GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO

INTECO
Instituto Nacional de Tecnologías de la Comunicación

Estudio sobre el fraude a través de Internet

Informe anual 2011 (8ª oleada)

INSTITUTO NACIONAL DE **TECNOLOGÍAS** DE LA **COMUNICACIÓN**

Edición: Agosto 2012

El informe de la 8ª oleada del "Estudio sobre el fraude a través de Internet (informe anual 2011)" ha sido elaborado por el Instituto Nacional de Tecnologías de la Comunicación (INTECO):

Pablo Pérez San-José (dirección)

Cristina Gutiérrez Borge (coordinación)

Eduardo Álvarez Alonso

Susana de la Fuente Rodríguez

Laura García Pérez

INTECO quiere señalar la participación en la realización del trabajo de campo e investigación de este estudio de:

ÍNDICE

PUNTOS CLAVE

El presente informe constituye la octava entrega del *Estudio sobre el fraude a través de Internet*. La metodología utilizada para la realización del informe combina entrevistas a usuarios de Internet y escaneo online de equipos de hogares españoles. El período analizado en este documento abarca el 3er cuatrimestre de 2011, esto es, los meses de septiembre a diciembre. Además, siendo este el informe que cierra el año, ofrece un análisis evolutivo de 2011, haciendo una comparativa con los datos de 2009 y 2010.

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

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

Se exponen a continuación los puntos clave del análisis.

I INTENTO DE FRAUDE Y MANIFESTACIONES

En la presente oleada se pone de manifiesto el avance el último año de la incidencia de situaciones que pueden ser constitutivas de fraude a través de Internet (aunque no necesariamente tienen que consumarse).

- En el último cuatrimestre de 2011, un 58,4% de los panelistas declara haber sufrido algún intento de fraude (no necesariamente consumado) a través de la Red. Este dato supone un incremento con respecto a los niveles de 2010.

- Los internautas identifican que las situaciones de intento (no consumado) de fraude más frecuentes son la recepción de correos electrónicos invitando a visitar páginas web sospechosas (43,3%) o promocionando servicios no solicitados (32,7%). Estos datos, si bien son inferiores a los del cuatrimestre anterior, muestran como dato anual un marcado incremento con respecto a 2010 y suponen un cambio en la tendencia observada entre 2009 y 2010, periodo en el que descendió la incidencia.

II FORMA ADOPTADA POR EL REMITENTE ORIGEN DE LA COMUNICACIÓN SOSPECHOSA DE SER FRAUDULENTA

Cuando navegan en la Red, los usuarios siguen recibiendo comunicaciones sospechosas de ser fraudulentas que simulan provenir principalmente de entidades de comercio electrónico y bancos. Sin embargo, en el último año otras fórmulas, como las redes sociales y los particulares, se vuelven más frecuentes.

- En el tercer cuatrimestre de 2011, los principales formatos utilizados en los mensajes con apariencia sospechosa son las web de comercio electrónico y las entidades bancarias (ambas con un 39,8%), seguidas de las loterías (30,8%).

- Estas fórmulas son las más frecuentes desde 2009, si bien han cedido terreno a favor de otros formatos, como los particulares (31,4%, 7,6 puntos porcentuales más que en 2009) y las redes sociales (26,1%, 4,8 puntos porcentuales de incremento).

III IMPACTO ECONÓMICO DEL FRAUDE

La incidencia de fraude con impacto económico se mantiene con el paso de los años en niveles inferiores al 5%. Sí se observa un cambio en las cuantías defraudadas, que tienden a ser cada vez más de pequeño importe (inferior a 400 €).

- Un 3,6% de los internautas dicen haber sido víctimas de un fraude con perjuicio económico a través de Internet en el tercer cuatrimestre de 2011. No se observan diferencias importantes al comparar esta incidencia con los datos de 2009 y 2010.

- La cuantía defraudada es inferior a 400€ en la mayoría de las ocasiones (un 93,3%). Esta proporción supone una mejora con respecto a los valores de 2009 (84,3%).

IV FRAUDE Y MALWARE

El malware orientado a la comisión de fraude sigue estando presente en más de un tercio de los equipos de los hogares españoles, lo que supone un indicador del fraude online en sí mismo. Esta amenaza persiste con el paso de los años.

- En diciembre de 2011, un 36,5% de los equipos analizados aloja algún tipo de troyano, un 5,7% troyanos bancarios y un 4,6%, rogueware.

- Tras un repunte en los valores a comienzos del año, la tendencia se ha mantenido bastante constante, con ligeros descensos en los valores a final de año. También se observa que la proporción de equipos infectados a finales de 2011 es levemente superior a la de 2009 en el caso de los troyanos genéricos e inferior en el de los troyanos bancarios y el rogueware.

V INFLUENCIA DEL INTENTO DE FRAUDE EN LOS HÁBITOS RELACIONADOS CON LA BANCA A TRAVÉS DE INTERNET Y EL COMERCIO ELECTRÓNICO

Año tras año, la confianza depositada por los internautas en la banca online y el comercio electrónico goza de buena salud. Los usuarios se muestran prudentes, tanto si han sufrido una pérdida económica a consecuencia de un fraude como si no y mantienen los niveles de uso de estos servicios.

- Los internautas que utilizan comercio electrónico y banca en línea se muestran bastante prudentes a la hora de utilizar estos servicios, con independencia de haber sufrido una pérdida económica a consecuencia de un intento de fraude. Las diferencias se observan en la preferencia por determinados comportamientos que adoptan unos u otros.

- Tampoco presenta diferencias el nivel de confianza depositado en la realización de compras en línea utilizando tarjetas de crédito/débito o de operaciones de banca online, tras sufrir una situación de fraude. En todos los casos, está entorno al 80%.

- En cuanto a las reacciones adoptadas tras experimentar una circunstancia de este tipo, de nuevo se observa fidelidad en el uso de estos servicios: más de un 70% dicen no modificar sus hábitos de comercio electrónico o banca online. Sin embargo, al tener en cuenta la evolución con respecto a años anteriores, resulta positivo el hecho de que cada vez son menos los que muestran una actitud pasiva y más los que adoptan opciones diferentes al abandono las compras online o la realización de operaciones bancarias en línea.

.

1 INTRODUCCIÓN Y OBJETIVOS

1.1 PRESENTACIÓN

El Instituto Nacional de Tecnologías de la Comunicación, S.A. (INTECO), es una sociedad estatal adscrita al Ministerio de Industria, Energía y Turismo a través de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información.

INTECO es un centro de desarrollo de carácter innovador y de interés público de ámbito nacional que se orienta a la aportación de valor, a la industria y a los usuarios, y a la difusión de las nuevas tecnologías de la información y la comunicación (TIC) en España, en clara sintonía con Europa.

Su objetivo fundamental es servir como instrumento para desarrollar la Sociedad de la Información, con actividades propias en el ámbito de la innovación y el desarrollo de proyectos asociados a las TIC, basándose en tres pilares fundamentales: la investigación aplicada, la prestación de servicios y la formación.

La misión de INTECO es aportar valor e innovación a los ciudadanos, a las PYMES, a las Administraciones Públicas y al sector de las tecnologías de la información, a través del desarrollo de proyectos que contribuyan a reforzar la confianza en los servicios de la Sociedad de la Información en nuestro país, promoviendo además una línea de participación internacional.

Para ello, INTECO desarrolla actuaciones en las siguientes líneas:

- **Seguridad tecnológica:** INTECO está comprometido con la promoción de servicios de la Sociedad de la Información cada vez más seguros, que protejan los datos personales de los interesados, su intimidad, la integridad de su información y eviten ataques que pongan en riesgo los servicios prestados. Y, por supuesto, que garanticen un cumplimiento estricto de la normativa legal en materia de TIC. Para ello coordina distintas iniciativas públicas en torno a la seguridad de las TIC, de las que se benefician ciudadanos, pymes, Administraciones Públicas y el sector tecnológico.

- **Accesibilidad:** INTECO promueve servicios de la Sociedad de la Información más accesibles, que supriman las barreras de exclusión, cualquiera que sea la dificultad o carencia técnica, formativa, etc., incluso discapacidad, que tengan sus usuarios. Y que faciliten la integración progresiva de todos los colectivos de usuarios, de modo que todos ellos puedan beneficiarse de las oportunidades que ofrece la Sociedad de la Información. En particular, INTECO dispone de amplia experiencia en el desarrollo de proyectos en el ámbito de la accesibilidad para la televisión digital, así como de aquellos orientados a garantizar los derechos de los

ciudadanos a relacionarse con las administraciones públicas por medios electrónicos, reconocidos en la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos

- **Calidad TIC**: INTECO promueve unos servicios de la Sociedad de la Información que cada vez sean de mayor calidad, que garanticen unos adecuados niveles de servicio, lo cual se traduce en una mayor robustez de aplicaciones y sistemas, un compromiso en la disponibilidad y los tiempos de respuesta, un adecuado soporte para los usuarios, una información precisa y clara sobre la evolución de las funcionalidades de los servicios, y en resumen, servicios cada vez mejores. En esta línea impulsa la competitividad de la industria del Software a través de la promoción de la mejora de la calidad y la certificación de las empresas y profesionales de la ingeniería del software.

- **Formación**: la formación es un factor determinante para la atracción de talento y para la mejora de la competitividad de las empresas. Por ello, INTECO impulsa la formación de universitarios y profesionales en las tecnologías más demandadas por la industria.

Es uno de los objetivos de INTECO describir de manera detallada y sistemática el nivel de seguridad, privacidad 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, la privacidad y la e-confianza.

El Departamento de Análisis y Estudios de INTECO toma el testigo del Observatorio de la Seguridad de la Información (http://observatorio.inteco.es), referente nacional e internacional a la hora de describir, analizar, asesorar y difundir la cultura de la seguridad, la privacidad y la confianza de la Sociedad de la Información.

Este departamento ha diseñado un Plan de Actividades y Estudios con el objeto de producir conocimiento especializado y útil en materia de seguridad y privacidad, así como de elaborar recomendaciones y propuestas que definan tendencias válidas para la toma de decisiones futuras por parte de los poderes públicos, que atiende, entre otros, a los siguientes objetivos:

- Elaboración y presentación de informes en materia de seguridad, privacidad y e-confianza, que sirvan de apoyo para la toma de decisiones por parte de la Administración, con especial énfasis en la seguridad en Internet.

- Seguimiento de los principales indicadores y políticas públicas relacionadas con la seguridad de la información y la confianza en el ámbito nacional e internacional.

- Generación de una base de datos que permita el análisis y evaluación de la seguridad y la confianza con una perspectiva temporal.

- Impulso de proyectos de investigación en materia de seguridad TIC.

- Difusión de estudios e informes publicados por otras entidades y organismos nacionales e internacionales, así como de información sobre la actualidad nacional y europea en materia de la seguridad y confianza en la Sociedad de la Información.

- Asesoramiento a las Administraciones Públicas en materia de seguridad de la información y confianza, así como el apoyo a la elaboración, seguimiento y evaluación de políticas públicas en este ámbito.

1.2 ESTUDIO SOBRE EL FRAUDE A TRAVÉS DE INTERNET

El *Estudio sobre el fraude a través de Internet* permite analizar de manera evolutiva los intentos de fraude a través de la Red que han sufrido los usuarios, las formas adoptadas por el remitente origen de la comunicación sospechosa de ser fraudulenta y, como consecuencia, el impacto económico sufrido. El presente informe constituye la 8ª entrega del mismo.

En esta ocasión, se presenta la actualización para el 3er cuatrimestre de 2011 de los datos de usuarios basados en entrevistas comparando estos resultados con los obtenidos en el 2º cuatrimestre de 2011 y, de esta manera, poder ofrecer un análisis evolutivo de 2011. Además, siendo este el informe que cierra el año, ofrece una comparativa con los datos de 2009 y 2010.

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

Se muestra también si el intento de fraude influye en la modificación de los hábitos de uso de comercio electrónico y banca en línea por parte de los usuarios. También se analiza la e-confianza que les genera estos hábitos tras sufrir un intento de fraude. Las conclusiones, en este caso, se basan en datos procedentes de la encuesta.

2 DISEÑO METODOLÓGICO

El *Estudio sobre el fraude a través de Internet* se realiza a partir del panel online dedicado compuesto por hogares con conexión a Internet repartidos por todo el territorio nacional.

En la definición de la metodología del estudio, se ha considerado una fórmula que permita obtener información, con una perspectiva evolutiva. La necesidad de unos datos robustos sobre los mismos hogares y usuarios en diferentes momentos del tiempo hace que el panel online dedicado resulte la metodología idónea para satisfacer los objetivos del proyecto.

El presente informe constituye la octava entrega del estudio.

En la actualidad el panel está compuesto por 3.655 hogares con conexión a Internet repartidos por todo el territorio nacional. Sobre los miembros del panel se aplican dos técnicas diferenciadas, que permiten obtener dos tipos diferentes de información:

- Encuesta online a usuarios españoles de Internet mayores de 15 años con acceso frecuente desde el hogar, llevadas a cabo con una periodicidad cuatrimestral. Los datos extraídos de las encuestas permiten obtener la percepción sobre la situación de la seguridad en Internet y nivel de e-confianza de los usuarios domésticos. En el período analizado en la presente entrega (3º cuatrimestre de 2011), 3.655 usuarios han respondido a la encuesta. 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%, el error muestral es de ±1,62%.

- Auditoría remota online del nivel de seguridad real de los equipos informáticos existentes en los hogares, realizada mensualmente. Para ello, se utiliza el software iScan, desarrollado por INTECO, que analiza los sistemas y la presencia de malware en los equipos gracias a la utilización conjunta de 43 motores antivirus. Este software se instala en los equipos y los analiza, detectando el malware residente en los mismos y recogiendo datos del sistema operativo, su estado de actualización y las herramientas de seguridad instaladas. La muestra en este tercer cuatrimestre de 2011 se compone de 2.505 hogares que escanearon online su ordenador entre septiembre y diciembre de 2011. El número total de análisis remotos en el período ha sido de 6.383.

2.1 UNIVERSO

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

2.2 TAMAÑO Y DISTRIBUCIÓN MUESTRAL

Para la encuesta, se ha extraído una muestra representativa de 3.655 usuarios de Internet, con participación estable en el panel en el cuatrimestre comprendido entre septiembre y diciembre de 2011.

De esta muestra se obtienen dos tipos diferentes de información: la proporcionada por los propios usuarios en la encuesta y la obtenida directamente mediante observación (análisis online de sus equipos).

Dado que la periodicidad de extracción de datos es diferente (cuatrimestral en el caso de la encuesta 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 indica el número de equipos escaneados mientras la Tabla 2 describe los tamaños muestrales de la encuesta.

Tabla 1: Número de equipos escaneados mensualmente

Período	Equipos escaneados	Período	Equipos escaneados	Período	Equipos escaneados
Ene'09	5.649	Ene'10	4.079	Ene'11-	2.083
Feb'09	4.325	Feb'10	3.751	Feb'11	1.461
Mar'09	4.695	Mar'10	4.024	Mar'11	1.329
Abr'09	4.954	Abr'10	3.746	Abr'11-	1.067
May'09	4.677	May'10	3.499	May'11	672
Jun'09	4.293	Jun'10	3.279	Jun'11	2.379
Jul'09	3.971	Jul'10	3.337	Jul'11	2.891
Ago'09	3.677	Ago'10	2.716	Ago'11	2.595
Sep'09	4.520	Sep'10	2.783	Sep'11	1.389
Oct'09	4.294	Oct'10	3.232	Oct'11	1.288
Nov'09	4.039	Nov'10	2.742	Nov'11	1.610
Dic'09	4.452	Dic'10	2.604	Dic'11	2.096

Fuente: INTECO

Tabla 2: Tamaños muestrales para la encuesta

Período	Tamaño muestral
1er trimestre 2009	3.563
2º trimestre 2009	3.521
3er trimestre 2009	3.540
4º trimestre 2009	3.640
1er trimestre 2010	3.599
2º trimestre 2010	3.519
3er trimestre 2010	3.538
4º trimestre 2010	3.571
2º cuatrimestre 2011	2.405
3er cuatrimestre 2011	3.655

Fuente: INTECO

2.3 CAPTURA DE INFORMACIÓN Y TRABAJO DE CAMPO

El trabajo de campo ha sido realizado entre septiembre y diciembre de 2011 mediante entrevistas online y análisis de equipos informáticos a partir de un panel de usuarios de Internet.

El análisis de equipos informáticos se realiza con la herramienta **iScan** (INTECO Scanner). Esta herramienta es un software multiplataforma desarrollado por INTECO, que se entrega a los panelistas con el fin de que lo instalen en sus ordenadores. iScan utiliza 43 motores antivirus. Este software analiza mensualmente los equipos de los panelistas, detectando el malware específico para la comisión de fraude residente en los mismos.

La herramienta de INTECO tiene como piedra angular una base de datos de más de 30 millones de archivos detectados por, al menos, uno de esos 43 antivirus. Esta base de datos está en constante crecimiento.

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

El uso de 43 antivirus asegura una mayor tasa de detección, pues ante las nuevas amenazas de carácter altamente indetectable es difícil que un espécimen escape a todos los motores.

El programa informático remite esta información a INTECO, que la trata de manera anónima y agregada. A lo largo de todo el proceso se cumple estrictamente con la normativa vigente en materia de protección de datos de carácter personal.

El escaneo de iScan no da información sobre si un determinado código malicioso se encuentra activo en el sistema. Podría darse el caso de que un sistema aloja malware pero no se encuentra infectado. Imagínese, por ejemplo, que un investigador tiene un

directorio con código malicioso para estudiar, su equipo sería catalogado por iScan como infectado pero dichas muestras nunca se habrían ejecutado en el sistema y por tanto no estaría infectado. Esto también ocurriría si un antivirus detecta un código malicioso y lo mueve a una carpeta de cuarentena sin ofuscarlo.

Con el fin de reducir el impacto de los falsos positivos se aplican una serie de filtros, que se explican a continuación:

Eliminación y ponderación de soluciones antivirus

a. *Eliminación de productos antivirus de perímetro que tras pruebas con grandes cantidades de malware y goodware[1] demostraron ser altamente paranoicos.*

b. *Eliminación de ciertas soluciones que comparten firmas, para sólo considerar un motor con el mismo conjunto de firmas.*

c. *Creación de un subconjunto de motores. Se han tomado los 11 antivirus más reputados (con mejor tasa de detección frente a especímenes detectados por más de 10 antivirus) para crear un subconjunto de productos que será referenciado como motores necesariamente exigidos. De este modo, para que un fichero sea marcado como malware, deberá ser detectado por 5 productos de los 43 considerados y, además, al menos uno de ellos deberá ser alguno de estos 11 motores exigidos.*

Verificación manual de un número acotado de ejemplares

El malware identificado se ordena por número de equipos en los que aparece cada ejemplar. Ante la imposibilidad de verificación de todos los ejemplares, se seleccionan los 50 ficheros más avistados y se analizan de forma manual mediante técnicas de análisis dinámico (monitorización de modificaciones de ficheros, registro y procesos, llamadas a funciones de la API de Windows, etc.) y estático (desensamblado y depurado). Este análisis busca determinar qué muestras han sido clasificadas incorrectamente como código malicioso una vez se ha llegado a esta fase del proceso de detección.

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

INTECO mantiene una base de datos de software de fabricantes confiables y de freeware[2] y shareware[3] confirmado como inocuo. Todos los ejemplares que siguen siendo detectados tras las dos primeras capas de filtrado son comparados con esta base de datos para eliminar más falsos positivos.

[1] Software y ficheros legítimos, archivos inocuos.

[2] Software gratuito.

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

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

Eliminación de detecciones concretas y corrección de categorías incorrectamente determinadas

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

Tras esto, se corrigen ciertas categorías de malware que fueron decididas de forma automática. Por ejemplo, todos los ficheros detectados como "shutdown", "patch", "wgapatch" y "keygen" son clasificados forzosamente como herramientas, con independencia de la categoría decidida por los antivirus.

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

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

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

2.4 ERROR MUESTRAL

De acuerdo con los criterios de muestreo aleatorio simple para variables dicotómicas en las que p=q=0,5, y para un nivel de confianza del 95,5%, se establecen que al tamaño muestral n=3.655 le corresponde una estimación del error muestral igual a ±1,62%.

Tabla 3: Errores muestrales de las encuestas (%)

Período	Tamaño muestral	Error muestral
1er trimestre 2009	3.563	±1,68%
2º trimestre 2009	3.521	±1,68%
3er trimestre 2009	3.540	±1,68%
4º trimestre 2009	3.640	±1,66%
1er trimestre 2010	3.599	±1,66%
2º trimestre 2010	3.519	±1,68%
3er trimestre 2010	3.538	±1,68%
4º trimestre 2010	3.571	±1,68%
2º cuatrimestre 2011	2.405	±2,00%
3er cuatrimestre 2011	3.655	±1,62%

Fuente: INTECO

3 SEGURIDAD Y FRAUDE ONLINE

3.1 INTENTO DE FRAUDE Y MANIFESTACIONES

Para comenzar este análisis, se estudia la incidencia declarada de situaciones de intento de fraude a través de Internet en los últimos tres meses.

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

- En primer lugar, los datos proporcionados en los gráficos de este apartado están basados en las respuestas a la encuesta aplicada al panel de usuarios de Internet españoles, ofreciendo por tanto la perspectiva del ciudadano. Esta percepción, según la sofisticación de los ataques, puede haber permitido o no identificar las posibles amenazas.

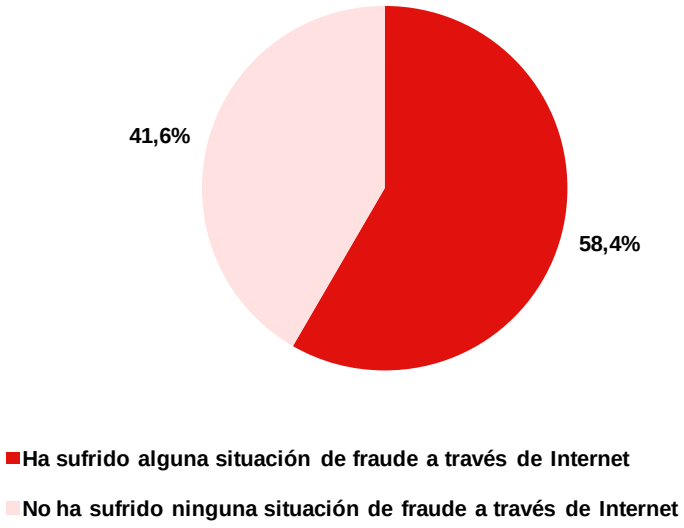
- En segundo lugar, no debe entenderse que las personas que afirman haber experimentado alguna de las situaciones analizadas son efectivamente víctimas de fraude. Se habla, por tanto, de intento de fraude y no de fraude consumado.

- A partir de la presente oleada, para elaborar el informe se tienen en cuenta únicamente las respuestas de los usuarios que han sufrido un intento de fraude a través de Internet, mientras que en informes anteriores el análisis se realizaba incluyendo también las respuestas de los que habían experimentado intentos de fraude a través del teléfono móvil[4].

En el tercer cuatrimestre de 2011, un 58,4% de los encuestados declara haber sido objeto de algún intento de fraude (no consumado) a través de Internet, frente a un 41,6% que no han constatado una situación de este tipo.

[4] Los datos de fraude a través del teléfono móvil se pueden consultar en el *Estudio sobre seguridad en dispositivos móviles y smartphones,* que estará disponible en agosto de 2012 en la web: http://observatorio.inteco.es

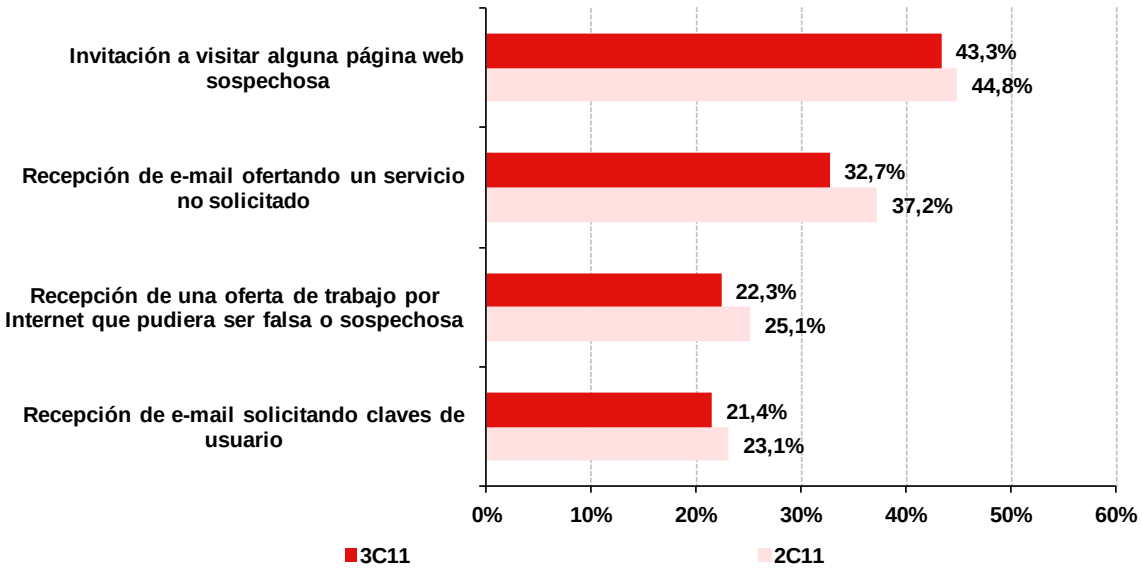
Gráfico 1: Incidencia declarada de situaciones de intento (no consumado) de fraude a través de Internet en los últimos 3 meses (%)



Base: Total usuarios (n=3.655 en 3er cuatrimestre 2011) *Fuente: INTECO*

El Gráfico 2 ofrece más detalle en cuanto a las incidencias de fraude que perciben los encuestados al utilizar la Red, mostrando una perspectiva evolutiva al comparar los datos del último cuatrimestre de 2011 con los del periodo anterior.

Gráfico 2: Evolución de la incidencia declarada de situaciones de intento (no consumado) de fraude a través de Internet en los últimos 3 meses (%)



Base: Total usuarios (n=3.655 en 3er cuatrimestre 2011) *Fuente: INTECO*

En el cuatrimestre analizado en el presente informe, haber recibido mensajes instando a visitar páginas web sospechosas es la circunstancia más frecuente en opinión de los internautas (43,3%), seguida de la recepción de correos ofreciendo servicios no solicitados (32,7%). En menor medida, los encuestados señalan las comunicaciones online con supuestas ofertas de trabajo (22,3%) y los correos electrónicos que solicitan al usuario sus claves personales (21,4%).

Los valores obtenidos a finales de 2011 son inferiores a los de la oleada previa, particularmente en el caso de los correos electrónicos ofertando servicios no solicitados (4,5 puntos porcentuales menos).

Para finalizar este apartado, la Tabla 4 ofrece la evolución interanual de 2009 a 2011 de la incidencia de situaciones de fraude a través de la Red. Para este análisis, tanto en 2009 como en 2010 se ha tomado el dato del último trimestre del año y en 2011 el del último cuatrimestre[5].

Tabla 4: Evolución de la incidencia declarada de situaciones de intento (no consumado) de fraude a través de Internet entre 2009 y 2011 (%)

Incidencia declarada de situaciones de intento (no consumado) de fraude (%)	2009	2010	2011	Evolución
Invitación a visitar alguna página web sospechosa	34,1	34,4	43,3	▲
Recepción de e-mail ofertando un servicio no solicitado	29,4	25,9	32,7	▲
Recepción de una oferta de trabajo por Internet que pudiera ser falsa o sospechosa	23,1	21,1	22,3	▶
Recepción de e-mail solicitando claves de usuario	21,6	19,9	21,4	▶

Fuente: INTECO

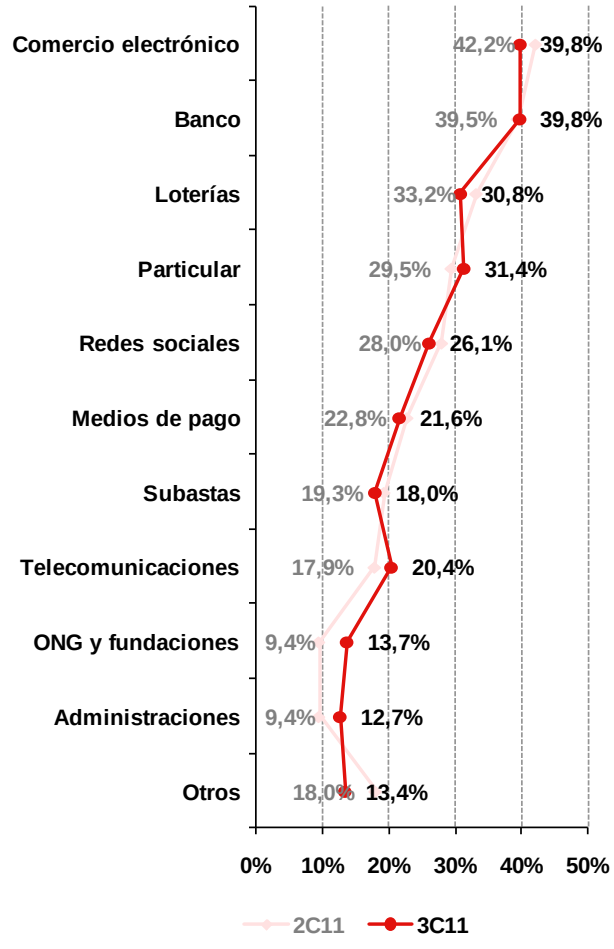
Como se observa, se ha producido una evolución interanual positiva en las situaciones más frecuentes, es decir, en la invitación a visitar una página web sospechosa (9,2 puntos porcentuales) y en la recepción de emails que ofertan servicios no requeridos (3,3 puntos). Estos incrementos suponen un cambio en la tendencia con respecto al periodo 2009-2010, en general de signo negativo.

[5] Para esta tabla y para todas las que ofrezcan un análisis interanual para 2009 y 2010 se toma el dato del último trimestre del año y en 2011 el del último cuatrimestre.

3.2 FORMA ADOPTADA POR EL REMITENTE ORIGEN DE LA COMUNICACIÓN SOSPECHOSA DE SER FRAUDULENTA

Al enviar comunicaciones sospechosas de ser fraudulentas, los atacantes optan por diferentes fórmulas de remite, haciéndose pasar por diversos tipos de entidades para dar credibilidad a las estafas. En tercer cuatrimestre de 2011, los principales formatos de remite utilizados en los mensajes con apariencia sospechosa son las web de comercio electrónico y las entidades bancarias (ambas con un 39,8%). Otras fórmulas adoptadas incluyen hacerse pasar por un particular, una página de loterías o una red social (31,4%, 30,8% y 26,1%), entre otras.

Gráfico 3: Evolución de las formas adoptadas por el remitente de la comunicación sospechosa de ser fraudulenta[6] (%)



Base: Usuarios que han sufrido algún intento de fraude (n= 2.133 en 3er cuatrimestre 2011) Fuente: INTECO

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

Comparando los datos con los del segundo cuatrimestre del año, con carácter general se observa un ligero retroceso en los valores situados en lo alto del ranking (a excepción de bancos y particulares) y un ascenso más marcado de los formatos menos utilizados, como operadores de telecomunicaciones, ONGs y Administración.

Asimismo, comercio electrónico y entidades bancarias se igualan como fórmulas más frecuentes, mientras que las loterías pierden la tercera posición a favor de los particulares.

En la Tabla 5 se profundiza en el análisis de las fórmulas de remite utilizadas por los ciberestafadores, teniendo en cuenta el tipo de situación de intento de fraude.

En general, la banca online y el comercio electrónico se corroboran como principales máscaras utilizadas, aunque existen particularidades en función del tipo de mensaje. Entre los usuarios que dicen haber recibido un e-mail solicitando sus claves de usuario, es destacable la proporción que reconoce que la comunicación procedía de un supuesto banco (78,1%).

Tabla 5: Formas adoptadas por el remitente según el tipo de comunicación sospechosa que ha experimentado el internauta[7] (%)

Tipo de incidencia declarada	Forma adoptada por el remitente de la comunicación										
	Administradciones	ONG y fundaciones	Telecomunicaciones	Subastas	Medios de pago	Redes sociales	Particular	Loterías	Banco	Comercio electrónico	Otros
Recepción de e-mail solicitando claves de usuario	10,3	7,3	9,2	8,9	23,9	14,7	10,7	14,2	**78,1**	14,9	2,7
Recepción de e-mail ofertando un servicio no solicitado	6,3	11,9	20,2	18,5	14,7	18,0	16,2	32,6	21,7	**44,7**	6,9
Invitación a visitar alguna página web sospechosa	6,5	7,5	13,8	13,8	14,2	21,7	28,2	26,2	21,6	**29,6**	7,3
Recepción de una oferta de trabajo por Internet que pudiera ser falsa o sospechosa	14,1	11,8	10,5	6,0	10,3	14,4	**33,3**	10,8	12,5	17,8	19,7

Base: Usuarios que han sufrido cada tipo concreto de intento de fraude *Fuente: INTECO*

El comercio electrónico es el remitente que predomina en los correos electrónicos que ofrecen servicios no solicitados (44,7%), seguido de loterías (32,6%) y entidades bancarias (21,7%). Las entidades de compra-venta online también están a la cabeza de

[7] Ver nota a pie número 6.

las invitaciones a acceder a páginas web sospechosas (29,6%), en este caso seguidas de particulares y loterías (28,2% y 26,2%, respectivamente). Asimismo, según los panelistas, individuos particulares son con mayor frecuencia los supuestos remitentes de ofertas de trabajo sospechosas o falsas (33,3%), aunque también se utilizan otras fórmulas (19,7%).

Por último, al cotejar los datos del último periodo analizado con los de años anteriores, se observa que las fórmulas más frecuentes ceden terreno en favor de otras como las redes sociales, los particulares o las organizaciones sin ánimo de lucro (de nuevo, es importante insistir que en el presente informe se tiene en cuenta únicamente las respuestas de los usuarios que han sufrido un intento de fraude a través de Internet[8]).

Así, se produce un avance en formatos de remitente como particulares (con un incremento de 7,6 puntos porcentuales desde 2009), redes sociales (4,8 puntos porcentuales) o la categoría "otros" (8,3 puntos). Los retrocesos más importantes de 2009 a 2011 se dan en los formatos de loterías (4,6 puntos porcentuales menos) y los bancos (3,3 puntos).

Tabla 6: Evolución de las formas adoptadas por el remitente de la comunicación sospechosa de ser fraudulenta entre 2009 y 2011 (%)

Forma adoptada	4T 2009	4T2010	3C2011	Evolución
Banco	43,1	42,7	39,8	▼
Comercio electrónico	41,9	39,0	39,8	▼
Loterías	39,0	35,7	30,8	▼
Particular	23,8	27,3	31,4	▲
Redes sociales	21,3	24,3	26,1	▲
Telecomunicaciones	21,4	19,8	20,4	▶
Medios de pago	23,1	20,7	21,6	▼
Subastas	20,9	16,3	18	▼
ONG y fundaciones	8,3	8,1	13,7	▲
Administraciones	9,1	6,3	12,7	▲
Otros	5,1	7,0	13,4	▲

Fuente: INTECO

Como se indica desde el propio sector de empresas de seguridad[9], en 2011 los ciberdelincuentes buscan nuevas fórmulas de ataque, por ejemplo explotado las redes sociales como medio para lanzar intentos de fraude, generalmente con métodos de ingeniería social que buscan un lucro económico a partir de la buena voluntad o

[8] Ver nota al pie 4.

[9] Fuente: PANDALABS (2011) *Informe anual. Resumen 2011*. Disponible en: http://pandalabs.pandasecurity.com/es/informe-anual-pandalabs-2011/

ingenuidad de los usuarios. Asimismo, los ataques se han perfeccionado y combinan varios métodos para maximizar el rendimiento obtenido, como es el caso de la campaña de fraude detectada en España en la que se combinaban el *phishing* tradicional con las llamadas y el envío de SMS. Esta última información se reflejaba en informes previos de INTECO[10].

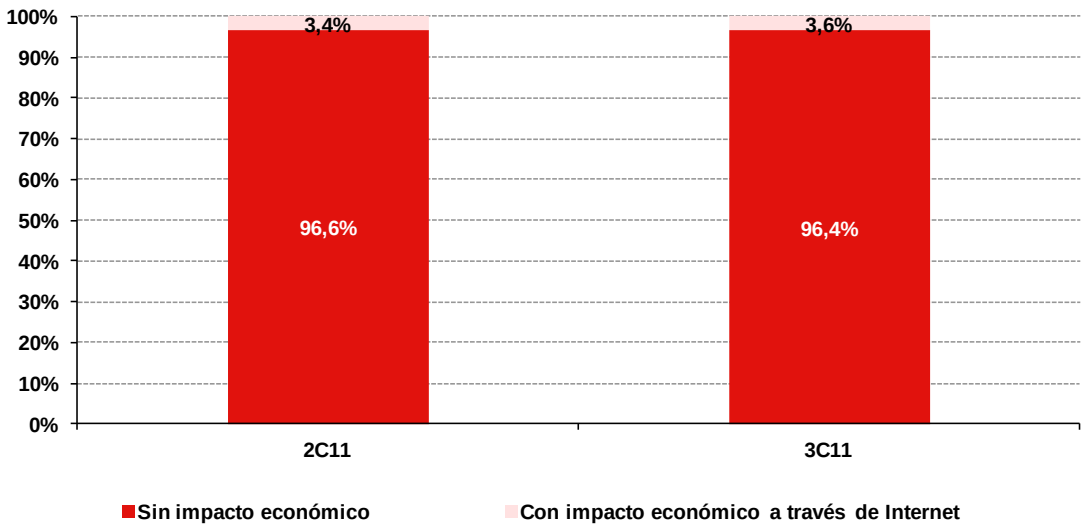
3.3 IMPACTO ECONÓMICO DEL FRAUDE

En ocasiones, los intentos de fraude a través de Internet generan un impacto económico para la víctima. Por ello, el análisis se centra en estudiar el daño objetivo y la distribución del importe defraudado.

El Gráfico 4 muestra la evolución del impacto económico del fraude que los usuarios han sufrido a través de la Red, comparando el último cuatrimestre de 2011 con el inmediatamente anterior. Adviértase que en el presente informe se tiene en cuenta únicamente el fraude relativo a comunicaciones a través de Internet (e-mails y otros mensajes vía Internet), mientras que en informes anteriores el análisis se realizaba incluyendo el fraude a través del teléfono móvil[11].

Así, un 3,6% de los usuarios declaran haber sufrido un perjuicio económico a través de Internet en el tercer cuatrimestre de 2011, frente a un 96,4% que contesta negativamente. Este dato supone un ligero repunte con relación a la oleada anterior (3,4%).

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



Base: Total usuarios (n=3.655 en 3er cuatrimestre 2011) *Fuente: INTECO*

[10] Fuente: INTECO (2012) *Estudio sobre el fraude a través de Internet. (7ª oleada)*. Disponible en: http://www.inteco.es/Seguridad/Observatorio/Estudios/Estudio_fraude_2C2011

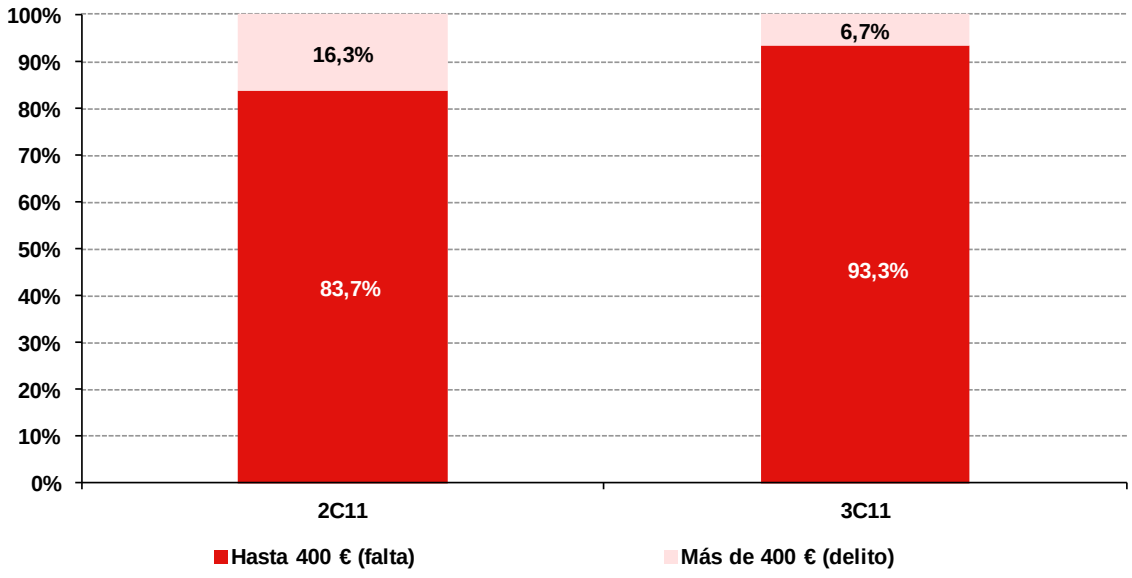
[11] Ver nota al pie 4.

En segundo lugar, el Gráfico 5 muestra la distribución de la cuantía económica derivada del fraude sufrido en Internet. En este sentido, el gráfico diferencia entre las pérdidas inferiores a 400€ y las superiores a esta cifra. Según el Código Penal español, esta cantidad constituye el umbral entre lo que se considera falta (si es igual o inferior a esa cifra la cantidad robada) y delito (si es superior).

En periodo actual, la mayoría de los internautas que han sufrido fraude con perjuicio económico en la Red (un 93,3%) declaran que la cantidad es inferior a 400€, frente a un 6,7% que considera este importe superior. La evolución indica que, a finales del año, las cantidades defraudadas son inferiores a las declaradas en el segundo cuatrimestre de 2011. Así, se incrementa en 9,6 puntos porcentuales la proporción de usuarios que han sufrido pérdidas de menor cuantía, mientras que se reduce el porcentaje de aquellos que se declaran víctimas de fraudes de más de 400€.

Desde el punto de vista de los atacantes, las consecuencias derivadas de la infracción se mitigan en el caso de cometer falta y no delito.

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



Base: Usuarios que han sufrido perjuicio económico como consecuencia de un fraude a través de Internet (n=130 en 3er cuatrimestre 2011) *Fuente: INTECO*

El análisis de la evolución entre 2009 y 2011 muestra que el impacto económico de las estafas online es similar desde el comienzo de la serie, mientras que en el caso de la cuantía defraudada, aumenta la proporción de estafas reportadas por un valor inferior a 400€, que no constituyen delito según la Ley. De nuevo, es necesario puntualizar que los valores de años anteriores tienen en cuenta el perjuicio económico sufrido a través de

Internet y teléfono, mientras que los datos de 2011 se refieren únicamente a pérdidas a través de Internet[12].

Tabla 7: Evolución del impacto económico del fraude entre 2009 y 2011 (%)

Impacto económico del fraude (%)		2009	2010	2011	Evolución
Impacto económico	Sin impacto económico	95,2	96,2	96,6	▶
	Con impacto económico	4,8	3,8	3,6	▶
Cuantía económica	Hasta 400 € (falta)	84,3	80,0	93,3	▲
	Más de 400 € (delitos)	15,7	20,0	6,7	▼

Fuente: INTECO

3.4 FRAUDE Y MALWARE

Los datos presentados a continuación proceden de los análisis empíricos obtenidos a través de iScan. Se analiza el porcentaje de malware catalogado como troyano, así como la proporción de troyanos bancarios y rogueware que se encuentran en los equipos de los hogares españoles.

1) Los troyanos bancarios son programas maliciosos que, utilizando diversas técnicas, roban información confidencial a los clientes de banca y/o plataformas de pago online[13].

   Para realizar el estudio, se han considerado las siguientes familias de troyanos bancarios más populares que efectúan ataques dirigidos contra entidades bancarias[14].

   Bancos, bank, banker, silentbanker, zbot, sinowal, torpig, fraud, zeus, infostealer, ambler, stealer, yessim, yaludle, banload, bankpatch, multibanker, nethell, chromeinject, goldun, banspy, bancodoor, bancodo, adrenalin, barracuda, blackenergy, spyeye, limbo y caberb.

2) El rogueware o rogue software es un tipo de malware cuya principal finalidad es hacer creer a la víctima que está infectada por algún tipo de virus, induciendo a pagar una determinada suma de dinero para eliminarlo. El concepto del pago suele ser la compra de un falso antivirus, que resulta en realidad el malware en

[12] Ver nota al pie 4.

[13] Fuente: glosario técnico PANDA SECURITY.

[14] Existen otras familias de troyanos que pueden emplearse para cometer fraude aunque éste no sea su cometido primordial o único. Por ejemplo, los capturadores genéricos de teclas en ocasiones pueden ser utilizados para capturar credenciales bancarias. De igual forma, los troyanos tradicionales de puerta trasera permiten hacer capturas de pantalla remotas y ver lo que el usuario escribe. Así, podrían ser empleados por un atacante para interceptar credenciales de servicios de banca o pagos online. Estas familias no se están considerando en el análisis.

sí. En los últimos tiempos, este tipo de malware está siendo muy difundido y se están detectando gran cantidad de variantes.

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

Rogue, rogueware, rogue-ware, fakeav, avfake, fakealert, fake-alert, alertfake alert-fake, FraudLoad, FakeVimes, Fakesecure, Fraudpack, AlertVir, SimulatedVir, WinFixer, XPAntivirus, LockScreen, Ransom, Zeven, FakeWarn y ArchSMS.

Cabe recordar, para interpretar correctamente las cifras, que los equipos que alojan malware bancario o rogueware no necesariamente terminan experimentando una situación de fraude. Así, para que un fraude por troyano bancario se consume, deben concurrir las siguientes circunstancias: en primer lugar, el equipo del usuario ha de estar infectado por este tipo de troyano; además, el espécimen que infectó la máquina ha de atacar a la entidad bancaria con la que opera el usuario; por último, el ciudadano ha de iniciar sesión en su espacio de banca electrónica y rellenar los datos adicionales que se le soliciten. Del mismo modo, para que se produzca efectivamente el fraude por rogueware, el usuario debe quedar infectado por ese tipo de troyano y además pagar la licencia del software malicioso.

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

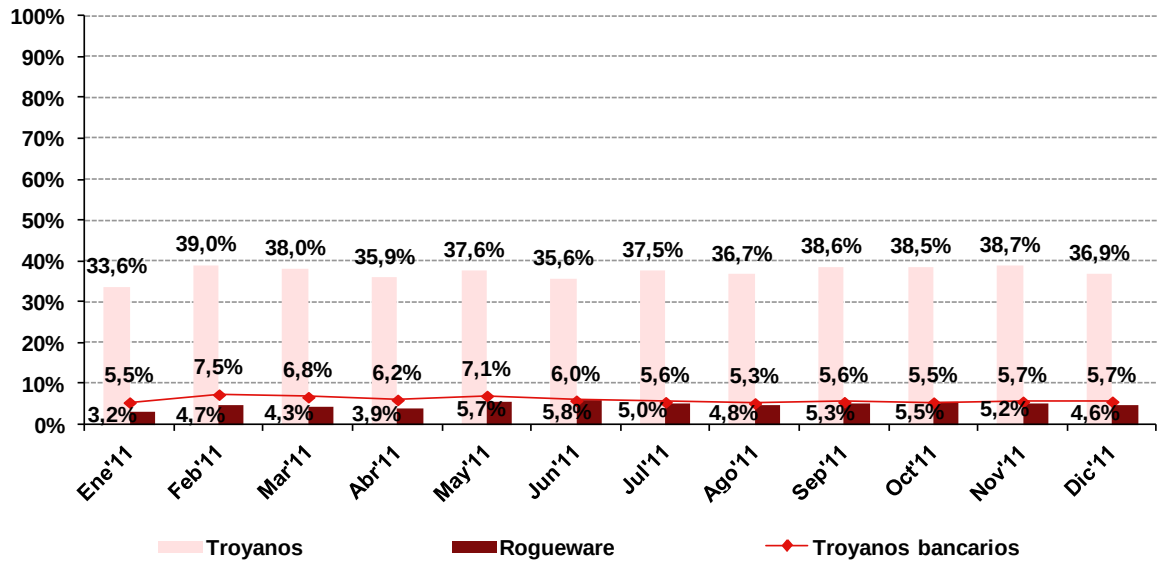
En el Gráfico 6 se representa la evolución a lo largo de 2011 del porcentaje de equipos en los que iScan reportó la presencia de malware orientado a la comisión de fraude.

Los últimos cuatro meses de 2011 muestran niveles bastante continuados. Así, la proporción de equipos que alojan troyanos genéricos apenas varía en septiembre, octubre y noviembre, aunque se produce un ligero descenso en diciembre (de un 38,7% en noviembre a un 36,5% en el último mes). De la misma forma, el rogueware llega al 4,6% al final del año, porcentaje ligeramente inferior al de los meses anteriores. Por último, los valores de infección por troyanos bancarios permanecen constantes durante este periodo, alcanzando el 5,7% en diciembre de 2011.

Teniendo en cuenta el conjunto de 2011, tras una subida inicial de los niveles de infección, la tendencia se ha mantenido bastante constante, con ligeros descensos a final de año. Destaca el repunte que experimentan los diferentes valores entre enero y febrero de 2011, con incrementos de 5,4 puntos porcentuales en el caso de los troyanos, 2 puntos en los troyanos bancarios y 1,5 puntos en el rogueware. Tras estos repuntes, se

ha producido una recuperación progresiva de los mismos, hasta terminar el año en cifras más cercanas a las de comienzos del año.

Gráfico 6: Evolución de equipos que alojan troyanos genéricos, bancarios y rogueware (%)



Fuente: INTECO

2011se ha caracterizado principalmente por ser el año de los ciberataques[15]. El malware aumenta en número y complejidad, desarrollándose nuevas combinaciones de código malicioso diseñadas específicamente para un determinado sector o actividad, como el sector financiero, pero también las infraestructuras críticas o los gobiernos. Así, se han detectado variantes de ZeuS creadas para entidades bancarias, pero también para sistemas de pago online o incluso gobiernos.

En este sentido, el objetivo pretendido con estos ataques es el robo de información (fundamentalmente credenciales bancarias), siendo el caso de Sony[16] quizás el más destacado. Sin embargo, el lucro no es el único objetivo, sino los impactos en la reputación o incluso la seguridad o estabilidad de empresas, organizaciones e incluyo gobiernos.

En cuanto a los datos obtenidos por INTECO, se puede afirmar que el notable incremento del malware y específicamente troyanos en 2011 señalado por empresas de seguridad no se observa de forma tan marcada en los niveles de infección de los equipos de los hogares españoles. Asimismo, la reducción de los falsos antivirus a finales de año está

[15] Ver nota al pie 9.

[16] Fuente: *Sony investiga el robo de datos de 77 millones de cuentas de PlayStation. Disponible en:* http://www.lavanguardia.com/internet/20110427/54146138829/sony-investiga-el-robo-de-datos-de-77-millones-de-cuentas-de-playstation.html

en línea con las informaciones publicadas por el sector de la seguridad, que ha observado un descenso en los ataques provocados por rogueware debidos a las mejoras en los algoritmos de cifrado de los motores de búsqueda y a los esfuerzos de los profesionales de seguridad y las fuerzas policiales para desmantelar algunas de las redes utilizadas por los ciberdelincuentes, como ChronoPay[17].

Teniendo en cuenta el ascenso en los valores producido entre 2009 y 2010, en 2011 se rompe la tendencia al alza y se recuperan, en el caso de los troyanos genéricos, valores más similares a los obtenidos a finales de 2009.

Para finalizar, el descenso en la proporción de infecciones en el último año puede considerarse también un dato positivo para la disminución del fraude, por varios factores:

- La identificación por firmas de los antivirus es cada vez más difusa. En mayor medida, utilizan nombres genéricos para detectar el malware por firmas, sin clasificar exactamente las familias. Por tanto, es posible que dentro de los troyanos genéricos nombrados como tal, se encuentren familias de troyanos bancarios todavía no identificadas específicamente como bancarios.

- Los troyanos genéricos, en realidad, también pueden permitir el fraude. Están destinados a controlar remotamente el sistema afectado y, por tanto, una de sus funcionalidades podría ser el robo de contraseñas. La diferencia frente a los que se consideran específicamente bancarios es que resultan más versátiles y permiten otras acciones sobre la víctima según las necesidades del atacante. Esto los convierte, en realidad, en más potentes.

Tabla 8: Evolución de equipos que alojan troyanos bancarios y rogueware entre 2009 y 2011 (%)

Equipos que alojan troyanos bancarios y rogueware (%)	2009	2010	2011	Evolución
Troyanos	35,6	39,8	36,9	▲
Troyanos bancarios	6,3	6,8	5,7	▼
Rogueware	n.d.	5,8	4,6	▼

Fuente: INTECO

[17] Fuente: *Disminuyen los ataques basados en falsos antivirus*, disponible en http://www.csospain.es/Disminuyen-los-ataques-basados-en-falsos-antivirus/seccion-actualidad/noticia-114922

3.5 INFLUENCIA DEL INTENTO DE FRAUDE EN EL COMERCIO ELECTRÓNICO Y LA BANCA A TRAVÉS DE INTERNET

3.5.1. Hábitos prudentes relacionados con el comercio electrónico y la banca en línea

Teniendo en cuenta aquellos usuarios que utilizan comercio electrónico y banca a través de Internet, a continuación se analizan los hábitos prudentes de estos panelistas, distinguiendo entre los que no han sufrido perjuicio económico derivado de fraude y los que sí.

Los usuarios que no han sufrido un impacto en su economía muestran una notable adopción de hábitos prudentes, como cerrar la sesión al terminar, evitar navegar en lugares en los que pueda ser visto o reducir en la medida de lo posible el uso de equipos públicos/compartidos (85,5%, 84,7% y 83,6%, respectivamente).

Gráfico 7: Hábitos prudentes relacionados con banca en línea y comercio electrónico entre los usuarios que han sido víctima de perjuicio económico por el fraude sufrido y los que no (%)

Base Usuarios que utilizan comercio electrónico y/o banca en línea (n=3.408 en 3er cuatrimestre 2011) *Fuente: INTECO*

Haber experimentado una pérdida económica derivada del fraude inclina la balanza hacia comportamientos como el control de los movimientos de la cuenta bancaria (91,0%), el cierre de la sesión una vez finalizada (78,6%) o la búsqueda de un lugar privado para realizar estas operaciones (76,0%).

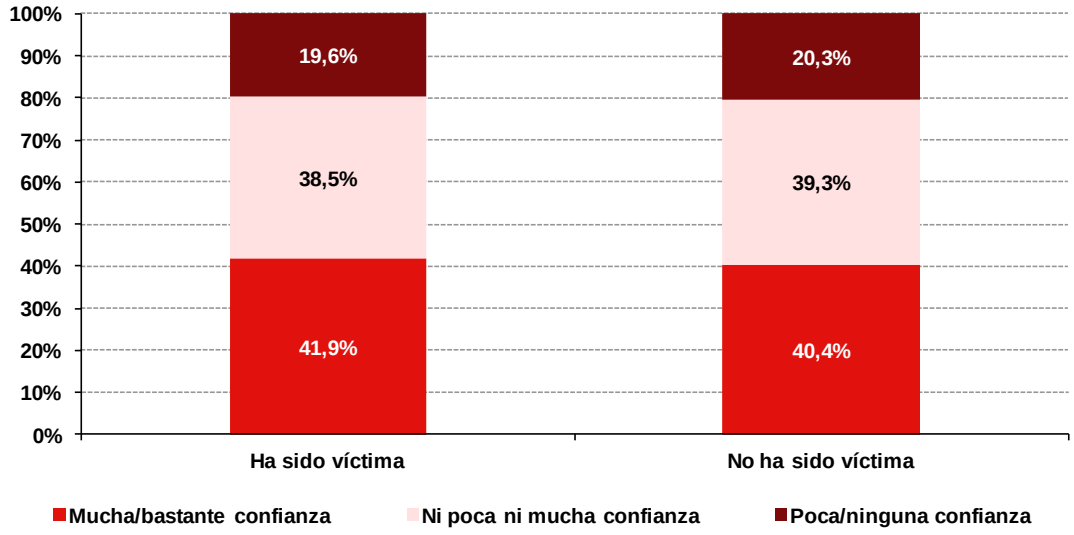
Por tanto, los internautas que utilizan comercio electrónico y banca en línea se muestran en general bastante prudentes a la hora de utilizar estos servicios, con independencia de haber sufrido una pérdida económica por un fraude en la Red. Destaca la diferencia en el hábito relativo a no proporcionar claves personales por email o teléfono, señalado por un 76,7% de los que no han sufrido perjuicio económico y por un 40,2% de los que sí. Al contrario ocurre en el uso de tarjeta prepago o monedero, realizado en mayor medida por los usuarios con pérdida económica (61,0%), que por los que no la han tenido (45,6%).

3.5.2. Nivel de confianza tras sufrir un intento de fraude y/o perjuicio económico

Tras estudiar los hábitos prudentes de los usuarios de banca en línea y comercio electrónico, se analiza a continuación el nivel de confianza en Internet como medio para realizar compras y operaciones bancarias. Al igual que en el análisis anterior, se enfrentan los datos de aquellos que han sufrido un intento de fraude y/ perjuicio económico y los que no.

El Gráfico 8 muestra un notable nivel de confianza en la realización de compras online utilizando tarjetas de crédito o débito, con independencia de haber sido víctima de fraude o no.

Gráfico 8: Nivel de confianza en la realización de compras en Internet entre los usuarios que han sufrido intento de fraude y/o perjuicio económico y los que no (%)



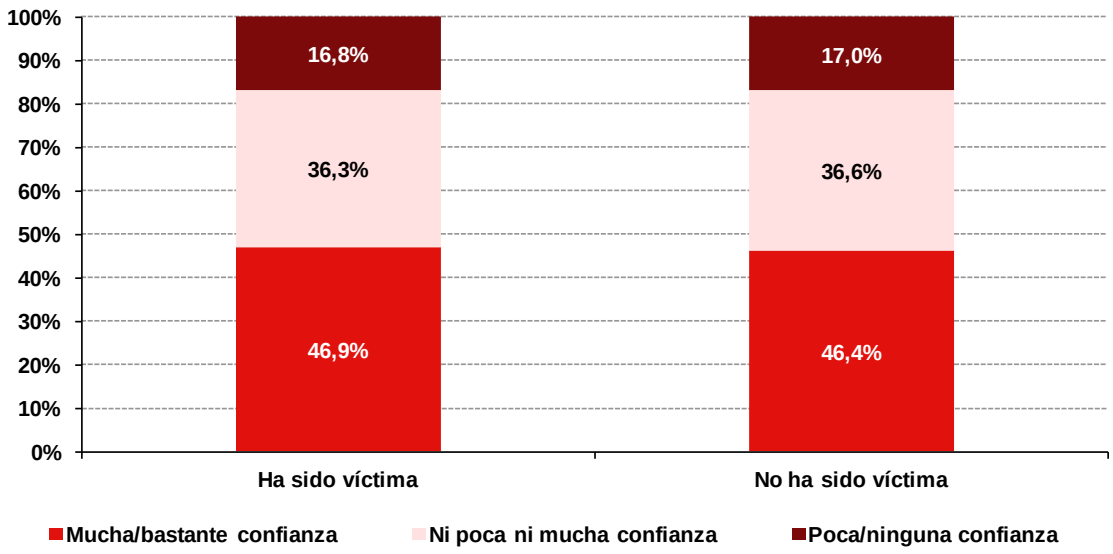
Base Usuarios que utilizan comercio electrónico (n=3.144 en 3er cuatrimestre 2011)

Fuente: INTECO

Así, un 41,9% de los que han experimentado un intento de fraude o pérdida económica confían mucho o bastante en estas operaciones, porcentaje ligeramente superior al de los que no han experimentado una situación de fraude (40,4%).

De forma similar al anterior, realizar operaciones bancarias en línea genera un buen nivel de confianza entre los usuarios de Internet, incluso después de sufrir un intento de fraude y/o perjuicio económico. Un 46,9% de los usuarios que no han sido víctimas confía mucho o bastante a la hora de hacer trámites de banca online, proporción similar entre los que sí lo han sido (un 46,4%).

Gráfico 9: Nivel de confianza en las operaciones bancarias en Internet entre los usuarios que han sufrido intento de fraude y/o perjuicio económico y los que no (%)

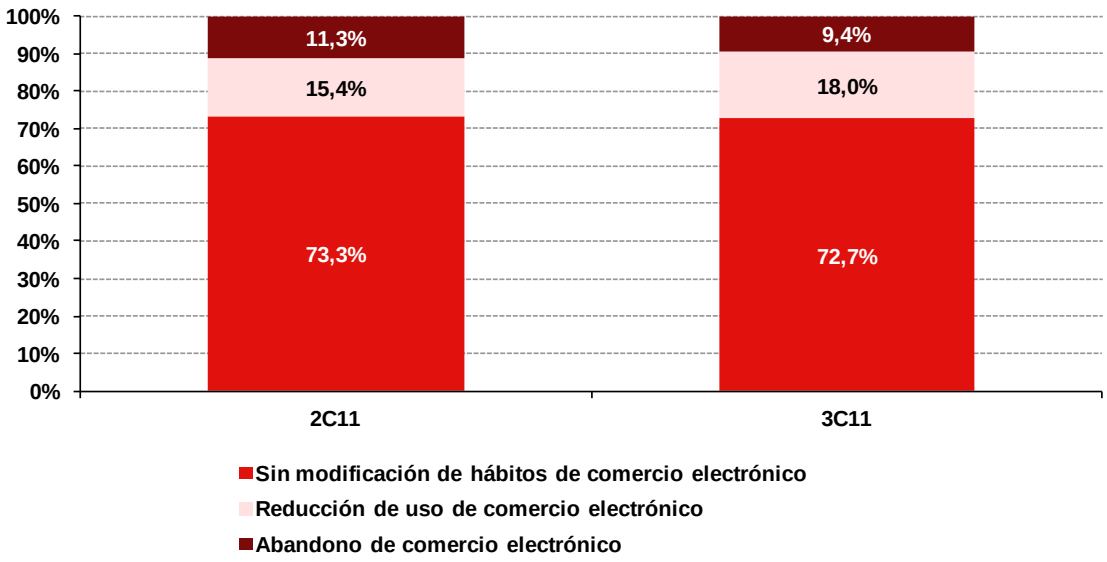


Base Usuarios que utilizan banca en línea (n=3.089 en 3er cuatrimestre 2011)
Fuente: INTECO

3.5.3. Modificación de hábitos de comercio electrónico y banca online tras sufrir un intento de fraude

El último apartado del análisis profundiza en la reacción de aquellos que han sido víctimas de un intento (no necesariamente consumado) de fraude y/o un perjuicio económico derivado del mismo, a la hora de volver a utilizar servicios de comercio y banca online.

Gráfico 10: Evolución de la modificación de los hábitos de comercio electrónico tras sufrir intento (no consumado) de fraude y/o perjuicio económico (%)



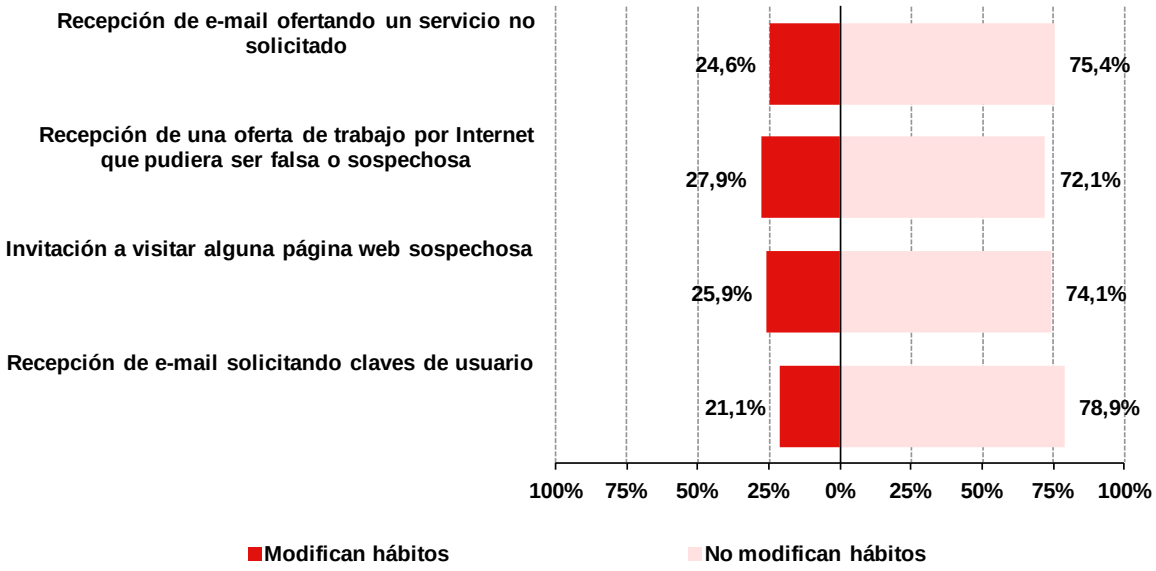
Base: Usuarios que han sufrido algún intento de fraude y/o un perjuicio económico (n=2.224 en 3er cuatrimestre 2011) *Fuente: INTECO*

En el tercer cuatrimestre de 2011, los usuarios de comercio electrónico siguen utilizando estos servicios aún cuando han sufrido una situación de fraude: el 72,7% no modifica sus hábitos, mientras que un 18,0% reduce el uso y un 9,4% abandona estos servicios.

Comparando estos valores con los del segundo cuatrimestre del año, se observa un incremento en la proporción de panelistas que reducen el uso del comercio electrónico (2,6 puntos porcentuales), si bien el grueso de los que no adoptan cambios permanece similar.

En función de la situación de fraude sufrida a través de Internet, la proporción de usuarios de comercio electrónico que modifican su comportamiento varía. El cambio se produce en mayor medida después de recibir un correo electrónico o similar ofertando un supuesto trabajo (27,9%), o invitando a visitar alguna página web sospechosa (25,9%).

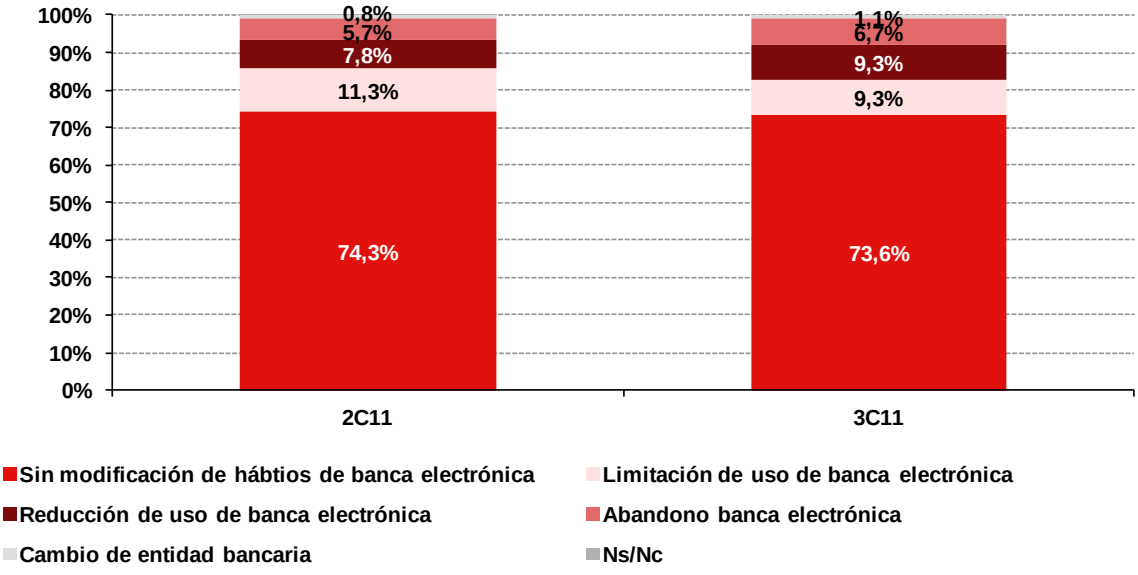
Gráfico 11: Modificación de hábitos del comercio electrónico con respecto al tipo de incidencia de fraude sufrida en los últimos tres meses (%)



Fuente: INTECO

Una vez analizado el comercio electrónico, se estudia a continuación la reacción de los internautas usuarios de banca online tras sufrir un intento de fraude.

Gráfico 12: Modificación de hábitos de banca online tras sufrir intento (no consumado) de fraude y/o perjuicio económico (%)



Base: Usuarios que han sufrido algún intento de fraude y/o un perjuicio económico (n=2.224 en 3er cuatrimestre 2011)

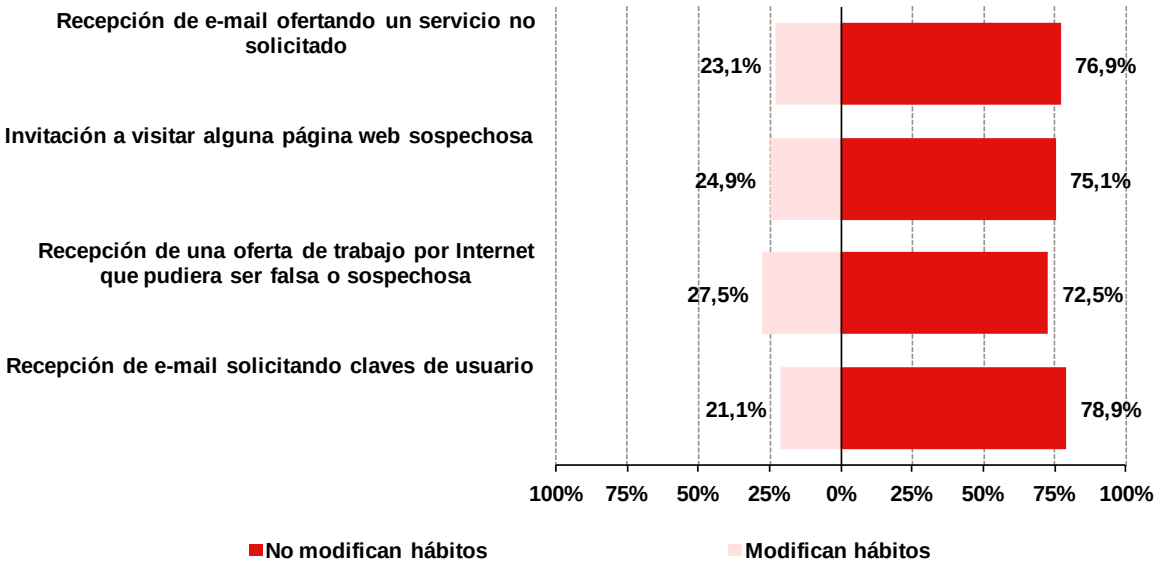
Fuente: INTECO

En el último cuatrimestre de 2011, los usuarios de banca online reaccionan de forma similar a los de comercio electrónico. Así, un porcentaje importante no altera sus hábitos (un 73,6%). En menor proporción están los que limitan o reducen el uso (un 9,3% en ambos casos), un 6,7% abandona la banca online y un residual 1,1% cambia de entidad bancaria virtual.

De nuevo, la comparación con los datos de la oleada anterior muestra que no existen variaciones significativas en las reacciones adoptadas.

En cuanto a la modificación de hábitos de banca online en función de las incidencias de fraude sufrido, de nuevo son las ofertas de trabajo por Internet sospechosas de ser falsas y las invitaciones a visitar determinadas páginas web las que más influyen en el comportamiento de los usuarios. Así, un 27,5% de los que han experimentado la primera situación y un 24,9% de los que señalan la segunda, declaran haber cambiado sus hábitos de banca online.

Gráfico 13: Modificación de hábitos de banca online con respecto al tipo de incidencia de fraude sufrida en los últimos tres meses (%)



Fuente: INTECO

Para finalizar este análisis, la Tabla 9 muestra la evolución interanual de los valores entre 2009 y 2011. En este punto es necesario advertir que los datos de 2011 están realizados en base al tipo de usuario concreto de cada servicio: mientras que en 2009 y 2010 se preguntaba sobre comercio electrónico y banca online al conjunto de usuarios que declaraba utilizar alguno de los dos servicios, en el último año únicamente se pregunta por hábitos de compra online a los que afirman ser usuarios de servicios de este tipo, y de forma similar ocurre con los internautas que realizan operaciones de banca en línea.

Desde el comienzo de la serie, destaca la reducción en la proporción de usuarios de comercio electrónico que no modifican sus hábitos en este servicio tras sufrir un incidente de fraude (9,1 puntos porcentuales), mientras que se incrementa la de aquellos que reducen el uso o lo abandonan (4,9 y 4,4 puntos porcentuales, respectivamente).

Esta situación es muy similar a la experimentada en la utilización de servicios de banca online tras ser víctima de un situación de este tipo, puesto que de nuevo se observa un trasvase desde los que no modifican hábitos (reducción de 14,2 puntos porcentuales) a favor de los que sí lo hacen, bien limitando el uso (opción no contemplada en años anteriores), bien abandonando el servicio (incremento de 3,8 puntos porcentuales) o, en menor medida, reduciendo la utilización o cambiando de entidad de banca online.

Tabla 9: Evolución de la modificación de hábitos tras sufrir un intento de fraude y/o perjuicio económico entre 2009 y 2011 (%)

Modificación de hábitos tras un intento (de fraude y/o perjuicio económico (%)		2009	2010	2011	Evolución
Comercio electrónico	Sin modificación de hábitos	81,8	84,0	72,7	▼
	Reducción del uso	13,1	11,1	18,0	▲
	Abandono	5,0	5,0	9,4	▲
Banca electrónica	Sin modificación de hábitos	87,8	89,4	73,6	▼
	Reducción del uso	8,9	7,4	9,3	▶
	Limitación del uso	nd	nd	9,3	▲
	Abandono	2,9	2,7	6,7	▲
	Cambio de entidad de banca electrónica	0,5	0,5	1,1	▶

Fuente: INTECO

4 CONCLUSIONES

La industria de seguridad ha caracterizado 2011 como el año de los ciberataques[18] dirigidos a multitud de sectores (no solo financiero), con ejemplos destacados como los de Sony, RSA, el FMI o Citigroup.

En este panorama influye de forma notable que el malware se perfecciona para lograr el mayor impacto, tanto en términos económicos, como reputacionales o incluso políticos. Así, se han detectado variantes de ZeuS creadas para entidades bancarias, pero también para sistemas de pago online o incluso gobiernos.

Junto a este factor, los atacantes se sirven de la tecnología para mejorar los mecanismos de ingeniería social. Por ejemplo, durante 2011 se ha observado una fuerte campaña de fraude en España en la que se combinan el *phishing* tradicional con llamadas y SMS.

¿Cómo afecta esta evolución a los internautas españoles?

A finales de 2011, un 58,4% de los usuarios declaran haber sido víctimas de un intento (no necesariamente consumado) de fraude a través de Internet en los últimos tres meses, lo que supone un avance del fraude online con respecto a años anteriores.

Asimismo, destacan otros indicadores de la evolución del fraude online:

- Al enviar comunicaciones sospechosas de ser fraudulentas, los atacantes optan por diferentes fórmulas de remite, haciéndose pasar por diversos tipos de entidades para dar credibilidad a las estafas. En 2011, los internautas españoles detectan más mensajes que simulan proceder de supuestas redes sociales y de particulares, fórmulas que se unen a las tradicionales (comercio electrónico, banca y páginas de loterías).

- En cuanto a la evolución del impacto económico derivado del fraude, no se observa una variación marcada con respecto a años anteriores, si bien es cierto que desde 2009 ha aumentado la proporción de fraudes reportados de cuantía inferior a 400 euros, reduciéndose los de importe superior a esa cifra. Es decir, el fraude de pequeñas cantidades es el que más afecta a los hogares españoles.

- El análisis online de los niveles de infección de los equipos muestra que, tras el ascenso en los valores de troyanos y troyanos bancarios producido entre 2009 y 2010, en el último año se rompe esta tendencia y se recuperan valores más cercanos a los de finales de 2009. Por tanto, el notable incremento del malware

[18] Ver nota al pie 4.

(específicamente troyanos) señalado por la industria de seguridad para 2011, no se observa de forma tan marcada en los equipos de hogares españoles. En el caso de los falsos antivirus, la reducción observada por INTECO sí está en línea con las informaciones publicadas por el sector.

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

En general, los internautas que utilizan comercio electrónico y banca en línea se muestran bastante prudentes a la hora de utilizar estos servicios, con independencia de haber sufrido una pérdida económica a consecuencia de un intento de fraude.

Las diferencias se observan en la preferencia por determinados comportamientos que adoptan unos u otros: mientras que los usuarios que no han sufrido un impacto en su economía declaran en mayor medida cerrar la sesión al terminar o evitar lugares en los que pueda ser visto, los que sí han experimentado una pérdida prefieren mayoritariamente controlar los movimientos de la cuenta bancaria.

En todo caso, los usuarios siguen mostrándose fieles a la compra y banca online y no retiran su confianza incluso tras haber vivido una situación de fraude.

Esta confianza sin duda está relacionada con el hecho de que la mayoría de usuarios no modifican el uso que hacen de estos servicios. Sin embargo, al tener en cuenta la evolución con respecto a años anteriores, resulta positivo el hecho de que cada vez son menos los que muestran una actitud pasiva y más los que adoptan opciones diferentes al abandono de servicios de banca online o comercio electrónico.

5 RECOMENDACIONES

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

- Utilizar cuentas de usuario con permisos limitados.
- Utilizar contraseñas seguras y no utilizar la misma en diferentes sitos.
- No enviar información personal o financiera a través del correo electrónico.
- Ser consciente de que los bancos o entidades financieras nunca piden los datos personales por correo electrónico.
- Cerciorarse de que se está utilizando un protocolo seguro (la URL debe comenzar por https en lugar de por http) siempre que se introduzcan los datos bancarios en una página web. En este sentido, disponer del navegador de Internet actualizado permite tener los protocolos de seguridad en regla.
- Mantener el equipo actualizado con los últimos parches de seguridad instalados.
- Guardar o imprimir la información cuando se realiza una operación económica a través de la Red.
- Controlar la privacidad de los perfiles en las redes sociales, teniendo conocimiento de qué tipo de información pueden obtener de mí otras personas.
- Usar programas de seguridad en los equipos en los que se realicen operaciones a través de Internet.
- Disponer de los programas de seguridad actualizados en todo momento.
- Evitar conectarse a redes inalámbricas sin ningún tipo de seguridad, y extremar la precaución a la hora de conectarse a una red pública, ya que puede existir cualquier persona conectada capturando las conexiones que pasan por ella.
- Tener precaución a la hora de descargar o abrir archivos adjuntos.
- Descargar software sólo desde sitios de confianza o desde las webs oficiales de los fabricantes.
- Mantenerse informado sobre cuestiones de seguridad informática, conocer los riesgos y las principales amenazas de las que protegerse.

La colaboración de los usuarios a la hora de evidenciar un intento de fraude es primordial para poder interceptarlos a tiempo y poder localizar lugares desde donde se publican páginas, se emiten mensajes fraudulentos o donde se reciben los datos capturados.

Para facilitar esta colaboración, la Oficina Seguridad del Internauta (OSI) pone a disposición del usuario el formulario de alta de incidentes, desde donde se puede indicar las entidades afectadas y toda la información disponible sobre el caso de fraude, y el teléfono de asistencia 901 111 121.

Por último, en caso de haber sido víctima de un fraude, es conveniente poner inmediatamente la denuncia correspondiente, para lo que el usuario puede ponerse en contacto con:

- El Cuerpo Nacional de Policía, a través de la Comisaría General de la Policía Judicial, dispone de la Brigada de Investigación Tecnológica (BIT) para combatir la delincuencia que utiliza los medios que proporcionan las nuevas Tecnologías de la Información y se puede contactar con ella a través del correo electrónico Buzón de delitos tecnológicos de la policía: delitos.tecnologicos@policia.es. La presentación de la denuncia se puede realizar a través del teléfono: 902 102 112, página web o en cualquier comisaría. Disponen de un formulario específico para la notificación de posibles fraudes.

- La Guardia Civil cuenta con el Grupo de Delitos Telemáticos (GDT) de la Unidad Central Operativa (UCO), con el que se puede contactar a través de la sección colabora de su página web o del correo electrónico: delitostelematicos@guardiacivil.org.

ÍNDICE DE GRÁFICOS

ÍNDICE DE TABLAS

Síguenos a través de:

Web

Envíanos tus consultas y comentarios a:

observatorio@inteco.es

Instituto Nacional
de Tecnologías
de la Comunicación