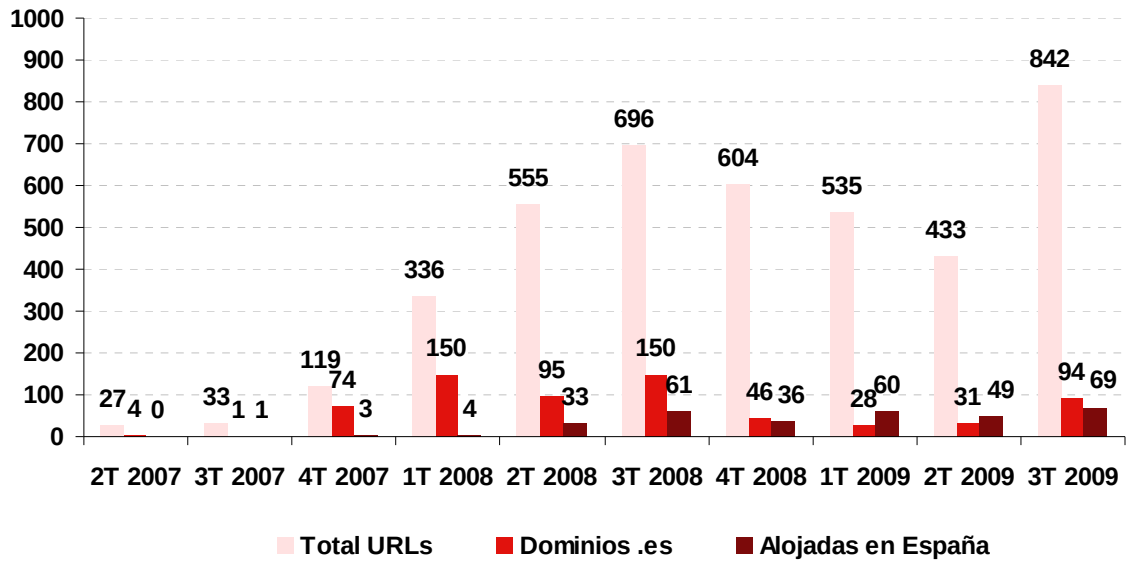
Se puede observar una alta proporción en la utilización del dominio .es durante el último trimestre de 2007 y los 3 primeros del 2008, produciéndose posteriormente una disminución en esta proporción con respecto al total de URLs utilizadas con fines

fraudulentos, recogidas y analizadas por el servicio de gestión de fraude electrónico de INTECO-CERT. En el tercer trimestre de 2009, último período analizado, se aprecia un nuevo repunte: de las 842 URLs identificadas, 94 pertenecen al dominio .es. Proporcionalmente, en cambio, se trata sólo de un 11%.

Por otro lado, analizando también la proporción en el número de URLs alojadas en servidores situados en España, el número total se mantiene en el rango de 30-60 URLs alojadas en España por trimestre. En línea con ello, en el tercer trimestre de 2009 se identificaron 69 URLs alojadas en España.

Los ciberdelincuentes suelen utilizar servidores ajenos, que comprometen explotando vulnerabilidades en alguno de los productos software que utiliza. La reducción del número de URLs alojadas en España se debe conseguir a través de la mejora en los mecanismos de control y actualización de los servicios proporcionados por los servidores. Se trata de un mecanismo de control dependiente de los administradores de estos servidores, pero que debería apoyarse en automatizaciones proporcionadas por el fabricante de la aplicación.

Gráfico 3: Evolución de URLs fraudulentas en España entre 2007 y 2009



Fuente: INTECO-CERT

5 TIPOLOGÍA DE FRAUDE EN INTERNET

En sus inicios, el fraude electrónico no era sino una traslación del fraude tradicional al mundo virtual. Así, las técnicas empleadas para cometer fraude representaban la actualización en Internet de los "timos" tradicionales. Esta dinámica se basaba en la explotación de vulnerabilidades sociales (es decir, engaños que buscan aprovecharse de la ingenuidad de la víctima), utilizando simples técnicas de ingeniería social con una baja complejidad tecnológica siendo hasta mediados de 2007 la manifestación más representativa del fraude electrónico.

Sin embargo, esta situación ha evolucionado y actualmente los fraudes tienen un componente tecnológico mucho más acusado. Así, cada vez tiene mayor relevancia el fraude basado en código malicioso o malware. Se trata de ataques más complejos técnicamente, personalizados y organizados, y por todo ello, más difíciles de prevenir, de identificar y de combatir.

El *Anti Phishing Working Group* (APWG) contempla ambas posibilidades en su definición de phishing, al que considera un mecanismo criminal que emplea tanto técnicas de ingeniería social como artificios técnicos con el objetivo de robar datos personales de los usuarios y credenciales bancarias. Las técnicas de ingeniería social incluyen correos electrónicos falsos, procedentes, en apariencia, de empresas o entidades legítimas, que dirigen al destinatario a webs falsas que replican las de la empresa o entidad legítima, para que introduzca datos personales o bancarios, tales como la clave de usuario y la contraseña para operar. Los artificios técnicos pretenden introducir malware en los equipos para robar directamente los datos bancarios, utilizando, por ejemplo, sistemas que interceptan clave de usuario y contraseña o programas que corrompen las infraestructuras de navegación y redirigen a los usuarios a webs falsas.

La problemática del origen del fraude (ingeniería social o malware) no es trivial ya que determina el carácter de la solución necesaria para enfrentarse a él:

- Soluciones centradas en el usuario, con medidas de sensibilización, educación y formación oportunas (en el caso de la ingeniería social).

- Soluciones más complejas, que exigen de un lado formación para el usuario, y de otro, herramientas de seguridad adecuadas (en el caso del malware).

En todos los casos, será clave, además, la actuación conjunta de la Administración, de las Fuerzas y Cuerpos de Seguridad del Estado, del ámbito judicial y fiscal, de los sectores afectados por el fraude, de las empresas de seguridad y de los diferentes actores relevantes para combatir el ciberdelito.

La evolución de los ataques y la sofisticación de los mismos hace que en muchas ocasiones nos encontremos con una combinación de técnicas para llevar a cabo el fraude.

Se analizan a continuación los incidentes de fraude detectados en España, diferenciando entre el fraude basado en técnicas de phishing y el que utiliza algún tipo de malware para llevarse a cabo. Para llevar a cabo el análisis se presentan datos procedentes de dos fuentes diferenciadas:

- INTECO-CERT
- S21sec

Los datos proporcionados por INTECO-CERT se ofrecen en la Tabla 5. En la interpretación de estos datos se debe tener en cuenta que una de las principales fuentes de información de INTECO-CERT son los usuarios finales, siendo mucho más sencillo para éstos detectar un phishing que un troyano bancario.

En cualquier caso, la información confirma una incidencia inicial mayor de los fraudes de tipo phishing. A partir de 2008 se observa un crecimiento de otros tipos de fraude, estabilizándose en los últimos trimestres la proporción entre los tipos phishing, malware y otros tipos.

Este es un indicio más de la tendencia a la diversificación de los tipos de fraude utilizados por los ciberdelincuentes intentando aprovechar todos los recursos a su alcance para conseguir sus fines (principalmente, de carácter económico).

Tabla 5: Incidentes de fraude detectados en España: número total

Tipos de fraude	2T 07	3T 07	4T 07	1T 08	2T 08	3T 08	4T 08	1T 09	2T 09	3T 09
Phishing	25	35	74	157	528	563	452	360	309	652
Malware						40	25	58	62	80
Otros							81	158	121	159
Total	**25**	**35**	**74**	**157**	**528**	**603**	**558**	**576**	**492**	**891**

Fuente: INTECO-CERT

La empresa española de seguridad S21sec también ofrece datos de los incidentes de fraude basados en phishing, código malicioso (principalmente troyanos) y redirectores[9]. Los datos se construyen por la unidad S21sec e-crime en base a actividades calificadas de fraude electrónico dirigidas a entidades en España.

[9] Se trata de una técnica utilizada para dificultar el cierre de los sitios, cambiando la redirección de la página de phishing de forma dinámica (una especie de sitios web encadenados).

En la tabla siguiente se ofrece el número total de incidentes detectados en España y el ritmo de crecimiento con respecto al año anterior. Los datos muestran la evolución anual desde 2006 hasta 2008, y el desglose según la técnica de ataque empleada: phishing, troyanos o redirectores.

De su análisis se obtiene la siguiente conclusión: la evolución de los incidentes de fraude detectados en España muestra una tendencia creciente, y con un ritmo que cada año prácticamente duplica al volumen del año anterior: de 830 casos identificados en 2006 se pasa a 1.644 incidentes en 2007 y 3.123 en 2008.

Tabla 6: Incidentes de fraude detectados en España: número total y *(ritmo de crecimiento con respecto al año anterior)*

Tipos de fraude	2006	2007	2008
Phishing	707	1.091 *(154)*	1.944 *(178)*
Troyanos	123	512 *(416)*	1.064 *(208)*
Redirectores		41	115 *(280)*
Total	**830**	**1.644 *(198)***	**3.123 *(190)***

Fuente: S21sec

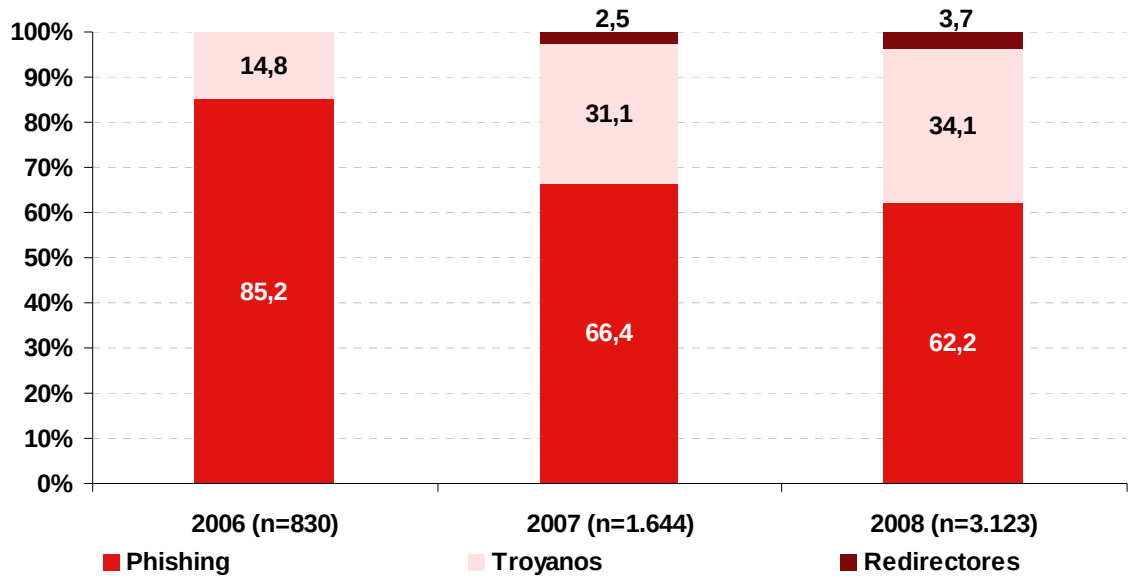
La técnica de ataque sigue siendo el phishing, en primer lugar, con ritmos de crecimiento muy importantes. No obstante, tras un período de hegemonía de los ataques basados en ingeniería social, la realidad actual se caracteriza por un incremento de las situaciones con origen en código malicioso o malware. El Gráfico 4 profundiza en esta afirmación, ofreciendo la evolución del peso de cada una de las tres técnicas de ataque sobre el total de incidentes anuales.

Desde 2007 se detectan cada vez más casos de códigos maliciosos (troyanos), programas especializados en el robo de información que se descargan sigilosamente en el ordenador del usuario, y que se han incrementado notablemente en 2008.

Además, los ataques causados por redirectores han empezado a adquirir protagonismo desde 2007, y se prevé que en los próximos años se intensifiquen los ataques de esta categoría.

El peso de los ataques de phishing sobre el total de incidentes se reduce progresivamente. Esto no debe interpretarse como un retroceso de la ingeniería social en aras de ataques más sofisticados, sino como un crecimiento desigual de cada una de las tres técnicas.

Gráfico 4: Evolución de los distintos tipos de fraude en Internet (%)



Fuente: S21sec

Nos encontramos en un contexto en el que, año tras año, el volumen total de incidentes aumenta. La proporción que phishing, troyanos y redirectores ocupan dentro de ese total se modifica porque el ritmo de crecimiento de los dos segundos es muy superior al ritmo de crecimiento del phishing.

En cualquier caso, lo que es cierto es que el fraude ya no se produce exclusivamente como consecuencia de un engaño (ingeniería social). En la actualidad, está llegando a través de códigos maliciosos, como los troyanos. Esto quiere decir que para ser víctima de un fraude no hace falta que un usuario acceda a un correo electrónico que redirija a una página fraudulenta, sino que, estando un ordenador infectado y conectándose al banco, le pueden robar sus credenciales de forma silenciosa: los datos son enviados a un sitio central donde los atacantes, bandas organizadas en la mayor parte de los casos, hacen las transferencias ilegítimas sin necesidad de contar con la interacción del usuario. Si bien en la cadena del fraude, es necesaria la intervención humana en la fase de blanqueo de dinero, habitualmente se utilizan “mulas” o “muleros”. Personas que, a cambio de una comisión, participan en la circulación del dinero desde las cuentas de los usuarios defraudados hasta las de los ciberdelincuentes, realizándolo a través de diversos medios que pretenden anonimizar al destinatario final de los mismos, como Western Union o medios de pago electrónico.

S21sec, en su *Informe sobre el fraude online 2008*, augura que durante 2009 se pegará el salto a una nueva forma de fraude, que denominan fraude 4.0, y en la que “*se utilizarán*

los datos recabados en las redes sociales para ganar credibilidad a la hora de cometer estos ataques".[10]

Lo que parece claro es que cada vez es más amplia la casuística. En este entorno, debemos asegurarnos de disponer de las herramientas y prácticas de seguridad adecuados para hacer frente a estas amenazas. Además debemos ser cautelosos con nuestra información personal ya que se han detectado casos en los que se utiliza esta información personal robada para llevar a cabo otros delitos relacionados con ciertos tipos de fraude o incluso con casos de pornografía infantil.

En conclusión, el fraude electrónico es cada vez más complejo desde el punto de vista técnico, se lleva a cabo de manera más personalizada a las particularidades del destinatario, y se está profesionalizando en su ejecución.

- Complejidad: la complejidad se aprecia tanto en la sofisticación de las herramientas para conseguir el fraude (robo de contraseñas mediante capturadores de pulsaciones, secuestros del navegador, redireccionamiento de webs…) como en la velocidad con que aparecen nuevas manifestaciones. Existen infinidad de variantes, dado que los creadores, para dificultar su detección, modifican sus códigos constantemente: en la actualidad, se crean miles de ejemplares de malware nuevos cada día.

- Personalización: además, la tendencia es a una mayor personalización, articulando mecanismos de ingeniería social más especializados y adaptados al perfil de la persona objetivo del fraude. Frente a los anteriores ataques masivos e indiscriminados, que en ocasiones adolecían incluso de fallos idiomáticos u ortográficos, están proliferando comunicaciones más personalizadas, que utilizan datos personales válidos de la víctima que son extraídos de redes sociales o a través de otras técnicas (por ejemplo, *whaling*[11] a directivos).

- Profesionalización: por último, es una realidad que el fraude está más profesionalizado: han irrumpido en el panorama bandas organizadas, especialmente procedentes de países del este de Europa, Rusia, China y el sudeste asiático, capaces de utilizar técnicas sofisticadas para cometer acciones fraudulentas. Se trata de redes de crimen organizado que disponen de recursos

[10] S21sec (2009). Informe sobre el fraude online 2008.

[11] El *whaling*, también llamado "caza de ballenas" (whale en inglés). Es una evolución del phishing en la que el ciberdelincuente recaba información de contacto de personas de influencia y alto poder adquisitivo, como empresarios, autoridades y gerentes, habitualmente a través de la información contenida en redes sociales. Posteriormente le remiten un correo electrónico personalizado en el que se le trata de engañar para robar credenciales de cuentas bancarias personales o de la propia compañía. Algunas variantes utilizan la difusión de algún código malicioso que realice una vez instalado el robo de esta información. Este tipo de ataques se caracterizan por el elevado contenido de ingeniería social ya que los contenidos son específicos para el objetivo del fraude, derivando en una carga de confianza mayor ante los detalles de la información utilizada. El ejemplo típico de correo es el que simula contener una citación para el juzgado y que contiene realmente un código malicioso para robar información personal y credenciales de acceso..

tanto económicos como técnicos (por ejemplo la utilización de *fast-flux*[12] en los dominios utilizados para alojar los contenidos fraudulentos).

Complejidad en su desarrollo, personalización a las particularidades del destinatario y profesionalización de su ejecución son características que definen la forma actual de llevar a cabo acciones de fraude electrónico y que, además, dificultan en cierto modo su detección, prevención y eliminación. Se trata de verdaderos ataques en los que ya no es suficiente el sentido común del usuario, sino que exigen la respuesta y actuación por parte de todos los actores implicados.

En el Anexo 1 se analiza desde un punto de vista práctico el funcionamiento de los troyanos bancarios en la comisión del fraude.

[12] El *fast-flux*, es una técnica de DNS utilizada por botnets (red de equipos comprometidos) para ocultar sitios fraudulentos, normalmente phishing o de distribución de malware. Se basa en la utilización de equipos comprometidos que actúan como *proxy*, ocultando el/los servidor/es maliciosos que realmente alojan el contenido fraudulento. Combina dos propiedades del servicio DNS para conseguir su finalidad, Round Robin DNS y definición de TTL bajo. Con esto se consigue cambiar de forma rápida las direcciones IP que actúan como *proxys* dotando de mayor disponibilidad al servicio fraudulento.

6 EL FRAUDE EN INTERNET EN ESPAÑA: DATOS ESTADÍSTICOS

6.1 Fraude e ingeniería social

Este epígrafe analiza la evolución de la incidencia de situaciones de fraude basado en técnicas de ingeniería social a través de Internet (Gráfico 5) y a través del teléfono móvil (Gráfico 6) entre los usuarios de Internet españoles.

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

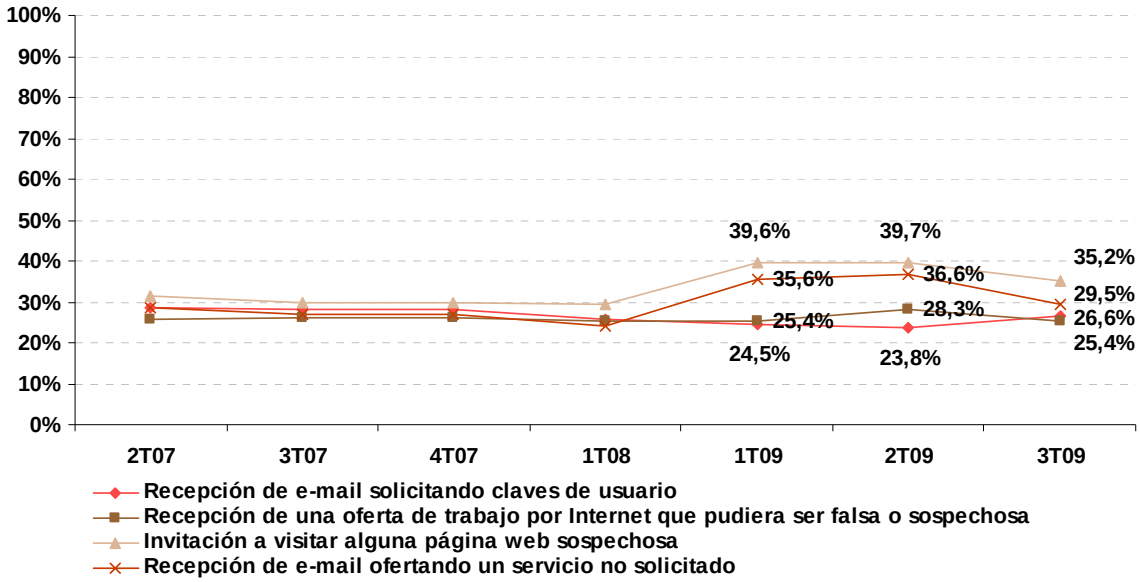
- En primer lugar, los datos proporcionados en ambos gráficos están basados en las respuestas proporcionados por el panel de usuarios de Internet españoles, ofreciendo por tanto la perspectiva del ciudadano.

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

El 35,2% de los usuarios de Internet españoles declara, en el 3er trimestre de 2009, haber recibido alguna petición de visitar páginas web sospechosas en los 3 meses previos a la realización de la encuesta. Por detrás de ella, el 29,5% afirman haber recibido e-mails ofertando servicios no solicitados. Son las dos incidencias declaradas con mayor frecuencia. Los casos de ofertas de trabajo potencialmente falsas o sospechosas y la recepción de un e-mail solicitando las claves de usuario son más infrecuentes, y son declarados por un 25,4% y 26,6% de los usuarios, respectivamente.

Respecto a la evolución experimentada desde 2007, se aprecia en el primer trimestre de 2009 un importante crecimiento de los dos comportamientos más frecuentes: la petición de visitar alguna página web sospechosa y la recepción de correos electrónicos ofertando servicios no solicitados. La tendencia se mantiene en el segundo trimestre de 2009, donde también se aprecia un repunte de la recepción de ofertas de trabajo potencialmente falsas o sospechosas, que alcanza su máximo histórico de incidencia con un 28,3% de usuarios que afirman haber recibido ofertas de trabajo falsas. En el tercer trimestre de 2009 el nivel de incidencia declarada de esta situación desciende ligeramente, hasta un 26,6% de los usuarios que afirman haberla experimentado. La misma tendencia decreciente se aprecia en la petición de visitar alguna página web sospechosa (-4,5 pp) y, sobre todo, en la recepción de e-mails ofertando servicios no solicitados (-7,1 pp).

Gráfico 5: Evolución de la incidencia declarada de situaciones de intento (no consumado) de fraude a través de Internet en los últimos 3 meses (%)



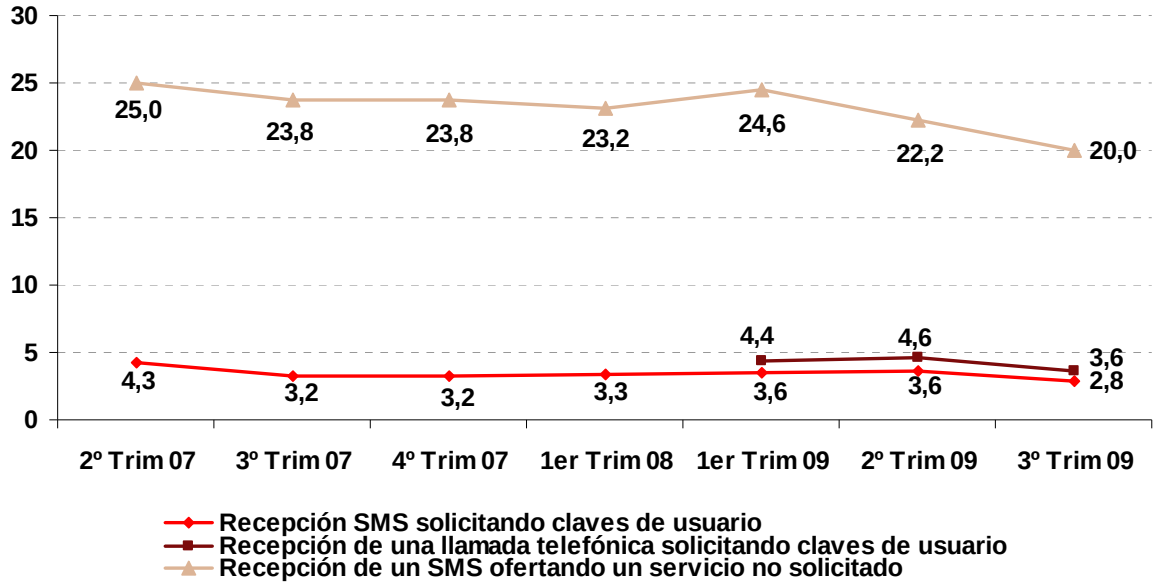
Fuente: INTECO

Las situaciones de fraude a través del teléfono móvil presentan frecuencias inferiores a las ocurridas a través de Internet, tal y como muestra el Gráfico 6.

De las tres analizadas, la única que adquiere una frecuencia relevante es la recepción de SMS ofertando servicios no solicitados, que sucede en el 3er trimestre de 2009 a un 20% de los usuarios de Internet españoles. Desde una perspectiva evolutiva, la incidencia de esta situación ha seguido una evolución decreciente desde 2007.

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 (2,8%).

Gráfico 6: Evolución de la incidencia declarada de situaciones de intento (no consumado) de fraude a través del teléfono móvil en los últimos 3 meses (%)

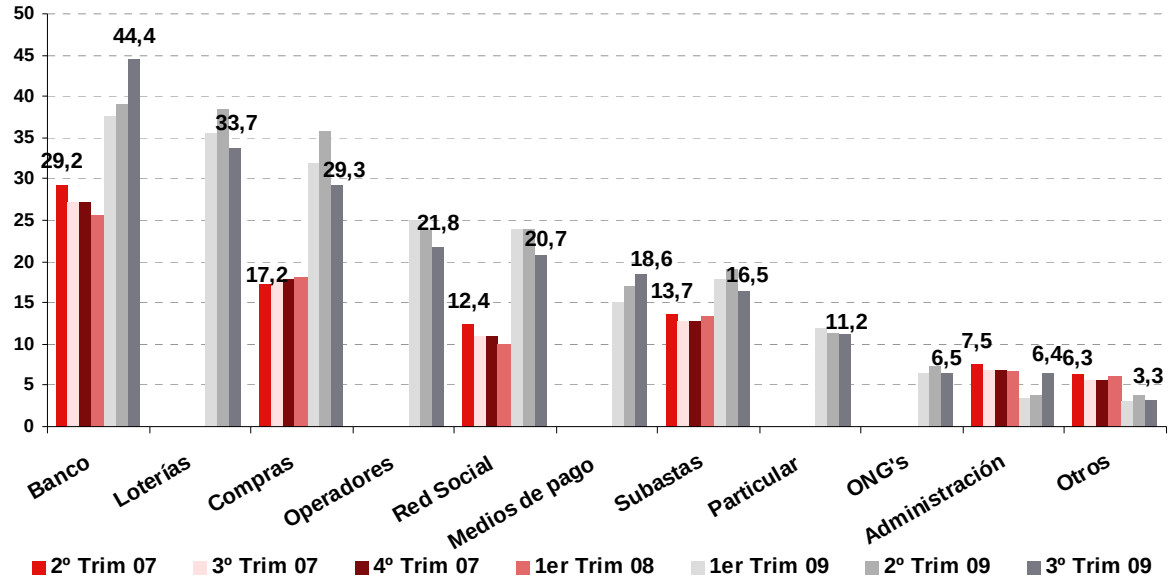


Fuente: INTECO

6.2 Forma adoptada por el remitente de la comunicación sospechosa de ser fraudulenta

¿Qué sectores están viéndose afectados por el fraude electrónico? El Gráfico 7 muestra los datos para España, basados en las respuestas de los panelistas a la pregunta: *¿qué tipo de entidad sospechosa decía ser la que solicitaba sus claves/datos?* En él se constata cómo la industria más afectada sigue siendo el sector bancario, con un 44,4% de los usuarios que afirmaron haber recibido comunicaciones fraudulentas de un supuesto banco en el 3er trimestre de 2009. Por detrás de las entidades bancarias, las webs de loterías (33,7%), las webs de compras online (29,3%), operadores de telecomunicaciones (21,8%), redes sociales (20,7%) y las páginas de subastas (16,5%) son los sectores más afectados por el fraude electrónico.

Gráfico 7: Evolución de las formas adoptadas por el remitente de la comunicación sospechosa de ser fraudulenta [13] (%)



Fuente: INTECO

A partir de la información recogida en los casos de fraude gestionados por el servicio de gestión del fraude de INTECO-CERT se puede obtener una tabla con información similar (basada, en este caso, en el análisis realizado por los técnicos de INTECO-CERT sobre los casos gestionados). Los datos confirman el predominio del sector financiero (el 77,4% de los casos gestionados en el 3er trimestre de están asociados con entidades de este tipo). Las webs de comercio electrónico, Administración y otros sectores están representados, en el mismo período, en un 18,4%, 2,3% y 2% de los casos, respectivamente.

Se han detectado casos más específicos, como compañías de transporte de viajeros y organismos policiales.

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

Tabla 7: Sectores afectados por el fraude en Internet (%)

Sector	2T 07	3T 07	4T 07	1T 08	2T 08	3T 08	4T 08	1T 09	2T 09	3T 09
Financiero	92,0%	97,1%	98,7%	89,1%	89,8%	80,7%	84,5%	73,5%	75,3%	77,4%
e-Comercio	8,0%		1,4%	8,9%	10,0%	19,2%	15,3%	25,1%	21,7%	18,4%
Administración		2,9%		1,9%	0,2%	0,2%	0,2%	0,6%	1,0%	2,3%
Otros								0,8%	2,0%	2,0%
Total	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**

Fuente: INTECO-CERT

Los datos proporcionados por el *Anti-Phishing Working Group* a nivel mundial muestran una realidad ciertamente similar a la española: en el segundo trimestre de 2009 (últimos datos facilitados por la organización APWG), un 32% de los ataques se dirigían al sector financiero y un 49% a servicios de pago[14].

6.3 Impacto económico del fraude

Un 3,8% de los usuarios de Internet españoles afirman, en el tercer trimestre de 2009, haber sufrido una pérdida económica como consecuencia de un fraude electrónico, y un 3,3% declaraba lo mismo el trimestre anterior.

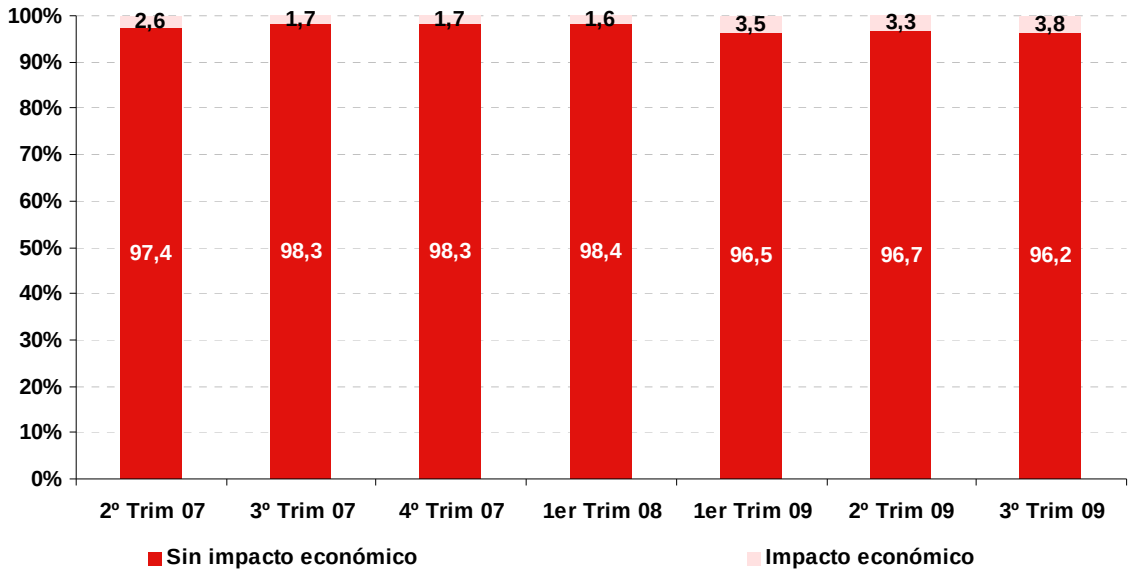
La serie temporal analizada se inicia con niveles de incidencia del 2,6% en el segundo trimestre de 2007, bajando posteriormente a cotas de 1,7% y 1,6% entre el tercer trimestre de 2007 y el 1º de 2008. En el 2009 la incidencia de fraude con perjuicio económico aumenta y se sitúa en torno al 3%.

La consultora Gartner publicaba en diciembre de 2007 el siguiente dato: un 3,3% de los consumidores que recibieron e-mails con phishing perdieron dinero a consecuencia del ataque, frente a un 2,3% que afirmaba lo mismo en 2006 y un 2,9% el año precedente. Los datos, referidos a la realidad norteamericana (están basados en una encuesta online a más de 4.500 usuarios de EE.UU)[15], muestran coherencia con la realidad española analizada en este estudio.

[14] Anti-Phishing Working Group (APWG) (2009). *Phishing Activity Trends Report, 1st Half 2009.*

[15] http://www.gartner.com/it/page.jsp?id=565125

Gráfico 8: Evolución del fraude con impacto económico para el usuario (%)



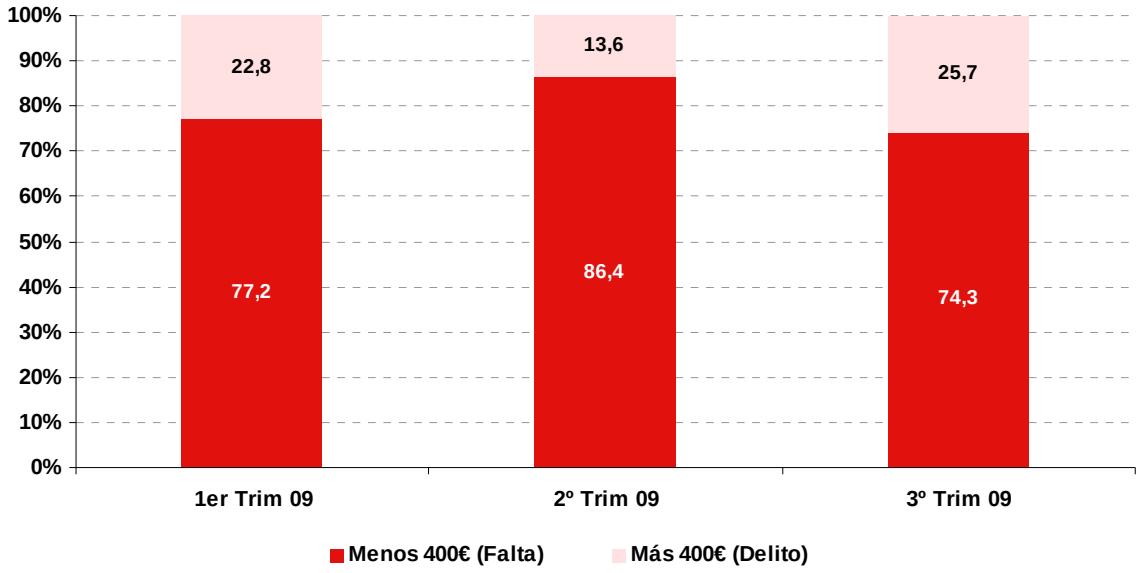
Fuente: INTECO

La mayor parte de las pérdidas económicas consecuencia del fraude son de escasa cuantía: el 74,3% son inferiores a 400 euros en el tercer trimestre de 2009. (Es más, el 44,5% de los usuarios españoles de Internet declara haber sufrido pérdidas inferiores a 100 euros.)

Dada la escasa trascendencia del importe, existe el riesgo de que el fraude pase inadvertido a la víctima y por tanto no sea denunciado ante la autoridad competente (ni declarado en el cuestionario). En este punto, es relevante recordar que los datos aquí presentados están basados en la percepción de las personas entrevistadas.

El Código Penal español establece en 400 € el límite entre lo que se considera falta y delito. La distinción es relevante, y afecta a la severidad de la pena a aplicar al estafador (más grave en el caso de un delito que de una falta). Quizás este sea el motivo que justifique la comisión de fraudes con cuantías reducidas: aproximadamente el 75% de los fraudes declarados por los usuarios en el tercer trimestre de 2009 no llegan a los 400 euros.

Gráfico 9: Evolución de la cuantía económica derivada del fraude (%)

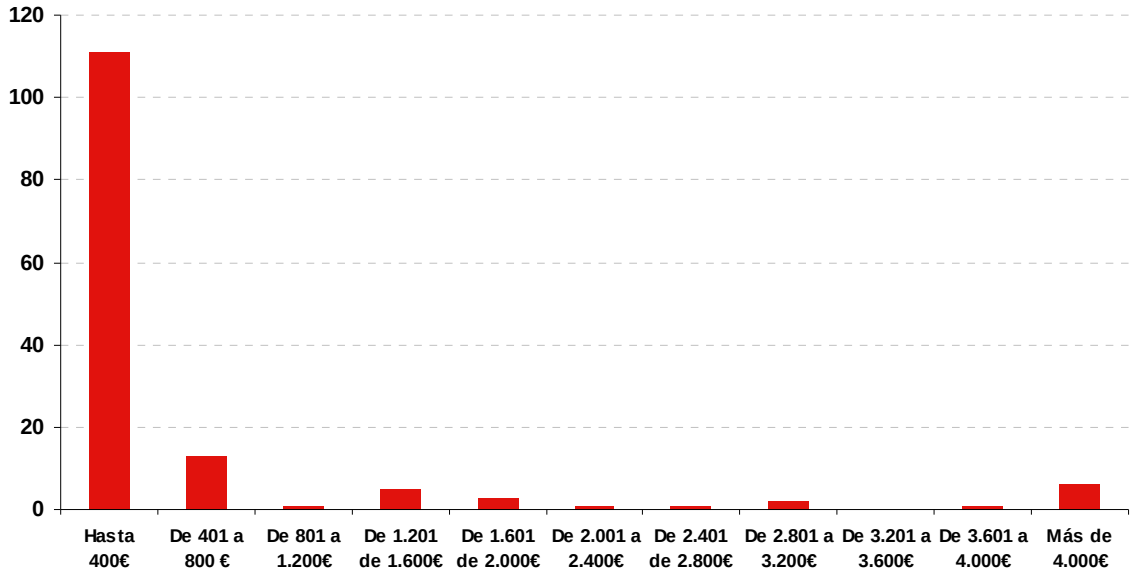


Fuente: INTECO

Profundizando en los datos del 3er trimestre de 2009, el Gráfico 9 muestra visualmente cómo se distribuye la cuantía defraudada. Se trata de una distribución asimétrica positiva, donde la mayor parte de los casos se concentran en las cantidades más reducidas.

La mediana se sitúa en 120 €, e indica el punto que deja a la mitad de los casos por debajo y por encima de él.

Gráfico 10: Distribución del importe defraudado en el 3er trimestre de 2009 (frecuencia)



Fuente: INTECO

6.4 Fraude y malware

Además de las técnicas basadas en el engaño tradicional, se veía al principio del informe que existen manifestaciones de malware que, en muchas ocasiones, se encuentran en el origen del fraude. Los ataques consisten en la introducción de malware en los equipos para robar credenciales de acceso o tomar control de un ordenador de forma remota. En general, la introducción de código malicioso se hace de forma no visible para el usuario, que no percibe nada anómalo.

Por ello, este capítulo analiza la presencia de código malicioso en los equipos españoles. Los datos que aquí se presentan han sido obtenidos a partir del escaneo de los equipos de los panelistas gracias a la herramienta iScan, programa desarrollado por INTECO que detecta el malware residente en los equipos mediante 46 motores antivirus distintos. (El apartado 2.3 Análisis de seguridad de los equipos ofrece una descripción detallada de la herramienta.)

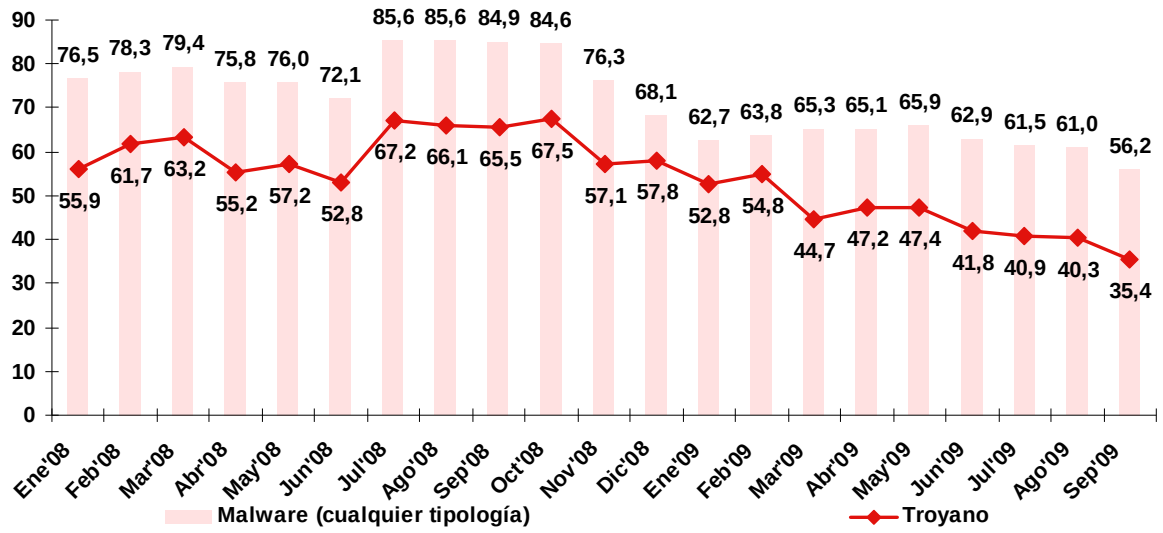
6.4.1 Evolución del código malicioso en los equipos españoles: troyanos

La categoría de malware más estrechamente relacionada con la incidencia de malware es la constituida por los troyanos. Un troyano o caballo de Troya es una pieza de software dañino disfrazado de software legítimo. No producen efectos realmente visibles o apreciables en el momento de llegar al equipo. Dentro de los troyanos, a su vez, existen diferentes tipos, en función de los efectos sobre el sistema. En general presentan un nivel de peligrosidad alta. Al final del informe se incluye un glosario donde el lector puede encontrar información más detallada al respecto.

El nivel de infección de los equipos se mantuvo a lo largo de 2008 en valores que oscilan entre 70 y 80%. En 2009, la presencia de malware en los equipos se sitúa en niveles ligeramente inferiores, entre el 60 y el 65%. Parece que, tras el pico experimentado en verano de 2008, los niveles han vuelto a recuperar la estabilidad. El 56,2% de los equipos analizados tiene alguna manifestación de código malicioso o malware en septiembre de 2009, último mes analizado por iScan. Se trata del dato más bajo desde el inicio de la serie temporal.

El tipo de código malicioso que con más frecuencia aparece en los equipos españoles es, precisamente, el tipo troyano: en septiembre de 2009 el 35,4% de los ordenadores alojaban troyanos. ¿Qué explica esta situación? La respuesta parece obvia: dada la alta “rentabilidad” que los troyanos proporcionan a sus creadores, medida en términos de beneficio económico derivado de acciones fraudulentas, es lógico pensar que éstos invierten más esfuerzo en la creación y difusión de este tipo de código malicioso. En general, el motivo de que se creen más troyanos que ningún otro tipo de malware es porque resultan los más lucrativos.

Gráfico 11: Evolución de equipos que alojan malware y específicamente troyanos (%)



Fuente: INTECO

En cualquier caso, los ratios de detección siguen siendo elevados, y confirman la proliferación del malware y en especial de los troyanos, punto en el que coinciden los principales agentes del sector.

6.4.2 Peligrosidad del código malicioso y riesgo del equipo

En este apartado se analiza el nivel de peligrosidad que presenta el código malicioso detectado en función del riesgo potencial que éste puede suponer para el equipo y para el usuario.

Para ello, se han definido tres categorías de riesgo: alto, medio y bajo. En la asignación de cada variante a uno u otro grupo se ha seguido el siguiente criterio:

- **Riesgo alto**: se incluyen en esta categoría los especímenes que, potencialmente, permiten el acceso remoto por parte de un atacante al sistema víctima; pueden suponer un perjuicio económico para el usuario; facilitan la captura de información confidencial o sensible de la víctima; se emplean como pasarelas para atacar otros equipos (pudiendo acarrear consecuencias legales para la víctima); minan el rendimiento y funcionalidad del sistema, ya sea borrando archivos, ralentizando el equipo, cerrando ventanas, etc.

  En base a este criterio, se asimilan a variantes de malware de riesgo alto los troyanos, dialers (marcadores telefónicos), keyloggers (registradores de pulsaciones de teclado), virus, gusanos, rootkits, exploits, y macros.

- **Riesgo medio**: se incluyen aquí ejemplares que, si bien tienen un impacto no deseado sobre el sistema, no perjudican de forma notoria su rendimiento: abren ventanas no deseadas al navegar; incrustan publicidad en páginas web legítimas que realmente no contienen publicidad; facilitan la captura de información no sensible de la víctima (por ejemplo, patrones de navegación para crear perfiles de publicidad dirigida, etc.).

  Las categorías consideradas son adware (software publicitario no deseado), spyware (programas espía), detecciones heurísticas[16] y scripts[17].

- **Riesgo bajo**: aquí se engloban las manifestaciones que menor nivel de afección tienen sobre los equipos. Se trata de útiles empleados para hacking (escaneo de puertos, modificadores de direcciones ethernet, etc.). En la mayoría de los casos son herramientas instaladas por el usuario de forma intencionada, para listar y matar procesos, o conectarse remotamente a su equipo, etc. Por otra parte, también se consideran especímenes de riesgo bajo los típicos programas broma (por ejemplo aquellos que despliegan una ventana que se va moviendo y resulta imposible cerrarla con el ratón) y los virus exclusivos para plataformas móviles pues estos no son capaces de ejecutarse sobre los equipos de los usuarios.

  A los efectos del estudio, se consideran como malware de bajo nivel de riesgo las herramientas[18], bromas y malware para plataformas Symbian.

Se trata de una clasificación genérica que, como cualquier clasificación que siga esta metodología, en ocasiones puede estar errada[19]. El sesgo puede proceder no sólo por la generalización a categorías en base a los criterios descritos, sino también por el propio entorno en donde se encuentre la muestra (por ejemplo, un dialer o marcador telefónico será en realidad de riesgo nulo para un equipo que no posee un modem convencional para red telefónica básica ya que por regla general los routers ADSL no tienen la posibilidad de hacer llamadas; sin embargo, en la clasificación empleada en el estudio se está considerando a los dialers como de riesgo alto, por su potencial impacto económico sobre la víctima.)

[16] Detecciones de códigos maliciosos que no están aún catalogados y que se basan en la búsqueda de un comportamiento sospechoso durante la ejecución del código.

[17] Las secuencias de comandos maliciosos (scripts) pueden representar riesgo alto en determinados casos.

[18] El malware del tipo "herramienta" puede tener un riesgo variable dependiendo de si ha sido instalada conscientemente por el usuario legítimo del equipo o por un tercero sin su conocimiento. Por ello, en este indicador se ha aplicado por defecto el nivel de riesgo bajo, aunque en algunas circunstancias un malware catalogado como herramienta pueda ser de riesgo alto.

[19] La determinación del riesgo de las muestras mediante análisis manual de lastadas las variantes, si bien más rigurosa, sería en exceso lenta y costosa. Considerando que las propiedades de las distintas categorías del malware estudiado siguen una distribución gaussiana, la desviación global de la adopción de un enfoque genérico es despreciable en términos estadísticos.

Según los datos procedentes del escaneo de septiembre de 2009, el 38% de los equipos analizados está infectado por código malicioso considerado de peligrosidad alta. El 12,5% contiene malware que implica un nivel de riesgo medio, y tan sólo un 5,8% alberga código con riesgo bajo. El resto de equipos no presenta riesgo.

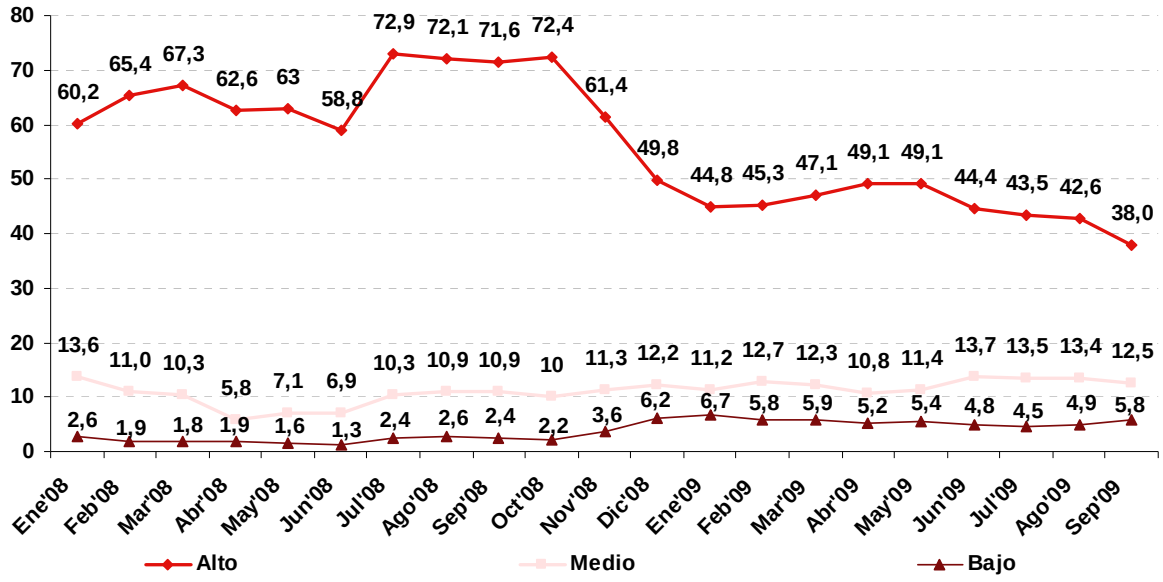
Esta clasificación es lógica, dada la alta presencia de troyanos, que son considerados en su totalidad como malware de riesgo alto, entre los equipos.

Entiéndase que este análisis se efectúa sobre los equipos, y no sobre el código malicioso en sí mismo. Es decir, un equipo infectado con troyano y adware, estará incluido en el grupo de riesgo alto (troyano), y no en el medio (adware). Es el llamado efecto pantalla, y hace que se disparen los niveles altos de riesgo (a causa de la elevada presencia de troyanos) en detrimento de los niveles más bajos.

En definitiva, los ordenadores analizados presentan patrones multi-infección con una gran incidencia de troyanos. Esto hace que el valor de riesgo alto prepondere sobre los demás, lo cual no quiere decir que las amenazas de riesgos medios y bajos no estén tan extendidas.

Desde una perspectiva evolutiva, la conclusión que arroja el análisis del Gráfico 12 es que los niveles de riesgo muestran una tendencia decreciente. Tras el pico experimentado en los meses de julio a octubre de 2008, cuando el nivel de equipos con riesgo alto subió por encima de lo habitual hasta alcanzar más del 70%, se ha vuelto a recuperar los niveles previos a ese período, con las lecturas de 2009 situándose siempre por debajo del 50%. Con un 38% de equipos con riesgo alto detectados en septiembre de 2009, se alcanza el mínimo histórico desde el inicio de la serie.

Gráfico 12: Evolución del nivel de riesgo de los equipos (%)



Fuente: INTECO

6.4.3 Diversificación del código malicioso

Para determinar el grado de diversificación del malware se analiza el número de detecciones de cada uno de los códigos maliciosos detectados, y en qué medida están presentes en los equipos.

La Tabla 8 ofrece el primer paso para efectuar el análisis: de todos los archivos maliciosos detectados, ¿cuántas "variantes únicas" se identifican? Es decir, ¿cuántos archivos distintos se han encontrado? Se muestra la serie correspondiente a los nueve últimos períodos analizados. De la relación entre ambos se extrae un índice de repetición, que representaría el número de veces que aparecería cada variante de malware.

Los datos confirman el alto nivel de diversificación del código malicioso: cada variante única detectada se encontraría (hipotéticamente) en tan sólo 2,2 archivos, de todos los archivos infectados identificados en el escaneo.

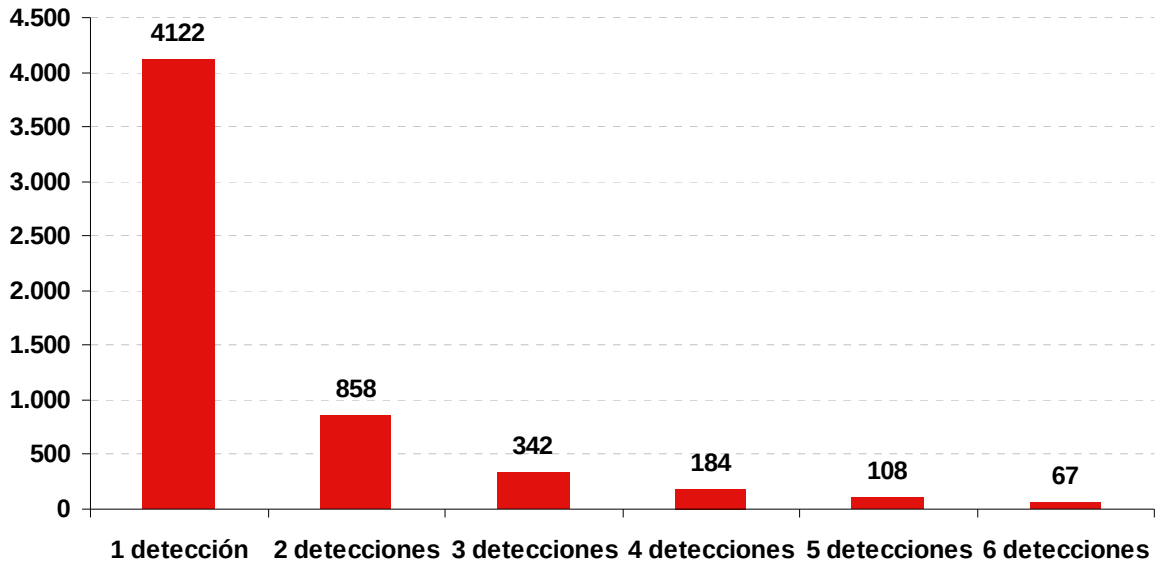
Tabla 8: Evolución del número total de archivos maliciosos, variantes únicas de malware e índice de repetición

	Dic.08	Ene.09	Feb.09	Mar.09	Abr.09	May.09	Jun.09	Jul.09	Ago.09	Sep.09
Núm. de archivos maliciosos	18.415	20.332	15.895	17.967	21.923	20.303	15.949	13.984	12.640	13.609
Variantes únicas de malware	6.943	7.410	6.208	6.774	9.141	8.425	6.930	6.246	5.682	5.952
Índice de repetición	*2,7*	*2,7*	*2,6*	*2,7*	*2,4*	*2,4*	*2,3*	*2,2*	*2,2*	*2,3*

Fuente: INTECO

Más aún, de las variantes únicas detectadas, dos tercios aparecen en un solo equipo: se trata de detecciones únicas de las variantes únicas. El análisis para mayo de 2009 (último mes del que se disponen datos) se muestra en el Gráfico 13, y confirma el alto nivel de diversificación y heterogeneidad del malware: de las 5.942 variantes únicas de malware identificadas en septiembre de 2009, 4.122 se detectan en una sola ocasión.

Gráfico 13: Número de detecciones de cada variante única de malware en septiembre de 2009



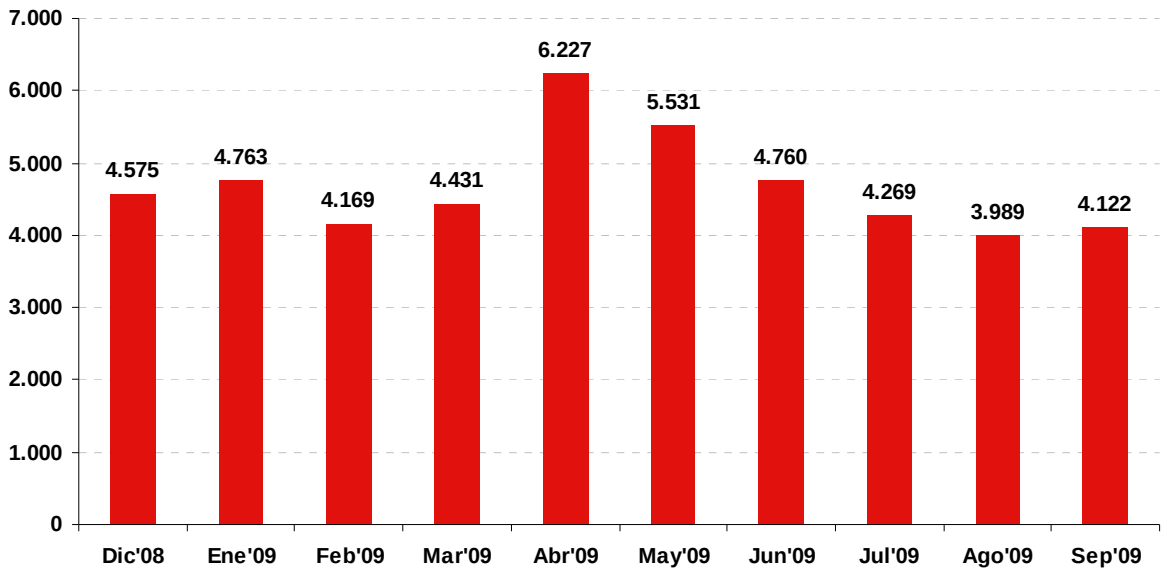
Fuente: INTECO

Este dato constata la velocidad con que aparecen nuevas manifestaciones. Existen infinidad de variantes, dado que los creadores, para dificultar su detección, modifican sus códigos constantemente: en la actualidad, se crean miles de ejemplares de malware nuevos cada día.

Este alto nivel de diversificación y heterogeneidad se convierte en el principal obstáculo para la efectividad de ciertos programas antimalware (aquéllos basados en el reconocimiento de especímenes como requisito para aplicar la correspondiente vacuna; en la medida en que el espécimen no sea reconocido por el programa, no podrá diseñar ni aplicar vacunas).

Desde una perspectiva evolutiva, ¿nos encontramos ante un código malicioso que cada vez tiende más a la diversificación? Se ofrece aquí la evolución experimentada en los últimos nueve períodos. Apréciese que, si bien el análisis de nueve meses quizás es insuficiente para definir una tendencia, los niveles de detecciones únicas se mueven en niveles inferiores a las 5.000 detecciones únicas mensuales, con excepción de los meses de abril de 2009 (6.227) y mayo de 2009 (5.531).

Gráfico 14: Evolución de la detección única de variantes únicas



Fuente: INTECO

6.4.4 Malware específico para el fraude. Análisis internacional

Keyloggers y troyanos bancarios

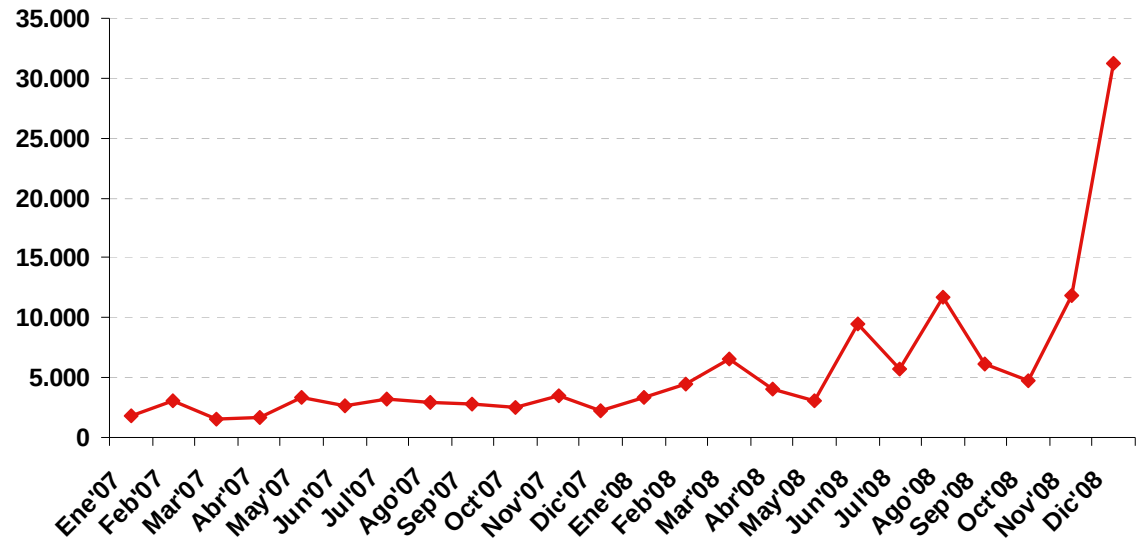
El *Anti-Phishing Working Group* analiza en particular el malware que tiene que ver específicamente con la comisión de fraude. Estos códigos maliciosos tienen una serie de componentes con el objetivo de controlar acciones específicas del usuario, realizadas durante el acceso a organizaciones específicas (principalmente, entidades financieras y de comercio electrónico) e intentan robar cierta información específica o falsear las operaciones del usuario.

Se recuerda, una vez más, que los datos proporcionados por el APWG tienen ámbito internacional y están construidos a partir de la información reportada por sus socios.

El volumen de URLs difusoras de código malicioso de captura de contraseñas alcanzó en diciembre de 2008 la cifra de 31.173, lo que supone un espectacular incremento del 827% desde los datos de enero de ese mismo año, con 3.362 URLs identificadas.

Se trata de un número elevadísimo, teniendo en cuenta el histórico. Habrá que esperar a sucesivas lecturas del APWG para confirmar si se trata del inicio de una tendencia, o de un hecho puntual.

Gráfico 15: URLs que alojan código malicioso específico para el fraude

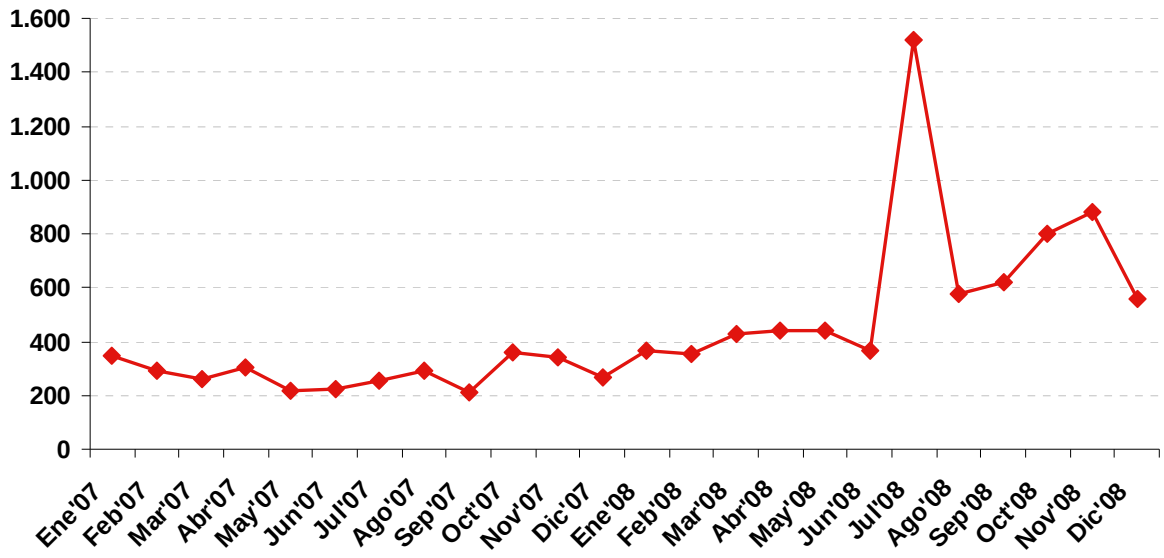


Fuente: Anti-Phishing Working Group (APWG)

Además de analizar el número de URLs con código malicioso específico para el fraude, el *Anti-Phishing Working Group* también proporciona datos sobre el número de variantes

únicas de este tipo específico de malware. Así, en el Gráfico 16 se puede apreciar cómo, tras un pico de 1.519 variantes únicas identificadas en julio de 2008, el volumen cae en diciembre hasta alcanzar las 559 unidades.

Gráfico 16: Variantes únicas de código malicioso de captura de contraseñas (keyloggers y similares)



Fuente: Anti-Phishing Working Group (APWG)

Rogueware

Con el término *rogueware* se identifica a aplicaciones que se hacen pasar por soluciones antivirus que cobran a los usuarios por eliminar amenazas que en realidad no existen. No existe un robo de información por parte de los ciberdelincuentes, sino que es el propio usuario el que, a través del engaño, accede a pagar la licencia de una herramienta de seguridad que en realidad no es tal.

La utilización de este tipo de aplicaciones se ha hecho masiva desde principios de 2008, y por ello requieren una atención especial. PandaLabs, conscientes de la proliferación de este tipo de programas, ha publicado el informe *El negocio de los falsos antivirus. Análisis del nuevo estilo de Fraude Online*[20].

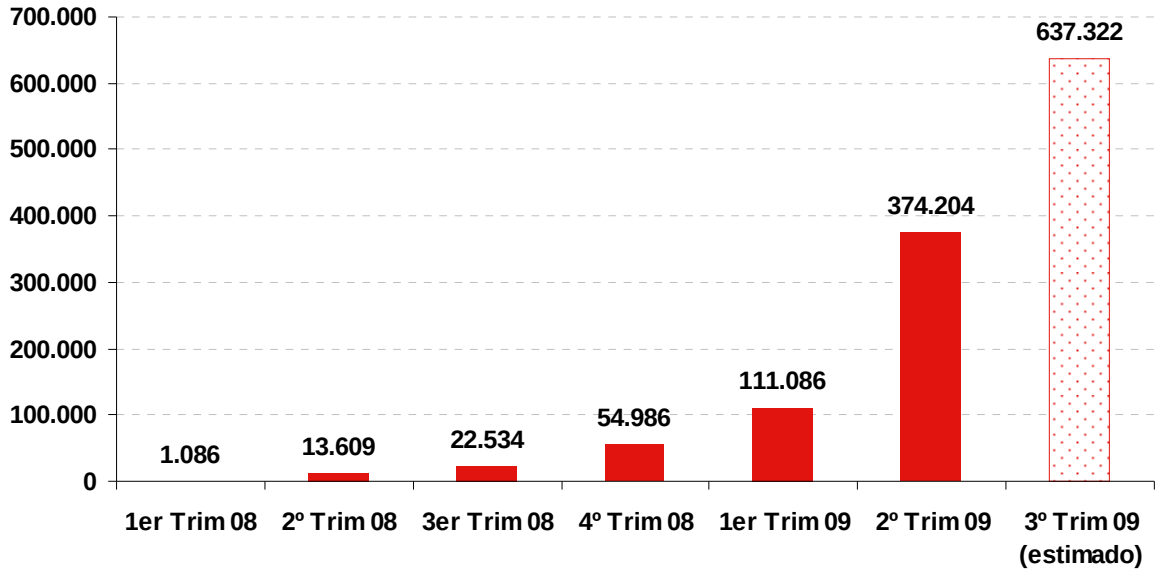
Los datos que aquí se presentan han sido extraídos de ese informe. En él, PandaLabs constata cómo el crecimiento de este tipo de programas de falsos antivirus o rogueware ha sido exponencial en este último año, tal y como muestra el Gráfico 17: en el primer

[20] Corrons, Luis y Correl, Sean-Paul (2009). *El Negocio de los Falsos Antivirus. Análisis del nuevo estilo de Fraude Online.* Panda Security. Versión online disponible en:

http://www.pandasecurity.com/img/enc/El%20Negocio%20de%20los%20falsos%20antivirus.pdf

trimestre de 2009 se crearon más ejemplares que durante todo el año 2008. El segundo trimestre fue aún peor, ya que surgieron cuatro veces más ejemplares que en el año 2008. PandaLabs calcula que en el tercer trimestre de 2009 el número total de ejemplares de malware superará la cifra surgida en los 18 meses anteriores.

Gráfico 17: Falsos antivirus o *rogueware*



Fuente: PandaLabs

6.5 Áreas de procedencia de los ataques detectados en España

Para completar el análisis, se ofrece una visión de las áreas de procedencia de los ataques de fraude detectados en España, consecuencia de acciones de phishing, código malicioso y redirectores.

Los datos que se ofrecen en este apartado han sido recogidos por S21sec que, en sus informes periódicos sobre el fraude electrónico, indica el número de ataques procedentes de cada país.

Como puede apreciarse, Estados Unidos es el país de procedencia de la mayor parte de los ataques detectados en España, ya se trate de phishing (41,7%), código malicioso (48,1%) o redirectores (62,6%).

Tabla 9: Área de procedencia de los ataques de phishing detectados en España

	2006		2007		2008	
	Nº incidentes	%	Nº incidentes	%	Nº incidentes	%
Alemania	23	3,3%	68	6,2%	65	3,3%
Canadá	26	3,7%				
Corea del Sur			22	2,0%		
China	22	3,1%	41	3,8%	71	3,7%
EE.UU.	420	59,4%	596	54,6%	810	41,7%
Francia			42	3,8%		
México					166	8,5%
Reino Unido	23	3,3%	40	3,7%	55	2,8%
Rumanía					40	2,1%
Rusia	54	7,6%	50	4,6%		
Turquía					188	9,7%
Otros	139	19,7%	232	21,3%	549	28,2%
Total	**707**	**100,0%**	**1.091**	**100,0%**	**1.944**	**100,0%**

Fuente: S21sec

Tabla 10: Área de procedencia de los ataques de código malicioso detectados en España

	2006		2007		2008	
	Nº incidentes	%	Nº incidentes	%	Nº incidentes	%
Alemania			18	3,5%	41	3,9%
Argentina					34	3,2%
Australia					50	4,7%
Canadá	1	0,8%				
China			17	3,3%	23	2,2%
Eslovaquia			15	2,9%		
España			25	4,9%	31	2,9%
EE.UU.	54	43,9%	280	54,7%	512	48,1%
Estonia	2	1,6%				
Letonia	1	0,8%				
Reino Unido	1	0,8%				
Rusia	62	50,4%	46	9,0%	75	7,0%
Turquía			23	4,5%		
Ucrania	2	1,6%				
Otros			88	17,2%	298	28,0%
Total	**123**	**100,0%**	**512**	**100,0%**	**1.064**	**100,0%**

Fuente: S21sec

Tabla 11: Área de procedencia de los redirectores detectados en España

	2007		2008	
	Nº incidentes	%	Nº incidentes	%
Alemania	3	7,3%		
Canadá			5	4,3%
China			4	3,5%
EE.UU.	27	65,9%	72	62,6%
Reino Unido	3	7,3%		
Rumania			5	4,3%
Rusia			4	3,5%
Otros	8	19,5%	25	21,7%
Total	**41**	**100,0%**	**115**	**100,0%**

Fuente: S21sec

6.6 Herramientas y hábitos de seguridad para prevenir el fraude

Es cierto que los ciberdelincuentes son muy activos en la creación de nuevas formas de mecanismos para la comisión del fraude. También es cierto que, tanto la industria de la seguridad informática, como las organizaciones de los sectores afectados (principalmente, entidades bancarias) están llevando a cabo grandes esfuerzos para garantizar la seguridad de sus webs y evitar, o minimizar, la incidencia de acciones fraudulentas sobre sus clientes. El tercer eje es el usuario, eslabón más débil de la cadena del fraude. Existen una serie de herramientas y hábitos de seguridad que pueden contribuir a una adecuada prevención contra el fraude.

Los programas anti-fraude están instalados, en opinión de los usuarios en un 34,7% de los equipos en el tercer trimestre de 2009, mismo porcentaje que el trimestre inmediatamente anterior y casi dos puntos porcentuales por encima de la presencia detectada en el primer trimestre del año.

Tabla 12: Herramientas de seguridad instaladas en los equipos (%)

	1T 09	2T 09	3T 09
Programas anti-fraude	32,9%	34,9%	34,7%

Fuente: INTECO

Por lo que respecta a los hábitos de seguridad, predominan los comportamientos prudentes sobre los imprudentes. En el tercer trimestre de 2009, son masivos los hábitos de vigilar periódicamente los movimientos de las cuentas online (75,7%), comprobar la conexión segura al efectuar transacciones online (73,1%), evitar el acceso desde equipos públicos (82,6%), no facilitar datos personales a través del correo electrónico o por

teléfono (79,9%) y cerrar la sesión de banca electrónica antes de salir de la página (83,0%).

El único hábito referido a transacciones económicas online que no está suficientemente implantado entre los usuarios de Internet españoles tiene que ver con la introducción de la dirección web del banco directamente en la barra de direcciones del navegador. Un 53,1% declara hacerlo habitualmente. A pesar de que son mayoría los usuarios que adoptan este hábito, todavía existe margen de crecimiento para alcanzar la tasa de cumplimiento del resto de comportamientos analizados.

El riesgo de no llevar a cabo este comportamiento puede tener implicaciones económicas, en el caso de los phishing: este tipo de fraudes tiene lugar a través de la recepción de un correo electrónico con un enlace falso que dirige a una página suplantada de la entidad que supuestamente envía el e-mail.

Si bien el hábito de teclear la dirección del banco en la barra del navegador en lugar de pinchar en un link minimiza el riesgo de phishing, es necesario indicar que no elimina completamente el riesgo de ser víctima de fraude. Con la premisa de que la seguridad total no existe, y con la certeza de que los creadores de códigos maliciosos avanzan deprisa, se pueden dar casos de fraude incluso habiendo tecleado directamente la dirección en la barra[21].

[21] Si el archivo hosts local resuelve los dominios del banco a direcciones IP donde escuchan servidores fraudulentos, este hecho es suficiente para que el hábito de teclear la dirección del banco en la barra del navegador no sea suficiente para evitar el fraude. Además también existen troyanos bancarios que roban las credenciales de acceso cuando el usuario está accediendo al propio portal de la entidad.

Tabla 13: Hábitos relacionados con la banca en línea y el comercio electrónico manifestados en el primer trimestre de 2009 (%)

Hábitos	1T 09	2T 09	3T 09	Balance	Evolución 1T-3T
Vigilo periódicamente los movimientos de la cuenta bancaria online	73,6	74,9	75,7	☺	▲
Cuando realizo transacciones online (pagos, compras, transferencias) compruebo que uso una conexión segura (protocolo https, validez y vigencia del certificado)	70,0	71,5	73,1	☺	▲
Evito usar equipos públicos o compartidos (cibercafés, estaciones o aeropuertos)	82,1	83,4	82,6	☺	▲
Cuando mi banco me pide mis datos personales o contraseñas por correo electrónico o por teléfono se los facilito *(desacuerdo)*	77,1	79,6	79,9	☺	▲
Cierro la sesión al terminar de realizar operaciones online con mi banco	81,5	84,5	83,0	☺	▲
Siempre tecleo la dirección web de mi banco en la barra de direcciones	49,9	52,5	53,1	😐	▲

Fuente: INTECO

6.7 Fraude y e-confianza

En este epígrafe se intenta dar respuesta a la siguiente pregunta, que constituye uno de los objetivos del estudio que se mencionaban al principio del documento: el fraude (tanto su mera existencia como el haber sido víctima de fraude), ¿ejerce algún tipo de influencia sobre el nivel de e-confianza que muestran los ciudadanos?

6.7.1 Desarrollo de la Sociedad de la Información y e-confianza

El primer paso para conocer el nivel de e-confianza de los usuarios españoles de Internet es analizar el grado de adopción de la Sociedad de la Información en nuestro país.

El Gráfico 18 ofrece una visión positiva: la Sociedad de la Información presenta un nivel de desarrollo más que aceptable en España, basándonos en la penetración de algunos de sus servicios en el tercer trimestre de 2008 y en su evolución positiva desde el mismo período del año 2006. Se trata de datos proporcionados por Red.es en su informe *Evolución de los usos de Internet en España 2009*.

Así, los buscadores y el correo electrónico son utilizados ampliamente en el tercer trimestre de 2008: por el 81,2% de usuarios de la Red en el primer caso y 79,3% en el segundo. Por detrás de ellos, la consulta de noticias y la mensajería instantánea presentan tasas de utilización considerables, del 70,6% y 57,7% respectivamente. La descarga de archivos a través de la Red (bien sea música, software, vídeo u otros

ficheros) es realizada en niveles considerables, entre un 42% y un 50% en función del tipo de contenidos descargados.

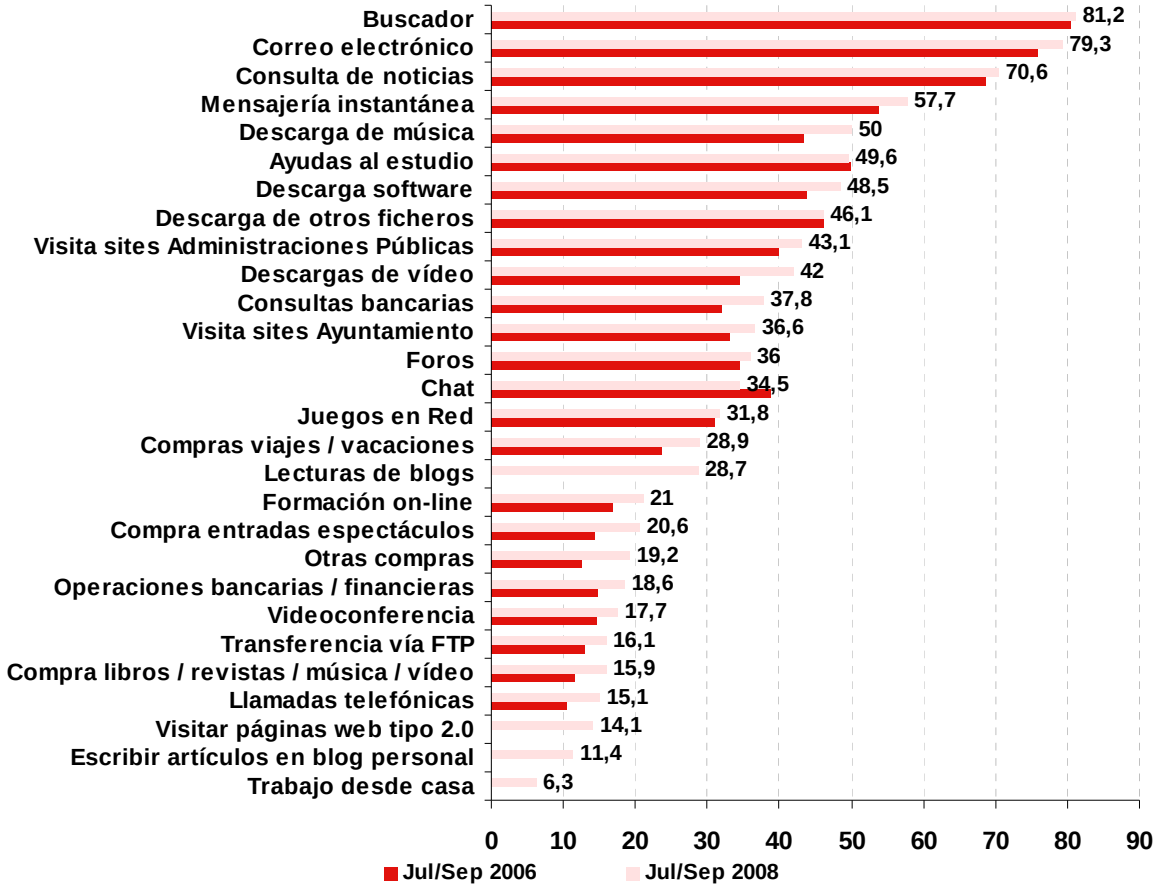
Desde una perspectiva evolutiva, se puede afirmar que la Sociedad de la Información está cada vez más implantada en España: basándonos en el nivel declarado de uso de los servicios de Internet analizados en el tercer trimestre de 2008 y en el mismo período de 2006, se aprecia una tendencia positiva en todos ellos excepto en la utilización del chat, que desciende desde niveles del 38,7% en 2006 hasta un 34,5% en 2008 (quizás motivado por el paralelo aumento de mensajería instantánea, que pasa de 53,9% a 57,7%); el uso de Internet como apoyo para el estudio y la descarga directa de otros archivos diferentes a música, software o vídeo se mantienen constantes.

La tendencia alcista se aprecia especialmente en servicios que implican la realización de transacciones bancarias y económicas.

Así, los servicios que implican transacciones económicas en Internet han visto aumentado su nivel de utilización entre los usuarios de Internet de forma importe: de un 31,9% de los usuarios que realizaban consultas bancarias online en 2006 se ha pasado a un 37,8% en 2008; la misma tendencia se aprecia en la realización de transacciones bancarias o financieras, donde se ha pasado de un 14,9% a un 18,6%, y en la realización de transferencias vía FTP, que ha crecido 3 puntos porcentuales (casi un 25%) en dos años, situándose en el tercer trimestre de 2008 en un 16,1% de nivel declarado de uso.

La realización de compras a través de la Red también ha aumentando considerablemente: los servicios más comprados a través de Internet son los viajes o vacaciones, utilizada esta opción por un 28,9% de usuarios (23,6% en 2006). Por detrás de los viajes, las entradas para espectáculos son adquiridas a través de Internet por un 20,6% de los usuarios (un aumento considerable desde la cifra mostrada en 2006, 14,3%). La compra de libros, música, revistas y vídeos es declarada por un 15,9%, creciendo desde 11,7%, y finalmente la realización de otro tipo de compras es realizado por un 19,2% (frente al 12,5% que lo hacía en 2006).

Gráfico 18: Actividades realizadas en Internet (%)



Fuente: Red.es

En definitiva, el avance de la Sociedad de la Información es muy positivo en España. Se identifica un alto nivel de utilización de servicios y una rápida evolución a lo largo del último año de todo tipo de servicios, incluidos aquéllos que implican la realización de transacciones económicas. Considerando el nivel de uso como el indicador más limpio respecto al nivel de e-confianza en la Sociedad de la Información, el balance es satisfactorio.

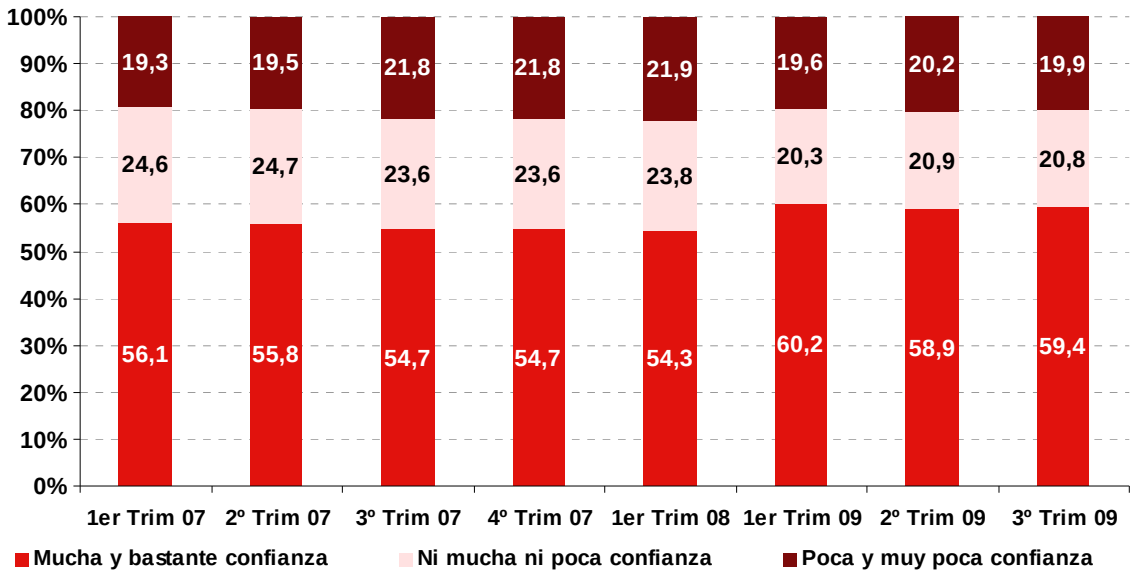
Tan importante como la adopción de servicios de la Sociedad de la Información entre los usuarios españoles es la confianza con la que llevan a cabo estos servicios. Es lo que se denomina e-confianza, y determina la actitud de aceptación, familiaridad y seguridad con que los usuarios abordan estos servicios.

El Gráfico 19 muestra la evolución del nivel de confianza declarada por los usuarios para la realización de operaciones bancarias a través de Internet. El dato es positivo: aproximadamente 6 de cada 10 usuarios (60,2% en el primer trimestre de 2009, 58,9% en el segundo y 59,4 en el tercero) muestran mucha o bastante confianza. La evolución parece mostrar una tendencia ligeramente ascendente: los últimos trimestres de 2007 el

nivel de usuarios que mostraban mucha y bastante confianza era de 54,7%; en el primer trimestre de 2008, del 54,3%; los datos para 2009 son de 60,2%, 58,9% y 59,4% respectivamente en el primer, segundo y tercer trimestre. Los usuarios de Internet muestran, cada vez, más confianza en la realización de operaciones bancarias a través de la web.

Una interpretación global permitiría concluir que cada vez existen más ciudadanos que confían mucho y bastante en la realización de operaciones bancarias en la Red, y cada vez hay menos ciudadanos "neutros", aquéllos que no se posicionan ni como muy / bastante confiados ni como poco / nada confiados. Sin embargo, el volumen de usuarios que muestran poca y muy poca confianza se mantiene bastante estable en torno al 20%.

Gráfico 19: Evolución del nivel de confianza declarada por los usuarios para la realización de operaciones bancarias online (%)

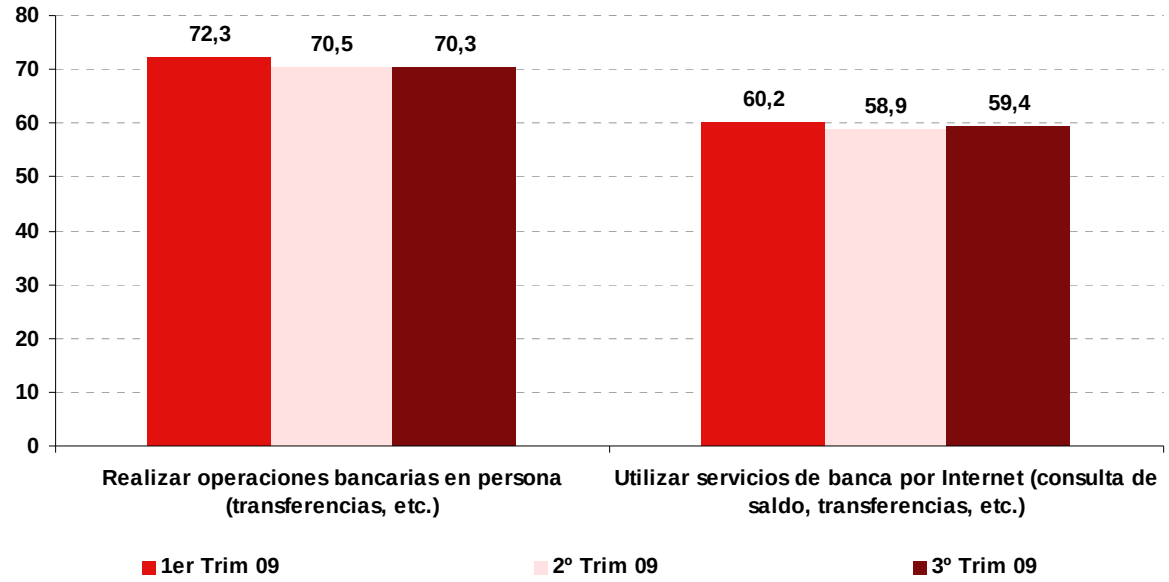


Fuente: INTECO

A pesar de que, como se decía, el nivel de confianza que los usuarios muestran hacia la realización de operaciones bancarias a través de Internet es considerable, los ciudadanos siguen mostrando más confianza en la utilización del servicio en persona.

El Gráfico 20 compara el grado en que los usuarios declaran tener mucha y bastante confianza en la realización de operaciones bancarias de forma física y a través de Internet: en el tercer trimestre de 2009, la realización de operaciones bancarias en persona ofrece mucha o bastante confianza al 70,3% de los usuarios, mientras que la confianza en la utilización de los servicios de la banca electrónica se sitúa en el 59,4%.

Gráfico 20: Porcentaje de usuarios que confían mucho y bastante en la realización de actividades físicas / online relacionadas con operaciones bancarias (%)

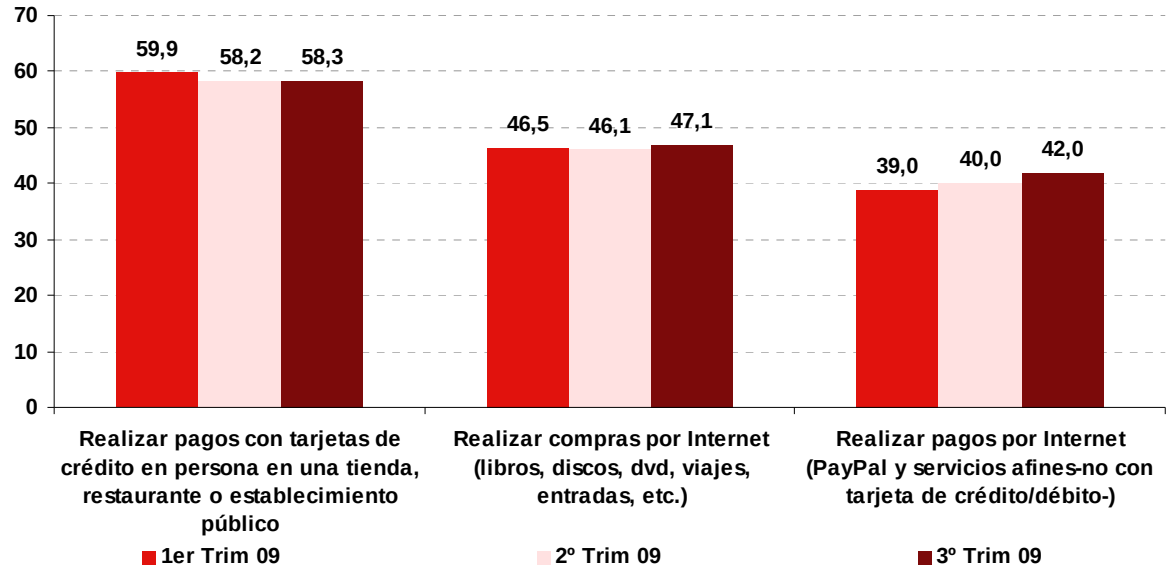


Fuente: INTECO

La misma tendencia se aprecia en la realización de actividades relacionadas con pagos y transacciones de comercio electrónico, tal y como muestra el gráfico siguiente. A un 58,3% de los usuarios les ofrece mucha o bastante confianza la realización de pagos con tarjetas de crédito en un establecimiento "físico" (restaurantes, comercios, etc). El nivel es de 47,1% cuando se trata de hacer compras por Internet, y un 42% cuando se analiza la realización de pagos (tipo PayPal y afines). Son los datos del tercer trimestre de 2009.

Apréciese, no obstante, que el porcentaje de ciudadanos que afirma confiar mucho y bastante en las operaciones que implican pagos y transacciones económicas a través de Internet se incrementa trimestre tras trimestre. En sucesivas lecturas se confirmará el carácter de esta tendencia.

Gráfico 21: Porcentaje de usuarios que confían mucho y bastante en la realización de actividades físicas / online relacionadas con pagos y transacciones de compraventa (%)



Fuente: INTECO

La comparativa entre el nivel de seguridad que ofrece a los ciudadanos la realización de operaciones económicas a través de Internet y sus *homólogas* a través de otros canales es muy interesante, ya que ofrece una perspectiva global de la cuestión. La *Asociación para la Investigación de Medios de Comunicación* (AIMC) analiza este dato desde 2006[22]. En el Gráfico 22 se muestra, con perspectiva evolutiva, el grado en que a los usuarios les ofrece mucha y bastante seguridad la realización de transacciones con componente económico a través de diferentes canales (físicos, online, telefónico, fax y correo postal). Las conclusiones son las siguientes:

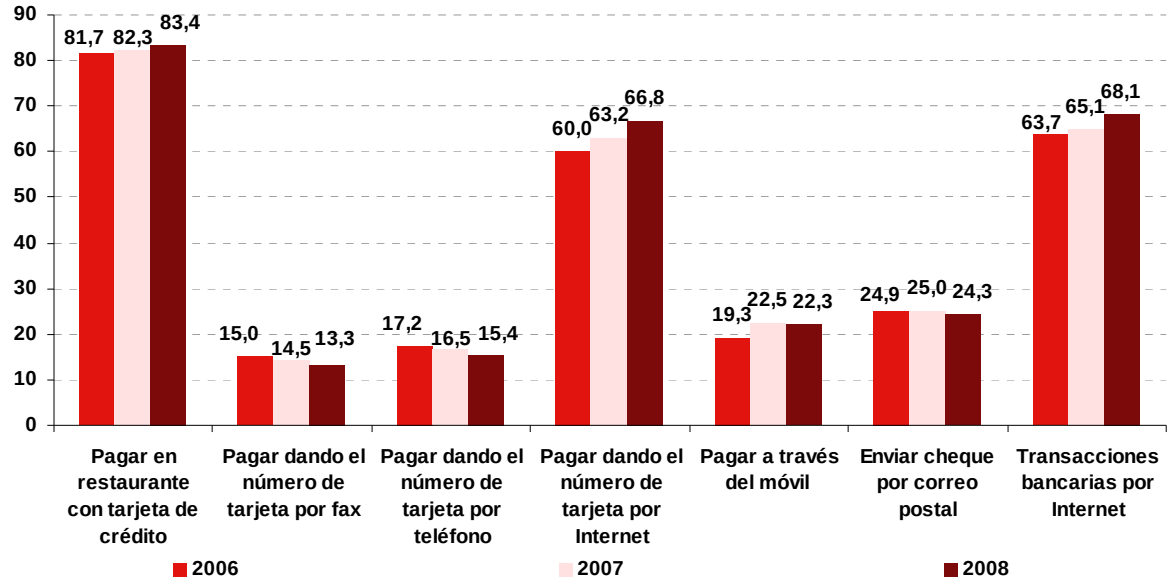
- Las operaciones realizadas en persona son las que proporcionan mayor seguridad a los usuarios: en 2008, un 83,4% consideraba muy o bastante seguro pagar en un restaurante con tarjeta de crédito.

- Por detrás de las acciones llevadas a cabo en persona, las transacciones ejecutadas a través de Internet son las más seguras, en opinión de los usuarios: los datos de 2008 muestran cómo un 68,1% encuentra muy o bastante seguro realizar operaciones bancarias por Internet y un 66,8% afirma lo propio con respecto al pago con tarjeta de crédito a través de la Red.

[22] Asociación para la Investigación de Medios de Comunicación (AIMC) (2009). *Navegantes en la Red*. Versión íntegra del informe disponible en http://www.aimc.es/aimc.php

- El resto de canales analizados son percibidos como menos seguros por los ciudadanos: sólo un 24,3% de los usuarios considera en 2008 muy o bastante seguro enviar un cheque por correo postal, un 22,3% pagar a través del móvil, un 15,4% pagar dando el número de tarjeta por teléfono, y sólo un 13,3% pagar dando el número de tarjeta por fax.

Gráfico 22: Evolución del porcentaje de usuarios que confían mucho y bastante en la realización de diferentes operaciones (%)



Fuente: Asociación para la Investigación de medios de comunicación (AIMC)

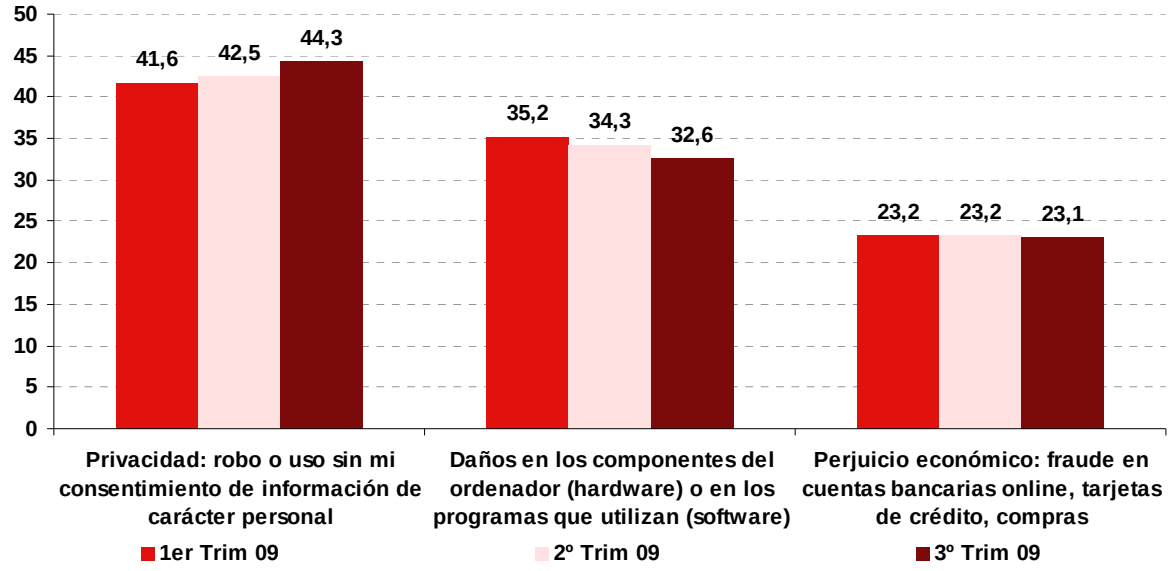
En conclusión, la Sociedad de la Información se encuentra razonablemente implementada en España, y también lo están los servicios que implican transacciones bancarias y económicas (en el contexto de los cuáles puede tener lugar un fraude), que han mostrado un nivel de penetración positivo desde 2006, según los datos proporcionados por Red.es. Tomando el grado de utilización como un indicador "puro" de la confianza que los usuarios depositan en ciertos servicios, el dato es positivo.

Cuando son preguntados expresamente por el nivel de confianza en la realización de ciertas transacciones económicas, el resultado es el siguiente: los usuarios de Internet españoles muestran mucha y bastante confianza en la realización de operaciones bancarias y económicas a través de la Red de forma considerable, aunque inferior a la confianza depositada en la realización de las mismas operaciones en el entorno físico habitual.

A pesar de ello, la Sociedad de la Información no está exenta de riesgos. Preguntados los usuarios por el riesgo al que consideran estar más expuestos, he aquí el resultado para el tercer trimestre de 2009: el 44,3% de los encuestados considera que el riesgo al que

están más expuesto es el referente a la privacidad; por detrás de éste, un 32,6% manifiesta que la amenaza a la que se encuentra más expuesto es a la incidencia de daños en el hardware o software; por último, el 23,1% de los usuarios de Internet menciona el fraude como riesgo al que se encuentra más expuesto.

Gráfico 23: Riesgo al que los usuarios consideran estar más expuestos (%)



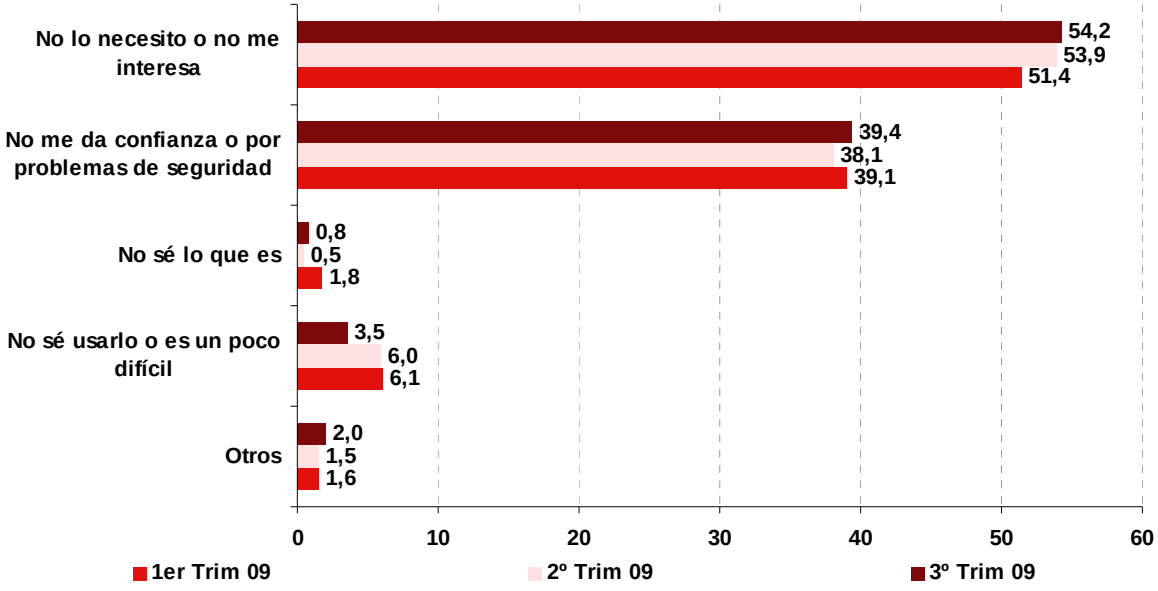
Fuente: INTECO

6.7.2 Posibles frenos al desarrollo de la Sociedad de la Información

Es interesante analizar los frenos al desarrollo de la Sociedad de la Información entre aquellos usuarios que no están utilizando algunos servicios de Internet. Se analizan los motivos proporcionados por aquéllos que no utilizan banca y comercio electrónico.

En el caso de la banca electrónica el motivo argumentado en mayor medida para su no utilización es la falta de necesidad o interés (54,2% en el tercer trimestre de 2009). Como segunda razón de peso aparece la falta de confianza y/o percepción de que existe un problema de seguridad. Un 39,4% de los encuestados declara esta opción en el último período analizado. Otros motivos, como No sé lo que es o No sé usarlo son declarados en mucha menor medida (0,8% y 3,5% respectivamente).

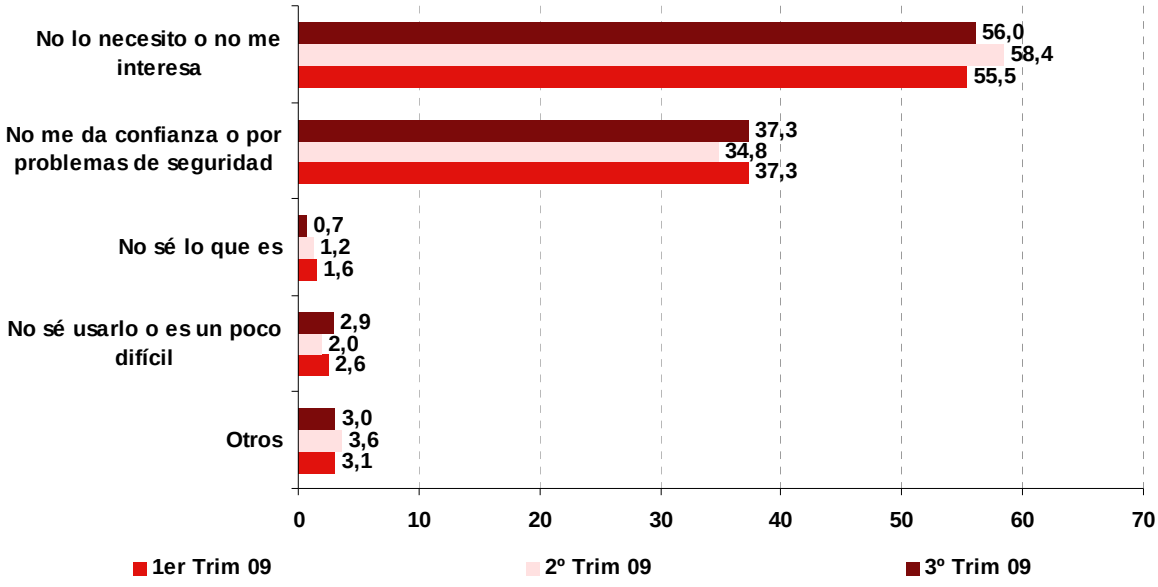
Gráfico 24: Motivos declarados para la no utilización de servicios de banca electrónica (%)



Fuente: INTECO

El caso del comercio electrónico reproduce la situación de la banca electrónica: un 56% no lo utiliza porque declara no necesitarlo, y para un 37,3% es la falta de confianza el motivo que está frenando su utilización.

Gráfico 25: Motivos declarados para la no utilización de servicios de comercio electrónico (%)



Fuente: INTECO

Es interesante este análisis: en los dos casos analizados, los ciudadanos no lo utilizan porque “no lo necesitan” como primera opción. Pero existe, además, un segundo factor de peso: la percepción de falta de confianza. Es posible que esta respuesta proceda de la sensibilidad que los ciudadanos muestran a cuestiones monetarias (posibilidad de fraudes o pérdidas económicas en las transacciones online).

Es importante que los ciudadanos conozcan los riesgos que existen en estos entornos, pero también lo es que conozcan las herramientas y pautas para combatirlos y disfrutar del servicio con total seguridad.

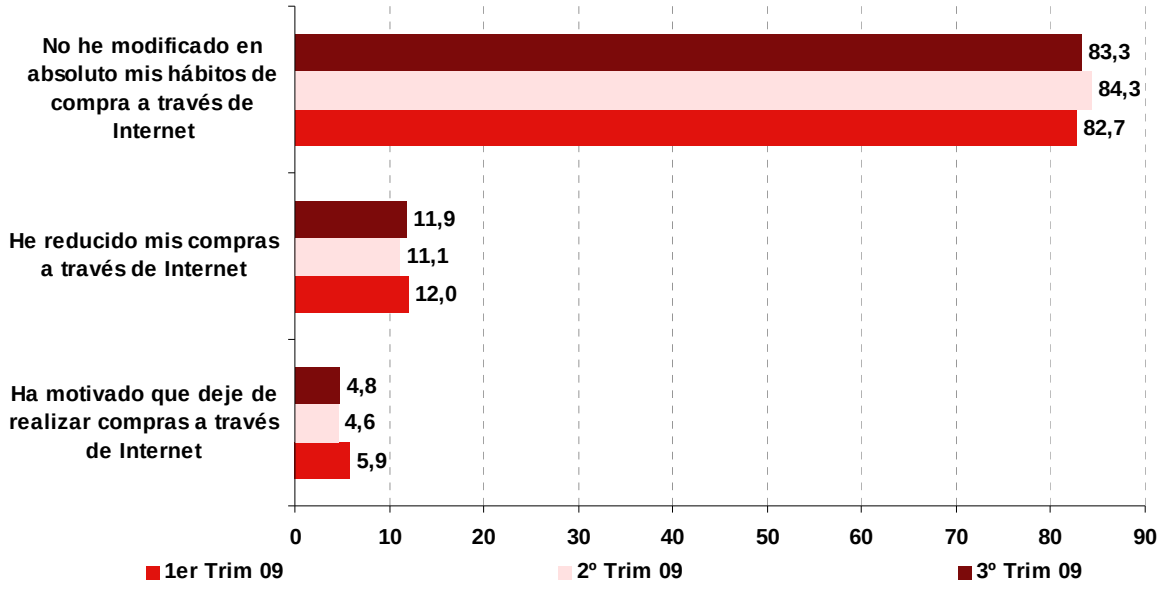
6.7.3 Relación entre fraude y e-confianza.

El hecho de haber sufrido un intento de fraude, ¿influye en el comportamiento del usuario de Internet? Se analizan a continuación los posibles cambios de hábitos de comercio electrónico (Gráfico 26) y banca electrónica (Gráfico 27) tras haber sufrido un intento de fraude, con una perspectiva evolutiva (primer, segundo y tercer trimestre de 2009).

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

En el caso del comercio electrónico, un 83,3% de los usuarios declara en el 3er trimestre de 2009 que no ha modificado en absoluto sus hábitos de compra en Internet tras haber sufrido un intento de fraude. Un 11,9% reconoce haber reducido sus compras y sólo un 4,8% afirma abiertamente haber dejado de utilizar los servicios de comercio electrónico. Los datos del primer y segundo trimestres de 2009 son similares.

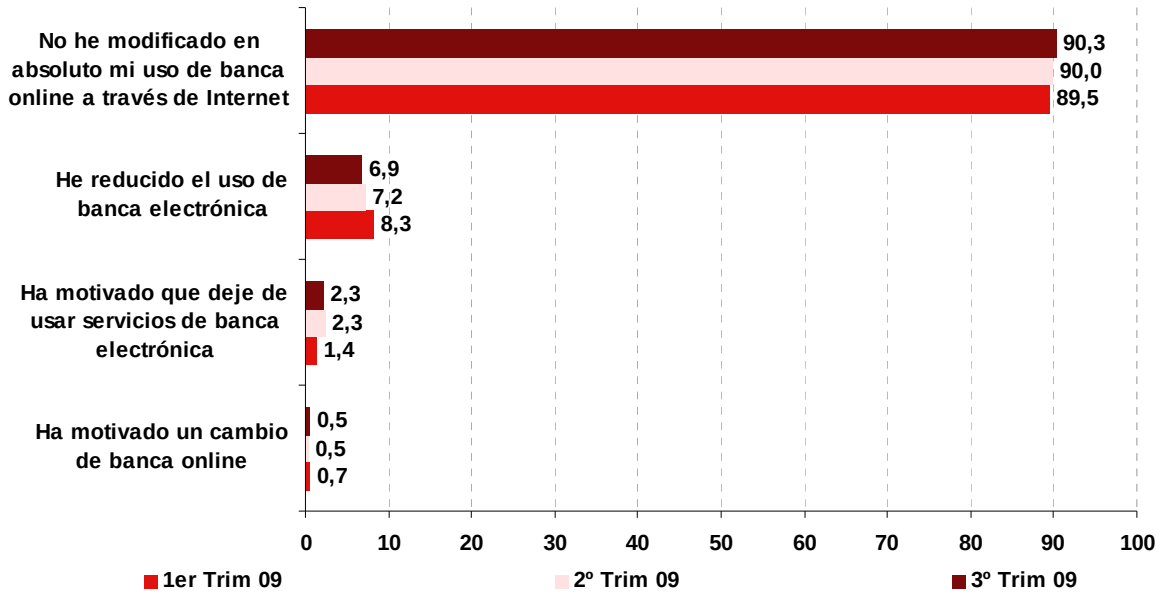
Gráfico 26: Modificación de hábitos de comercio electrónico tras sufrir intento (no consumado) de fraude (%)



Fuente: INTECO

Por lo que respecta a la banca electrónica, los datos son muy similares a los que se ofrecían para el comercio electrónico: un 90,3% no modifica en absoluto el uso de la banca electrónica tras sufrir un intento de fraude; un 6,9% reduce su uso y un 0,5% cambia de banco. Sólo un 2,3% reconoce abandonar los servicios de banca electrónica.

Gráfico 27: Modificación de hábitos de banca electrónica tras sufrir intento (no consumado) de fraude (%)



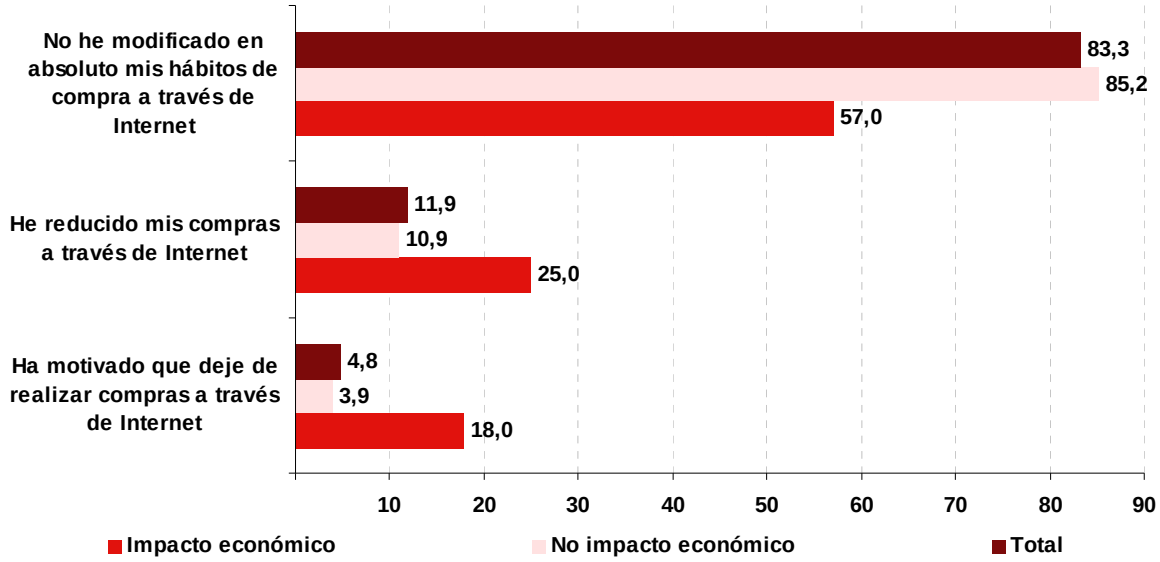
Fuente: INTECO

¿Qué ocurre cuando, consecuencia del intento de fraude, existe un perjuicio económico para la víctima? ¿Influye en este caso sobre su comportamiento de Internet?

Se analizan a continuación las diferencias entre los usuarios que han sufrido un perjuicio económico y los que no. Los datos presentados corresponden al último período disponible (3er trimestre de 2009). Nótese, en cualquier caso, que el porcentaje de usuarios que afirma haber sufrido un perjuicio económico en este período es del 3,8% (ver Gráfico 8) y, por tanto, la base considerada en este caso es muy pequeña, lo que exige cautela a la hora de interpretar los datos. En cualquier caso, la relevancia de las conclusiones aconseja la presentación de los datos.

Veíamos antes la incidencia de un intento de fraude no modificaba, en general, los hábitos de compra a través de Internet del usuario. Analizando el caso particular de los usuarios que han sufrido una pérdida económica derivada del fraude, el Gráfico 28 muestra cómo, a pesar de que sigue siendo mayoritaria la opción de no modificar sus hábitos de comercio electrónico (57%), sí tienen un peso considerable la reducción del nivel de compras a través de Internet (25%) y el abandono del servicio (18%).

Gráfico 28: Modificación de hábitos de comercio electrónico tras sufrir intento de fraude y relación con haber sido víctima de fraude con perjuicio económico en el 3er trimestre de 2009 (%)

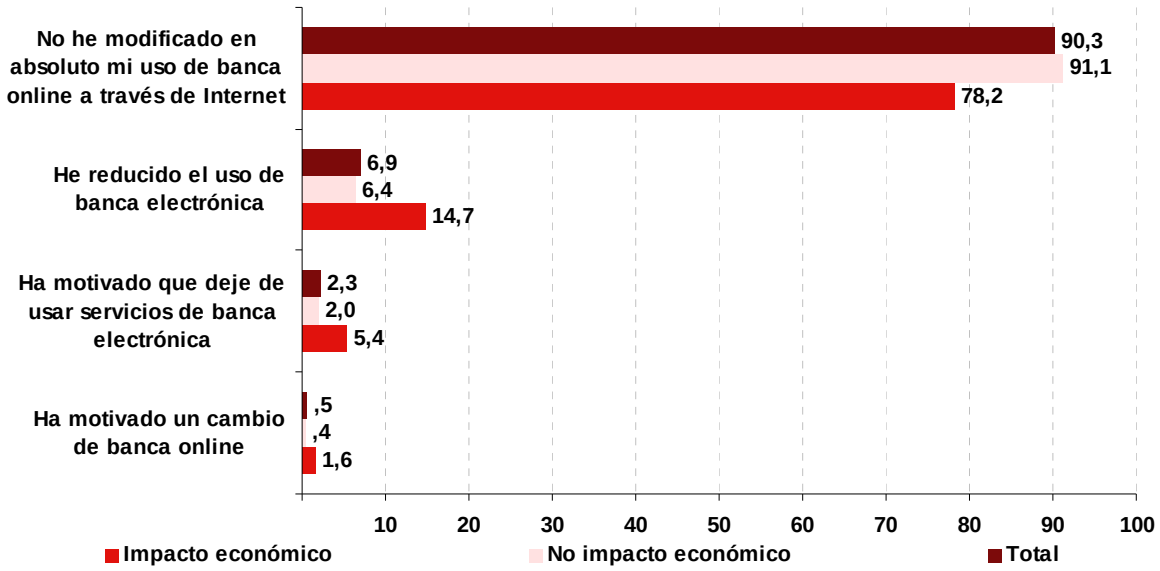


Fuente: INTECO

En el caso de la banca electrónica, la situación es ligeramente diferente, en base al análisis de los datos del tercer trimestre de 2009 (ver Gráfico 29). Si bien es cierto que el nivel de abandono, reducción o cambio del servicio es superior entre los que han sido víctimas de un perjuicio económico que entre los que no lo han sufrido, las diferencias no son tan significativas: así, un 78,2% de los que han perdido dinero a consecuencia del

fraude siguen declarando no haber modificado en absoluto el uso de la banca electrónica (frente a un 90,3% en el caso de los que han sufrido perjuicio económico).

Gráfico 29: Modificación de hábitos de banca electrónica tras sufrir intento de fraude y relación con haber sido víctima de fraude con perjuicio económico en el 2º trimestre de 2009 (%)



Fuente: INTECO

A la vista de los datos presentados hasta ahora, se esbozan las siguientes conclusiones:

- El mero hecho de haber sufrido un intento de fraude electrónico no está provocando un abandono del servicio de comercio o banca electrónica, respuesta que podría poner en peligro el desarrollo de la Sociedad de la Información. La gran mayoría de los usuarios mantienen sus hábitos.

- En cambio, sí se considera decisivo haber perdido dinero a consecuencia de un fraude electrónico. En este caso, los usuarios sí adoptan medidas de reducción, modificación o abandono del servicio en mayor medida. No obstante, incluso en estos casos de perjuicio económico, la reacción mayoritaria nunca es el abandono del servicio.

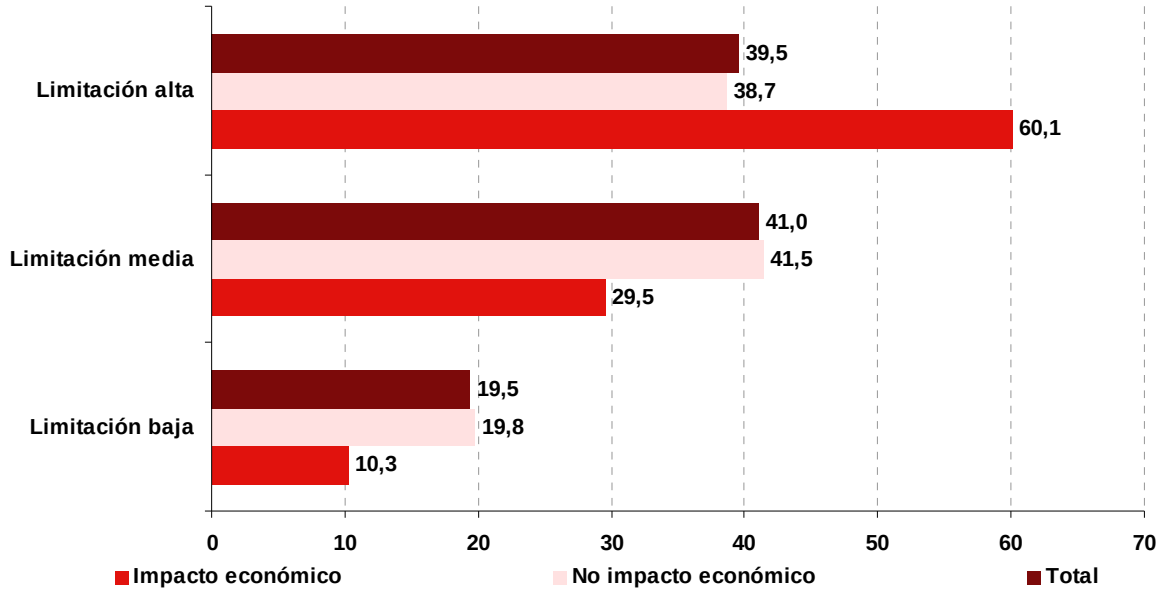
- Aun siendo minoritarias en ambos casos, la tasa de abandono del servicio de comercio electrónico es superior a la de banca electrónica: 4,8% frente a 2,3% respectivamente (datos del 3er trimestre de 2009). En paralelo, el nivel de usuarios que mantienen sus hábitos inalterables es superior en el caso de la banca que en del comercio electrónico. Ambos datos podrían suponer un indicio de que, entre los usuarios de cada servicio, la banca electrónica está más arraigada que el comercio electrónico.

- Un dato que apoya la afirmación anterior es la reacción de los usuarios que han perdido dinero a consecuencia de un fraude electrónico: entre los que han perdido dinero, sólo un 5,4% deja de utilizar la banca electrónica, frente a un 18% que abandona los servicios de comercio electrónico.

Por último, se analiza el grado en que la seguridad constituye una limitación alta, media o baja para la utilización de nuevos servicios de Internet, diferenciando los datos entre aquéllos que han sufrido impacto económico y los que no.

En general, la seguridad constituye una limitación, tal y como muestran los datos del Gráfico 30: incluso entre los usuarios que no han sufrido perjuicio económico, un 38,7% reconoce que la seguridad es una limitación alta para la utilización de nuevos servicios, mientras que un 41,5% considera que es una limitación media. Para las personas que han sido víctimas de una pérdida económica, obviamente, la limitación es mayor: un 60,1% afirma que la seguridad les limita de manera alta a la hora de utilizar nuevos servicios en Internet.

Gráfico 30: La seguridad como factor que limita la utilización de nuevos servicios (3T 2009) (%)



Fuente: INTECO

7 CONCLUSIONES

El fraude es un fenómeno de magnitud y trascendencia considerables, y, aunque es difícil la medición objetiva de sus dimensiones, las cifras del *Anti Phishing Working Group* hablaban de 49.084 sitios web fraudulentos en junio de 2009 (número de sitios identificados sólo en ese mes) y 35.918 campañas únicas detectadas ese mismo mes (por campañas únicas se entiende cada e-mail dirigido a varios usuarios, apuntando a una misma página web, con un mismo asunto en el correo electrónico).

En ese mismo sentido, el área de Servicios Reactivos y Operaciones de INTECO-CERT detectó 1.846 casos de phishing en 2008 y 1.959 en los tres primeros trimestres de 2009. Igualmente, identificó 2.191 URLs fraudulentas en 2008 y 1.810 en 2009 (hasta el mes de septiembre).

En un plano puramente teórico, la realidad del fraude se ha desplazado desde técnicas basadas en explotar la ingenuidad de las víctimas hasta la utilización de metodologías mucho más complejas y sofisticadas, basadas en el código malicioso, para dificultar la localización y bloqueo de los recursos implicados. ¿Qué causas están detrás de este desplazamiento del modus operandi? En primer lugar, el hecho de que las técnicas basadas en malware sean “amenazas silenciosas” y por tanto inadvertidas por el usuario, facilita las cosas al estafador, que ejecuta sus acciones sin la implicación consciente de su víctima. Este sigilo se mantiene en todo el proceso, con cantidades defraudadas lo suficientemente pequeñas como para que puedan pasar desapercibidas a la víctima.

Respecto al plano organizativo, los ciberdelincuentes han evolucionado desde una organización unipersonal o de pocas personas a verdaderas organizaciones enfocadas al ciberdelito y que se encuentran muy estructuradas en cada una de las tareas. Esto también es derivado de la complejidad añadida a estos ciberdelitos ya que, con el fin de escapar al control de las Fuerzas y Cuerpos de Seguridad, añaden nuevas técnicas y complejidad al proceso de llegada del dinero a manos del ciberdelincuente.

Otro motivo que parece estar detrás del creciente éxito de técnicas de fraude electrónico basadas en código malicioso radica en la mayor concienciación ciudadana: la importancia que se ha dado al fenómeno por parte de medios de comunicación, Administraciones, asociaciones de usuarios de Internet, sector bancario e industria de la seguridad, entre otros, ha aumentado la cautela de los ciudadanos a la hora de facilitar sus datos.

Según datos extraídos de los más de 128.325 análisis practicados a equipos de usuarios de Internet españoles entre enero de 2007 y septiembre de 2009, la presencia de malware es importante, tanto en términos cuantitativos (en el último período analizado, un 56,2% de los equipos informáticos están infectados con algún tipo de código malicioso) como cualitativos o riesgo que entraña el código malicioso (en un 35,4% de los casos, los

equipos alojan troyanos, tipología de malware más relacionada con la comisión de fraude online).

Evidentemente, el hecho de identificar malware en un equipo no implica fraude, ni tan siquiera un riesgo más o menos cierto de ser víctima de fraude, aunque es cierto que los equipos infectados por malware constituyen una amenaza silenciosa. En cualquier caso, se debe seguir incidiendo en la concienciación a los ciudadanos acerca de la importancia de disponer de herramientas de seguridad adecuadas y actualizadas, y de seguir adoptando medidas y pautas de seguridad correctas.

La incidencia efectiva de fraude que implique un perjuicio económico a la víctima es limitada, aunque creciente desde 2007: en concreto, el 3,8% de la población española usuaria de Internet afirma haber experimentado una pérdida monetaria derivada de un fraude electrónico en el tercer trimestre de 2009.

La proporción de usuarios que creen haber recibido un intento de fraude, aunque no haya llegado a consumarse (en términos de impacto económico), es bastante superior: así, el 35,2% de los usuarios de Internet españoles declara, en el 3er trimestre de 2009, haber recibido alguna petición de visitar páginas web sospechosas en los 3 meses previos a la realización de la encuesta. Por detrás de ella, el 29,5% afirman haber recibido e-mails ofertando servicios no solicitados. Son las dos incidencias declaradas con mayor frecuencia. Los casos de ofertas de trabajo sospechosas de ser falsas y la recepción de un e-mail solicitando las claves de usuario son más infrecuentes, y son declarados por un 25,4% y 26,6% de los usuarios, respectivamente.

Estos datos, obtenidos a través de una encuesta realizada a 32.484 ciudadanos españoles usuarios de Internet (repartidas en ocho tomas de datos entre 2007 y 2009) muestra la realidad percibida desde la óptica del usuario final, eslabón más débil en la cadena del fraude. Lo relevante del dato (y del estudio) es que se trata de la primera vez en España en que se realiza el análisis desde el punto de vista de los usuarios. La información identificada hasta la fecha de publicación del estudio analizaba el fenómeno desde el punto de vista de la industria (por ejemplo, cómo afecta el fraude electrónico al sector bancario). Una de las limitaciones encontradas deriva del carácter parcial y la falta de homogeneidad de los datos publicados. De esta limitación deriva la recomendación de un acercamiento de los actores implicados para complementar sus metodologías y ofrecer una visión global de la incidencia real de la situación.

Para este 3,8% de la población española usuaria de Internet que afirma que ha sufrido un perjuicio económico fruto de un fraude electrónico, la cuantía defraudada es reducida: inferior a 50 € para el 44,5%, e inferior a 400 € (cuantía a partir de la cual el fraude tiene consideración de delito, y no de falta, según el código penal español) en el 75% de los casos. Esto permite una doble lectura: de un lado, que el impacto puramente económico del fraude es limitado; y de otro, que, precisamente por la poca relevancia de la cuantía,

pueden pasar desapercibidos a los ojos de los ciudadanos. Ello implicaría que el fenómeno está siendo infradiagnosticado. De ahí la importancia de vigilar cuidadosamente los movimientos de banca electrónica e indagar acerca de cualquier apunte sospechoso.

Pero, además de la evidente consecuencia económica, el fraude electrónico tiene un efecto sobre la confianza de los ciudadanos en Internet como canal a través del que realizar sus operaciones. Cuantificar de un modo más o menos objetivo el impacto sobre la confianza no es tarea sencilla, dado lo subjetivo del objeto de análisis. Por ello en el estudio se identifican y analizan una serie de indicios que permiten extraer conclusiones interesantes.

¿Qué confianza declaran los usuarios tener en Internet como canal para realizar transacciones bancarias y económicas?

El nivel de confianza en Internet para realizar operaciones económicas es alto: aproximadamente 6 de cada 10 usuarios muestran mucha o bastante confianza en la utilización de banca electrónica.

A pesar de este considerable nivel de confianza en Internet como canal de realización de transacciones económicas, los ciudadanos siguen mostrando más confianza en la utilización del servicio en persona.

Quizás resulte demasiado ambicioso esperar que el nivel de confianza en la realización de transacciones económicas online llegue a superar, o al menos igualar, a la confianza mostrada en sus homólogas en el mundo físico; en cualquier caso, la reducción del gap existente entre ambos constituye, sin duda, un excelente indicador del nivel de e-confianza y adopción efectiva de la Sociedad de la Información.

El haber sido víctima de fraude, ¿en qué afecta al comportamiento del usuario?, ¿modifica la forma de aproximarse a las TIC?

Una primera conclusión es que el intento de fraude que no llega a consumarse (es decir, que no implica perjuicio económico para el usuario) no afecta al comportamiento en Internet, ni en lo relativo al comercio electrónico, ni en la banca electrónica.

En cambio, la conducta del usuario se modifica cuando el fraude comporta una pérdida económica para la víctima. Aún en este caso, no es mayoritaria la opción de dejar de utilizar los servicios de comercio electrónico y/o banca electrónica. Parece que estos servicios, sobre todo la banca por Internet, han calado de tal modo en los hábitos de los usuarios que no son fácilmente sustituibles.

Todo ello apunta a que se debe continuar la lucha contra el fraude electrónico desde todos los frentes afectados: la Administración debe continuar su labor de concienciación a

la ciudadanía y asegurar la eficacia normativa; la industria debe mantener el esfuerzo en la búsqueda de soluciones de seguridad que den respuesta a amenazas cada vez más sofisticadas; los sectores afectados (en especial, el bancario) han de implantar las medidas necesarias para que sus webs ofrezcan seguridad en las transacciones; y por último, la ciudadanía, el eslabón más débil, debe mantenerse alerta y actuar con cautela y prudencia.

Ha de remarcarse la importancia de los proveedores de servicios de Internet en esta lucha, ya que son ellos los que tienen la respuesta inmediata en el bloqueo y análisis de los fraudes electrónicos alojados en sus servidores. Los agentes de registro de dominio también tienen mucho que aportar, ya que, mediante el refuerzo de los servicios de registro con medidas de comprobaciones exhaustivas y la rápida respuesta ante la detección de dominios utilizados con fines fraudulentos, aportarán herramientas muy valiosas para evitar que el usuario final se vea afectado por ciertos tipos de fraudes electrónicos.

Se hace por tanto necesario fomentar la colaboración entre todas las organizaciones afectadas de una forma u otra por el fraude electrónico, con el fin de conseguir una lucha más eficaz en este ámbito.

En INTECO somos conscientes de la necesidad de aunar esfuerzos en este aspecto manteniendo colaboraciones con todos estos actores y poniendo a disposición de estos el Repositorio de Fraude Electrónico, con el fin de facilitar la integración de los esfuerzos realizados por cada uno de los actores. Además pone a disposición del ciudadano tanto los servicios del INTECO-CERT como los de la Oficina de Seguridad del Internauta para que esté adecuadamente informado, protegido y tenga a su disposición los servicios necesarios para la gestión de los casos de fraude que el propio ciudadano haya detectado o sufrido.

8 RECOMENDACIONES

De los datos presentados en el informe se desprende la trascendencia del fenómeno del fraude, su crecimiento, y la sofisticación de las técnicas empleadas por los ciberdelincuentes. Como consecuencia de ello, todos los actores implicados deben adoptar una posición activa en la prevención y lucha contra el fraude.

El sector financiero y las entidades que se dedican a ofrecer servicios de comercio electrónico han realizado esfuerzos importantísimos, ya que sólo garantizando un adecuado nivel de seguridad pueden transmitir la confianza necesaria para fidelizar a sus usuarios y captar nuevos clientes. En este sentido, hace tiempo que estas empresas están considerando la seguridad como un aspecto crítico para su negocio, y se están implicando en la inversión de recursos destinados a ello. Algunos mecanismos utilizados habitualmente por la banca son: utilización de títulos de página dinámicos, empleo de nombres de variables aleatorios para los campos de sus formularios, implementación de ofuscaciones en el lado cliente de las credenciales enviadas hacia el servidor de banca, autenticación de transacciones además de la de usuario, etc.

Otros están apostando por mecanismos sólidos que conjugan los tres pilares básicos de la robustez: algo que se conoce, algo que se tiene y algo que se es. Se trata de un dispositivo que combina contraseñas, aparato físico y uso de huellas dactilares. La ventaja desde el punto de vista de la seguridad es indudable, pero el éxito de la herramienta requiere una extensión en su uso que a día de hoy no existe.

Ilustración 1: Ejemplo de dispositivo para autenticación bancaria que combina credenciales, uso de huellas dactilares y dependencia de las claves de transferencia de la cuenta destino

Fuente: INTECO

También la industria de la seguridad está trabajando constantemente en la investigación y actualización de las manifestaciones más actuales del malware y en la introducción constante de nuevas herramientas y servicios para combatir el fraude.

El esfuerzo se está llevando a cabo de manera conjunta por parte de empresas del sector privado, administraciones públicas, Fuerzas y Cuerpos de Seguridad del Estado, asociaciones y organizaciones de carácter nacional e internacional, etc. En un contexto caracterizado por una industria del malware cada vez más sofisticada y organizada, sólo una actuación conjunta puede garantizar el cumplimiento de objetivos.

En cualquier caso, y a pesar de los avances y esfuerzos adoptados hasta la fecha, los ciberdelincuentes siguen atacando, y no se prevé que reduzcan su actividad en el corto plazo. Es importante que los usuarios, como eslabón más débil en la cadena de seguridad, siga una serie de pautas y recomendaciones de seguridad para prevenir y combatir el fraude online. Las siguientes recomendaciones han sido elaboradas por la Oficina de Seguridad del Internauta (OSI).

8.1 Pautas de seguridad básica en los equipos

Una vez que se conocen las amenazas y se han valorado los riesgos es momento de protegerse. La mejor manera para hacerlo es la prevención. Es sencillo con unos buenos hábitos en el uso de la tecnologías y preparando correctamente los sistemas.

8.1.1 Protección del equipo

No todas las amenazas se pueden evitar. Es necesario proteger correctamente los sistemas, se puede ser víctima de virus y usuarios maliciosos simplemente al conectarse o navegar por Internet. Se recomienda:

- Mantener el sistema operativo actualizado. Si el sistema tiene vulnerabilidades, se facilita la entrada de software malicioso al mismo. La forma más simple de mantener el sistema actualizado es activar las actualizaciones automáticas del sistema.

- Tener actualizado el software instalado. Es sabido que los desarrolladores de software malicioso aprovechan tanto las vulnerabilidades del sistema operativo como del software instalado. Para realizar esta tarea es posible apoyarse en herramientas que comprueban las versiones del software instalado que, aunque no incluyen todo el software, sí el más usual. Dentro de estás se dispone de herramientas de escritorio y online.

- Tener activado un cortafuegos, bien el del sistema o uno externo de otro fabricante. Esta herramienta previene accesos no autorizados de aplicaciones a Internet y de Internet al PC. La forma de trabajar es simple: cuando alguna aplicación inicia una comunicación a través de la red (desde el sistema a Internet, o de Internet al sistema) muestra un aviso al usuario indicándole el nombre de la aplicación que inicia la comunicación. El usuario puede permitir o denegar esa

comunicación, y hacer que esa decisión sea recordada en el futuro. En la sección cortafuegos del portal OSI hay varios gratuitos.

- Tener instalado y actualizado un antivirus. Es tan importante tenerlo instalado como tenerlo actualizado, ya que en caso de no estar actualizado, permitirá que entren virus/troyanos etc. en el sistema. Hay disponibles varios en la sección de antivirus de escritorio. También es aconsejable cada cierto tiempo utilizar antivirus online como segunda opinión para contrastar los resultado con nuestro antivirus de escritorio.

- Tener instalado un software antiespías. En función del producto, suelen detectar software espía, troyanos, rootkits, y algunos tipos más de software malicioso. Hay algunos programas de este tipo en la sección de antiespías de escritorio. Ocurre lo mismo que con los antivirus, es recomendable analizar el sistema con otro antiespías de vez en cuando y los antiespías online aportan la ventaja de que no se instala más que un pequeño programa.

8.1.2 Recomendaciones de uso

En este apartado se recogen una serie de recomendaciones de utilización general de los ordenadores, y en concreto en el ámbito de utilización de Internet. Se sugiere que estas indicaciones sean seguidas en todo momento. Son:

- Utilizar contraseñar seguras y cambiarlas a menudo. Para que una contraseña se considere segura ha de:
    - Tener una longitud de al menos 8 caracteres.
    - Estar compuesta por al menos un carácter de cada uno de los siguientes grupos:
        - Letras mayúsculas y minúsculas
        - Números
        - Caracteres especiales, por ejemplo $, %, &, /, etc.
    - No ser deducible de la información personal del usuario (fechas de nacimiento, dirección, matrículas de vehículos, DNI, teléfono, etc.)
    - No ser una palabra común de un diccionario, ni un nombre de persona o personaje de ficción, ni actor etc. Lo ideal es algo que solo tenga sentido para nosotros como RR7776cslc$$.

Hay aplicaciones que sirven para comprobar la fortaleza (calidad respecto de un ataque de fuerza bruta) de una contraseña, como www.passwordmeter.com.

Para no olvidarse de las contraseñas se puede utilizar un gestor de contraseñas, que además permite generarlas tan fuertes como se desee, de forma que usemos contraseñas fuertes de una manera muy sencilla.

En caso de utilizarse la opción de recordar contraseñas del navegador, se ha de proteger la opción instaurando una contraseña maestra, sino cualquier persona que acceda a nuestro sistema podría ver las contraseñas almacenadas.

- No utilizar sistemas de los que se desconozca las garantías de seguridad. En ningún caso utilizar equipos públicos como los de la biblioteca, cibercentros, kioscos públicos, etc. También hay que tener en cuenta que, además del equipo con el que el usuario se conecta a Internet (ordenador, PDA, teléfono móvil), también debe ser segura la línea a utilizar. De este modo no es recomendable utilizar redes Wifi abiertas, ya que se desconoce quién puede estar conectado a ellas.

- Utilizar usuarios con derechos limitados, esto es, no trabajar habitualmente como administradores. Si un usuario malicioso logra poder ejecutar comandos en el sistema, en la mayoría de los casos esos comandos se ejecutaran con los derechos del usuario que esté trabajando en ese momento. En cambio, si se trata de un usuario con pocos privilegios, el daño será limitado y las posibilidades de modificar el sistema serán menores.

- Es importante mantenerse informado sobre cuestiones de seguridad informática, conocer los riesgos y las principales amenazas de las que protegerse. INTECO-CERT dispone de un servicio de avisos de seguridad con el fin de alertar tempranamente a los usuarios ante nuevos casos de fraude, así como otras consideraciones para estar correctamente prevenido. Desde la página de INTECO un usuario puede suscribirse a los diferentes boletines de seguridad: actualidad, avisos no técnicos, avisos técnicos y vulnerabilidades.

- Limitar la información personal que se proporciona en las redes sociales, y evitar datos que permitan identificar al usuario (dirección, teléfono, DNI, etc.). Además, se recomienda activar todas las opciones de seguridad y privacidad posibles, de forma que sólo puedan acceder al perfil personal los contactos a los que previamente el usuario propietario del perfil haya dado acceso.

8.2 Consejos de seguridad en el contexto de una transacción económica

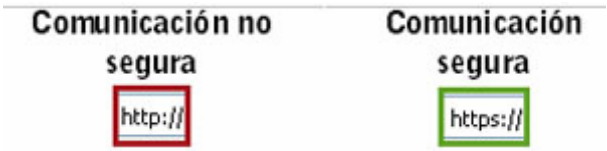
Dentro de una transacción económica, hay que tener en cuenta en especial la legitimidad de los sitios Web a los que se accede, y comprobar de forma exhaustiva que se está

visitando el sitio que realmente se pretende, y no copias falseadas de los mismos. Para asegurarse de esto, se debe prestar especial atención a los distintivos que indican la autenticidad del sitio visitado.

8.2.1 Protocolo seguro

Al enviar información desde un ordenador a otro a través de Internet, debemos utilizar un protocolo de comunicaciones seguro. El más utilizado es el HTTPS, que nos asegura que la información que se envía/recibe lo hace cifrada. El indicativo de uso de este protocolo es que la URL a la que nos conectamos comienza por HTTPS en lugar de HTTP.

Ilustración 2: Comunicaciones no seguras y seguras según el indicativo del protocolo utilizado en la comunicación



Fuente: INTECO

8.2.2 Certificados válidos

Un certificado digital es un documento digital mediante el cual un tercero confiable (una autoridad de certificación) garantiza la vinculación entre la identidad de un sujeto o entidad y su clave pública.

Cuando una página Web tiene un certificado válido, aparecen como indicativo un candado que indica que estamos usando un protocolo de comunicación seguro, el HTTPS.

Además, en función del tipo de certificado SSL que esté utilizando (SSL o EV-SSL), puede aparecer la barra de dirección o parte de la misma de color verde o azul.

Certificado SSL-EV (extended-validation)

Es el certificado SSL que incorpora mas medidas de seguridad. Es el más seguro y confirma que la legitimidad de la página. En los distintos navegadores se vería así:

Internet Explorer

Aparece el nombre de la entidad al lado del candado en fondo verde.

Ilustración 3: Barra de dirección del navegador Internet Explorer cuando accedemos a una página Web que posee un certificado SSL-EV

Fuente: INTECO

Firefox

En el icono de la página aparece el nombre de la entidad y todo ello con fondo verde.

Ilustración 4: Barra de dirección del navegador Mozilla Firefox cuando accedemos a una página Web que posee un certificado SSL-EV

Fuente: INTECO

Safari

Aparece el nombre de la entidad, con fondo verde cuando se pasa el cursor por encima

Ilustración 5: Barra de dirección del navegador Safari cuando accedemos a una página Web que posee un certificado SSL-EV

Fuente: INTECO

Certificado SSL

En este caso, el tipo de certificado que usa la página no proporciona información de identidad, es decir, no se ha llegado a verificar que la dirección pertenece realmente a la entidad.

Por este motivo para poder utilizar la página con unas mínimas garantías se debe estar seguro de:

- La dirección de la página que vas a visitar pertenece a la entidad.
- La dirección en la barra de navegación está bien escrita. En ocasiones los estafadores intentan suplantar las páginas utilizando direcciones similares y creando páginas prácticamente idénticas.

Pero si se está seguro de que esa dirección pertenece a la empresa, se puede utilizar.

En los distintos navegadores se ve así:

Internet Explorer

Aparece un candado con fondo azul, que al pulsarlo nos muestra el certificado que garantiza la conexión segura y el nivel de legitimidad.

Ilustración 6: Barra de dirección del navegador Internet Explorer cuando accedemos a una página Web que posee un certificado SSL

Fuente: INTECO

Firefox

En el icono de la página que está a la izquierda de la barra de direcciones, aparece el nombre de la entidad y todo ello con fondo azul.

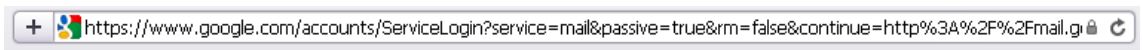
Ilustración 7: Barra de dirección del navegador Mozilla Firefox cuando accedemos a una página Web que posee un certificado SSL

Fuente: INTECO

Safari

Aparece un candado en el extremo derecho de la barra de direcciones, pero no aparece el fondo verde, ni el nombre de la entidad.

Ilustración 8: Barra de dirección del navegador Safari cuando accedemos a una página Web que posee un certificado SSL



Fuente: INTECO

8.2.3 Ante un caso de phishing

Ante un caso de phishing, se debe contactar urgentemente con la entidad bancaria. También se puede enviar un correo electrónico al servicio de gestión del fraude de INTECO, fraude@cert.inteco.es, que ofrece información al usuario y realiza las notificaciones a las entidades implicadas, con el fin de minimizar los posibles daños

En caso de que se constate la operación económica del fraude electrónico, cabe interponer una denuncia ante las Fuerzas y Cuerpos de Seguridad del Estado. Las

entidades ante las que los ciudadanos pueden interponer las denuncias correspondientes son:

- Policía Nacional. Brigada de Investigación Tecnológica:

  http://www.policia.es/bit/index.htm

- Guardia Civil. Grupo de Delitos Telemáticos:

  https://www.gdt.guardiacivil.es/

- Mossos d'Esquadra:

  http://www.gencat.cat/mossos/

- Ertzaintza:

  http://www.ertzaintza.net/public/wps/portal/ertzaintza

¿Qué medios de prueba se deben aportar? Es importante aportar el mayor número de datos y pruebas respecto al hecho delictivo. Para ello, se recomienda al afectado que, en la medida de lo posible, recabe y presente anexa a la denuncia la siguiente información y pruebas:

- Comprobar y acreditar documentalmente a través de la entidad bancaria todos los movimientos económicos relativos a la operación fraudulenta. De esta forma, tanto la entidad financiera, como el afectado tendrán constancia del momento en el que se realizaron cargos no autorizados y se conocerán las cantidades concretas y el destino de las mismas.

- Así mismo y dependiendo de los conocimientos informáticos del usuario, sería conveniente recabar toda aquella información relacionada con el fraude, tales como: correo electrónico fraudulento, dirección Web fraudulenta, IP asociada, entidad afectada, etc. En cualquier caso estos y otros datos pueden o no aplicar dependiendo del tipo de fraude perpetrado. Siempre que el usuario requiera ayuda para obtener dicha información, podrá contactar con el servicio INTECO-CERT.

8.2.4 Recomendaciones estratégicas

A medida que aumentan las capacidades tecnológicas de la información y las comunicaciones lo hacen también sus riesgos, comprobado que no es suficiente tener claras las estrategias de continuidad de negocio en las organizaciones.

La cooperación nacional es necesaria, pero insuficiente. Este escenario deja de manifiesto la necesidad de llevar a cabo una coordinación internacional para combatir el

ciberdelito. Por este motivo, se están llevando a cabo varias iniciativas en el ámbito internacional:

- **CCDCOE**: iniciativa de la OTAN con el objetivo de mejorar la capacidad, cooperación e intercambio de información entre las naciones OTAN en materia de ciberdefensa. Entre sus tareas destacan la educación y doctrina y la investigación y desarrollo. Y entre sus actividades, el proyecto I+D sobre intercambio de información entre CERTs.

- **Agencia Europea de Seguridad (ENISA)**: constituye un centro de asesoramiento sobre cuestiones de seguridad para los Estados miembros y las Instituciones de la UE. Se centra en principalmente en asesorar y asistir a la Comisión y a los Estados miembros en materia de seguridad de la información, pero también en otras acciones como: hacer frente a los problemas de seguridad del sector empresarial, recoger y analizar datos sobre las incidencias que se producen en Europa en materia de seguridad, fomentar la evaluación y métodos de gestión de riesgos, intercambiar buenas prácticas en materia de sensibilización, fomentar la cooperación, etc.

- **Proyecto MS3i**: proyecto promovido por el programa europeo para la Protección de Infraestructuras Críticas, cuya misión es establecer determinados estándares para el intercambio de información de seguridad.

GLOSARIO

Backdoor o puertas traseras

Permite al atacante tomar el control remoto del sistema infectado, pudiendo llevar a cabo diversas acciones (espiar el escritorio remoto, realizar capturas de pantalla o de la webcam, subir o descargar archivos, alterar el funcionamiento normal del sistema, etc.).

Detecciones heurísticas

Detecciones de códigos maliciosos que no están aún catalogados y que se basan en la búsqueda de son detectados el antivirus ante un comportamiento sospechoso durante en la ejecución del código.

Dialers o marcadores telefónicos

Programas que, una vez instalados en el equipo, desvían la conexión telefónica original hacia otro número de tarificación especial (806, 807, etc.) con el consecuente perjuicio económico para el afectado. Únicamente pueden afectar a los usuarios que acceden a Internet a través de banda estrecha mediante RTB (Red Telefónica Básica) o RDSI (Red Digital de Servicios Integrados), por eso se trata de una categoría con menor impacto ya que habitualmente el acceso a Internet se realiza por banda ancha.

Fast-flux

Es una técnica de DNS utilizada por botnets (red de equipos comprometidos) para ocultar sitios fraudulentos, normalmente phishing o de distribución de malware. Se basa en la utilización de equipos comprometidos que actúan como proxy, ocultando el/los servidor/es maliciosos que realmente alojan el contenido fraudulento. Combina dos propiedades del servicio DNS para conseguir su finalidad, Round Robin DNS y definición de TTL bajo. Con esto se consigue cambiar de forma rápida las direcciones IP que actúan como proxys dotando de mayor disponibilidad al servicio fraudulento.

Falso positivo

Detección errónea de un fichero inocuo como malicioso.

Herramientas

El malware del tipo “herramienta” puede tener un riesgo variable dependiendo de si ha sido instalada conscientemente por el usuario legítimo del equipo o por un tercero sin su conocimiento. Por ello, en este indicador se ha aplicado por defecto el nivel de riesgo bajo, aunque en algunas circunstancias un malware catalogado como herramienta pueda ser de riesgo alto.

Ingeniería social

Técnica del fraude basada en la explotación de vulnerabilidades sociales (es decir, engaños que buscan aprovecharse de la ingenuidad de la víctima), con una baja complejidad tecnológica.

Keyloggers o capturadores de pulsaciones

Tienen capacidad para capturar y almacenar las pulsaciones efectuadas sobre el teclado. Posteriormente esta información (que puede contener contraseñas, datos bancarios, etc.) se envía a un atacante, que las puede utilizar en su propio provecho. En definitiva, se trata de una variedad que también se centra en el fraude.

Mula o mulero

Personas que, a cambio de una comisión, participan en la circulación del dinero desde las cuentas de los usuarios defraudados hasta las de los ciberdelincuentes, realizándolo a través de diversos medios que pretenden anonimizar al destinatario final de los mismos, como Western Union o medios de pago electrónico.

Ofuscación

Acto deliberado de realizar un cambio no destructivo, ya sea en el código fuente de un programa informático o código máquina cuando el programa está en forma compilada o binaria, con el fin de que no sea fácil de entender o leer. Es decir, se hace ininteligible específicamente para ocultar su funcionalidad.

Troyanos bancarios

El año 2003 supuso el nacimiento de los troyanos bancarios. Desde entonces, estos códigos maliciosos, diseñados para robar las credenciales de acceso a servicios de banca electrónica, se han convertido en la actualidad en una de las formas más habituales de malware. Cada día salen a la luz nuevas variantes que han evolucionado tecnológicamente para esquivar las medidas de seguridad de los bancos. La información robada depende de la implementación de seguridad del sitio contra el que actúa y los mecanismos utilizados para llevar a cabo el robo de la información son modificados constantemente por los ciberdelincuentes. Estos mecanismos incluyen las grabaciones en formato video de las operaciones realizadas en el navegador web, la superposición sobre las casillas de introducción de información de casillas generadas por el propio troyano, inyecciones de código HTML en el propio navegador del usuario o los más recientes que realizan la modificación en tiempo real de las operaciones realizadas por el propio usuario. Este tipo de malware está en alza, y su objetivo, obviamente, se centra en el fraude electrónico.

Whaling

También llamado “caza de ballenas" (whale en inglés). Es una evolución del phishing en la que el ciberdelincuente recaba información de contacto de personas de influencia y alto poder adquisitivo, como empresarios, autoridades y gerentes, habitualmente a través de la información contenida en redes sociales. Posteriormente le remiten un correo electrónico personalizado en el que se le trata de engañar para robar credenciales de cuentas bancarias personales o de la propia compañía. Algunas variantes utilizan la difusión de algún código malicioso que realice una vez instalado el robo de esta información. Este tipo de ataques se caracterizan por el elevado contenido de ingeniería social ya que los contenidos son específicos para el objetivo del fraude, derivando en una carga de confianza mayor ante los detalles de la información utilizada. El ejemplo típico de correo es el que simula contener una citación para el juzgado y que contiene realmente un código malicioso para robar información personal y credenciales de acceso.

BIBLIOGRAFÍA

- **Anti-Phishing Working Group (APWG)** (2009). *Phishing Activity Trends Report, 1st Half 2009* (y anteriores)
- **CyberSource (**2009). Online fraud report, 2009 edition. Online payment fraud trends, merchant practices and benchmarks.
- **Kaspersky Labs** (2008). *Atacks on banks*.
- **McAfee** (2009). Mapping the Mal Web. The World's Rieskiest Domains.
- **Panda Security** (2009). El Negocio de los Falsos Antivirus. Análisis del nuevo estilo de Fraude Online.
- **Red.es** (2009). Evolución de los usos de Internet en España 2009.
- **RSA** (2009) Online Fraud Report December 2009 (y anteriores).
- **S21sec** (2009). *Informe fraude online 2008* (y anteriores).
- **S21sec** (2009). Informe especial de fraude en videojuegos.
- **Symantec** (2008). *Informe sobre economía sumergida*.

ÍNDICE DE GRÁFICOS

ÍNDICE DE TABLAS

ÍNDICE DE ILUSTRACIONES

Instituto Nacional
de Tecnologías
de la Comunicación

http://www.inteco.es

http://observatorio.inteco.es

http://cert.inteco.es

http://www.osi.es