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

1er cuatrimestre de 2012 (9ª oleada)

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

Edición: Diciembre 2012

El informe de la 9ª oleada del "Estudio sobre el fraude a través de Internet (1er cuatrimestre de 2012)" 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

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 novena entrega del *Estudio sobre el fraude a través de Internet*. La metodología utilizada para la realización del informe incluye entrevistas a usuarios de Internet y análisis online de equipos de hogares españoles. El período analizado en este documento abarca el 1er cuatrimestre de 2012, esto es, los meses de enero a abril.

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

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

El período analizado en este documento abarca los meses de enero a abril de 2012.

Se exponen a continuación los puntos clave del análisis.

I INTENTO DE FRAUDE Y MANIFESTACIONES

En el primer cuatrimestre de 2012 se produce un descenso en la incidencia de situaciones que pueden suponer fraude, lo que supone un cambio de tendencia con respecto a 2011.

- A comienzos de 2012, un 52,9% de los internautas afirma haber sido objeto de un intento de fraude a través de Internet (no necesariamente consumado). Desciende por tanto la proporción de usuarios que han recibido correos con supuestos fraudes con respecto a oleadas anteriores.

- Los intentos de fraude online que se producen más frecuentemente son los correos electrónicos con enlaces a páginas web sospechosas (37,4%), o que ofertan servicios no solicitados (30,8%). Al igual que en el punto anterior, en el último año se observa una tendencia descendiente en los valores.

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

Los atacantes tratan de engañar a los usuarios enviando correos en nombre de supuestas entidades, principalmente bancos online y páginas de comercio electrónico. Las técnicas se modifican y perfeccionan constantemente, lo que puede explicar el incremento de la fórmula de remitente "otros" en 2012.

- Con mayor frecuencia, las candidatas a ser suplantadas por los ciberestafadores son las entidades de banca online (41,2%) y comercio electrónico (38,6%). Es destacable igualmente la utilización de fórmulas como supuestas páginas de loterías (30,2%), particulares (28,3%) o redes sociales (26,4%).

- Comparando el último periodo de 2011 con el primero de 2012, se observan en general valores muy similares. Sin embargo, la fórmula "otros" es cada vez más utilizada, en contraposición a "usuarios particulares", que desciende a comienzos de 2012.

III IMPACTO ECONÓMICO DEL FRAUDE

Sólo una pequeña proporción de los usuarios de Internet sufre una pérdida económica a consecuencia del fraude. Por primera vez, este dato se sitúa por debajo del 3%

- Un 2,5% de los encuestados afirma que el intento de fraude se consumó, provocándole un perjuicio económico. Por primera vez, el fraude cae por debajo de la barrera del 3%.

- En 7 de cada 10 ocasiones, el fraude no supera los 100€. Sin embargo, en el último periodo los fraudes superiores a 400 € han crecido de un 6,7% a un 17,2%.

IV FRAUDE Y MALWARE

El nivel de infección por malware orientado a la comisión de fraude se mantiene bastante estable. Sin embargo, nuevas familias de malware como el denominado "virus de la policía" pueden ser la causa del repunte del malware en enero de 2012.

- En abril de 2012, un 38,3% de los ordenadores de los hogares españoles aloja algún tipo de troyano, un 4,4% está infectado por troyanos bancarios y un 4%, por rogueware.

- La evolución en los valores es bastante constante salvo por ligeros repuntes, como el experimentado en enero de 2012. Entre las posibles causas de este incremento está el elevado número de infecciones provocadas por nuevas familias de malware, como el llamado "virus de la policía".

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

El comercio electrónico y la banca online son servicios cada vez más imprescindibles para los ciudadanos, quienes depositan su confianza en estos servicios, aún cuando experimentan alguna situación de fraude online.

- En general, se aprecia una notable adopción de comportamientos que pueden evitar futuros fraudes online (por encima del 70% en la mayoría de los casos), tanto si el usuario ha sufrido una pérdida derivada del fraude online y como si no la ha tenido.

- Existe un buen nivel de confianza en la realización de compras y operaciones bancarias online, destacando que aquellos usuarios que han sido víctimas de fraude online dicen confiar más que los que no lo han sido.

- En general, los usuarios de banca y comercio en línea que experimentan fraude online no abandonan estos servicios. La modificación de hábitos es incluso inferior a comienzos de 2012 que la observada a finales de 2011. Un perfil de usuario intensivo explicaría esta conducta de fidelidad.

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 9ª entrega del mismo.

En esta ocasión, se presenta la actualización para el 1er cuatrimestre de 2012 de los datos de usuarios basados en entrevistas comparando estos resultados con los obtenidos en el 2º y 3er cuatrimestres de 2011 y, de esta manera, poder ofrecer un análisis evolutivo de los últimos doce meses.

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 novena entrega del estudio.

En la actualidad el panel está compuesto por 3.646 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 entrevistas 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 (1er cuatrimestre de 2012), 3.646 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 primer cuatrimestre de 2012 se compone de 2.643 hogares que escanearon online su ordenador entre enero y abril de 2012. El número total de análisis remotos en el período ha sido de 7.723.

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 3.646 usuarios de Internet, con participación estable en el panel en el cuatrimestre comprendido entre enero y abril de 2012.

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

Año 2007	Equipos	Año 2008	Equipos	Año 2009	Equipos
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
7Jul'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	Oct'09	4.294
Nov'07	3.959	Nov'08	3.661	Nov'09	4.039
Dic'07	3.376	Dic'08	4.286	Dic'09	4.452

Año 2010	Equipos	Año 2011	Equipos	Año 2012	Equipos
Ene'10	4.079	Ene'11	*n.d.*	Ene'12	1.606
Feb'10	3.751	Feb'11	*n.d.*	Feb'12	1.948
Mar'10	4.024	Mar'11	*n.d.*	Mar'12	2.102
Abr'10	3.746	Abr'11	*n.d.*	Abr'12	2.067
May'10	3.499	May'11	*n.d.*		
Jun'10	3.279	Jun'11	2.379		
Jul'10	3.337	Jul'11	2.891		
Ago'10	2.716	Ago'11	2.595		
Sep'10	2.783	Sep'11	1.389		
Oct'10	3.232	Oct'11	1.288		
Nov'10	2.742	Nov'11	1.610		
Dic'10	2.604	Dic'11	2.096		

Fuente: INTECO

Tabla 2: Tamaños muestrales para las encuestas

Período	Tamaño muestral
1er trimestre 2009	3.563
2º trimestre 2009	3.521
3er trimestre 2009	3.540
4º trimestre 2009	3.640
1er trimestre 2010	3.599
2º trimestre 2010	3.519
3er trimestre 2010	3.538
4º trimestre 2010	3.571
2º cuatrimestre 2011	2.405
3er cuatrimestre 2011	3.655
1er cuatrimestre 2012	3.646

Fuente: INTECO

2.3 CAPTURA DE INFORMACIÓN Y TRABAJO DE CAMPO

El trabajo de campo ha sido realizado entre enero y abril de 2012 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 40 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, es decir, que catalogan un alto número de archivos no maliciosos como malware.*

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*

[1] Software y ficheros legítimos, archivos inocuos.

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.

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

En primer lugar se elimina toda detección de la familia "Annihilator" porque se trata del nombre que emplean algunos antivirus para detectar (erróneamente) los ficheros legítimos de 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.

[2] Software gratuito.

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

Todos estos filtros son mejoras importantes de cara a la fiabilidad de los datos, pero no eliminan por completo la problemática de los falsos positivos (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 de este análisis, los datos que el informe ofrece cuentan con un margen de error que da una perspectiva de los problemas actuales a los que se enfrenta la industria de seguridad a la hora de desarrollar sus programas antivirus.

2.4 ERROR MUESTRAL

De acuerdo con los criterios del muestreo aleatorio simple para variables dicotómicas en las que p=q=0,5 y para un nivel de confianza del 95,5%, se establece un error muestral inferior a ±1,62% en cada uno de los períodos analizados, tal y como se recoge en la siguiente tabla.

Tabla 3: Errores muestrales de las encuestas (%)

Período	Tamaño muestral	Error muestral
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%
1er cuatrimestre 2012	3.646	±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.

- Desde el 3er cuatrimestre de 2011, 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].

A comienzos de 2012, un 52,3% de los usuarios de Internet afirma haber sufrido una situación de fraude a través de Internet (aunque no necesariamente tienen que consumarse). Este dato supone un descenso del fraude con respecto a los datos de 2011.

[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

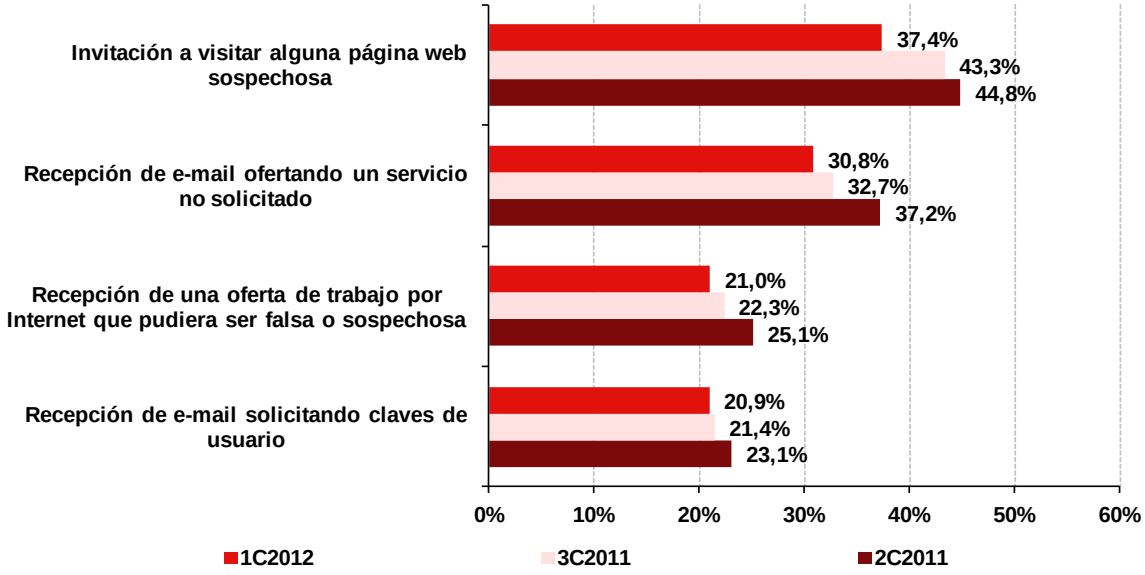
Gráfico 1: Incidencia declarada de situaciones de intento de fraude a través de Internet en los últimos 3 meses (%)

Base: Total usuarios (n=3.646 en 1er cuatrimestre 2012) *Fuente: INTECO*

En opinión de los encuestados, las situaciones de intento de fraude más frecuentes son la recepción de correos electrónicos invitando a visitar páginas web sospechosas (37,4%) o promocionando servicios no solicitados (30,8%). Les siguen la recepción de supuestas ofertas de trabajo (21,0%) y solicitudes de claves personales (20,9%) a través de email.

En todas las situaciones analizadas, los valores muestran un progresivo descenso desde el 2º cuatrimestre de 2011, sobre todo en las más frecuentes, tanto en el caso de los enlaces a web sospechosas (7,4 puntos porcentuales menos) como en el de los correos electrónicos ofertando servicios no solicitados (6,4 puntos).

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=3.646 en 1er cuatrimestre 2012) *Fuente: INTECO*

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

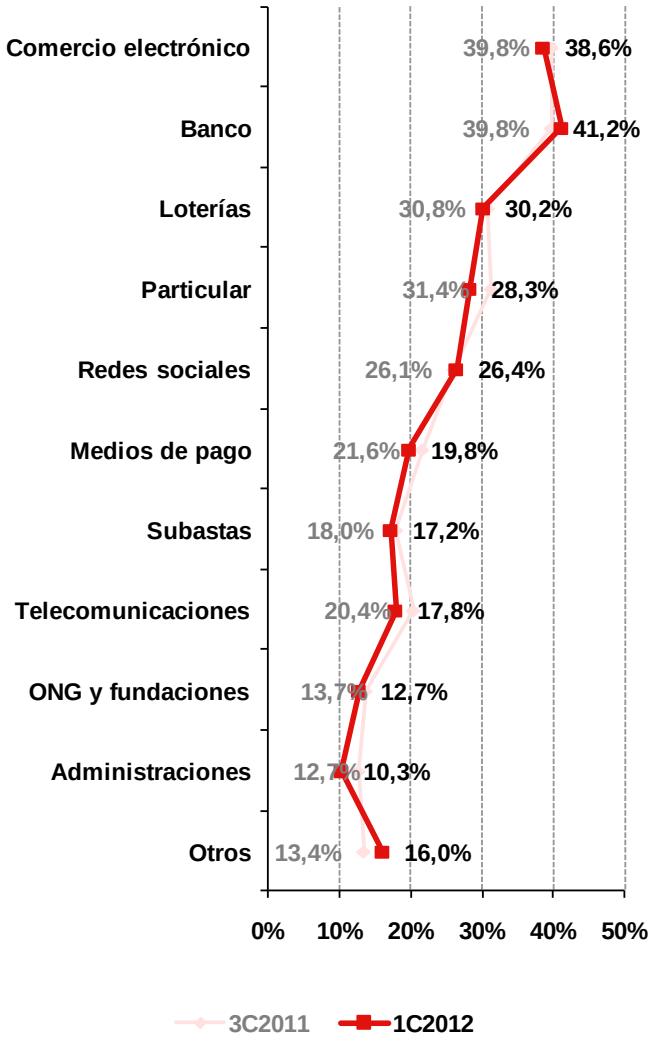
Para llevar a cabo el fraude online, los atacantes envían comunicaciones que simulan provenir de supuestas entidades oficiales. En el Gráfico 3 se comparan los datos del los dos últimos periodos estudiados, esto es, los cuatro últimos meses de 2011 frente a los cuatro primeros de 2012.

Con mayor frecuencia, las candidatas a ser suplantadas son las entidades de banca online (declarada por un 41,2% de los usuarios) y comercio electrónico (38,6%), destacando asimismo otras opciones, como las páginas de loterías, los particulares o las redes sociales (30,2%, 28,3% y 26,4%, respectivamente).

Con respecto a finales de 2011, la tendencia general muestra valores muy similares o leves descensos en las diferentes categorías. Sobre todo, se han declarado menos intentos provenientes particulares (3,1 puntos porcentuales menos) y de supuestos operadores de telecomunicaciones (2,6 puntos) y administraciones (2,4 puntos).

Los únicos incrementos se han producido en el caso de las entidades bancarias en línea (que asciende 1,4 puntos porcentuales), las redes sociales (0,3 puntos) y la fórmula “otros” (2,6 puntos).

Gráfico 3: Evolución de las formas adoptadas por el remitente de la comunicación sospechosa de ser fraudulenta[5] (%)



Base: Usuarios que han sufrido algún intento de fraude (n=1.929 en 1er cuatrimestre 2012) Fuente: INTECO

Complementando el análisis anterior, el tipo de situación de fraude experimentada guarda relación con el remitente utilizado por el atacante para enviar la comunicación. La banca online y el comercio electrónico siguen siendo fórmulas frecuentes, aunque se pueden observar particularidades en función del tipo de mensaje.

[5] 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, 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.

De esta forma, los correos que solicitan claves al destinatario suelen estar encabezados por supuestos bancos online, como afirma un 69,6% de estos usuarios, seguidos de webs de comercio en línea (21,2%) y medios de pago (21%).

Entre los usuarios que han recibido mensajes electrónicos que ofertan servicios no solicitados, un 41,3% identifica a las entidades de comercio electrónico como remitentes, seguidas de las loterías (28,2%).

Las mismas fórmulas empleadas en el caso anterior son las más frecuentes en el envío de comunicaciones que invitan a visitar páginas web sospechosas (30% en el caso de supuestas empresas de comercio electrónico y 28,2% en el de loterías).

Por último, en opinión de los encuestados, los particulares suelen estar detrás de las falsas ofertas de trabajo (36,1%), aunque también se utilizan otras fórmulas (20,6%).

Tabla 4: Formas adoptadas por el remitente según el tipo de comunicación sospechosa que ha experimentado el internauta[6] (%)

Tipo de incidencia declarada	Forma adoptada por el remitente de la comunicación										
	Banco	Comercio electrónico	Loterías	Particular	Redes sociales	Medios de pago	Subastas	Telecomunicaciones	ONG y fundaciones	Administraciones	Otros
Recepción de e-mail solicitando claves de usuario	**69,6**	21,2	13,9	9,0	14,3	21,0	7,9	10,3	6,5	7,0	5,0
Recepción de e-mail ofertando un servicio no solicitado	25,9	**41,3**	28,2	14,5	19,7	14,0	14,2	16,3	8,1	5,7	8,0
Recepción de e-mail con invitación a visitar alguna página web sospechosa	25,6	**30,0**	28,2	23,4	19,9	13,1	15,6	12,0	8,3	5,6	10,5
Recepción de una oferta de trabajo por Internet que pudiera ser falsa o sospechosa	9,0	13,7	8,6	**36,1**	16,5	7,7	6,4	8,4	10,0	10,0	20,6

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

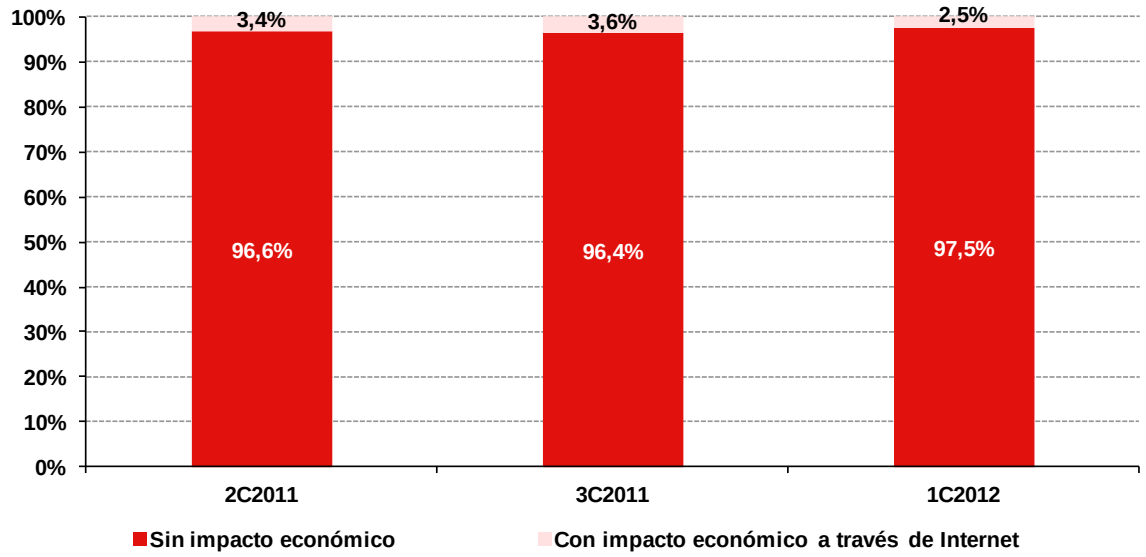
[6] Ver nota a pie número 3

3.3 IMPACTO ECONÓMICO DEL FRAUDE

Cuando el fraude llega a consumarse, en ocasiones se produce un perjuicio económico para la víctima. Por ello, en el siguiente epígrafe se contempla el daño objetivo del fraude a través de Internet y la distribución del importe defraudado.

En primer lugar, se observa en el siguiente gráfico cómo el fraude con impacto económico representa un pequeño porcentaje: un 2,5% del total de usuarios de Internet. Este porcentaje supone un dato positivo con respecto a los datos de 2011: por primera vez el fraude se sitúa por debajo de la barrera del 3%, experimentando una caída de 1,1 punto porcentual desde el periodo anterior.

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

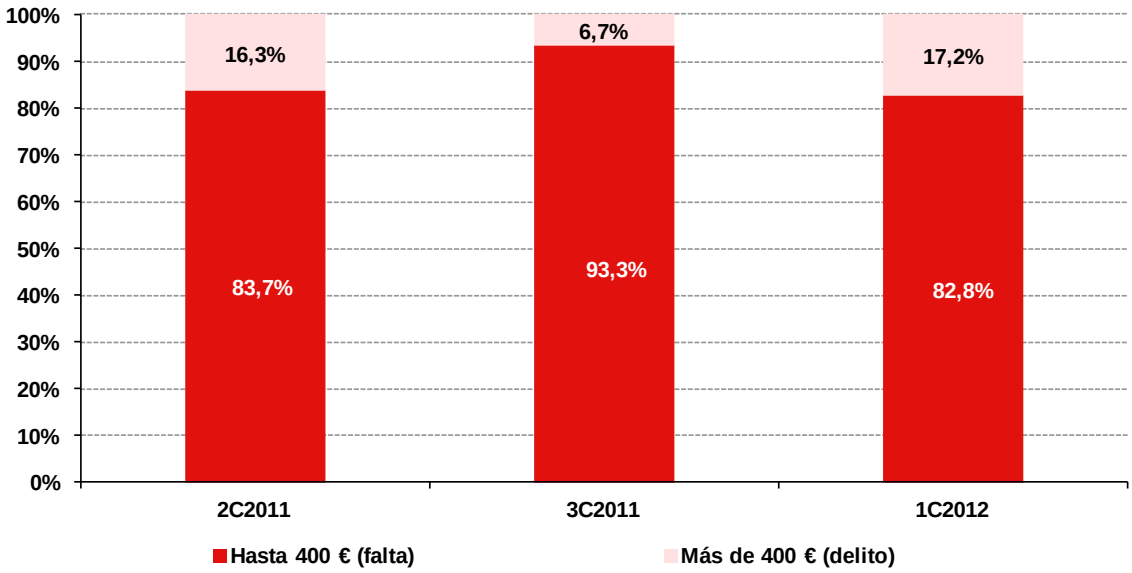


Base: Total usuarios (n=3.646 en 1er cuatrimestre 2012) *Fuente: INTECO*

En segundo lugar, se estudia la distribución de los importes defraudados. Así, el Gráfico 5 compara las cuantías sustraídas en los últimos cuatrimestres, diferenciando entre aquellas iguales o inferiores a 400 € y las superiores a esta cantidad. Según el Código Penal español, se establece hasta en 400 € la cuantía del fraude considerado como falta. Todas aquellas estafas superiores a 400 € reciben el tratamiento de delito.

En el primer cuatrimestre de 2012, un 17,2% de los usuarios declaran que el fraude experimentado es superior a 400€, frente a un 82,8% que considera este importe inferior. Tras un periodo anterior atípico, en el que los fraudes de pequeña cuantía ascendieron hasta el 93,3%, de nuevo se recuperan valores similares al 2º cuatrimestre de 2011 y los fraudes considerados como faltas se sitúan en torno al 80%. Es importante tener en cuenta que el número absoluto de encuestados no es elevado, por lo hay que tomar estos datos con cierta cautela.

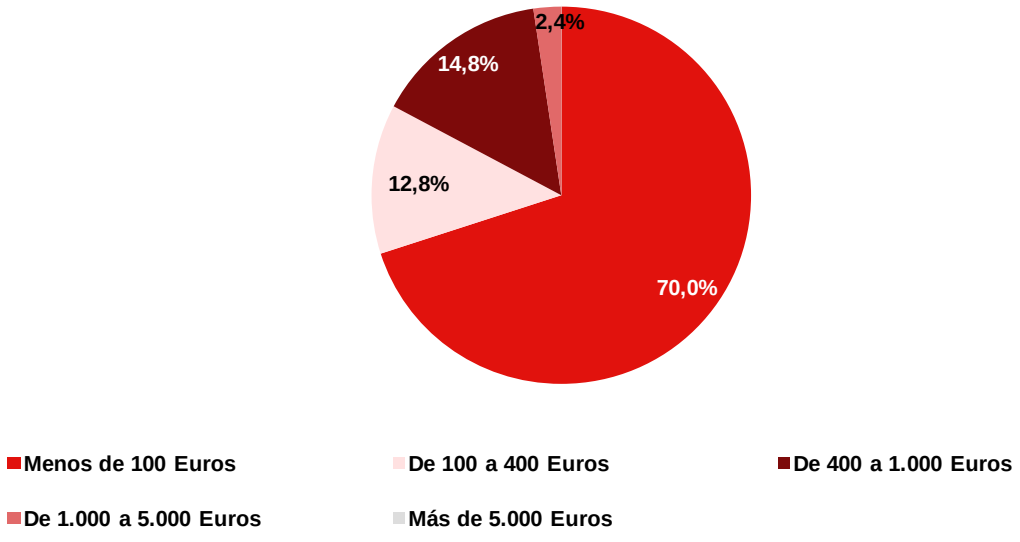
Gráfico 5: Evolución de la cuantía económica derivada del fraude (%)



Base: Usuarios que han sufrido perjuicio económico como consecuencia de un fraude a través de Internet (n=90 en 1er cuatrimestre 2012) *Fuente: INTECO*

En último lugar, una distribución pormenorizada de las cuantías defraudadas indica que para siete de cada diez usuarios las incidencias de fraude implicaron una pérdida económica inferior a los 100 €.

Gráfico 6: Distribución del importe defraudado (%)



Base: Usuarios que han sufrido perjuicio económico como consecuencia de un fraude a través de Internet (n=90 en 1er cuatrimestre 2012) *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.

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

   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, carberb y murofet.

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 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 una correcta interpretación de 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.

Se presenta en el siguiente gráfico la evolución, a lo largo de los doce meses desde mayo de 2011 hasta abril de 2012, del porcentaje de equipos en los que iScan reportó la presencia de algún tipo de troyano. Con el objetivo de presentar un gráfico más orientado al fraude online, se diferencian las variantes de troyanos bancarios y rogueware, otras de las principales fuentes de fraudes online.

En el caso de los troyanos genéricos, la evolución muestra una tendencia bastante estable, aunque con ligeras fluctuaciones, como la experimentada a comienzos de 2012, cuando este valor se sitúa en el punto más alto de la serie (41,8%). En los meses posteriores, la proporción de equipos que alojan troyanos se sitúa de nuevo en valores en torno al 38%.

El repunte en enero puede tener su explicación en el elevado número de infecciones causadas por el ransomware llamado comúnmente "virus de la policía"[7], sin nombre concreto por parte de las casas antivirus y detectado como troyano (o incluso no detectado) por buena parte de las casas antivirus. Desde finales de 2011, esta familia de malware ha infectado millones de sistemas en Europa, centrándose especialmente en Alemania y España. Usando el nombre de la Policía Nacional, extorsionaba al infectado para desbloquear su sistema.

Por su parte, el nivel de troyanos bancarios experimenta leves descensos en los cuatro primeros meses de 2012 hasta situarse en un 4,4% en abril de 2012, lejos del 7,1%, alcanzado en mayo de año pasado.

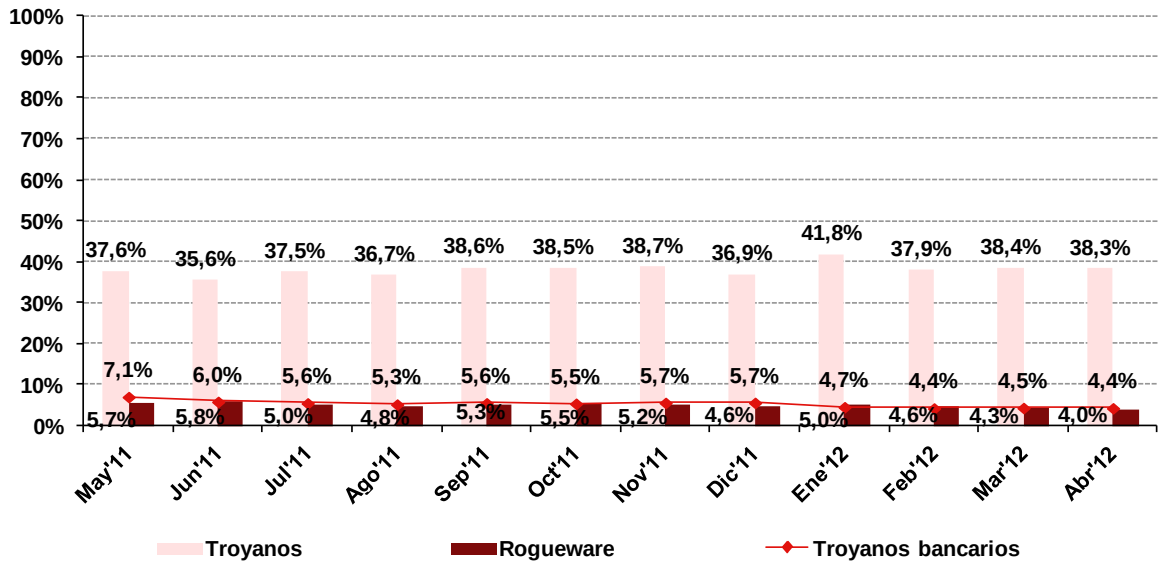
Es importante destacar que al clasificar un troyano bancario, debido a la dificultad técnica actual de esta tarea, puede darse el caso de que un motor antivirus lo clasifique como troyano genérico. Cualquier troyano, aun no estando destinado a propósitos fraudulentos, puede dar lugar a situaciones de fraude gracias a la versatilidad de la que últimamente están dotados.

Por último, el rogueware también experimenta un repunte en enero de 2012 (de un 4,6% en diciembre de 2011 a un 5%), para caer progresivamente hasta el 4% en abril de 2012

[7] Fuente "Crónica del virus de la policía", disponible en http://www.inteco.es/blogs/post/Seguridad/BlogSeguridad/Articulo_y_comentarios/Post_viruspolicia

en el. Desde mayo de 2011, la evolución muestra un lento pero progresivo descenso del rogueware.

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



Fuente: INTECO

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

¿Haber sufrido un perjuicio implica un cambio de comportamiento en la utilización de la banca online o en las compras en Internet?

El Gráfico 8 trata de responder a esta cuestión al analizar los hábitos prudentes de los usuarios de banca en línea y comercio electrónico, distinguiendo entre los que han sufrido un perjuicio económico a consecuencia del fraude vivido y los que no.

En general, se aprecia una notable adopción de comportamientos que pueden evitar el fraude, tanto si el encuestado ha tenido una pérdida económica como si no ha experimentado dicha circunstancia. La mayoría de hábitos presentan tasas de adopción superiores al 70%, sin grandes diferencias entre los dos tipos de usuarios analizados. Así, es frecuente cerrar la sesión al terminar (puesto en práctica por un 89,3% de los usuarios con pérdida económica y un 81,7% de los que no), buscar intimidad a la hora de conectarse (87,9% y 80,3%, respectivamente) o vigilar los movimientos de la cuenta (85,3% y 81,1%, respectivamente).

.

Por el contrario, haber sufrido un perjuicio es determinante a la hora de no suministrar datos por correo electrónico o por teléfono, puesto que es declarado por un 78% de estos frente a un 42,7% de los que no han tenido una pérdida. La misma relación se observa al evitar el uso de equipos públicos o compartidos (adoptada por un 87% de los primeros y un 69,7% de los segundos).

Finalmente, la pérdida económica no siempre se traduce en mayor prudencia: los usuarios que no han sufrido fraude destacan el en uso de tarjetas prepago (un 62,8% frente a un 49%).

Gráfico 8: 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=3.072 en 1er cuatrimestre 2012) *Fuente: INTECO*

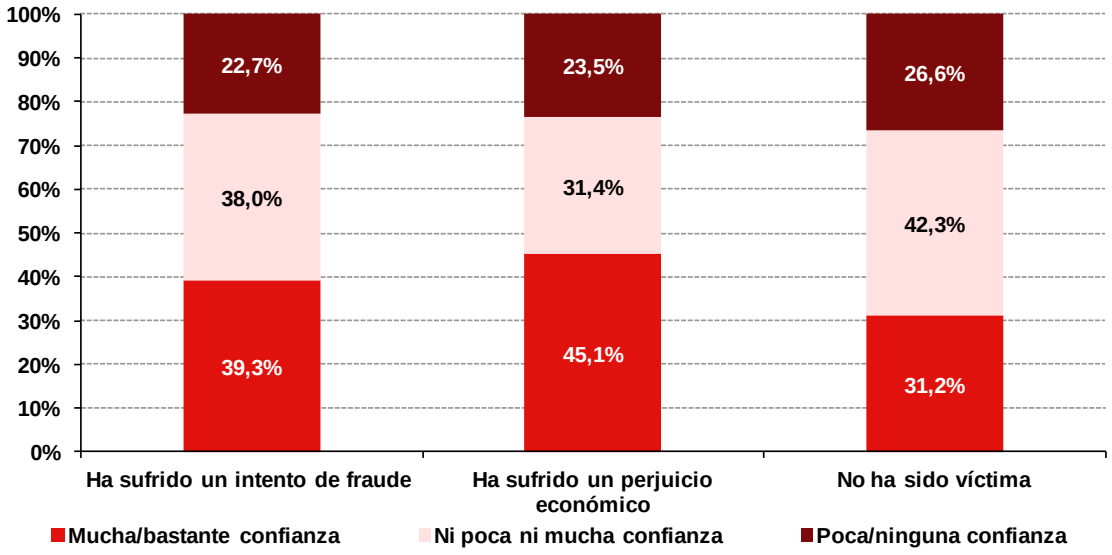
3.5.2 Nivel de confianza tras sufrir un intento de fraude y/o perjuicio económico

Después de estudiar los hábitos prudentes, ¿es también similar el grado de confianza en la compra y banca online de los usuarios que han experimentado una situación de fraude de los que no?

Tanto si se ha vivido un intento de fraude (no necesariamente consumado), como si este ha derivado en una pérdida económica, el nivel de confianza en las compras y

transacciones online es ligeramente superior al de aquellos que no han visto este impacto. Así, un 45,1% de los usuarios que han sufrido perjuicio económico y un 39,3% de los que han vivido un intento (no consumado) de fraude dicen confiar mucho o bastante en las compras a través de Internet, porcentaje inferior en el caso de los que no han sido víctimas (31,2%).

Gráfico 9: 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 (%)

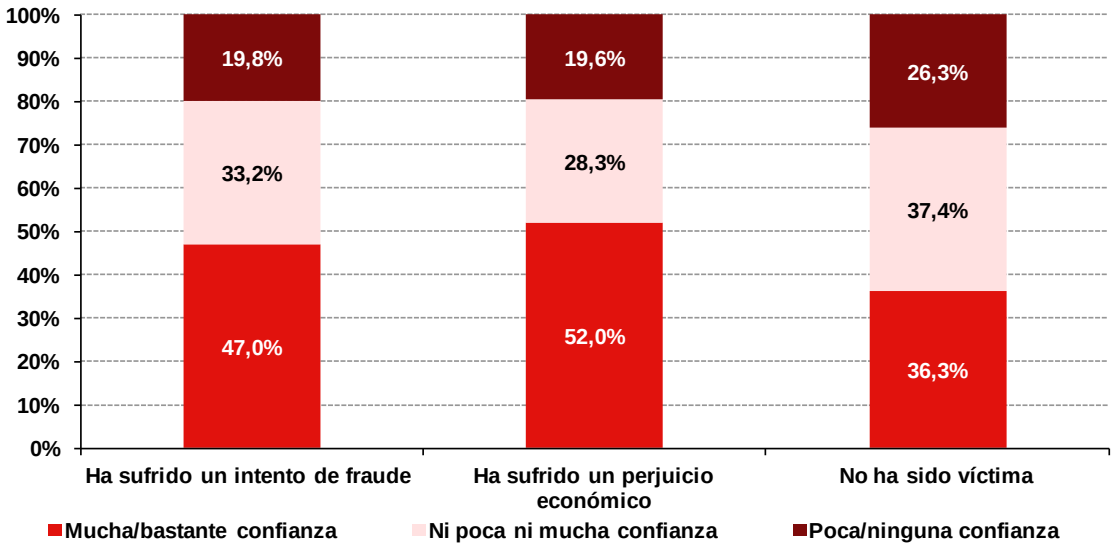


Base: Total usuarios (n=3.646 en 1er cuatrimestre 2012) *Fuente: INTECO*

Una situación similar se observa en el caso de las operaciones bancarias a través de Internet: existe un buen nivel de confianza en estos servicios, si bien aquellos que han sido víctimas de fraude muestran una cierta ventaja (un 52% de los internautas que declaran pérdida económica y un 47% de los que han tenido un intento de fraude confían mucho o bastante en la banca online) frente a los que no (36,3%).

Tanto en el caso de la compra online como en el de la banca, una posible explicación estaría en el perfil de los usuarios: son navegantes más “intensivos” y por tanto usan más estos servicios, sufren más intentos de fraude y confían más.

Gráfico 10: Nivel de confianza en las operaciones bancarias en Internet entre los usuarios que han sufrido intento de fraude y/o perjuicio económico y los que no (%)



Base: Total usuarios (n=3.646 en 1er cuatrimestre 2012) *Fuente: INTECO*

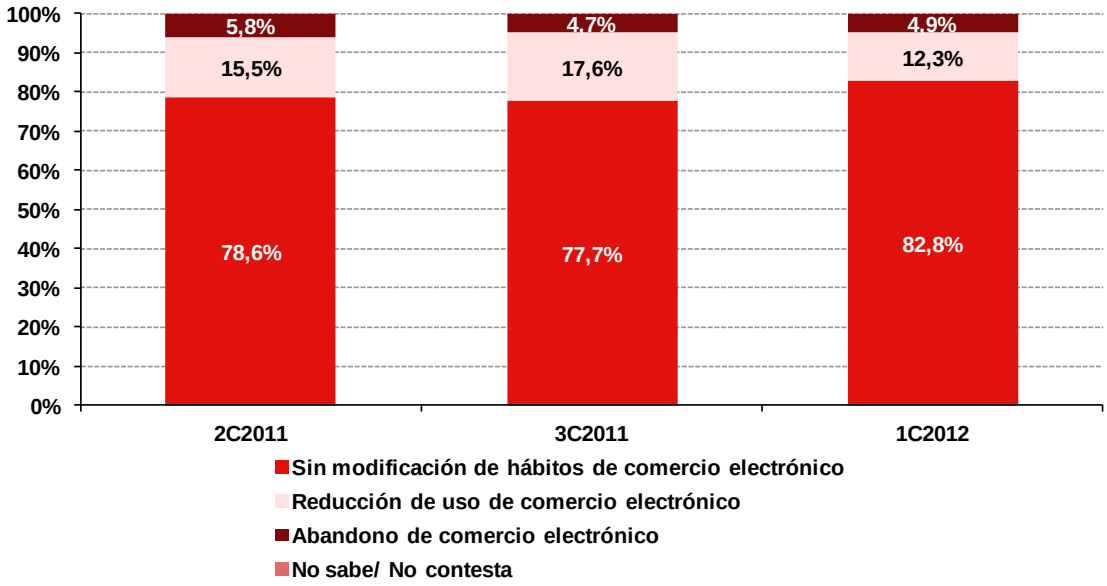
3.5.3 Modificación de hábitos de comercio electrónico y banca online tras sufrir un intento de fraude

En último lugar, el informe trata de comprobar si el hecho de experimentar una circunstancia de fraude o una pérdida a consecuencia del mismo provoca una reacción en el usuario de comercio electrónico y banca en línea, que influye en futuros usos.

Comenzando por el comercio electrónico, en el primer cuatrimestre de 2012 la mayoría de los ciudadanos sigue utilizando estos servicios a pesar de haber sufrido una situación de fraude (82,8%), mientras que un 12,3% reduce su uso y un 4,9% abandona estos servicios.

Se produce así un aumento en la proporción de usuarios que no adoptan ninguna reacción con respecto a oleadas anteriores (4,2 puntos porcentuales desde el segundo cuatrimestre de 2011).

Gráfico 11: Evolución de la modificación de los hábitos de comercio electrónico tras sufrir intento (no consumado) de fraude y/o perjuicio económico (%)

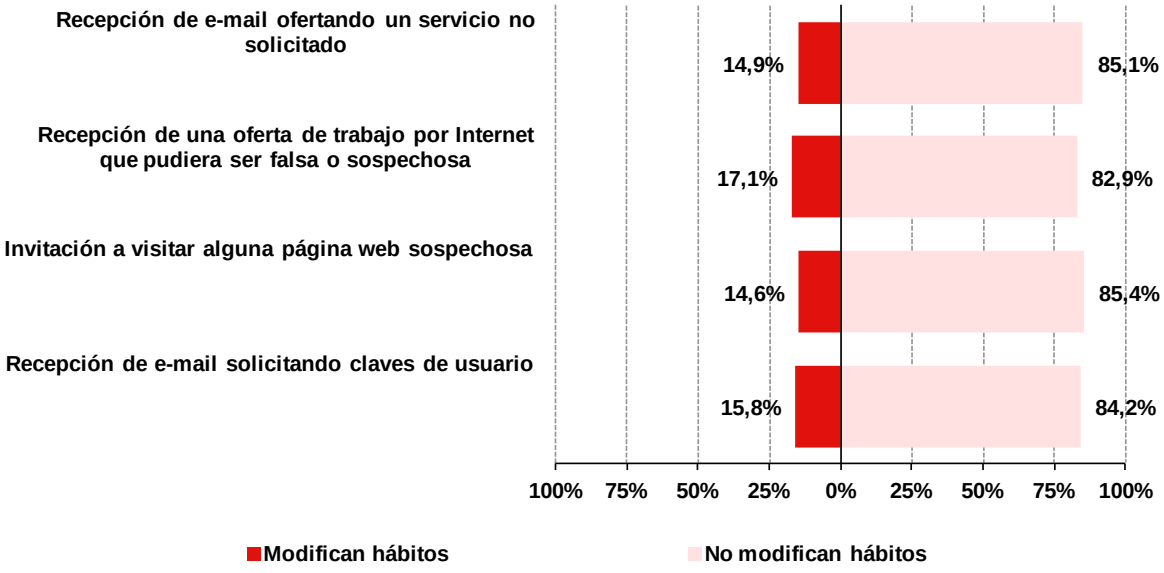


Base: Usuarios de comercio electrónico que han sufrido algún intento de fraude online y/o un perjuicio económico (n=1.171 en 1er cuatrimestre 2012) *Fuente: INTECO*

Teniendo en cuenta el tipo de incidencia de fraude sufrida, se observa que las respuestas se toman en mayor medida tras recibir una oferta de trabajo falsa por Internet (un 17,1%).

Una posible explicación puede estar en el hecho de que el uso de este tipo de esquema de fraude a través de la Red es muy común desde hace tiempo, y favorece a que gran parte de los internautas haya tomado conciencia de ellos así como de las medidas oportunas para evitarlos.

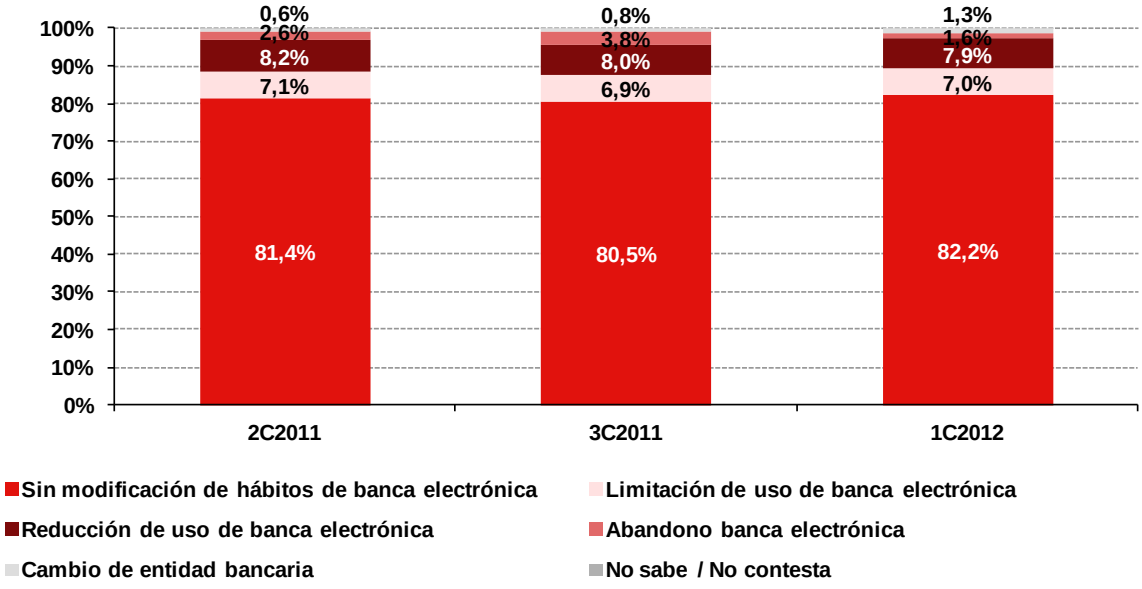
Gráfico 12: Modificación de hábitos del comercio electrónico con respecto al tipo de incidencia de fraude sufrida en los últimos 3 meses (%)



Fuente: INTECO

En el caso de la banca online, también los usuarios muestran una gran fidelidad a pesar de ser víctimas de fraude online: un 82,2% no abandona el uso, mientras que un 7% lo limita y un 7,9% lo reduce. La tendencia en los últimos 3 cuatrimestres es constante.

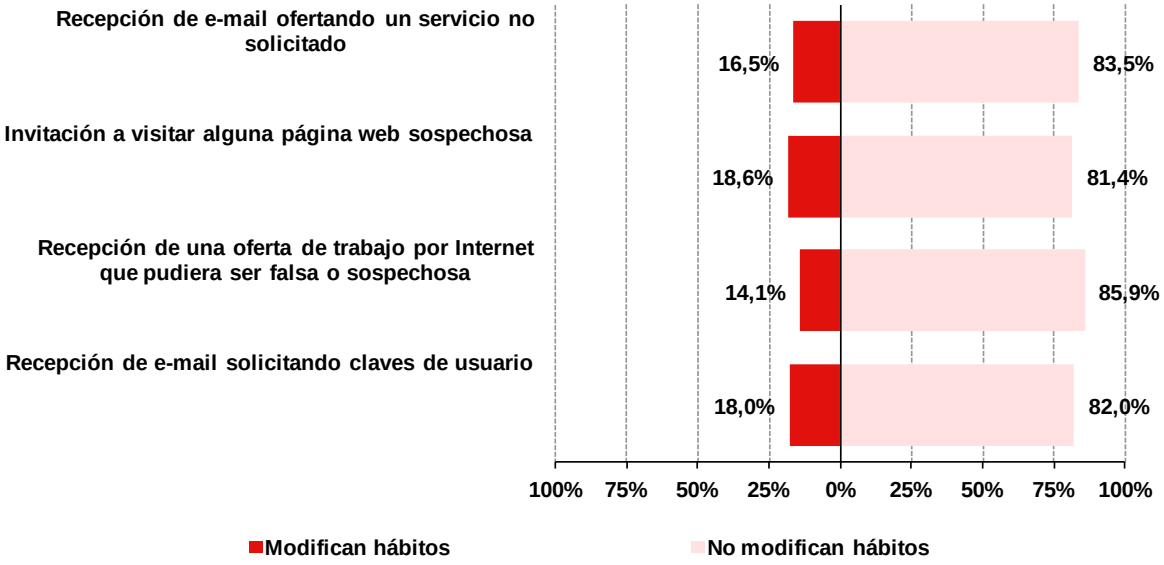
Gráfico 13: Evolución de la modificación de los hábitos de banca online tras sufrir intento (no consumado) de fraude y/o perjuicio económico (%)



Base: Usuarios de banca online que han sufrido algún intento de fraude online y/o un perjuicio económico (n=1.585 en 1er cuatrimestre 2012) *Fuente: INTECO*

En este caso, las reacciones se adoptan en mayor medida tras recibir un email invitando a visitar una página web sospechosa de ser falsa (18,6%), así como en las comunicaciones que piden credenciales bancarias (18%).

Gráfico 14: Modificación de hábitos de banca online con respecto al tipo de incidencia de fraude sufrida en los últimos 3 meses (%)



Fuente: INTECO

4 CONCLUSIONES

El año 2012 comienza con un descenso en el porcentaje de usuarios que ha experimentado en los últimos meses alguna situación que podría suponer fraude. Así, en la presente oleada un 47,1% afirma que no ha sufrido ningún problema relacionado con el fraude.

Este descenso puede estar fundamentado en los siguientes factores:

- Los usuarios han tomado las medidas de precaución adecuadas para evitar que las situaciones de fraude generen un impacto en su economía.

- Los atacantes no han innovado en sus campañas de fraude, o no han sido suficientemente insistentes o eficaces en su actividad fraudulenta.

Analicemos qué factores han podido pesar más sobre el descenso experimentado.

Medidas de protección y prevención frente al fraude online adoptadas por los internautas españoles

Existen una serie de hábitos prudentes que ayudan a prevenir que los intentos de fraude que recibe el usuario se consumen y puedan provocar un perjuicio económico. Como atestigua el informe[8], los internautas se muestran en general prudentes, aún después de haber sufrido una merma en su economía a causa de un fraude online. Sin embargo, destaca que aquellos usuarios que no han sufrido un perjuicio económico adoptan en mayor medida dos hábitos concretos:

- Evitar el uso de lugares públicos para operar en Internet. Los sistemas públicos pueden estar infectados por malware, al ser sistemas no controlados por el usuario. Esto los convierte en focos de malware y no deben usarse para operar con datos sensibles.

- Evitar facilitar datos y contraseñas por canales inseguros. Se consideran canales inseguros todos aquellos que no garanticen que los datos son enviados por canales cifrados y que no pertenecen realmente al destinatario. Esto incluye chats, mensajería instantánea, correo no cifrado, etc.

A la vista del informe, es notable la concienciación de los usuarios en la prevención del fraude online. Junto con estos hábitos, cada vez es más importante conocer y mantenerse informado sobre los nuevos tipos de ataque perpetrados por los estafadores y las campañas de fraude puestas en marcha en cada momento. Por ejemplo, durante

[8] Ver Apartado 3.5.1 *Hábitos prudentes relacionados con el comercio electrónico y la banca en línea.*

este primer cuatrimestre de 2012, se han sufrido dos fuertes campañas de intento de fraude.

- La campaña lanzada en febrero[9] basada en la imagen de la Agencia Tributaria. El mensaje fraudulento alegaba que "después de los cálculos anuales pasados de su actividad fiscal hemos determinado que usted es elegible para recibir un reembolso de impuestos de 223,56 euros", bajo el logotipo del Ministerio de Hacienda y Administraciones Públicas. Si la víctima visitaba el enlace, era conducido a una supuesta web donde se instaba a que proporcionara los datos bancarios. Este mensaje tuvo una alta difusión durante los meses de febrero a abril de 2012.

- El ransomware llamado comúnmente "virus de la policía"[10], sin nombre concreto por parte de las casas antivirus, consiguió unos niveles de infección muy altos durante los primeros meses del año. Centrándose especialmente en Alemania y España, ha usando el nombre de la Policía Nacional, extorsionando al infectado para desbloquear su sistema. Aunque no se ha reflejado en los indicadores de malware de este mismo estudio a causa de la difusa clasificación por parte de las casas antivirus, este malware ha podido influir en la percepción de intento de fraude a los usuarios por parte de la administración pública, si las víctimas han creído real el mensaje fraudulento.

Frente al desarrollo de campañas de fraude online como las indicadas, es positivo que en este periodo el porcentaje de usuarios que declara haber sufrido impacto económico ha descendido hasta un 2,5%, situándose por primera vez por debajo de la barrera del 3%. Una posible explicación puede estar en que los usuarios españoles no lleven a término los intentos de fraude propuestos por los atacantes, de manera que, aunque sufran la incidencia, la estafa no se ve culminada. Esto se confirmaría con los datos de cambio de hábitos estudiados: la mayoría de usuarios (unos tres de cada cuatro) no modifica sus hábitos cuando recibe correos sospechosos, lo que puede deberse a que conoce su naturaleza y los evita.

Actividad desarrollada por los ciberestafadores a comienzos de 2012

Como indican diversas fuentes de información, algunos tipos de actividad fraudulenta han descendido en los últimos meses. En concreto, el correo basura ha descendido casi a la

[9] Fuente: La Agencia Tributaria advierte de un intento de fraude tipo "phishing" a través de correos electrónicos fraudulentos, disponible en http://www.consumer.es/web/es/tecnologia/2012/02/15/207272.php

[10] Fuente " Crónica del virus de la policía", disponible en http://www.inteco.es/blogs/post/Seguridad/BlogSeguridad/Articulo_y_comentarios/Post_viruspolicia

mitad con respecto a 2010[11]. Si en 2009 el spam podía suponer hasta un 90% de todo el correo enviado en Internet[12], en abril de 2012 no llegó al 50%[13]. Siendo el correo electrónico uno de los principales vectores de ataque de fraude online (es el principal vehículo por el que se comunica al usuario las potenciales estafas), un descenso en el volumen de spam se traduce en un menor número de intentos de fraude percibido por los usuarios. Aunque en este contexto influyan otros factores (mejora de los filtros anti-spam de los usuarios, uso de otras vías de intento de fraude...) el hecho de que el correo basura descienda de esta forma influye en la percepción del fraude por parte de los usuarios.

¿Se puede afirmar, por tanto, que los atacantes han relajado en 2012? No, simplemente modifican sus hábitos. El correo basura puede que no surta el mismo efecto entre los usuarios, de forma que alternativamente se buscan nuevos métodos de infección y engaño. El llamado "virus de la policía" ha conseguido una alta tasa de infección que ha redundado en un mayor beneficio para el atacante sin utilizar el spam para su difusión.

Por tanto, se atisba un cambio de modelo de fraude online: un escenario en el que los usuarios están cada vez más concienciados y los ciberatacantes buscan y aplican nuevas técnicas que les generen lucro además del tradicional correo basura (que va a seguir siendo la base de muchos ataques por su extremada simplicidad y bajo coste). Este escenario obliga a los internautas a reforzar su estado de alerta para evitar que los nuevos intentos de fraude se consuman y los atacantes logren el lucro perseguido.

[11] Fuente: "El spam desciende un 50% y los fabricantes de software resuelven con agilidad las vulnerabilidades" disponible en: http://www.techweek.es/seguridad/informes/1010855004801/informe-ibm-x-force-spam-desciende.1.html

[12] Fuente: "Estudio sobre la seguridad de la información y la e-confianza de los hogares españoles ", disponible en http://www.inteco.es/file/zUeNsALe33anSjvyZnPW2w

[13] Este dato procede de la red de sensores de INTECO, y refleja el porcentaje de spam detectado entre el 1 y el 30 de abril de 2012. Datos disponibles en: http://cert.inteco.es/estadisticas/?option=com_sanetajax&Itemid=55&lang=es

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 sitios. El uso de gestores de contraseñas[14] puede facilitar esta tarea.
- 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.

[14] Un gestor de contraseñas es un programa que permite almacenar credenciales de forma segura en un solo archivo. Para acceder al archivo es necesario conocer una clave de acceso y/o poseer un archivo clave que descifren su contenido. Algunos de ellos incluyen utilidades entre las que se encuentran generadores de contraseñas seguras. http://cert.inteco.es/software/Proteccion/utiles_gratuitos/Utiles_gratuitos_listado/?idLabel=2230254

- 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