UNIVERSITAT JAUME·I

Fraudes en Internet

TRABAJO FINAL DE GRADO.

CURSO 2015/2016

ALUMNO: **Claudia Florentina Dinca**

TUTOR: **Manuel Mollar Villanueva**

INDICE:

Extended Summary

The current society is defined by technological development, especially computer technology. This has a strong influence on our daily life as people constantly use their smartphone, tablet or PC. The excessive use of technology has caused/influenced the emergence of new illegal acts.

According to several studies, Internet frauds are the most frequent cybercrimes. For this reason, this document analyses the new illegal behaviour criminals use to perpetrate these crimes. The purpose of the present paper is to thoroughly examine Internet frauds and to investigate in depth the problems these crimes generate to our society, as well as to provide general recommendations to Internet users in order to prevent these crimes.

First, a general definition of cybercrime and Internet fraud will be provided in order to better understand these concepts. Second, how scams are regulated in the Spanish Penal Code will be illustrated. Third, the most common characteristics of cybercriminals and their victims will be explained. Additionally, a classification of Internet frauds, the main point of the present paper, based on the transmission channels through which these criminals reach their victims will be provided.

The main categories of this listing are: phishing, email frauds, online fraud pages' listings, social networking sites, mobile phones, online advertising and software. Moreover, this paper also includes some statistics in order to better perceive the negative effects of Internet frauds in today's society. Finally, a conclusion summarising the main points of this project will be presented. Furthermore, several personal remarks will be stated.

With this purpose, the term cybercrime will be defined. Therefore, the European Convention on Cybercrime describes this term as an illegal behavior "against the confidentiality, integrity and availability of computer systems, networks and computer data as well as the abuse of such systems, networks and data" (Council of Europe, 2001). Further, this Convention elucidates that Internet fraud is a crime committed through a large range of procedures such as alteration, deletion or suppression of computer data or any interference with the functioning of a computer system. The goal of this illegal action is to procure, without right, an economic benefit for oneself or for another person (Council of Europe, 2001).

What is more, some studies prove that criminals who perpetrate Internet frauds present the following characteristics: the majority are middle aged men, married and economically stable, they have a high level of education, and they do not consider themselves criminals (Garrido, Stangeland & Redondo, 2006). Moreover, victims have an important role in the pursuit of perpetrators suspected of committing cybercrimes as they are the ones who report such crimes to the law enforcement body. Hence, complaints have a large significance as through

them police are able to investigate the acts and announce their existence to Internet users (Gallego Lluste, 2012).

In order to commit Internet frauds, criminals make use of a large series of means that facilitates the entry into the systems. These tools are generally known as malware. This term refers to a software that is specifically designed to disrupt or damage a computer system. Consequently, the most common malwares criminals use to achieve their purpose are the following: viruses, trojans, spywares, botnets and worms. As previously mentioned, the main categories of the classification of Internet frauds are: phishing, email frauds, online fraud pages' listings, social networking sites, mobile phones, online advertising and software.

Phishing is a type of social engineering that uses deceitfulness in order to obtain personal information including passwords or account data among others. Fraudsters employ means such as emails, SMS messages or networking sites. They send messages to a large number of people in an attempt to deceive their victims. These communications contain false information as their purpose is to obtain the addressee's personal data. The most frequent means criminal use are emails. Thus, these emails redirect Internet users to an URL which emulates an official webpage, commonly a bank website. Victims are misled by these false webpages, so they introduce their account details, which will be used by fraudsters to commit unlawful acts. There are numerous types of phishing in this area. Nonetheless, the paper in hand describes pharming and spear phishing as they are considered to generate the severest financial losses.

Pharming is very similar to traditional phishing, but it does not use emails or other electronic messaging systems. In addition, pharming redirects Internet users to a false website even though the URL in correctly typed. With the aforementioned aim, pharmers employ malware. Therefore, it is necessary to previously install a malicious application into the victim's computer as this malicious software is the one that redirects Internet users to a false webpage (Avilés, 2013).

Spear phishing is also very similar to original phishing, but fraudsters are well-informed about their future victims as they send them personalized messages. Moreover, this fraud is more dangerous than the traditional phishing because criminals send emails or use other electronic messaging systems in order to have access to highly sensitive information such as trade secrets, strategic technology plans or confidential government communications (Wyman, Scrivens, Hoffman & Rudis, 2013).

Although email has been around for long, it is a tool widely used by fraudsters to commit their crimes. This is perhaps one of the most prevalent scams on the Internet nowadays. For this reason, this paper explains the most frequent frauds committed by email: pyramidal fraud,

Nigerian fraud 419, lottery scam, advices about stocks, CEO fraud, extortion scam, false job offers and sentimental frauds.

Pyramidal fraud is a business model where associates attract more people to produce benefits to the initial participants. Accordingly, the number of new participants has to be higher than the number of first associates. In addition, email is the most frequent means fraudsters use to commit pyramidal frauds (ASFI, 2009).

Nigerian fraud 419 generates severe financial losses. This scam takes place when an email that contains false information is sent to a large number of people. Generally, this false information involves a promise to earn lots of money if the victim helps a person to transfer money from Nigeria. Supposedly, a percentage of that amount of money will be given to victims (FBI, 2011).

In lottery scam, emails are sent to an unspecified number of people. Hence, these messages inform email recipients they have won a prize and in order to get it, they have to pay a certain sum of money, but obviously if victims pay that amount of money, they won't get any award (Guardia Civil, 2014).

Besides, advice about stocks also takes place by sending emails to a large number of people. These emails are advertising messages which contain promotions related to stocks. The following message is very common: “buy now while the stock price is still very low”. However, when Internet users try to buy these shares, there is more demand and consequently the price is higher. Scammers sell their stocks leaving the victim with nothing (ASFI, 2009).

CEO fraud involves spoofing the email account of a company executive to wire sums of money to fraudulent accounts. By posing as the company's CEO, fraudsters are able to steal money from a company through money transfer requests. It is similar to spear phishing, except that the malware is commonly optional or even nonexistent (Scannel, 2016).

A different sort of email frauds is the extortion scam. In this type of crime, an alleged murderer contacts a victim, usually by email. This perpetrator explains that a third person has hired him to kill the victim, but he will not carry out this act if the victim is willing to remunerate a higher amount of money (Guardia Civil, 2014).

False job offers are very frequent as nowadays lots of people are looking for employment opportunities on the Internet. Moreover, “work from home doing manual tasks" is an instance of this scam. Fraudsters give a bank account to their victims and a transfer must be made in order to book the job. Evidently, the victim is deceived since the job does not exist and scammers do not return the amount of money (INCIBE, 2014c).

Sentimental fraud takes place when a person receives an email from a young woman. This email redirects the email recipient to a webpage where the person can chat to a large number appealing and young women, generally from East European countries. The victim starts to chat to one of them with whom promptly he falls in love. She persuades her new lover to make

a bank transfer as she desires to purchase a flight in order to meet him. Doubtlessly, the sum of money received from the alleged lover is not intended to buy the ticket. Thus, the young woman, who actually is a fraudster, will not return the amount of money to its owner (INCIBE, 2014b).

There are some characteristics online fraud pages' listings share: scammers ask for money in advance, product prices are too low compared to their value, fraudsters generally use generic photographs to promote their false products and in numerous occasions these photographs can be found on the Internet. Likewise, other characteristics are the following: the adverts frequently present grammar mistakes, scammers do not identify themselves or they provide insufficient personal data and criminals explain they live abroad and for this reason an intermediary is needed (INCIBE, 2014d). This project also gives an account of frauds committed on purchases and sales of goods, rental houses and private lending sites.

Similarly, the present paper expounds frauds perpetrated through social networking sites, especially Facebook as it has the largest number of users compared to its competitors. One of the most prevalent scams on Facebook is explained as follows: it was very common to see on Facebook advertisements such as "change the color of your Facebook". Through these adverts, users are encouraged to change the blue color of Facebook to another by using an application. Nevertheless, the app asks users to enter personal data. (INCIBE, 2015a).

Criminals used to take advantage of the excessive usage of text messages to commit various frauds by Premium SMS service. However, the use of SMS has decreased, so fraudsters were forced to find other methods of deceiving. Even though users do not directly use text messages to communicate, scammers found a new method that allow them to use Premium SMS service to defraud their victims: instant messaging applications. In the present paper, numerous frauds committed through WhatsApp are depicted as it has the largest number of users compared to other instant messaging applications (INCIBE, 2012).

Furthermore, spim is a scam perpetrated via mobile phones. It is very similar to spam, but spim messages are sent through instant messaging applications such as WhatsApp or Line, while spam uses email. Generally, spim messages include an URL which asks Internet users for personal data (INCIBE, 2014e).

Vishing is also a fraud committed via mobile phones. It occurs as follows: fraudsters randomly mark phone numbers until someone answers. Scammers deceive this person as they say their credit card is being used illegally or their confidential data needs to be updated. In order to sort out these problems, criminals give the victim a phone number. When calling, the victim hears a recording asking for account data (Amanor & Yeboah-Boateng, 2014).

Moreover**,** one of the most prevalent online advertising frauds is called traffic robots or non-human traffic generated by botnets. The purpose of this fraud is to dilute the real value of the

advertiser's inventory as botnets produce false visits to advertisements. Real and fake visits will be mixed, so an error occurs in the advertiser's inventory (Matarranz, 2016).

To continue, we will give a brief explanation of frauds perpetrated on software, in particular ransomware and fake antivirus programs. We can define ransomware as the use of malware in order to block access to computers or data until a payment is made (NIST, 2011). In order to justify this circumstance, generally ransomware claims users that they committed a cybercrime and for this reason they have to pay a fine. However, these petitions are completely false and even if the user pays the alleged sanction or does what the ransomware demands, there is no guarantee that the user will have access to his computer (Microsoft Corporation, 2015).

The purpose of fake antivirus programs is to convince users to install fraudulent antivirus software. Criminals persuade victims their computers are infected with malware and in order to solve the issue, some specific antivirus programs are required. So, victims get these programs by paying an amount of money (INTECO-CERT, 2008).

As we said at the beginning of this extended summary, we also included some statistics in the present paper in order to better perceive the negative effects of Internet frauds in our today's society. We have been able to ascertain that the total initiated judicial proceedings on cybercrimes in Spain has been increasing year over year. Moreover, crimes committed on the Internet impact both business and citizens as their consequences often suppose serious economic impact.

The main conclusions of this project are expounded as follows. Internet helps us in many ways: it offers us the opportunity to access information very quickly and it also offers us the possibility to communicate in a simple and economical way. However, Internet also has some disadvantages as it could be used by criminals to perpetrate a large number of crimes.

After finishing our classification of Internet frauds, we understood criminals' *modus operandi* in this area, the methods they use to commit their illegal acts and we also comprehended that the techniques they use are renovating quickly as there is a constant evolution of the hi-tech and digital sectors.

Cybercrimes are continuously increasing and Internet frauds are the most frequent. So, these scams are an issue in today's society as criminals always find new ways to commit these illegal acts. All this and the constant technological development have a significant influence on the increase of Internet frauds. Cybercrimes have also negative consequences for global economy as they generate serious economic losses at national and international level.

Resumen: En la sociedad actual, estamos experimentando un gran avance tecnológico, destacando la tecnología informática por su gran influencia en casi todas las áreas de la vida social. Sin embargo, esta circunstancia ha dado lugar a diversos comportamientos ilícitos, denominados de forma genérica delitos informáticos. De entre estos últimos, el presente documento se centra en los fraudes en Internet por ser estos los más frecuentes. El objetivo es llevar a cabo un análisis de los diversos fraudes online con los que nos podemos encontrar actualmente, entender la problemática que estos pueden suponer para nuestra sociedad, además de proporcionar unas pautas generales para los internautas con el fin de prevenir de forma eficaz la comisión de este tipo de delito. Para ello, en este texto se recogen definiciones generales del delito informático y del fraude online, las diferentes características de las que gozan los sujetos intervinientes y diversos consejos para evitar ser víctima. Además, se explica brevemente el delito de estafa recogido en el Código Penal y se proporcionan algunos datos estadísticos para poder ver el impacto que tienen estas infracciones penales en nuestra sociedad. Aparte de lo anteriormente mencionado, este trabajo también recoge una clasificación de los fraudes en Internet, núcleo central del mismo, basada básicamente en los canales de transmisión mediante los cuales estos delitos llegan a sus víctimas. Las categorías principales en los que hemos dividido nuestra clasificación son los siguientes: phishing, fraudes a través del correo electrónico, fraudes en páginas de anuncios online, en redes sociales, en teléfonos móviles, en publicidad online y en programas informáticos.

Palabras clave: *delito, fraude, Internet, malware, phishing, correo electrónico, red social, app*

Abstract: The current society is characterized by a significant technological progress, highlighting the computer technology due to its great influence in almost all social domains. However, this fact has generated unlawful behavior, generically called cybercrimes. Considering their occurrence, the present paper focuses on Internet frauds, a type of cybercrime. The aim of this paper is to accomplish an analysis of several online frauds that are currently common and to comprehend the issue they imply to our society. Besides, this thesis also aims to provide general guidelines for the Internet users to efficiently prevent the commission of this crime. To this end, general definitions of cybercrime and online fraud are included in this work, as well as features of the parties involved and advice so that this crime is avoided. Additionally, how fraud offences are regulated in the Spanish Penal Code is briefly examined and some statistics are presented in order to observe the impact of these crimes on our society. Aside from the abovementioned, this analysis also includes a categorization of Internet frauds, mainly based on transmission channels used to approach the victims. The principal categories of this paper's classification are phishing, email frauds, online fraud pages' listings, social networking sites, mobile phones, online advertising and software.

Keywords*: crime, fraud, Internet, malware, phishing, email, social networking site, app*

1 Introducción

El objetivo del presente trabajo es dar una visión global de lo que son los fraudes cometidos vía Internet, entender la problemática que este delito supone para nuestra sociedad, realizar una clasificación de los fraudes en Internet con la finalidad de poder identificar este delito con facilidad y evitar ser víctimas del mismo, además de proporcionar unas pautas generales para los internautas con el fin de prevenir de forma eficaz la comisión de este tipo de delito. No podemos no observar el problema que los delitos en Internet suponen para nuestra sociedad a causa de las herramientas que son empleadas en su comisión, ya que es evidente que la mayor parte de la población dispone de las mismas. Esto supone una cierta facilidad para la realización de este tipo de delincuencia y además explica el continuo aumento que están teniendo año tras año estos delitos, destacando los fraudes por haber ganado el primer puesto.

Internet nace como una herramienta para esparcir información y como un mecanismo de interacción entre las personas sin que la ubicación geográfica constituya una barrera para tal fin. Sin embargo, aunque encontramos muchos beneficios para el uso de Internet, tales como el acceso a la cultura y ciencia a millones de personas de una forma más rápida, no podemos no observar una gran desventaja: muchos infractores encontraron una forma de cometer delitos a través de Internet, y lo que es más preocupante es que muchos de ellos lo hacen de forma impune. Esta problemática y el auge que están teniendo hoy en día los fraudes cometidos mediante las nuevas tecnologías explican el porqué de la elección del tema de los fraudes cometidos vía Internet.

Para cumplir con el objetivo fijado en nuestro trabajo, explicaremos en qué consisten los delitos informáticos y los fraudes online. Además, aunque el tema es muy amplio tanto a nivel internacional como nacional, por ser el fraude en Internet un tema muy extenso, haremos una breve referencia a la legislación española en materia de delitos informáticos para ser capaces de tratar desde una perspectiva legal el fraude en Internet. Nos centrándonos en el delito de estafa regulado en el Código Penal para conseguir subsumir en el tipo penal correspondiente los comportamientos ilícitos que describiremos en el presente documento. Dedicaremos también un pequeño apartado a la explicación de los perfiles del delincuente y de la víctima, haciendo hincapié en el del delincuente ya que somos conscientes de que Internet destaca por ser una buena herramienta para ofrecer el anonimato a las personas que llevan a cabo este tipo de acciones, por lo que resulta muy complicado saber quién está detrás de estas fechorías. Mediante el análisis de este perfil se pretende conseguir identificar al delincuente informático de una forma más rápida. Proporcionaremos además una clasificación de los fraudes en Internet, tema central del presente trabajo, ya que consideramos imprescindible tener claro el *modus operandi* de estos delincuentes en cada uno de los tipos de fraudes online con la finalidad de ser capaces de identificar estos delitos y poder evitar su comisión. Esto sumado a que la legislación generalmente es muy poco explícita en cuanto a los tipos

de fraudes electrónicos, hace de la clasificación de los fraudes en Internet el tema principal de nuestro trabajo.

Para establecer esta ordenación, nos hemos centrado básicamente en los canales de transmisión porque de esta forma podemos hablar de los fraudes cometidos a través de los medios más utilizados actualmente en Internet, como pueden ser el correo electrónico, redes sociales o aplicaciones para los smartphones. Además, de esta forma podemos conseguir hacer un análisis de las conductas más novedosas del mundo de la delincuencia informática que están teniendo un gran auge en los últimos años. Mediante este estudio también podemos llegar al mayor número de personas, por gozar estos medios utilizados en Internet de muchos usuarios, conseguir concienciar a los internautas de los riesgos a los que pueden estar expuestos al utilizar este tipo de canales y conseguir cumplir una de las funciones más importantes de la Criminología: la prevención del delito.

2 Marco conceptual. Ciberdelincuencia y fraudes en Internet

Para ser capaces de llevar a cabo un correcto análisis y profundizar en nuestra investigación, consideramos imprescindible comprender qué es un delito informático y tener claras sus características ya que el tema que nos ocupa, los fraudes en Internet, no son más que un delito informático que tiene lugar mediante el empleo de las TIC.

Muchos autores y organismos han intentado proporcionar una definición de delito informático. Algunos expertos en la materia han llegado a afirmar que delito informático y delito común es lo mismo, que no hay que hacer una diferenciación entre estos dos conceptos, ya que el resultado final de los delitos informáticos y de los delitos tradicionales viene a ser el mismo, diferenciándose entre sí solo por el medio empleado para llevar a cabo el acto ilícito (Ramírez Bejerano & Aguilera Rodríguez, 2015).

Una definición válida podría ser la siguiente: los delitos informáticos son aquellas conductas que, tanto por el medio utilizado como por el objeto sobre el que recaen, son realizadas a través de procesos electrónicos, teniendo como característica común un ámbito de riesgo centrado en la expansión de la tecnología informática (Garrido, Stangeland & Redondo, 2006).

Otra definición es la que se establece en el Convenio de la Ciberdelincuencia Europeo. Según este los delitos informáticos son “los actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos” (Consejo de Europa, 2001).

Hay una serie de características que comparten todos los delitos informáticos. Destaca tanto la dificultad probatoria, ya que es mucho más difícil seguir un delincuente informático porque estos pueden cometer sus infracciones de una forma muy rápida y sin importar el área geográfica en la que se encuentran, como su perseverante evolución y proliferación, cosa que dificulta mucho su persecución. Además, estos delitos también se caracterizan porque

no cualquier persona los puede llevar a cabo, ya que para su comisión es necesario tener ciertos conocimientos informáticos (Gallego LLuste, 2012).

Respecto al fraude online, hay que decir que este está recogido en el artículo 8 del Convenio de Budapest del Consejo de Europa sobre Ciberdelincuencia, definiendo el mismo como "(…) los actos deliberados e ilegítimos que causen un perjuicio patrimonial mediante una amplia gama de procedimientos (…) con la intención fraudulenta o delictiva de obtener ilegítimamente un beneficio económico para uno mismo o para otra persona" (Consejo de Europa, 2001, p. 31).

Según INTECO, los elementos que concurren en el fraude a través de Internet son los siguientes: voluntad, carácter lucrativo, perjuicio patrimonial de un tercero y empleo de medios electrónicos o informáticos para la comisión del delito.

En cuanto a los tipos de fraudes cometidos a través de medios electrónicos, generalmente la legislación es poco explícita. Es muy frecuente recoger tipos genéricos, en los que se puedan encajar los diferentes supuestos de estafa o fraude en Internet que puedan cometerse (INTECO, 2007).

3 Actores

Al igual que en el resto de delitos, encontramos dos sujetos que se ven involucrados en la comisión de un delito en Internet: el sujeto activo, es decir la persona que lo comete y el sujeto pasivo, el sujeto que resulta ser víctima.

3.1 Sujeto activo

Somos conscientes de que Internet destaca por ser una buena herramienta para ofrecer el anonimato a las personas que cometen este tipo de comportamientos ilícitos, por lo que resulta muy difícil saber quién está detrás de estas actividades. Por este motivo, en el presente apartado nos centraremos principalmente en ofrecer una descripción de las características comunes de los delincuentes informáticos con la finalidad de poder identificarlos más fácilmente. Es importante mencionar que el fraude informático lo pueden cometer también las personas jurídicas según el artículo 251 bis CP (BOE, 2015).

El individuo que comete este tipo de delitos no es considerado un delincuente común, porque se diferencia de este último en el mecanismo y medio empleado para producir el resultado. Es importante mencionar que no existe un único perfil que pueda describir a estos delincuentes, lo que sí se ha intentado hacer es extraer una serie de características comunes (Garrido, Stangeland & Redondo, 2006). Por tanto, podemos decir que las personas que cometen estas conductas antijurídicas poseen algunos rasgos que los delincuentes tradicionales no tienen: disponen de habilidades en el manejo de sistemas informáticos y

normalmente su puesto de trabajo brilla por gozar de información de carácter sensible (Gallego LLuste, 2012).

En cuanto a los autores de los fraudes informáticos, una investigación de la universidad Yale de Estados Unidos demuestra que normalmente los delincuentes que cometen fraudes informáticos reúnen las siguientes características: la mayor parte de los mismos son hombres de edad media mayor, casados y económicamente estables porque disponen de un puesto fijo de trabajo, tienen un alto nivel de educación, buena consideración de sí mismos y no se consideran delincuentes (Garrido, Stangeland & Redondo, 2006).

A los individuos que cometen delitos informáticos se les denominó comúnmente hackers, sin embargo, observamos que hoy en día las actividades que desarrollan los hackers solo constituyen una pequeña parte de este tipo de infracciones.

A continuación, explicaremos cuál es la clasificación más importante de los infractores informáticos. Esta es la siguiente: hackers, destacando el hecho que no tienen una finalidad económica, crackers y phreakers, que sí que son movidos por una finalidad económica y por tanto son de especial interés en nuestra investigación.

El hacker muestra mucho interés en el funcionamiento de los sistemas operativos. Su finalidad no es económica y tampoco quiere producir ningún tipo de daño. Le motiva la investigación de las nuevas tecnologías y lleva a cabo estas actividades como un reto intelectual. Sus actividades se basan en adquirir nuevos conocimientos y descubrir si el sistema tiene debilidades. Si descubre errores o fallos en el sistema se lo comunica a la empresa u organización y sugiere soluciones. Sin embargo, es evidente que generalmente esta conducta constituye un delito ya que acceden de una forma ilícita a los sistemas informáticos.

El cracker[1] debe tener conocimientos avanzados en informática para llevar a cabo sus acciones que básicamente consisten en romper la seguridad de los programas comerciales con la finalidad de beneficiarse económicamente. Mediante sus acciones puede llegar a destruir o robar información, para posteriormente venderla. Aunque las empresas y organizaciones emplean protección para asegurar sus productos, el cracker siempre consigue romper la seguridad de los programas. Además, en la mayoría de las ocasiones, cuando este infractor descubre una debilidad en el sistema, la difunde por Internet. Esto último constituye un problema, ya que al hacerse pública dicha debilidad es evidente que el número de infractores puede aumentar notablemente.

El vocablo phreaker[2] empezó a utilizarse a mediados de los años 80 para referirse a las personas que utilizaban diversas técnicas con la finalidad de evitar el pago de las llamadas. Actualmente, el phreaker basa sus actividades en la manipulación del sistema informático de

---

1 *Crack* es sinónimo de rotura y por tanto cubre buena parte de la programación de *Software* y *Hardware*; por tanto, el cracker debe saber perfectamente el funcionamiento de estos dos.

2 Este vocablo, *phreaker,* deriva de las palabras inglesas *phone* y *freak.*

la compañía telefónica, por lo tanto, deben tener amplios conocimientos en informática (Gallego LLuste, 2012).

3.2 Sujeto pasivo

El sujeto pasivo viene a ser la persona o ente sobre el que recae la acción del sujeto activo. Por tanto, es la víctima del delito. En el caso de los fraudes informáticos, las víctimas pueden ser personas, instituciones crediticias, gobiernos, etcétera, que tengan conexión más o menos permanente a Internet.

Generalmente, las víctimas de estos delitos suelen gozar de una o algunas de las siguientes características: ingenuidad, desconocimiento, falta de educación, desatención, necesidad, avaricia y búsqueda de venganza. El carácter anónimo de Internet provoca que la víctima no confíe en la justicia penal ya que está convencida de que no se puede descubrir al autor del delito a causa de la invisibilidad que le aporta Internet.

El sujeto pasivo adquiere una gran importancia porque generalmente es él el que denuncia las infracciones. Por tanto, en la gran mayoría de los casos, es este el que da a conocer la comisión de un delito informático. Se deduce la importancia de que goza la denuncia en estos casos, ya que sin esta las autoridades competentes no podrían estudiar el hecho o avisar de la existencia de este al resto de usuarios. Por tanto, si la víctima no da a conocer la existencia del acto delictivo resultaría muy complicado identificar y detener las amenazas que diariamente circulan por la red. Sin embargo, la mayor parte de las víctimas no denuncian, lo que hace que la cifra negra sea muy elevada. Para poder conseguir la prevención de la criminalidad informática, y con ello la protección de los sujetos pasivos, es necesario que las potenciales víctimas comprendan los métodos de manipulación que utilizan estos infractores (Gallego Lluste, 2012).

4 Procedimientos

Para poder cometer este tipo de prácticas ilegales, los delincuentes utilizan una serie de medios que les facilita la entrada en los sistemas, y a partir de allí realizan sus fechorías. En este apartado, es importante mencionar el término malware[3], que engloba de modo genérico el conjunto de diferentes tipos de software malicioso que traerán prácticas indeseadas en los sistemas informáticos. Los explicamos a continuación:

- Virus: Una vez en el sistema operativo, los objetivos fundamentales del virus son propagarse y llevar a cabo otras funciones que afectan al sistema. Generalmente los virus se unen a un archivo ejecutable. Por tanto, el *malware* estará inactivo y no infectará otros programas hasta que el usuario abra o ejecute el archivo malicioso, el

[3] También es conocido bajo otros nombres: *badware*, código maligno, software malicioso o malintencionado. Es un tipo de software cuyo objetivo es el de introducirse en sistemas operativos sin el consentimiento del propietario para realizar diversas tareas con fines ilegítimos.

programa hospedador. A partir de este momento, el virus queda activado y se propaga a otros programas del sistema. Los virus son los primeros ejemplos de *malware* que se han creado. Sin embargo, observamos que su uso por parte de los delincuentes ha quedado restringido, porque con el paso del tiempo se han creado otros tipos de software malicioso que llevan a cabo mejor sus "funciones" (CERT-UK, 2014).

- Gusano: Los gusanos[4] son muy parecidos a los virus, tanto que se considera que son una subclase de virus. La diferencia es que estos son capaces de operar como un programa independiente además de tener la capacidad de propagarse por la red directamente (CERT-UK, 2014). Por lo tanto, estos son más dañinos que los virus ya que no necesitan de un programa para poder replicarse.
- Troyano: Se trata de un pequeño programa que se encuentra dentro de una aplicación (archivo). El usuario queda engañado porque el troyano[5] parece ser un programa útil, sin embargo, esto no es así. Por tanto, al considerar que es un programa de procedencia segura, el usuario acaba ejecutando este malware, por lo que el troyano queda activado en el ordenador. Al igual que los virus, algunos troyanos están programados para causar serios daños en el sistema, como por ejemplo eliminar información importante, mientras que otros están diseñados solo para ser molestos (Aycock, 2006).
- Spyware: Es un software que recolecciona información de una computadora y después la transmite. Estos datos pueden ser contraseñas, direcciones de correo electrónico, cuentas bancarias, etcétera. Por tanto, observamos que lo que se extrae es información confidencial de la víctima.
- Botnet: Es un nuevo ataque informático que consiste en un conjunto de ordenadores programados para recibir una serie de instrucciones y en ciertos momentos enviar información a través de la red. Es el delincuente informático el que maneja estos ordenadores sin que la víctima tenga conocimiento de ello (Aycock, 2006).
- Scareware: mediante el scareware aparece en la pantalla de la víctima un mensaje para acceder a diversos enlaces. Se pretende que la víctima acceda en el

[4] Fue John Brunner quien utilizó este término por primera vez (*worm)* en 1975. Aparece en su novela de ficción *The Shockwave Rider.*

[5] También se le conoce como caballo de Troya o *Trojan Horse* por su gran similitud con el famoso caballo de Troya de los griegos.

enlace porque al hacer clic en el link se ejecuta un malware que tiene como finalidad robar datos confidenciales.

- Keylogger: el objetivo es que la víctima pulse diversas teclas para que los delincuentes informáticos descubran la contraseña de la víctima (González Suárez, 2014).

5 Phishing

Tanto la velocidad de evolución que caracteriza a la red como la evolución permanente en la que se encuentra este fenómeno, influyen en la dificultad de proporcionar una única definición de lo que viene a ser phishing.

Los infractores que realizan sus actividades ilícitas mediante el phishing utilizan una combinación de trucos que implican la web, correo electrónico y software malicioso para robar información personal y credenciales de cuentas financieras. El medio más empleado es el correo electrónico (Kevin McGrath & Minaxi Gupta, 2008).

El comunicado de INTECO nos propone la siguiente definición de phishing: “el phishing es una forma de ataque basada en técnicas de ingeniería social, utilización de código malicioso o la combinación de ambas, en la que el delincuente, haciéndose pasar por alguna empresa o institución de confianza, y utilizando la tecnología de la información y las comunicaciones, trata de embaucar al atacado para que le proporcione información confidencial, que posteriormente es utilizada para la realización de algún tipo de fraude” (INTECO, 2007, p. 38).

Por tanto, el phishing es un tipo de ingeniería social que desea obtener a través del engaño información personal del usuario (como contraseñas o datos bancarios). Los sujetos que cometen este tipo de actividades ilícitas tienen conocimientos informáticos avanzados y los utilizan para enviar diversos tipos de mensajes a un número indeterminado de personas. Generalmente emplean el correo electrónico y redireccionan a los usuarios a sitios web falsos que imitan a una página web oficial, y a causa de la gran semejanza entre el sitio web original y el falsificado, los usuarios quedan engañados y finalmente introducen sus datos personales. Los delincuentes utilizan la información obtenida de forma ilegítima para acceder a las cuentas personales de la víctima y provocar pérdidas económicas o suplantación de identidad (Avilés, 2013).

Podemos encontrar muchas clasificaciones de phishing: por ejemplo, destacan las clasificaciones en base al servicio atacado o atendiendo al *modus operandi* del autor. En el presente trabajo nos centraremos en el pharming y el spear phishing por considerar que son las subclasificaciones que pueden generar las pérdidas económicas más graves.

El pharming consiste en redirigir al usuario a una página web falsa, al igual que el phishing original, sin embargo, en esta ocasión no es necesario el mensaje de correo electrónico o

similar, ya que el delincuente manipula los registros DNS[6] de los servidores globales. Los pharmers[7] redirigen a sus víctimas a una página web falsa incluso si previamente han tecleado de forma correcta la URL[8]. Para entender cómo funciona el pharming es importante comprender lo siguiente: al escribir en nuestro navegador una dirección web, en realidad le comunicamos al ordenador que se dirija a un servidor, en concreto al servidor[9] de la página web que hemos escrito. Para poder ser identificados, los servidores tienen asignados una serie de números denominada dirección IP (Internet Protocol), que normalmente no cambia para su fácil localización en Internet. Al ser esta serie de números difícil de recordar, a cada página web con su dirección IP se le asigna un dominio, que viene a ser el nombre de la página web. De esta forma, al teclear en el navegador el nombre del sitio web que deseamos visitar, nuestro servidor de Internet lo traduce de forma automatizada en la dirección IP de la página web.

Los pharmers llevan a cabo sus acciones ilícitas con la ayuda de un software malicioso, es decir mediante malware. Por tanto, es necesario que en el ordenador a atacar se instale alguna aplicación. Mediante el software malicioso logran manipular los nombres de los sitios web que tecleamos en nuestro navegador. Por tanto, al escribir una determinada página web, el malware nos redirecciona a la página web fraudulenta, que brilla por su similitud a la original (Avilés, 2013).

En cuanto al spear phishing, podemos decir que los delincuentes actúan de la misma manera que en el phishing. Sin embargo, en este caso buscan información sobre sus objetivos, revisando sus cuentas personales en las redes sociales o leyendo los mensajes que publican en foros y blogs públicos, ya que enviarán un correo electrónico fraudulento que se caracteriza por ser altamente personalizado.

Por tanto, el spear phishing consiste en el envío de correos electrónicos, simulando ser de parte de una organización o persona de confianza, a un número reducido de personas u organizaciones previamente seleccionadas. Por esto último, los que están detrás de estos actos realizan una investigación minuciosa sobre sus víctimas. Los objetivos de estos infractores van más allá de los motivos económicos, ya que lo que desean conseguir es acceso a información altamente confidencial, como secretos comerciales corporativos, planes estratégicos de tecnología o comunicaciones confidenciales del gobierno. Con estos datos,

---

6 *Domain Name System* (DNS): Es una base de datos distribuida con información que se utiliza para traducir los nombres de dominio, fáciles de recordar y usar por las personas, en números de protocolo de Internet (IP) que es la forma en la que las máquinas pueden encontrarse en Internet.

7 Se denomina *pharmers* a las personas que llevan a cabo el *Pharming.*

8 *Uniform Resource Locator* (URL): Es una cadena de caracteres que identifica los recursos de una red de forma unívoca; la dirección puede apuntar a recursos variables en el tiempo.

9 El servidor es una aplicación en ejecución que atiende las solicitudes de un cliente proporcionando una respuesta adecuada.

evidentemente pueden causar graves impactos de diversos tipos en sus víctimas, incluso daños económicos (Wyman, Scrivens, Hoffman & Rudis, 2013).

Con las características de que goza el spear phishing, observamos que este es un ataque mucho más peligroso que el phishing tradicional porque los ataques consisten en el envío de correos electrónicos a personas u organizaciones muy específicas, lo que conlleva un aumento en la probabilidad del éxito de los delincuentes además de una mayor dificultad de detectarlos (Trend Micro, 2012).

La última parte de este apartado la hemos dedicado a explicar las fases en las que tiene lugar el phishing. Estas son las siguientes: planificación, preparación, ataque, recolección, fraude y post-ataque.

En la fase de planificación, el delincuente toma las decisiones más importantes: determina el objetivo del fraude, quién es la víctima, cómo y dónde va a llevar a cabo el ataque, etcétera. El infractor decide si realizará la conducta ilícita individualmente o de forma colectiva como también la clase de información que desea conseguir mediante el phishing: contraseñas, información de cuentas bancarias, nombres de usuario, etcétera. Esta fase tiene lugar independientemente del tipo de phishing de que se trate.

A través de la fase de preparación, el phisher consigue el software, los datos de contacto, organiza los materiales que necesita para llevar a cabo el fraude, establece los destinos de sus ataques y diseña las páginas web fraudulentas. Cuando la víctima no es elegida de forma indiscriminada, es necesaria una mayor elaboración si el objetivo es una persona o entidad concreta.

En cuanto a la fase de ataque, hay que decir que teniendo en cuenta el tipo de phishing que desea realizar, el atacante se centrará en el servidor de la empresa o en preparar las trampas para la víctima. El ataque mediante malware, tiene lugar mediante los siguientes siete elementos: el malware, la infección, la ejecución, el almacenamiento, la entrada de datos, el atacante y el servidor legítimo.

En la fase de recogida de datos, el atacante permanece a la espera, ya que es la víctima la que tiene que responder al mensaje, visitar la página web falsa o entrar en el servidor infectado, para que, de esta forma, el delincuente pueda disponer de sus datos personales. Si el ataque se dirige a servidores, para que el infractor pueda obtener información confidencial, es necesario que el software malicioso se ejecute.

Respecto a la fase de ejecución del fraude, podemos decir que, al disponer de la información necesaria de las víctimas, la siguiente etapa es la ejecución del fraude, bien de forma directa o vendiendo la información descubierta.

La última fase es la de post-ataque. El objetivo es borrar todos los indicios que han podido originarse tras el delito. Además, es evidente que los delincuentes procederán al blanqueo

de los beneficios obtenidos del phishing y a otras actividades ilegítimas con el objetivo de pasar desapercibidos (INTECO, 2007).

6 Scam o fraudes a través del correo electrónico

El término scam[10] es utilizado mayoritariamente para referirse a las estafas que se llevan a cabo mediante el correo electrónico. Esta vía, a pesar de los años desde su aparición, sigue siendo muy utilizada por los delincuentes para cometer diversos fraudes. Para eso, solo necesitan conocer el correo electrónico de sus futuras víctimas. Mediante el spam recibimos diversos correos electrónicos tales como publicidad o hoax; además observamos que muchos de estos correos electrónicos ocultan diferentes fraudes. Normalmente lo que buscan los delincuentes con los fraudes a través del correo electrónico es una transferencia de dinero por parte de la víctima (GDT, 2016).

6.1 Esquemas de Pirámide

Este tipo de fraude es uno de los más antiguos. En general, los esquemas piramidales son ilegales y fraudulentos. Sin embargo, observamos que existen compañías de mercado en red o de multinivel que son legales, pero estas son pocas y los estafadores hacen creer a sus víctimas que son una de estas compañías legítimas.

La estafa piramidal es un esquema de negocios que destaca por el hecho de que los participantes captan a más personas a participar con la finalidad de que los nuevos introducidos en el esquema produzcan beneficios a los participantes iniciales. Es necesario que el número de los nuevos individuos que participan sea superior al ya existente (ASFI, 2009).

Este fraude se sigue cometiendo hoy en día y observamos que el correo electrónico es una de las vías más frecuentes de propagarse. En el mensaje hay una explicación sobre la gran cantidad de dinero que puede ganar la persona que participa en el esquema. Normalmente, en dicho correo electrónico también aparece una lista de personas. A los primeros individuos que aparecen en dicha lista la víctima ha de enviar una pequeña cantidad de dinero y alterar el orden de los nombres eliminando al primero y subiendo los demás una posición, además de inscribirse la persona que ha sido víctima de este fraude en la última posición. Por tanto, los primeros de la lista reciben una cantidad de dinero de los últimos que han entrado en el esquema piramidal (ASFI, 2009).

[10] La palabra *scam* es un término anglosajón que en español se traduce como estafa.

6.2 Estafa nigeriana o Fraude 419

Este fraude es uno de los más antiguos. Aunque parece difícil caer en este engaño, este tipo de estafa genera grandes pérdidas económicas cada año. Se lleva a cabo principalmente mediante correo electrónico no solicitado. Se le conoce bajo el nombre de estafa nigeriana porque estos correos electrónicos provienen de Nigeria. Este fraude viola el artículo 419 del Código Penal nigeriano, y por este motivo también se le denomina fraude 419.

Lo más frecuente es prometer a la víctima un porcentaje de los millones de dólares que el remitente está tratando de transferir fuera de Nigeria supuestamente de forma legal. Se le solicita a la víctima datos personales como nombres de bancos y número de cuentas bancarias, así como enviar dinero al remitente de estos correos electrónicos en forma de pagos parciales. Se le promete al destinatario el reembolso de estos gastos que debe pagar, que evidentemente nunca se efectuará. Se han dado casos en los que el autor de estas fechorías, con la información personal que ha conseguido, ha llegado a suplantar la identidad de la víctima y a vaciar sus cuentas bancarias (FBI, 2011).

6.3 Timo de la lotería

Los delincuentes llevan a cabo un envío masivo de correos electrónicos a distintas direcciones. Es muy frecuente que estos correos empleen ilícitamente los logotipos del Organismo Nacional de Loterías y Apuestas del Estado (ONLAE).

En estos mensajes se informa al usuario que ha ganado un premio, aunque este no ha participado en ningún tipo de sorteo. Para justificar esto último, se le explica que fue seleccionado al azar por medio de su dirección de correo electrónico o de entre las diversas personas que han visitado determinadas páginas web. Para poder conseguir el premio, el “agraciado” ha de pagar una cantidad de dinero. Este pago es justificado mediante la existencia de unos supuestos impuestos, aranceles, costes de transferencia, etcétera. Para poder efectuar el pago se facilita una cuenta bancaria o se solicita una transferencia.

Es muy común que los estafadores utilicen los logotipos de empresas aseguradoras o bancarias muy conocidas o de algún Ministerio con la finalidad de convencer a los destinatarios que se trata de mensajes de correos electrónicos legítimos. Al efectuar el pago, la víctima no vuelve a tener noticia del premio (Guardia Civil, 2014).

6.4 Consejos sobre acciones

Este fraude también es conocido bajo el nombre de “carga y descarga”. Se lleva a cabo mediante correos electrónicos. Estos son mensajes publicitarios para que el usuario compre acciones de una determinada compañía. Es muy frecuente el siguiente mensaje: “compre ahora mientras el precio de las acciones es aún muy bajo”.

Sin embargo, a la hora de comprar dichas acciones, hay más demanda y como consecuencia el precio de las acciones es más elevado. Ese es el momento en el que el delincuente vende sus acciones, dejando a la víctima con nada (ASFI, 2009).

6.5 Estafa del director ejecutivo

Este es un nuevo fraude que se comete utilizando el correo electrónico. También se conoce bajo el nombre de fraude al CEO[11]. Este consiste básicamente en la suplantación de identidad del director ejecutivo de una empresa creando una cuenta falsa con su dirección de correo electrónico muy similar a la original para inducir a error a las personas que lo reciben. En el mensaje ordena al contable de la empresa a realizar una transferencia bancaria en el extranjero. Al darse cuenta la empresa que ha sido víctima de un fraude, es demasiado tarde (Scannel, 2016).

Para poder suplantar la identidad del CEO, los autores estudian durante mucho tiempo su comportamiento, llegando a realizar un seguimiento de esta persona para poder averiguar dónde vive y trabaja, descubrir más datos sobre sus relaciones personales y profesionales, etcétera. Pueden llegar incluso a hackear sus cuentas o la wifi de casa. Al disponer ya de la suficiente información, empieza la estafa propiamente dicha (Molist, 2016).

6.6 Extorsiones

Un supuesto asesino contacta a su víctima, generalmente por correo electrónico, y le explica que otro individuo le ha contratado para matarle, sin embargo, no llevará a cabo esta acción si le ofrece una cantidad de dinero mayor que la que le han prometido por realizar el homicidio.

Estas amenazas pueden variar. Por ejemplo, puede aparecer en el mensaje que un ser querido ha sido secuestrado y que se ha de pagar una determinada suma de dinero para el rescate. El estafador también puede amenazar a su víctima con un secuestro o una agresión. Todos los casos tienen en común que se le propone a la víctima ofrecer una cantidad de dinero superior a la que se le ha prometido al delincuente para llevar a cabo el acto ilícito, con

[11] En inglés americano CEO se traduce como *chief executive officer* (director ejecutivo).

la finalidad de desistir en su empeño. Estos correos electrónicos son totalmente falsos y cuando la víctima queda engañada, no se le devuelve el dinero (Guardia Civil, 2014).

6.7 Engaños sentimentales

Este tipo de fraude tiene lugar de la siguiente manera: una persona recibe un correo electrónico donde una chica jóven y guapa está interesada en chatear con el destinatario. Normalmente en el correo electrónico hay un link que redirecciona a quien ha pinchado en él a una página web en la que hay un elevado número de chicas guapas, normalmente de los países del Este de Europa, ansiosas por conocer a sus nuevos enamorados.

La víctima de este fraude empieza a chatear con alguna de estas jóvenes y esta se muestra muy enamorada al pasar poco tiempo. Pronto está interesada en viajar para conocer a su nuevo enamorado, pero no tiene el dinero suficiente para ello. Por tanto, consigue una transferencia bancaria de su enamorado. Sin embargo, evidentemente este dinero no va destinado a comprar ningún billete de avión. Por tanto, la chica, que en realidad se trata de un delincuente, se queda con la cantidad de dinero facilitada por la víctima del fraude (INCIBE, 2014b).

6.8 Falsas ofertas de trabajo

A causa de la situación económica en la que nos encontramos actualmente, este tipo de fraude es muy frecuente ya que un elevado número de personas está buscando ofertas de trabajo en Internet. Los estafadores se están aprovechando de esta situación y están utilizando principalmente el correo electrónico como vía para engañar a sus víctimas prometiéndoles el trabajo de sus vidas. Algunos ejemplos de falsas ofertas de empleo que circulan por Internet son los siguientes:

- "Trabaja desde casa haciendo tareas manuales": Se le facilita al usuario una cuenta bancaria en la que tiene que efectuar una transferencia para poder reservar el puesto de trabajo. Evidentemente la víctima queda engañada porque el puesto de trabajo no existe y los estafadores no devuelven la cantidad de dinero que esta ha ingresado.
- "Rellena encuestas y gana mucho dinero": Se le engaña a la víctima que se convertirá en una persona rica con tan solo rellenar encuestas de algunas empresas conocidas que necesitan la opinión de sus clientes para poder mejorar. El fraude está en que, para poder acceder a las encuestas, el usuario ha de pagar una cantidad de dinero.
- "Trabajo fácil, solo hay que realizar transferencias bancarias": Se engaña al usuario que por recibir determinadas cantidades de dinero en una cuenta bancaria y transferirlas a otra se gana mucho dinero. Sin embargo, el dinero recibido procede de negocios ilegales, y llevando a cabo la acción anteriormente mencionada, la víctima

de este fraude incurriría en un delito, lo que le causaría problemas con la ley (INCIBE, 2014c).

7 Fraudes en páginas de anuncios online

Es muy frecuente que a través de páginas de anuncios se lleven a cabo diversos fraudes. Por este mismo motivo, hemos intentado en el presente apartado dar una visión general de los fraudes más comunes que se cometen mediante estos anuncios fraudulentos.

Las características que suelen presentar estas estafas son las siguientes: el defraudador pide dinero por adelantado, el precio del producto es demasiado económico comparado con el valor del artículo, las fotografías son muy genéricas y suelen encontrarse en Internet, la redacción del artículo normalmente presenta errores gramaticales, el defraudador normalmente no se identifica u ofrece muy pocos datos personales, el delincuente explica que se encuentra en el extranjero y por este motivo es necesario un intermediario y por último el método de pago que recomienda no es el habitual (INCIBE, 2014d).

7.1 Fraudes en la compraventa de productos

Son muchos los casos en los que los delincuentes aprovechan Internet para engañar a los usuarios mediante la venta de productos falsificados o inexistentes utilizando técnicas de ingeniería social.

Es muy común que utilicen la buena fama de alguna empresa importante, como puede ser eBay, para ganarse la confianza de los usuarios. Estas empresas se declaran libres de responsabilidad: “[nombre de la empresa] no será responsable, indirecta ni subsidiariamente, de los daños y perjuicios de cualquier naturaleza derivados de la utilización de los Servicios y Contenidos del Portal por parte de los Usuarios o que puedan derivarse de la falta de veracidad, exactitud y/o autenticidad de los datos o informaciones proporcionadas por los Usuarios, o de la suplantación de la identidad de un tercero efectuada por un Usuario en cualquier clase de actuación a través del Portal” (INCIBE, 2013a).Son los usuarios los que han de ser más precavidos a la hora de efectuar compras online. Sin embargo, las empresas también deben intentar prevenir la comisión de este tipo de fraudes, proporcionando mecanismos de denuncia adecuados y colaborando con las Fuerzas y Cuerpos de Seguridad del Estado.

Además de aprovecharse de la fama de la que goza una empresa muy conocida, también puede darse el caso de que los estafadores creen sitios web fraudulentos en los que vendan todo tipo de productos inexistentes o con un valor muy inferior al que prometen tener. Ejemplos de este tipo de bienes son: vehículos, entradas de conciertos falsas, bisutería,

dispositivos tecnológicos, etcétera (INCIBE, 2013a). En este trabajo nos hemos centrado en la venta de vehículos y smartphones por ser los casos más numerosos.

7.1.1 Venta de vehículos

Según Capgemini, más del 90% de las personas que desean comprar vehículos, inician su actividad buscando anuncios en la red. Además, con la aparición de la crisis económica, cada vez son más frecuentes los anuncios en Internet sobre la venta de este tipo de productos. Por tanto, los delincuentes han aprovechado estos factores para llevar a cabo diversos fraudes que giran en torno a la venta de vehículos, especialmente de segunda mano. A continuación, explicaremos las circunstancias más frecuentes con las que nos podemos encontrar a la hora de ser víctimas de este tipo de fraudes. De este modo, seremos capaces de identificar este tipo de estafa a la vez que podremos evitar ser víctimas.

El esquema más típico es el siguiente: el usuario tras visitar una página de anuncios sobre la venta de vehículos en Internet, decide contactar con el anunciante porque la oferta le ha resultado interesante. El usuario recibe respuesta rápidamente, sin embargo, en la contestación se ofrecen datos muy genéricos. Además, es muy común que se le explique al usuario que el vehículo se encuentra fuera de España típicamente para justificar el bajo precio de este. Tras esta primera respuesta, al haber solo información genérica el interesado en el vehículo vuelve a contactar con el anunciante con la esperanza de que esta vez sus dudas van a ser aclaradas. Sin embargo, a los pocos minutos recibe otra contestación muy genérica, similar a una plantilla que se envía a todos los usuarios interesados en el vehículo. Por tanto, el usuario no recibe una respuesta a sus dudas. Esto debe ser un signo de alarma de que nos encontramos ante un fraude en Internet. Además de este esquema típico, las respuestas que recibe la víctima del supuesto propietario del vehículo gozan de las características que hemos explicado al iniciar el apartado de fraudes en páginas de anuncios online, tales como la presencia de errores gramaticales, el precio del vehículo es muy inferior comparado con el valor real que debería tener, etcétera (INCIBE, 2013c).

7.1.2 Venta de smartphones

Es muy frecuente encontrar anuncios en Internet que vendan este tipo de dispositivos. Sin embargo, muchos de estos casos destacan por ser fraudes. Un usuario desea comprar un smartphone. Tras una búsqueda en Internet encuentra una página web que le ofrece el mejor smartphone a un precio muy económico.

Al analizar el anuncio ya podemos observar algunas de las características típicas de los fraudes que se cometen mediante páginas de anuncios online: se promete el mejor producto a un precio muy bajo, no se facilita información sobre el vendedor y la descripción de que goza el producto es muy pobre. Al contactar el usuario con el anunciante, este le proporciona una respuesta rápida y con información muy genérica al igual que ocurría con los fraudes en la venta de vehículos. El usuario sigue estando interesado en el producto, y finalmente decide

realizar la transferencia bancaria para finalizar su compra online. Sin embargo, efectuada esta no recibe el smartphone y al contactar con el supuesto vendedor no recibe respuesta alguna (INCIBE, 2013a).

7.1.3 Subastas

Los fraudes en las subastas son uno de los medios más empleados por los delincuentes. El fraude se comete cuando el vendedor no cumple con lo prometido, ya que cobra el dinero de la víctima, pero no envía el producto que esta ha comprado. Este fraude también puede ser cometido por el comprador cuando utiliza medios de pago que en realidad no funcionan o emplea tarjetas bancarias robadas. En los fraudes en subastas, al conseguir el delincuente engañar a su víctima, está ya no podrá volver a recuperar el dinero perdido. Este fraude es muy sencillo y en palabras de INTECO "(...) es considerado por algunos como el rey de los engaños en Internet (...)" (INTECO, 2007, p. 34). Hay diversas variantes de fraudes en las subastas, de entre las cuales destacamos las siguientes:

- El fraude de los medios de pago "escrow": Con la finalidad de dar seguridad a las personas que realizan compras online, nacieron las empresas consignatarias. Estas empresas funcionan de la siguiente manera: el pago se efectúa a estas empresas y estas no le ofrecerán el dinero al vendedor hasta que el comprador no recibe el bien. Sin embargo, pronto los estafadores hicieron uso de esta situación para beneficiarse ellos mismos mediante la creación de falsas empresas consignatarias.
- El fraude de los servicios de paquetería: Después de efectuar una compra online normalmente a través de páginas de subastas, el ciberdelincuente contacta al comprador diciéndole que es el empleado de la empresa que le enviará el nuevo producto adquirido. Por este motivo, convence a la víctima a facilitarle diversos datos confidenciales, que serán utilizados por el defraudador con fines ilícitos.
- El fraude del reenvío: La víctima accede a una oferta de trabajo. Este empleo consiste en recibir diversos productos y enviarlos al extranjero. Sin embargo, la víctima pronto será avisada por las autoridades que está cometiendo un delito ya que dichos productos provienen de actividades ilegítimas, concretamente de compras mediante tarjetas de crédito robadas a través de Internet (INTECO, 2007).

7.2 Fraudes en el alquiler de viviendas

Este tipo de fraude aumenta cuando se acercan los períodos vacacionales. Generalmente se trata de anuncios en Internet. La víctima queda engañada porque el anuncio va acompañado de unas estupendas fotos, además de prometerle el estafador que el piso está situado en una zona céntrica y es muy económico.

Al contactar con el supuesto dueño del piso, es muy frecuente que este se muestre muy interesado, sin embargo, afirma que se encuentra fuera de España por lo que las llaves y el contrato del alquiler les serán enviados al usuario mediante una empresa de mensajería. El

único requisito para poder alquilar la vivienda es pagar una pequeña cantidad de dinero a modo de fianza, dándole la opción de efectuar el pago completo para poder obtener un descuento. Al efectuar la transferencia bancaria, la víctima de este fraude ya no tendrá noticias del supuesto arrendador (INCIBE, 2013b).

7.3 Préstamos de dinero a particulares

Este fraude tiene lugar principalmente en páginas web de anuncios. Las víctimas quedan engañadas por los delincuentes porque estos ofrecen préstamos de dinero a un interés mínimo. Esta estafa va dirigida especialmente a las personas que necesitan dinero para poder hacer frente a diversos pagos y a los que normalmente los bancos les han denegado un préstamo. Por tanto, es un fraude que se aprovecha de la situación económica actual de la víctima.

Las características comunes de estos anuncios son las siguientes: estos préstamos van dirigidos a personas con necesidades financieras, la cantidad prometida es muy elevada y además goza de un interés mínimo, la redacción del anuncio presenta errores gramaticales y por último destaca que la única forma de ponerse en contacto con el anunciante es vía correo electrónico (INCIBE, 2013d).

8 Fraudes en redes sociales. Especial referencia a la red social Facebook

Es difícil negar que estamos enganchados a las redes sociales. La mayoría de nosotros no podemos pasar por alto lo que está ocurriendo en Facebook, Instagram o Twitter, por citar solo los sitios más populares. Los delincuentes han aprovechado el gran uso que damos a estas redes sociales para cometer diversos fraudes. Somos muchos los que utilizamos estos medios sociales y prácticamente todos somos víctimas potenciales de las estafas que se cometen a través de estos. Por este motivo, hemos dedicado este apartado a explicar los fraudes más comunes que se cometen en las redes sociales, haciendo hincapié en Facebook por ser el sitio más popular.

Uno de los fraudes más frecuentes que se cometen a través de las redes sociales son los llamados cupones descuento. Los delincuentes engañan a sus víctimas diciendo que se regalan cupones descuento de diversas empresas con solo rellenar algunas encuestas. Finalmente solicitan al usuario que facilite diversos datos personales y el número de teléfono (ABC, 2015).

El phishing también tiene lugar a través de redes sociales. La finalidad que se busca es robar datos personales del usuario como son las contraseñas. Un ejemplo es el siguiente: el estafador envía un mensaje privado a su víctima, porque supuestamente se ha detectado una

actividad anómala en la cuenta. Por este motivo se le indica al usuario que ha de verificar las claves de acceso (INCIBE, 2016a).

También es muy frecuente el fraude a través de vídeos falsos. Hace poco circulaba por diversas redes sociales el vídeo “Girl is in critical condition after being forced to do this”, es decir “chica en estado crítico tras haberse visto forzada a hacer esto”. Al pinchar en el enlace, aparece un mensaje advirtiendo de imágenes explícitas y el usuario ha de confirmar que tiene más de trece años. Esta supuesta verificación de la edad no es real, sino que se trata de un robo de datos personales, como puede ser la dirección de correo electrónico, que después será vendida por los infractores a diversas empresas para que envíen spam.

Las invitaciones a juegos o a sorteos, diversos cuestionarios, concursos o simplemente un test de personalidad son algunos de los medios de los cuales los delincuentes se aprovechan para llevar a cabo las acciones ilícitas a través de las redes sociales. Un ejemplo es el siguiente: “¿Qué tipo de personaje de STAR WARS es usted? ¡Averígüelo con nuestro cuestionario! Todos sus amigos lo hicieron”. Si el usuario intenta realizar el cuestionario, se le solicita el número de teléfono. Una vez facilitado, se le suscribe al servicio de SMS Premium[12], cuyos mensajes tienen una tarificación especial (Symantec Corporation, 2012).

Como bien sabemos una de las redes sociales más populares en la actualidad es Facebook. Por este motivo, explicaremos a continuación los fraudes más comunes con los que nos podemos encontrar en este sitio con la finalidad de evitar ser víctimas.

Una de las estafas más comunes a través de Facebook son los típicos fraudes románticos. Los delincuentes envían todo tipo de mensajes a personas que no conocen, durante un tiempo relativamente largo, porque su finalidad es ganarse la confianza de su víctima para que esta posteriormente le envíe dinero para un supuesto viaje o por otros motivos. Los defraudadores suelen engañar a su víctima diciéndole que están divorciados, viudos o que se encuentran en un matrimonio inestable. Además, es muy común que utilicen fotos descargadas por Internet. Si la víctima queda engañada, finalmente esta le enviará una suma de dinero por diversos motivos que el estafador se inventa.

Otros ganchos utilizados por los estafadores son usurpar el perfil de Facebook de una persona del vínculo de amigos de la víctima o crear un perfil falso que supuestamente representa a una institución legítima. El usuario recibirá un mensaje en el cual se afirma que ha ganado un premio y que para poder cobrarlo ha de pagar una pequeña cuota por adelantado. También pueden enviar mensajes en los que piden donaciones en nombre de

[12] Los SMS Premium son un servicio de mensajería con una tarifación mayor que la de un SMS estándar, mediante el cual la persona suscrita goza de algunos beneficios: acceso a música, juegos, participar en diversos concursos, etcétera. Sin embargo, los usuarios no son conscientes de su alta en este servicio y del coste que este supone.

alguna institución. Las personas que los reciben pueden quedar engañadas y facilitar dichas donaciones.

Otra estafa que puede cometerse a través de esta red social son las típicas herencias. En este caso, el defraudador afirma ser un abogado que gestiona la herencia de una persona fallecida. Le envía mensajes a la víctima diciéndole que tiene derecho a la herencia. Para ello, solo ha de proporcionar diversos datos personales (Facebook, 2016).

Hace poco que veíamos en este medio social anuncios parecidos a este: "¡Cambia el color de tu Facebook!". Mediante estos anuncios se anima a los usuarios a cambiar el color azul de su Facebook a otro con la ayuda de una aplicación. Se le engaña a la víctima que si comparte quince veces el mensaje, podrá lograr cambiar el color de su perfil de Facebook. Sin embargo, la aplicación le pedirá que introduzca información confidencial (INCIBE, 2015a).

Otro fraude común que tiene lugar a través de esta conocida red social es "Hackear Facebook". Esta estafa se lleva a cabo mayoritariamente mediante ciertas aplicaciones. Si una persona intenta hackear alguna cuenta de Facebook mediante este tipo de aplicaciones, estas le avisarán que necesitan verificar que se trata de una persona real, por lo que le facilitan un link para introducir cierta información personal, datos que serán utilizados posteriormente por los ciberdelincuentes para lucrarse mediante actividades ilícitas (Proaño Alcívar, 2015).

9 Fraudes en teléfonos móviles

9.1 Los SMS Premium. Especial atención a la aplicación WhatsApp

Actualmente es muy frecuente utilizar aplicaciones como WhatsApp o Telegram para enviar mensajes a través del móvil a nuestros contactos. Por tanto, cada vez es menos habitual el uso de los antiguos SMS. Los delincuentes se aprovecharon del excesivo uso que los usuarios les daban a los mensajes de texto para cometer diversos fraudes mediante el servicio de SMS Premium. Sin embargo, al haber una notable disminución en el empleo de los SMS, los delincuentes se vieron obligados a encontrar otro método para cometer estos fraudes. Así, aunque el usuario no utiliza directamente los mensajes de texto para comunicarse, los infractores volvieron a inventar un método mediante el cual poder utilizar el servicio de SMS Premium para defraudar a sus víctimas: las aplicaciones de mensajería instantánea.

Por tanto, el elevado uso de las nuevas aplicaciones es aprovechado para generar aplicaciones estafa, que utilizan la fama de una empresa conocida, como puede ser WhatsApp o Telegram, para engañar a las víctimas prometiéndoles una funcionalidad que a esta le podría interesar a cambio de facilitar el número de teléfono. Si el usuario es víctima

de este engaño, se le dará de alta en el servicio de SMS Premium, que le mandará muchos mensajes con un coste elevado (INCIBE 2012).

Los delincuentes han aprovechado el elevado número de usuarios de los que goza WhatsApp para llevar a cabo sus actividades ilícitas, lo que ha generado la comisión de varios tipos de defraudaciones vía esta app, especialmente estafas haciendo uso de los servicios de SMS Premium. Pasaremos a continuación a explicar los fraudes más comunes que se han dado a través de WhatsApp, la mayor parte de los cuales tienen en común que se le engaña a la víctima para que facilite su número de teléfono, después de lo cual será suscrita a servicios de SMS Premium que tienen una tarificación especial.

Cuando WhatsApp lanzó su versión para navegadores, los estafadores pronto generaron sitios web fraudulentos, cuya finalidad era conseguir el número de teléfono del usuario para un servicio de tarificación especial o hacer que la víctima se descargue una supuesta aplicación, que en realidad se trata de un troyano mediante el cual se puede tener acceso a datos personales ajenos.

Los defraudadores han utilizado el lanzamiento que hizo WhatsApp de su conocido doble check azul a su favor, prometiendo a los usuarios diversos servicios que les permita desactivar esta función. Sin embargo, la persona que decidía utilizar estos servicios no conseguía eliminar el doble check azul. Lo que sí obtenía era suscribirse a un servicio de SMS Premium sin su voluntad. Actualmente, es la propia aplicación la que permite desactivar esta función, con lo que no hay motivo alguno en ser víctima de este fraude.

La Policía Nacional y la Guardia Civil avisaban hace unos meses de un nuevo fraude que tiene lugar mediante diversos mensajes propagados en redes sociales: el llamado WhatsApp Oro. Se invita a los usuarios a hacer clic en un link para conseguir actualizar su aplicación de WhatsApp a la nueva versión WhatsApp Oro, en realidad inexistente. Si la persona pincha en el enlace, se le avisa que para poder disfrutar de todas las facilidades que esta nueva versión le ofrece, solo tiene que facilitar el número de teléfono (Panda Security, 2015). Otra estafa similar a las anteriores es WhatsApp Spy, que promete ser una aplicación que una vez descargada te permite ver conversaciones ajenas. Evidentemente esto no es posible y lo único que conseguirá la víctima es suscribirse sin su voluntad a un servicio de tarificación especial.

Otro ejemplo de fraude es el falso contestador de WhatsApp. Este fraude tiene lugar mediante un correo electrónico que recibe el usuario, en el que se le avisa que tiene un mensaje en el contestador de WhatsApp, servicio inexistente. La finalidad de este fraude es infectar con malware el ordenador del internauta o inscribirlo a servicios de SMS Premium.

Recientemente, la Policía Nacional y FACUA (Federación de Asociaciones de Consumidores en Acción) advertían de la estafa del falso cupón de McDonald’s que circula por WhatsApp. La finalidad es robar información personal y suscribir a la víctima a un servicio de tarificación especial. El fraude consiste en un mensaje enviado a través de WhatsApp que

promete al usuario que al completar una miniencuesta de cuatro preguntas, recibirá un cupón para comer gratis en McDonald's. Tras completar dicha encuesta, se engaña al usuario que para recibir el cupón ha de compartir el mensaje con diez amigos o tres grupos. De esta manera, se propaga el fraude (El País, 2016a).

El fraude más actual que se ha venido cometiendo a través de esta aplicación de mensajería instantánea es la promoción del supuesto nuevo servicio, videollamadas. Aunque se espera que pronto WhatsApp ofrecerá esta función, a fecha de hoy este servicio no está activado. El fraude consiste en recibir un mensaje por WhatsApp en el que se ofrece al destinatario activar las videollamadas. En dicho mensaje, aparece un enlace que simula estar verificando la versión de WhatsApp, además de pedir al usuario que comparta el mensaje recibido ya que de lo contrario es imposible activar la nueva función. Así es como se propaga el fraude. Después de difundir el mensaje, el usuario puede pinchar en la opción de "Descargar videollamadas" y en ese momento se le informa que es necesario introducir su número de teléfono (El País, 2016b).

9.2 Spim

El spim es muy similar al spam que nos llega a través del correo electrónico. Sin embargo, estos dos se diferencian por el medio que utilizan: los mensajes de spim nos son enviados mediante aplicaciones de mensajería instantánea como pueden ser WhatsApp o Line, mientras que el spam utiliza el correo electrónico.

Por tanto, el spim es un fraude online que tiene lugar mediante aplicaciones automatizadas que obtienen direcciones de contactos de nuestras aplicaciones de mensajería instantánea. Los mensajes aparecen en forma de ventanas emergentes o de texto añadido en las conversaciones. También se facilitan unos enlaces, que al pincharlos nos llevan a páginas web fraudulentas. El spim tiene lugar cuando el dispositivo ha sido infectado con malware o cuando el usuario ha añadido algún desconocido en su lista de contactos.

Un ejemplo de spim es el siguiente: "¿Quieres ganar un viaje a Londres con todos los gastos pagados? ¡Haz clic en el siguiente enlace y participa!". El spim es más difícil de detectar que el spam, porque cuando nos llega un correo electrónico de spam lo podemos identificar antes de abrirlo y eliminarlo, sin embargo, los mensajes de spim generalmente nos llegan mientras estamos manteniendo una conversación con algún conocido nuestro y por tanto caemos en el error de creer que el mensaje y el link fueron enviados por la persona con la que estábamos conversando.

La finalidad de este fraude es engañar al usuario para que pinche en el link fraudulento que aparece en los mensajes, ya que si esto ocurre la víctima se descarga en su dispositivo troyanos o virus, mediante los cuales los delincuentes que están detrás del spim podrán tener acceso a la información confidencial de la víctima (INCIBE, 2014e).

9.3 Vishing

El vishing[13] es un fraude que se lleva a cabo a través de los dispositivos móviles. Para su comisión se utiliza el Protocolo Voz sobre IP (VoIP) y técnicas de la ingeniería social. Los delincuentes utilizan este protocolo para ganar la confianza de sus víctimas, ya que esta voz automatizada es muy similar a las empleadas por las entidades financieras.

Este tipo de fraude ha existido desde hace muchos años, sin embargo, el avance de la tecnología ha hecho que los defraudadores puedan llevar a cabo esta estafa sin preocuparse apenas por ser descubiertos, porque al utilizar el Protocolo Voz sobre IP se puede ocultar fácilmente la dirección física de donde se ha efectuado la llamada ya que se puede realizar desde cualquier ordenador alrededor del mundo. Además, mediante el uso de esta tecnología el coste de la llamada es muy bajo, lo que ha contribuido a un mayor uso de este método ya que los que están detrás de estas fechorías, pueden hacer uso de esta técnica con un coste mínimo.

Este fraude tiene lugar de la siguiente manera: se marcan de forma aleatoria algunos números de teléfono hasta que una persona contesta. A esta se le engaña diciéndole que su tarjeta de crédito está siendo empleada ilegalmente, que sus datos personales necesitan ser actualizados, que se ha detectado algún problema con su cuenta bancaria, etcétera. Con la finalidad de solventar estas cuestiones, se le facilita a la víctima un número de teléfono. Al llamar, lo que se escucha es una grabación que le solicita a la víctima información bancaria (Amanor & Yeboah-Boateng, 2014).

10 Fraudes en la publicidad online

La publicidad engañosa es uno de los orígenes de fraudes online más frecuentes, y los banners publicitarios son un elemento que los infractores utilizan a menudo para llevar a cabo sus actividades ilícitas. Los banners suelen ser muy llamativos y se integran dentro de los sitios web, comúnmente en la parte superior o lateral. Estos han evolucionado y además de la típica imágen estática con texto, pueden incluir audios o vídeos. La información que incluyen puede ser engañosa o no. El fraude en este campo puede llegar a causar pérdidas multimillonarias al año (INCIBE, 2016b).

El tipo de fraude que se comete con más frecuencia es el tráfico de robots o también denominado tráfico no humano generado por botnets. Estos bots pueden ser fáciles de detectar si se trata de botnets sencillos que se ejecutan desde direcciones fijas. Sin embargo, estos también pueden gozar de unas secuencias muy complejas y por tanto pueden llegar a controlar un ordenador que previamente ha sido infectado con malware. El tráfico de robots tiene como finalidad diluir el valor del inventario real del anunciante, ya que los botnets

[13] El término *Vishing* proviene de la unión de dos palabras inglesas: *voice* y *phishing.*

generan visitas falsas a los anuncios publicitarios y estas se mezclarán con las visitas reales. Al mezclarse las visitas auténticas y las simuladas se produce un error en el inventario del anunciante, y por tanto este llega a pagar una suma de dinero al delincuente por sus visitas falsas.

Además del tráfico no humano, este fraude también se comete mediante impresiones no visibles, es decir anuncios que ocupan muy pocos pixels y por esta razón no llegan a ser visibles para el ojo humano. Otra modalidad muy similar el el denominado ad stacking, que consiste en incluir banners superpuestos, de forma que solo sea visible el último. Por tanto, aunque los usuarios no llegan a ver los anuncios por ser estos muy pequeños o por haber varios anuncios superpuestos y poder ver solo el último, las visitas de las personas contarán como impresiones para los anunciantes (Matarranz, 2016). También existen otras técnicas que tienen que ver con la suplantación de sitios y visitantes, como pueden ser ad injection o domain spoofing.

El ad injection viene a ser un malware que se instala en nuestro ordenador o smartphone de forma ilegal. Este malware muestra al usuario publicidad de diversos sitios y le cobra por dichas visualizaciones al anunciante. El domain spoofing es una técnica que utilizan los publicadores. Estos muestran la publicidad de los anunciantes, sin embargo, no utilizan el dominio del anunciante, sino que usan otro que goza de más visitas. Por tanto, el anuncio recibe más visitas, sin embargo, al utilizar otro dominio, estas visitas no son reales (Marketech forum, 2015).

Es también interesante comentar en este apartado el pago por clic (PCP) o Pay Per Click en inglés, ya que este puede ser utilizado por los defraudadores para cometer la estafa online conocida en lengua inglesa bajo el nombre de click fraud. El PCP es un tipo de publicidad online en el que el anunciante paga a una página web para que presente sus anuncios. Este pago se basa en la cantidad de veces que los visitantes del sitio web hacen clic en el anuncio. Por tanto, la página web es el espacio publicitario y el anunciante es el demandante del espacio publicitario para poder promocionar sus productos (Bernard Jansen, 2007).

El fraude por clic o click fraud es una actividad ilícita que tiene lugar en Internet, concretamente en los formatos de publicidad online de pago por clic. Este fraude consiste en que una persona o un sistema automatizado sin estar interesado en el producto que se publicita hace clic en un anuncio online, generando de esta forma un coste para el anunciante. En estos casos, al no estar la persona que hace clic en la publicidad o el sistema automatizado interesados en el producto que se anuncia, se produce un cargo al anunciante por cada clic causándole una pérdida económica. Una de las principales finalidades de este fraude es beneficiar a los sitios web en donde se encuentran los anuncios publicitarios porque con esta práctica se genera un aumento de las comisiones que han de pagar los anunciantes a estas páginas web. Otra finalidad del click fraud es perjudicar al anunciante porque mediante este fraude, este tendrá un mayor gasto publicitario sin ganar ningún tipo de beneficio. En este

último caso el que comete el fraude evidentemente es la competencia de la empresa que ha publicado los anuncios (Microsoft Corporation, 2016).

11 Fraudes en programas informáticos

11.1 Ransomware

NIST[14] nos proporciona la siguiente definición de ransomware[15]: el uso de malware con el fin de bloquear el acceso a ordenadores o datos hasta que un pago es efectuado (NIST, 2011). Normalmente reclaman al usuario la comisión de una acción ilegal con su ordenador y por este motivo afirman que tiene que pagar una multa. Sin embargo, estas afirmaciones son completamente falsas y aunque el usuario llega a satisfacer la supuesta sanción o llega a hacer lo que el ransomware le demanda, no hay ninguna garantía de que el usuario volverá a tener acceso a su ordenador (Microsoft Corporation, 2015).

Podemos clasificar el ransomware en ransomware de cifrado y de bloqueo. En el ransomware de cifrado, destaca el Cryptlocker por ser el más conocido. Al infectar el sistema, el ransomware de cifrado procede a efectuar una búsqueda por todas las unidades accesibles con la finalidad de cifrar los ficheros. Al realizar este cifrado, presenta un mensaje al usuario advirtiéndole del cifrado de sus archivos e indicándole que ha de pagar para poder volver a tener acceso a estos. Al efectuar el pago, que generalmente se lleva a cabo mediante bitcoin[16], supuestamente se le facilitará al usuario la clave privada RSA.

El ransomware de bloqueo es un malware que imposibilita el uso del ordenador de la víctima hasta que esta no satisface el pago del rescate. Un ejemplo típico de este tipo de ransomware es Reveton, conocido también bajo el nombre de “virus de la policía”. La técnica más utilizada es utilizar una pantalla en la que se anuncia al usuario que ha cometido algún delito (destaca la descarga de pornografía ilegal) y por este motivo ha de proceder al pago de una multa. Este método ha ido evolucionando con el tiempo, y por tanto se ha conseguido que la pantalla que presenta el aviso al usuario, pueda adaptarse en función del país de que se trate, consiguiendo utilizar el idioma local y presentando diversas imágenes que

14 National Institute of Standards and Technology

15 La palabra *ransomware* se forma al juntar *ransom* (en inglés se traduce como secuestro) y el sufijo *ware* que se emplea para hablar de un componente informático como por ejemplo el hardware o software.

16 Bitcoin tiene su origen en el año 2009 cuando Satoshi Nakamoto, pseudónimo de una o varias personas, decidió lanzar una nueva moneda electrónica cuya peculiaridad es que solo servía para poder realizar operaciones dentro de la Red.

representen a las fuerzas del estado correspondientes con la finalidad de conseguir que el usuario confíe en dichos avisos (INCIBE, 2015b).

Por tanto, hay muchos tipos de ransomware, sin embargo, todos tienen un denominador común: todos impiden al usuario a utilizar su ordenador de forma normal y con la excusa de poder volver a tener acceso a los archivos del ordenador o al sistema operativo, el ransomware pide al usuario pagar una determinada cantidad de dinero (Microsoft Corporation, 2015).

11.2 Falsos antivirus

Este fraude consiste en convencer al usuario de que su ordenador está infectado con software malicioso y que para solucionar el problema es necesaria la instalación de programas específicos de seguridad que los puede adquirir pagando una cantidad de dinero. Este fraude online tiene como finalidad vender a los usuarios soluciones falsas de seguridad y adquirir los datos de las tarjetas de crédito de los internautas.

Para conseguir sus objetivos, los delincuentes hacen uso de mensajes de error, anuncios falsos utilizando ventanas emergentes o resultados de falsos análisis similares a los de antivirus legítimos. Convencen a los usuarios que la infección con malware de su ordenador, que puede existir o no, solo se puede solventar mediante la adquisición de los antivirus que ellos recomiendan.

La víctima de este fraude compra el falso antivirus utilizando la tarjeta de crédito, y por tanto los que están detrás del delito consiguen los datos bancarios del usuario además de quedarse con el dinero facilitado por la víctima a la hora de la adquisición de la supuesta herramienta de seguridad. Es importante destacar el hecho que la instalación del falso antivirus puede ser aprovechada por los estafadores para instalar algún tipo de código malicioso en el ordenador de la víctima (INTECO-CERT, 2008).

Por tanto, mediante este fraude los delincuentes consiguen de sus víctimas una cantidad de dinero tras la compra del falso antivirus, sus datos de la tarjeta bancaria, además de tener la posibilidad de infectar el ordenador con código malicioso tras la instalación de la herramienta de seguridad ilegítima.

Los métodos que se emplean para hacer llegar los falsos avisos y mensajes de error a los usuarios son: una infección previa del ordenador de la víctima, que en numerosas ocasiones es inofensiva ya que puede tener como única finalidad asustar al propietario del ordenador para que compre el falso antivirus, o mediante la visita de una página web fraudulenta por parte del propio internauta (Panda Security, 2009).

A continuación, explicaremos un ejemplo para ver de una forma más clara el *modus operandi* de los delincuentes. El usuario recibe un correo electrónico o un mensaje a través de una aplicación de mensajería instantánea. En dicho mensaje aparece un enlace. Se engaña al internauta que al pinchar en la URL podrá descargar un antivirus. Al acceder al

enlace, se inicia un supuesto análisis en línea del ordenador. El resultado es que la máquina está infectada por numerosos virus. Se le informa al usuario que, para poder solventar el problema, es necesario un antivirus, que podrá ser instalado tras el pago de una determinada cantidad de dinero. Para ello, se redirecciona al internauta a una página web en la cual se le solicitan los datos bancarios. Es en este momento cuando los datos confidenciales de la tarjeta bancaria de la víctima son facilitados a los delincuentes ya que se solicita el CVC2 que permitirá a los que están detrás del fraude realizar cargos a la tarjeta bancaria sin ser necesaria la aprobación del dueño de la cuenta (INTECO-CERT, 2008).

12 Delito de estafa

Antes del Código Penal de 1995, la mayor parte de los delitos referentes a la informática no se castigaban, sin embargo, nuestro actual Código Penal sí que contempla delitos cometidos a través de la informática.

La limitación más importante del Código Penal anterior era que no se podía aplicar la norma penal a bienes intangibles, solo se podía aplicar esta a bienes u objetos físicos. En el Código Penal de 1995 se empezó a regular también bienes intangibles como los datos informáticos. Por ejemplo, se introducen tipos penales como el descubrimiento de secretos o el espionaje industrial. Por tanto, tuvo lugar un cambio importante y se observaba que cada vez era más necesario regular el fraude informático de forma específica, ya que este no se podía subsumir en el tipo básico de estafa.

La figura básica del delito de estafa se encuentra regulada en el artículo 248.1 del Código Penal, el cual establece que “cometen estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno” (BOE, 2015). Por tanto, los elementos del tipo básico son: ánimo de lucro, engaño bastante, error, acto de disposición en perjuicio propio o ajeno, y por último una relación motivacional entre los elementos mencionados (Orts Berenguer, González Cussac, Matallín Evangelio & Roig Torres, 2010).

El elemento de engaño es el que causa problemas a la hora de subsumir la estafa informática en el tipo básico de estafa, ya que no se puede engañar a una máquina; solo se puede manipular esta para producir un error en las personas. La estafa llevada a cabo mediante medios informáticos tampoco podría subsumirse en los tipos penales de hurto o apropiación indebida, por lo que se introdujo el apartado a) en el artículo 248.2 del Código Penal. El artículo 248.2 a) sanciona a las personas que “con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante consigan la transferencia no consentida de cualquier activo patrimonial en perjuicio de otro” (BOE, 2015). Es una variante del tipo básico de estafa en la que ocurren varios elementos de esta: ánimo de lucro, transferencia de un activo patrimonial en perjuicio de un tercero, y una relación de causalidad entre la

manipulación informática o artificio semejante y la transferencia bancaria (Orts Berenguer et al., 2010).

El legislador introdujo la figura del fraude informático en el art. 248.2.a) del Código Penal, porque era necesario un tipo penal que pueda castigar los casos en los que no podía darse un elemento esencial del tipo básico de estafa, como es el engaño ya que una máquina no puede ser engañada.

Un aspecto esencial es saber qué conductas se pueden subsumir en la estafa penal, ya sea la estafa común o informática. Anteriormente hemos mencionado los elementos básicos de la estafa común. El problema aparece cuando algunos de los elementos básicos de la estafa no pueden darse, como pueden ser el engaño y el error (González Suárez, 2014).

Los fraudes a través de correos electrónicos mediante los cuales se consigue engañar a la víctima a realizar una transferencia patrimonial, son casos que se subsumen en el tipo básico de estafa del artículo 248.1 CP ya que hay una transferencia autorizada, aunque sea debida a un engaño (Miró Linares, 2013). Los fraudes en la compraventa de productos en los que el comprador no recibe el bien o el vendedor no recibe el dinero, y los fraudes en subastas también entran en el tipo básico de estafa. Por tanto, los casos en los que se dan todos los elementos de la estafa se englobarían en el tipo básico de estafa.

Sin embargo, los supuestos en los que no se dan los elementos básicos de engaño y error, es cuando debemos estudiar si estos son susceptibles de subsunción en el tipo básico, o por el contrario en la estafa informática del artículo 248.2 a) del Código Penal en el que tiene lugar una manipulación informática.

En los supuestos de spyware en los que la víctima no recibe de forma directa un mensaje, sino que el estafador se beneficia económicamente en perjuicio de la víctima mediante un programa informático, no podemos hablar de engaño y error, por lo que se subsumiría el hecho en la estafa informática del 248.2 a) (González Suárez, 2014).

Los casos de phishing, en los que el estafador manda un mensaje mediante correo electrónico, redes sociales o medios similares a un grupo de personas sin especificar (sujeto pasivo masa del artículo 74.2 CP), también se subsume en el delito de estafa informática. Actualmente, la mayor parte de la doctrina considera que la página web fraudulenta que se utiliza para averiguar los datos bancarios de la víctima, a causa del uso de un determinado lenguaje informático en su confección, debe ser considerada como un programa informático. Los phishers lo que consiguen son los datos bancarios, no una transferencia bancaria consentida de parte de la víctima como pasaba en los fraudes a través del correo electrónico. Estos datos bancarios los utilizarán para llevar a cabo una transferencia patrimonial no consentida. Por tanto, el phishing se considera una estafa informática del artículo 248.2 a) CP (Miró Linares, 2013).

Además de lo comentado anteriormente, hay otros artículos en el Código Penal que regulan el delito de estafa. El artículo 248.2 CP b) castiga a “los que fabricaren, introdujeren,

poseyeren o facilitaren programas informáticos específicamente destinados a la comisión de las estafas previstas en este artículo" (BOE, 2015). Como observamos no se exige el ánimo de lucro. Si se encuentran programas informáticos que podrían ser utilizados para cometer una estafa, pero no están específicamente diseñados para tal fin, no se está ante la conducta típica (Orts Berenguer et al., 2010).

El artículo 248.2 c) CP castiga a "los que, utilizando tarjetas de crédito o débito, o cheques de viaje, o los datos obrantes en cualquiera de ellos, realicen operaciones de cualquier clase en perjuicio de su titular o de un tercero".

El siguiente artículo, el 249 CP, establece la pena que se impondrá a las personas que han incurrido en un delito de estafa, tanto del tipo básico como fraude informático. Este artículo fue modificado por la Ley Orgánica 1/2015, de 30 de marzo. Esta reciente reforma introduce la pena de multa de uno a tres meses para el llamado delito leve (cuando la cuantía de lo defraudado no excediere de 400 euros). Por tanto, la falta pasa a ser delito leve. En los demás casos, es decir cuando la cuantía es superior a 400 euros, se impondrá la pena de prisión de seis meses a tres años (BOE, 2015).

El siguiente artículo, el 250 CP, establece las agravaciones del delito de estafa, tanto del tipo básico como de las estafas informáticas. Este artículo también ha sido modificado por la Ley Orgánica 1/2015, de 30 de marzo. Tras esta reciente reforma, el artículo 250.1 CP se compone de ocho numerales, antes eran siete. Los primeros cuatro no se han cambiado, sin embargo, el quinto se ha modificado para añadir la alternativa de que lo defraudado afecte a un elevado número de personas. Los numerales 6 y 7 no se han modificado. El número 8 es nuevo, antes no existía. Establece la siguiente circunstancia agravante: "al delinquir el culpable hubiera sido condenado ejecutoriamente al menos por tres delitos comprendidos en este Capítulo. No se tendrán en cuenta antecedentes cancelados o que debieran serlo" (BOE, 2015).

El artículo 250.2 CP goza de dos novedades tras la última reforma. Por una parte, eleva la pena también cuando concurra la circunstancia 1ª con el numeral 7º. Antes de la reforma, solo se preveía esta agravante al concurrir la circunstancia 1ª con alguno de los numerales del 4º al 6º; después de la reforma se incluye también la concurrencia de la circunstancia 1ª con la 7ª. Por otra parte, otra novedad que incluye la LO 1/2015, de 15 de marzo es que se impondrá la pena establecida en el artículo 250.2 CP cuando la estafa alcance los 250.000 euros (BOE, 2015).

En el artículo 251 CP se establecen una serie de estafas específicas (Orts Berenguer et al., 2010). Este artículo no se ha visto modificado tras la nueva reforma. Por último, es

importante mencionar que este delito lo pueden cometer también las personas jurídicas según el artículo 251 bis CP, artículo introducido por la LO 5/2010, de 22 de junio (BOE, 2015).

13 Medidas de prevención

El objetivo del presente apartado es proporcionar los consejos y las medidas de seguridad adecuadas para una eficaz prevención de los fraudes informáticos. Por tanto, se intenta dar las pautas necesarias para impedir en la medida de lo posible ser víctima de un fraude informático.

El Grupo de Delitos Telemáticos (GDT) de la Guardia Civil nos proporciona los siguientes consejos de seguridad con la finalidad de evitar ser objeto de un delito informático:

- Es preferible actualizar el sistema operativo y el software instalado, sobre todo cuando se trata del navegador web que utilizamos. Además, se ha de utilizar un software legal y evitar descargar programas de sitios web sospechosos, ya que detrás de la palabra "gratis" se encuentran fuentes de malware. Así mismo, es aconsejable realizar copias de seguridad del sistema con el fin de no perder los datos almacenados por incidentes de seguridad.
- Las contraseñas que usamos deberían tener más de ocho caracteres combinando números, letras, mayúsculas y caracteres especiales. De este modo, conseguiremos proteger nuestra identidad. Debemos sospechar de los correos electrónicos en los que aparecen mensajes atractivos y además nos piden que los reenviemos a nuestra lista de conocidos, ya que, mediante un mensaje similar, generalmente lo que los ciberdelincuentes buscan es conseguir más direcciones de correo electrónico para llevar a cabo sus fechorías. Además, si los correos que nos llegan tienen un emisor desconocido, es aconsejable eliminarlos directamente sin leer el contenido.
- Es conveniente trabajar con una cuenta de usuario que no goza de privilegios de administrador, porque de esta forma se puede impedir la instalación de programas maliciosos. Además, hay que tener cuidado con las redes P2P, porque son una fuente importante de descarga de malware.
- Es aconsejable realizar la compra online de sitios con acreditada reputación. No hay que caer en el engaño de las súper ofertas, porque estas suelen ser un fraude. Para asegurarse que los vendedores y los anuncios son de confianza, se aconseja buscar referencias de los mismos en la World Wide Web[17]. Además, se debe tener cuidado con los vendedores que sostienen vivir en el extranjero y prefieren el pago

[17] World Wide Web es un sistema de información compuesto de un número indeterminado de páginas (páginas web), que contienen enlaces que al ser activados por el usuario conducen a otras páginas.

del producto a través de sistemas tipo PayPal, que ofrecen al delincuente un gran anonimato. Debemos de tener en cuenta que las empresas serias gozan de su propio dominio, y por tanto no envían correos con los dominios de Gmail, Hotmail o Yahoo. Las herencias, loterías, premios, inversiones millonarias o negocios piramidales son estafas, por lo que no hay que creer los mensajes que nos aseguran la riqueza mediante estos métodos.

- Muchos de los fraudes en Internet se llevan a cabo usurpando la identidad de entidades bancarias. Por lo tanto, hay que tener cierta precaución. Los consejos que nos proporciona la GDT de la Guardia Civil en este sentido son los siguientes: no debemos acceder a la web del banco a través de enlaces que nos son proporcionados mediante un mensaje de correo electrónico, es aconsejable verificar si el banco utiliza el protocolo criptográfico SSL/TLS[18] para proporcionar una comunicación segura (https), no debemos olvidarnos de cerrar la sesión al salir de la página web del banco y por último desconfiar de todos los correos electrónicos y SMS cuyos emisores sean entidades bancarias.
- En redes sociales, es aconsejable limitar el acceso de la información, ya que si solo tienen acceso a la misma las personas conocidas hay menos riesgo de ser víctima de un fraude online. Hay que tener cuidado a la hora de suscribirse a grupos o eventos en las redes sociales porque no podemos saber con certeza a qué personas les estamos facilitando nuestra información personal. También es aconsejable utilizar la navegación segura mediante https para prevenir el robo de contraseñas y otros datos confidenciales (GDT, 2011).

Symantec Corporation nos proporciona algunos consejos de cómo actuar si cualquier usuario es víctima de este tipo de delitos. Así, el primer paso que ha de hacer es acudir a la policía para presentar una denuncia. Además, es aconsejable cerrar las cuentas bancarias afectadas inmediatamente, cambiando o cancelando las tarjetas de crédito o bancarias para que el delincuente no pueda hacer uso de las mismas. Así mismo, es conveniente preguntar a los trabajadores de la institución financiera de las posibles consecuencias y de las actuaciones que la persona objeto del fraude puede realizar al verse su cuenta bancaria afectada tras el fraude online. La víctima debería ponerse en contacto con una de las tres agencias nacionales de verificación de crédito para consumidores, Equifax, Experian o TransUnion, ya que al comunicarse con alguna de estas, se les avisará inmediatamente a los

[18] El protocolo SSL (*Secure Sockets Layer*, en español Capa de Conexiones Seguras) fue desarrollado en los años 90 por la empresa *Netscape Comunications Corporation*. Lo crea con el fin de obtener comunicaciones seguras en la red. El protocolo SSL es un protocolo criptográfico que tiene por finalidad proporcionar confidencialidad, integridad y autentificación de la información en una comunicación cliente-servidor.

acreedores que tienen que ponerse en contacto con la víctima antes de realizar algún tipo de modificación en las cuentas bancarias.

También sería de gran ayuda que el usuario solicite sus informes de crédito a las tres agencias citadas para poder llevar a cabo un examen exhaustivo de los mismos en búsqueda de anomalías. Si se realizan estas comparaciones entre los informes de crédito de las tres agencias, se puede comprobar si en cada uno de ellos se reflejan los mismos datos y movimientos, pudiendo observar si hay alguna diferencia en la información que cada informe aporta. Se puede sospechar que los últimos movimientos realizados son de procedencia ilícita.

Por último, es importante que la víctima busque indicios de robo de identidad, observando si recibe algún envío postal que no haya solicitado, si determinados proveedores le comunican algún asunto sobre cuentas bancarias de las que no tiene conocimiento o si se le solicita el ingreso de una determinada suma de dinero por compras que no haya realizado. Estos son claros indicios de problemas relacionados con el robo de identidad (Symantec Corporation, 2015).

14 Impacto

El presente apartado tiene como finalidad observar la realidad de esta problemática a través de estadísticas, porque mediante este método seremos capaces de comprender de una forma más clara el auge que está teniendo este tipo de delincuencia. Además, proporcionaremos diversos datos para entender el impacto económico que tienen los delitos en Internet a escala global. Tras el año 2011, la Fiscalía General del Estado crea un área especializada en criminalidad informática, porque es evidente el incremento de los procedimientos incoados en estos delitos (Torres-Dulce Lifante, 2014).

A continuación, vamos a observar el notable aumento de estos procedimientos que ha tenido lugar en los últimos años en España mediante diversos datos estadísticos proporcionados por la Fiscalia General del Estado. Para conseguir estos datos estadísticos hemos hecho uso de las Memorias de la Fiscalía General del Estado, sin embargo, consideramos importante mencionar que la información son datos orientativos ya que somos conscientes que la cifra negra[19] en estos casos es muy elevada.

El total de procedimientos incoados en materia de delincuencia informática en el año 2011 fue de 6.532, mientras que en el año 2012 fue de 7.957. Por tanto, ha habido un aumento de 21,82% entre 2011 y 2012. En el año 2011, se han registrado un total de 4.204 procedimientos incoados por delitos de estafa informática. El siguiente año esta cifra experimenta un aumento

[19] Este término, cifra negra, se utiliza en Criminología para hacer referencia a la cantidad de delitos que no se reflejan en las estadísticas generalmente por la falta de denuncia por parte de las víctimas.

notable, ya que se han registrado 5.992 procedimientos incoados por este delito (Torres-Dulce Lifante, 2014).

Para cumplir con el objetivo del presente apartado y para conseguir comprender más fácilmente la realidad del problema, hemos incluido dos cuadros aportados por las Memorias de la Fiscalía General del Estado, específicamente las de 2014 y 2015, que representan los procedimientos incoados en materia de delincuencia informática que han tenido lugar durante los años 2013 y 2014 respectivamente. Esta información ha sido facilitada por todas las Fiscalías provinciales.

Memoria del año 2014 (representa los procedimientos incoados en el año 2013)

	TOTAL	%
Daños, sabotaje informático	84	0,70
Acceso sin autorización	195	1,63
Descubrimiento y revelación de secretos	343	2,86
Contra los servicios de radiodifusión	17	0,14
Estafa	9.663	80,59
Acoso a menores de 13 años	69	0,58
Pornografía y corrupción de menores o discapacitados	521	4,35
Contra la propiedad intelectual	32	0,27
Falsificación documental	32	0,27
Injurias y calumnias contra funcionario público	231	1,93
Amenazas y coacciones	249	2,08
Contra la integridad moral	160	1,33
Apología o incitación a la discriminación	14	0,12
Otro tipo delictivo	380	2,99
TOTAL	**11.990**	**100,00**

El año 2013 brilla por un mayor incremento de estos procedimientos con respecto al año anterior, ya que tal y como se observa en el cuadro, en 2013 se han registrado un total de 11.990 de procedimientos judiciales. Por tanto, observamos un aumento de 50,64% de los delitos informáticos entre 2012 y 2013, y un incremento de 83,50% entre 2011 y 2013 (Torres-

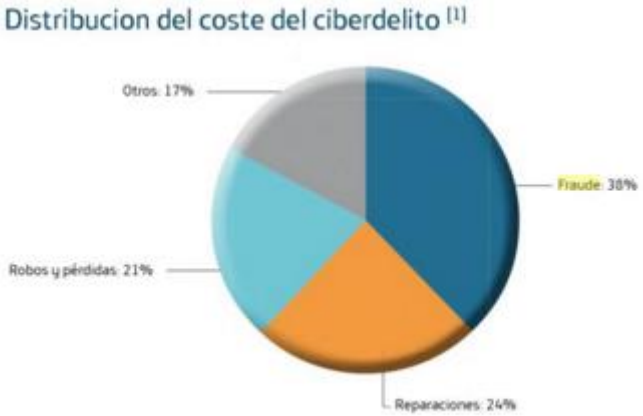
Dulce Lifante, 2014). En 2013, el número de procedimientos judiciales por delito de estafa ha experimentado un gran aumento ya que pasa de 5.992 a 9.663.

Memoria del año 2015 (representa los procedimientos incoados en el año 2014)

	TOTAL	%
Daños, sabotaje informático.	143	0,70
Acceso sin autorización	297	1,45
Descubrimiento y revelación de secretos.	561	2,73
Contra los servicios de radiodifusión.	15	0,07
Estafa	17.328	84,39
Acoso a menores de 13 años	60	0,29
Pornografía y corrupción de menores o discapacitados.	581	2,83
Contra la propiedad intelectual	58	0,28
Falsificación documental	156	0,76
Injurias y calumnias contra funcionario público	381	1,86
Amenazas y coacciones	527	2,57
Contra la integridad moral	130	0,63
Apología o incitación a la discriminación	30	0,15
Otra tipología delictiva.	150	0,73
– Denuncias por suplantación de identidad	117	0,57
TOTAL	**20.534**	**100,00**

En 2014 también aumentan estos delitos, pasando a un total de 20.534. En las tablas precedentes, queda reflejado de manera clara que el delito de estafa informática es el que se comete con más frecuencia de entre todos los delitos informáticos, ya que representa en 2013 un 80,59% del total de ciberdelitos cometidos y en 2014 un 84,39% (Madrigal Martínez-Pereda, 2015). Podemos afirmar que con los datos que hemos expuesto anteriormente, queda reflejado que los delitos en Internet se encuentran en continuo aumento, destacando el delito de estafa por ser la infracción penal más frecuente en este ámbito.

Además, este tipo de delincuencia trae consecuencias negativas tanto a los ciudadanos como a las empresas, ya que genera muchas repercusiones económicas a nivel mundial. Diversos estudios muestran que el coste de los delitos informáticos a nivel global ha sido entre 370.000 y 575.000 millones de dólares en 2013.



Como podemos observar en el gráfico, el 38% de este coste lo representan los fraudes online, el 24% lo representan las reparaciones necesarias que se ido realizando tras los

ataques, el 21% indican los robos de información y por último el 17% de este coste se debe a otras causas. Por lo tanto, los fraudes en Internet son los que más repercusiones económicas generan.

En nuestro país, el 64,4% de los usuarios han tenido algún tipo de incidencia online, el 48% de los cuales han sufrido intentos de fraudes. En 2014, el gasto en ciberseguridad a nivel mundial fue de 72.000 millones de dólares. Por todas estas pérdidas económicas, los diferentes Estados invierten cada vez más cantidad de dinero con la finalidad de obtener una mejora en la seguridad en la red. Por ejemplo, Reino Unido ha desarrollado un programa denominado Programa Nacional de Ciberseguridad 2011-2016, en el que invirtió 860 millones de libras. Es también interesante mencionar que se estima que en 2019 el coste de los incidentes de seguridad en Internet será de 2,1 billones de dólares (Fundación Telefónica, 2016).

Por tanto, mediante estos datos queda clara la problemática que está generando el fraude informático en la actualidad, ya que se encuentra en continuo aumento y es la infracción penal más común de los delitos informáticos, además de generar grandes pérdidas económicas a nivel nacional e internacional

15 Caso Práctico

El objetivo del presente apartado es aportar un caso para poder comprender de una forma más práctica el tema del fraude en Internet. La información la hemos extraído de la sentencia dictada por el Tribunal Supremo, concretamente la STS 5102/2015, encontrada a través del buscador de jurisprudencia del Consejo General del Poder Judicial. Para cumplir con nuestro objetivo, vamos a explicar a continuación los hechos probados de la sentencia, es decir los hechos que el tribunal admite como reales y demostrados, y también mencionaremos si el acusado ha resultado absuelto o por el contrario se le ha impuesto una pena.

El acusado es Juan Alberto, mayor de edad y sin antecedentes penales. En fecha indeterminada (próxima al 19 de septiembre de 2012), se puso en contacto con diversas personas desconocidas vía Internet, concretamente a través del correo electrónico. Estas personas desconocidas le ofrecieron un trabajo a Juan Alberto: trabajar para la empresa Career Builder como agente bancario, empresa inexistente. El trabajo consistía en recibir varias transferencias a su cuenta bancaria, y después enviar inmediatamente el dinero en el extranjero haciendo uso de empresas de transporte de dinero como Money Gram o Wester Union. En este caso, se le mandaba la transferencia en Kiev, Ucrania, a una persona denominada Eleuterio. Mediante este supuesto trabajo, Juan Alberto ganaba un 8% o un 10% de las transferencias que recibía a su cuenta bancaria.

Había varios indicios para darse cuenta de que se trata de una actividad ilegal: el contrato que se le ofreció a Juan Alberto no era el habitual, el idioma que se utilizaba no era el español, los individuos para los que trabajaba no eran personas conocidas y los datos que estos le

proporcionaron no eran verificables. Además, Juan Alberto era consciente de que las sumas recibidas procedían de actividades delictivas. A pesar de todas estas circunstancias, estuvo de acuerdo en colaborar con estas personas desconocidas con ánimo de beneficiarse de sus actividades.

Juan Alberto les facilitó a las personas desconocidas su número de cuenta de la Caja Rural CAJAMAR, y el día 19 de septiembre de 2012 recibió en esta cuenta 2.167,29 euros. Esta cantidad de dinero procedía de otra cuenta también de la Caja Rural CAJAMAR, cuyo titular es Juaquín. Fueron estas personas desconocidas quienes robaron las contraseñas a Juaquín mediante el fraude en Internet llamado phishing, estafa informática que ya hemos explicado en nuestro trabajo. Evidentemente, Juaquín resultó perjudicado por estos hechos, ya que los infractores le dejaron el saldo a cero. La Caja Rural CAJAMAR no le ha reintegrado a Juaquín el dinero sustraído.

Se observa que no concurren circunstancias modificativas, y por tanto se condena al acusado Juan Alberto como autor de un delito de estafa bancaria por Internet, a la pena de 10 meses de prisión, "(…) con la accesoria de inhabilitación especial del derecho de sufragio pasivo durante el tiempo de la condena privativa de libertad, y al pago de las costas procesales causadas, siendo de abono para el cumplimiento de la pena el tiempo que haya estado privado de libertad en la presente causa." (STS 5102/2015). Además, se indemnizará como responsabilidad civil a Juaquín en la cantidad de 2.167,29 euros, más el interés legal según el artículo 576 LeCrim.

Por tanto, mediante este caso práctico hemos podido observar cómo se ha llevado a cabo un delito de estafa bancaria por Internet. En el presente trabajo hemos clasificado este delito dentro de los fraudes cometidos a través del correo electrónico, concretamente en el tipo de falsas ofertas de trabajo. Como hemos visto Juan Alberto recibió un correo electrónico en el cual se le ofrece una oferta de trabajo realizando transferencias bancarias. Al llevar a cabo estas transferencias, y además a sabiendas de la procedencia ilícita del dinero, Juan Alberto incurrió en un delito penal por el cual ha sido condenado. Además, mediante este caso práctico también hemos podido ver cómo los delincuentes utilizan el phishing: han empleado este fraude para robar los datos bancarios del perjudicado Juaquín.

16 CONCLUSIONES

A continuación, expondremos las conclusiones a las que hemos llegado tras la finalización de nuestro trabajo. Las hemos dividido en dos bloques: conclusiones generales y personales.

- **Conclusiones generales**

PRIMERA: Internet es una herramienta que nos proporciona muchos beneficios desde varios puntos de vista. Así, nos facilita la realización de muchas tareas en el puesto de trabajo, nos permite el acceso a la información de una forma rápida y nos proporciona la posibilidad de

poder comunicar entre nosotros de una forma sencilla y económica independientemente del lugar en el que nos encontramos. Sin embargo, como hemos podido comprobar, el uso de Internet también puede tener sus inconvenientes, ya que los delincuentes aprovechan este instrumento para cometer diversos delitos.

SEGUNDA: Al realizar una clasificación de los fraudes en Internet, hemos podido comprender el *modus operandi* de los delincuentes en este ámbito, los diversos procedimientos que estos utilizan para llevar a cabo sus acciones ilegítimas, además de entender que las técnicas que emplean van evolucionando día tras día.

TERCERA: Es muy frecuente que los usuarios consideren que el uso de los smartphones y tablets es algo seguro. Sin embargo, como hemos visto el hacer uso de estas nuevas tecnologías puede ocasionar diversos riesgos, como por ejemplo ser víctima de un fraude en Internet, aumentando esta posibilidad cuando el usuario emplea estas herramientas sin ningún tipo de precaución.

CUARTA: Los delitos en Internet están en continuo aumento, destacando el fraude por ser el más frecuente. Por tanto, esta estafa brilla por ser una problemática en la sociedad actual ya que los delincuentes no paran de encontrar nuevas modalidades de cometer esta infracción penal. Todo esto, más el constante desarrollo tecnológico que nuestra sociedad está experimentando, influye en el incremento de estas acciones ilícitas.

QUINTA: Los delitos online, especialmente el fraude, traen consecuencias negativas en la economía global, ya que generan graves pérdidas económicas tanto a nivel nacional como internacional.

SEXTA: La realización del Trabajo de Final de Grado me ha permitido investigar en el tema de los fraudes cometidos a través de Internet, lo que supuso un enriquecimiento de los conocimientos en esta materia, que a su vez serán utilizados para una eficaz prevención en este campo tan preocupante.

- **Conclusiones personales**

PRIMERA: Desde mi punto de vista, el incremento de la delincuencia online se debe a diversos motivos. En primer lugar, los delincuentes no paran de encontrar nuevas modalidades de cometer estas acciones ilícitas. En segundo lugar, las personas prefieren la comisión de este tipo de infracciones penales porque estas proporcionan un cierto confort al poder realizarlas desde el propio hogar. Por último, observamos que la sociedad actual experimenta un constante desarrollo tecnológico lo que hace que cada vez haya un número elevado de herramientas para la comisión de estos delitos y una mayor disponibilidad de las mismas para los delincuentes.

SEGUNDA: Considero que para poder solucionar las problemáticas que están generando los delitos en Internet, tanto su disparado aumento como las pérdidas económicas que implican

para los Estados, es necesario abordar el tema desde diversos ámbitos: tecnológico, jurídico y económico.

TERCERA: Actualmente es muy común que se utilicen las nuevas tecnologías e Internet desde una edad muy temprana, por lo que los menores de edad pueden ser víctimas de todo tipo de delitos. Por este motivo, desde mi punto de vista es necesario un control parental y una educación encaminada a evitar que los niños se conviertan en víctimas.

CUARTA: Considero que el internauta, además de aplicar los consejos que hemos expuesto en el presente trabajo, debe estar mejor informado de los riesgos a los que se expone al conectarse a la red, ya que es el único que puede evitar, en primera instancia, ser víctima de estos delitos.

QUINTA: Muchos de los fraudes en Internet se cometen prometiendo a la víctima hechos que a primera vista parecen imposibles. Por este motivo, opino que además de tener unos conocimientos básicos sobre los riesgos en la red, un buen arma para el usuario en contra de estos delitos es aplicar el sentido común. Que bien decía Marlene Dietrich: “la imaginación exagera, la razón subestima, el sentido común modera.”

17 BIBLIOGRAFIA

Amanor, P. M.& Yeboah-Boateng, E.O. (2014). Phishing, SMishing & Vishing: An Assessment of Threads against Mobile Devices. *Journal of Emerging Trends in Computing and Information Sciences, 5* (4), 299-300. Recuperado de http://www.cisjournal.org/journalofcomputing/archive/vol5no4/vol5no4_6.pdf

APWG. (2015). *Phishing Activity Trends Report.* Recuperado de https://docs.apwg.org/reports/apwg_trends_report_q1-q3_2015.pdf

ASFI. (2009). *Estafas y Chantajes: Una guía educativa para prevenir Fraudes Financieros.* Recuperado de https://www.nfa.futures.org/nfa-investor-information/publication-library/scams-and-swindles-spanish.pdf

Avilés A. P. (2013), *Red+Segura Informando y educando V 1,* España: Safe Creative.

Aycock, J. (2006), *Computer Viruses and Malware,* Canada: Springer.

Bernard Jansen, J. (2007). *Click Fraud.* USA, Pennsylvania: The Pennsylvania State University. Recuperado de https://faculty.ist.psu.edu/jjansen/academic/jansen_click_fraud.pdf

CERT-UK. (2014), *An introduction to malware.* Recuperado de https://www.cert.gov.uk/wp-content/uploads/2014/08/An-introduction-to-malware.pdf

Cinco estafas que circulan por redes sociales y cómo mantenerse a salvo. (2015, 12 de septiembre). *ABC.* Recuperado de http://www.abc.es/tecnologia/redes/20150912/abci-cinco-estafas-circulan-redes-201509111807.html

Consejo de Europa. (2001). *Convenio sobre la Ciberdelincuencia.* Recuperado de https://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/consejo_europa/convenios/common/pdfs/Convenio_Ciberdelincuencia.pdf

El Anuario Estadístico del MInisterio del Interior. (2013). *Cibercriminalidad*. Recuperado de: http://www.interior.gob.es/documents/10180/1207668/Avance+datos+ciberciminalidad+2013.pdf/5de24ec6-b1cc-4451-bd06-50d93c006815

España. Tribunal Supremo. Sala de lo Penal. Sentencia del 20 de noviembre de 2015. Ponente: Juan Saavedra Ruiz. Copia recuperada del buscador de jurisprudencia del Consejo General del Poder Judicial:

http://www.poderjudicial.es/search/doAction?action=contentpdf&databasematch=TS&reference=7557487&links=phishing&optimize=20151218&publicinterface=true

Facebook. (2016). *What are some common money scams I should look out for when sending or receiving money in Messenger?* USA: Facebook. Recuperado de: https://www.facebook.com/help/224906417682965/

FBI. (2011). *Fraude de carta de Nigeria sigue defraudando.* USA: the Federal Bureau of Investigation. Recuperado de https://www.fbi.gov/espanol/historias/fraude-de-carta-de-nigeria-sigue-defraudando

Fraude en un supuesto servicio de videollamadas para Whatsapp. (2016b, 19 de abril). *El País.* Recuperado de http://tecnologia.elpais.com/tecnologia/2016/04/18/actualidad/1461015879_508470.html

Fundación Telefónica. (2016). *La sociedad de la información en España 2015.* Barcelona: Ariel.

Gallego Lluste, A. (2012). *Delitos informáticos: malware, fraudes y estafas a través de la red y cómo prevenirlos.* Universidad Carlos III de Madrid, Leganés, España. Recuperado de http://e-archivo.uc3m.es/bitstream/handle/10016/16868/pfc_alberto_gallego_yuste.pdf?sequence=1

Garrido, V., Stangeland, P.& Redondo, S. (2006). *Principis de criminologia, 3a edic.* Valencia, España: Tirant lo Blanch.

GDT. (2011). *Consejos de seguridad.* España: Guardia Civil.Recuperado de https://www.gdt.guardiacivil.es/webgdt/consejos.php

GDT. (2016). *¡CUIDADO! Vuelven los SMS maliciosos.* España: Guardia Civil. Recuperado de https://www.gdt.guardiacivil.es/webgdt/popup_alerta.php?id=233

González Suárez, P. (2014). Fraudes en Internet y estafa informática. Universidad de Oviedo, España.

Guardia Civil. (2014). *Para no ser víctima de estafa,* España: Guardia Civil. Recuperado de http://www.guardiacivil.es/es/servicios/consejos/estafa.html

INCIBE. (2014a), *Aprende a identificar correos electrónicos maliciosos.* España: Oficina de Seguridad del Internauta. Recuperado de https://www.osi.es/actualidad/blog/2014/08/18/aprende-identificar-correos-electronicos-maliciosos.html

INCIBE. (2015a). *¿Cambiar el color azul de Facebook? Mejor no.* España: Oficina de Seguridad del Internauta. Recuperado de https://www.osi.es/es/actualidad/avisos/2015/08/cambiar-el-color-azul-de-facebook-mejor-no.html

INCIBE. (2016a). *El phishing, la moda que nunca pasa.* España: Oficina de Seguridad del Internauta. Recuperado de https://www.osi.es/es/actualidad/blog/2016/03/15/el-phishing-la-moda-que-nunca-pasa.html

INCIBE. (2013a). *Fraudes online (I): estafas en la venta de productos.* España: Oficina de Seguridad del Internauta. Recuperado de

https://www.osi.es/actualidad/blog/2013/04/02/fraudes-online-i-estafas-en-la-venta-de-productos.html

INCIBE. (2014b). *¿Chicas rusas por Internet? ¡No es lo que parece!.* España: Oficina de Seguridad del Internauta. Recuperado de https://www.osi.es/actualidad/blog/2014/01/03/chicas-rusas-por-internet-no-es-lo-que-parece.html

INCIBE. (2016b). *Con la publicidad demasiado llamativa, ¡no bajes la guardia!* España: Oficina de Seguridad del Internauta. Recuperado de https://www.osi.es/es/actualidad/blog/2016/02/01/con-la-publicidad-demasiado-llamativa-no-bajes-la-guardia.html

INCIBE. (2015b). *Enfrentándonos al ransomware.* España: INCIBE. Recuperado de: https://www.incibe.es/blogs/post/Seguridad/BlogSeguridad/Articulo_y_comentarios/EnfrentandonosRansomware

INCIBE. (2013b). *Fraudes online (II) estafas en el alquiler de viviendas.* España: Oficina de Seguridad del Internauta. Recuperado de https://www.osi.es/actualidad/blog/2013/04/10/fraudes-online-ii-estafas-en-el-alquiler-de-viviendas.html

INCIBE. (2013c). *Fraudes online (III) Venta de vehículos ¡Qué no te vendan la moto!.* España: Oficina de Seguridad del Internauta. Recuperado de https://www.osi.es/actualidad/blog/2013/04/17/fraudes-online-iii-venta-de-vehiculos-que-no-te-vendan-la-moto.html

INCIBE. (2014c). *Las 8 falsas ofertas de empleo más utilizadas por ciberdelincuentes en Internet.* España: Oficina de Seguridad del Internauta. Recuperado de https://www.osi.es/actualidad/blog/2014/03/04/las-8-falsas-ofertas-de-empleo-mas-utilizadas-por-ciberdelincuentes-en-in.html

INCIBE. (2012). *Conoce los fraudes utilizados en Internet II: los SMS Premium.* España: Oficina de Seguridad del Internauta. Recuperado de https://www.osi.es/es/actualidad/blog/2012/07/05/conoce-los-fraudes-utilizados-en-internet-ii-los-sms-premium.html

INCIBE. (2014d). *Aprendiendo a identificar estafadores online en páginas de anuncios.* España: Oficina de Seguridad del Internauta. Recuperado de https://www.osi.es/es/actualidad/blog/2014/06/16/aprendiendo-identificar-estafadores-online-en-paginas-de-anuncios.html

INCIBE. (2013d). *Fraudes online (V) Préstamos de dinero a particulares.* España: Oficina de Seguridad del Internauta. Recuperado de https://www.osi.es/actualidad/blog/2013/05/29/fraudes-online-v-prestamos-de-dinero-particulares.html

INCIBE. (2014e). *Pharming y Spim: los primos hermanos del phishing y el spam.* España: Oficina de Seguridad del Internauta. Recuperado de https://www.osi.es/actualidad/blog/2014/10/07/pharming-y-spim-los-primos-hermanos-del-phishing-y-el-spam.html

INTECO. (2007). A study of users and public and private organisations affected by the fraudulent practice known as phishing.

INTECO-CERT. (2008). *Falsos antivirus y antiespías. Intento de fraude a través de la venta de falsas herramientas de seguridad.* Recuperado de

https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_est_antivirusfalsos_081023_v13.pdf

Kevin McGrath, D., Gupta, M. (2008). *Behind Phishing: An Examination of Phisher Modi Operandi,* Computer Science Department, Indiana University, Bloomington, IN, U.S.A. Recuperado de http://docs.apwg.org/reports/behindPhishingWhitePaper.pdf

Ley Orgánica 10/1995, del 23 de noviembre del Código Penal.. Bolentín Oficial del Estado, Madrid, España, 23 de noviembre de 1995. Recuperado de https://www.boe.es/buscar/act.php?id=BOE-A-1995-25444

Madrigal Martínez-Pereda, C. (2015). *Memoria elevada al Gobierno de S. M.* Recuperado del sitio de internet de https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/MEMFIS15.pdf?idFile=989ed5e3-7339-4575-91d5-3a3b246db8af

Marketech forum. (2015, 19 de noviembre). *Acaba con los bots en tus anuncios: el ROI te lo agradecerá* [Web log post]. Recuperado de http://marketechforum.com/articulo/acaba-con-los-bots/

Matarranz, A. (2016, 21 de febrero). *Publicidad display online: un fraude de miles de millones [Web log post].* Recuperado de https://conversisconsulting.com/2016/02/21/pubicidad-display-online-un-fraude-de-miles-de-millones/

Microsoft Corporation. (2016). *Modernice su negocio.* España. Recuperado de http://www.microsoft.com/es-es/business/business-news/plan-de-marketing-en-internet

Miró Linares, F. (2013). La respuesta penal al ciberfraude. Especial atención a la responsabilidad de los muleros del phishing. *Revista electrónica de ciencia penal y criminología, 15* (12), 11-13. Recuperado de http://criminet.ugr.es/recpc/15/recpc15-12.pdf

Molist, M. (2016, 15 de febrero). “Fraude al CEO” el email que está costando miles de euros a empresas españolas. *El Confidencial.* Recuperado de http://www.elconfidencial.com/tecnologia/2016-02-15/el-fraude-al-ceo-le-cuesta-miles-de-euros-a-decenas-de-pymes-espanolas_1151597/

NIST. (2011). *Malware risks and mitigation report.* Recuperado de http://www.nist.gov/itl/upload/BITS-Malware-Report-Jun2011.pdf

Orts Berenguer, E., González Cussac, J. L., Matallín Evangelio, A. & Roig Torres, M. (2010). *Tomo VII Esquemas de derecho penal Parte Especial 2ª Edición.* Valencia: Tirant lo Blanch.

Panda Security. (2009). *El negocio de los falsos antivirus. Análisis del nuevo estilo de fraude online.* Recuperado de http://www.pandasecurity.com/spain/mediacenter/src/uploads/2014/07/El-Negocio-de-los-falsos-antivirus.pdf

Panda Security. (2015). *WhatsApp: 6 estafas a las que debes prestar atención.* (2015). España: Panda Security. Recuperado de

http://www.pandasecurity.com/spain/mediacenter/dispositivos-moviles/whatsapp-6-estafas-a-las-que-debes-prestar-atencion/

Proaño Alcívar, J.R. (2015, 24 de marzo). *"Hackear" Facebook es una mentira. Un fraude* [web log post]. Recuperado de https://www.parlox.net/blog/hackear-facebook-es-una-mentira-un-fraude/

Ramírez Bejerano, E. E. & Aguilera Rodríguez, A.R. (2015, 13 de febrero). Los delitos informáticos. Tratamiento internacional. *La Razón.* Recuperado de http://www.la-razon.com/suplementos/la_gaceta_juridica/delitos-informaticos-Tratamiento-internacional-gaceta_0_2216178537.html

Scannel, K. (2016, 1 de marzo). La "estafa del CEO", la última moda en ciberdelitos. *Expansión.* Recuperado de http://www.expansion.com/economia-digital/companias/2016/03/01/56d5eed146163f12628b464c.html

Symantec Corporation. (2016). *Las 5 estafas principales de los medios sociales.* España: Norton. Recuperado de http://securityresponse.symantec.com/es/mx/norton/clubsymantec/library/article.jsp?aid=cs_top5_social_media_scams

Symantec Corporation. (2015). *Qué debe hacer si es víctima de un ataque.* España: Norton. Recuperado de http://es.norton.com/victim/article

Torres-Dulce Lifante, E. (2014). *Memoria elevada al Gobierno de S. M.* Recuperado del sitio de internet de https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/MEMFIS14.pdf?idFile=dd3ff8fc-d0c5-472e-84d2-231be24bc4b2

Trend Micro. (2012). *Spear Phishing Email: Most Favored APT Attack Bait. Recuperado de http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-spear-phishing-email-most-favored-apt-attack-bait.pdf*

Un falso cupón de McDonald's roba datos personales en WhatsApp. (2016a, 27 de febrero). *El País.* Recuperado de http://tecnologia.elpais.com/tecnologia/2016/02/25/actualidad/1456405457_735246.html?rel=mas

Wyman, B., Scrivens, W., Hoffman, P. & Rudis, B. (2013, Julio), Spear phishing, *OUCH!* Recuperado de https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201307_sp.pdf