UNIVERSITAT JAUME·I

Fraudes En Internet

Trabajo Final de Grado.

Grado en criminología y seguridad 2015/2016.

Estudiante: **Félix Sanz Párraga.**

Tutor: **Manuel Mollar Villanueva.**

A mi tutor, por su paciencia durante este trabajo;
Y a Alejandro Gutiérrez, por su apoyo
en aquel mes de mayo…

ÍNDICE.

Extended summary.

Fraud is a type of crime that has been discussed internationally before the use of electronic means, but now the connection between various users in different countries through the Internet requires the existence of an international regulation to deal with this problem with the greatest possible diligence. Given that there are several concepts and understandings under the term fraud, having to clarify definition as complete as possible to address the problema in the most appropriate manner.

Understanding by fraud or scam any practice that can be carried out either by a person or a group of these for-profit, to mislead a person or a group of these with enough deception, using devices that can be a computer or not, with the aim of provoking a provision to produce a benefit for the person who causes it or a third party, and harm to the owner of the provision.

Nothing of what we mean by fraud can make a differentiation of fraud committed through computer and produced without it, seeing the differences between this two and then focus on fraud committed via computer system.

- The common fraud, which is done by conduct developed by a person or a group of people, which aims to cause mistake rather in a person or a group of people making believe that something is real when it is not, seeking to generate an act of disposition that will produce a benefit to him or them or third parties, within a limited field of action.
- The computer fraud is an offense which consists in any fraudulent conduct in a field of action of unlimited expansion with the aid of computer systems with the intent to deceive a person, group of people or organization, modifying incorrectly the result of an automated data process, leading to an illegitimate benefit to those who perform it or third parties.

Staying with the last point, which is relevant to our interests, we see how it changes the way to perform the criminal act, being easier for computer fraud suit people calling their interest more in this area than in the real world, due to the globalization of this tool together with the spread of internet that leaves trace of likes, interests and motivations ofusers.

Frauds that use these new tools are far, in the actuation field, from traditional ones which are very limited, because if the fraudster is not in the social groups that influence him in one way or another, he may not know the motivations and likes of these, making it difficult to persuade someone to scam. Leaving aside the general conceptions, we say that Internet fraud can be developed in various forms depending not only on the cyber

criminal profile, but generally tend to have the same characteristics, but also by the variety of ways that they have to carry out the scam.

Assuming that the crimes of fraud develop entirely by economic motivations of the cyber criminal, logically all behaviors aimed to perpetrate a fraud will look for an act of patrimonial disposal by the user to the swindler in benefit of the last one or a third party.

Frauds can be made by two basic ways, directly or indirectly:

- Direct: Fraud that is done without an intermediary, having no interruptions or deviations, where the scammer is presented abusing on his situation, trust or deceive on the victim by offering or selling him something that does not correspond to reality or what is expected by the victim after hearing the fraudster, in exchange for receiving an economic compensation. Example: The purchase of a car where the scammer sells a vehicle that promotes as fabulous and at first glance looks like it but then by using it the victim proves that is in poor condition.

- Indirect: Fraud that is done through intermediaries, with some interruptions or deviations, where the fraudster is not presented directly to the victim, but uses the image given by a certain company, message or email, (being the scammer behind this company) as a way to produce a mistake on this person (the victim) to provide a series of personal data to access their cash accounts or to make them pay for a certain object or service that they will never receive. This is the most popular form of fraud in the Internet. Ex. phishing technique with spam or ghost companies formed to provide a number of services that were never carried out with the only objective of taking money from people seeking for those services.

After seeing both ways fraud can be done, now we will analyse the most typical frauds that happen on the Internet:

- Frauds on house trading or rental: Consists in online publication of an offer of a property for rent or sale, having a resistless prize. But when the buyer contacts the owner, he is abroad and he encourage the buyer to decide to pay because he has other offers. The buyer makes the payment but the property does not exist.

- Fraud on buying and selling online, committed both by the buyer and the seller (EBay): In this scam often the user makes a purchase and is swindled; even by a false announcement, with a remarkably deteriorated product, a crude imitation or simply while reaching anything.

- SMS fraud and high pricing phone calls: It consists generally in a SMS received by the victim that when is opened activates a series of broadcasts of messages directed to the victim's number with the cost reflected in the bill.

- Pyramidal Networks: It refers to the of Ponzi scheme, being a fraud where there is no real investment activity to support it, Nevertheless benefits that users get come from money invested by new users.
- Nigerian Scam: Consists on emailing several random people, telling them that a supposed quantity of money is given in exchange for aid getting a fortune from a particular place. After that certain amount of money is required to the victim to access the inheritance or helping the millionaire who then will reward the victim. However, this reward will never happen.
- Electronic Fraud (use of payment instruments): This fraud falls on instruments which online payment is made with. It happens when a credit card owner realizes a series of expenses have been made from his credit card after an authorised purchase. The user's service provider must check if an irregularity has occurred. If it does not happen, the user will not be able to recover his money.
- Ransomware: This fraud stems is based on the infection of computer systems by viruses that block the computer, operating system or files demanding to release an amount of money that must be paid in different ways to a person or an organization.
- Phishing: This involves sending massive spam emails, which simulate coming from banks imitating the official message of these entities. Sometimes it fully takes official appearance, getting users to trust and put private data as is required.

After analyze which are the most common online computer fraud types, it is time to talk about the different ways which you can defraud on the Internet by. Currently not only computers have access to the global connectivity that allows the network but we have a huge field where perpetrate unlawful conduct from different devices such as tablets and smartphones, using operating systems like Android or iOS that enable a variety of features. Appearing these new devices emerge new fraudulent conducts, seeking to trick users that in this new field are more innocent and trustful.

Assuming that most fraudulent behaviors are based on phishing, we can show fraud conducts that are carried out in these new devices:

- Pharming: This is similar to phishing, but less generic. The scammer by delivering an email redirects through the modification of system name resolution (DNS) the victim to an impersonated website. It produces that when the victim sets the domain of the page he wants to access, is redirected to the copy of that page. So the user sets his personal data there.
- Smishing: Fraudulent activity is generally done using text messages (SMS), aimed to Smartphone users, trying to convince them, with attractive claims, to make a particular call, visit a fraudulent website, answer to a received SMS and all those behaviors that

suppose an additional cost. This technique is not only used to charge the costs of these services but also to try to extract user's personal and private data.
- Vishing: This scam uses the voice as the way to perpetrate deception and fraud. It involves sending an email where criminals set details of bank data via a free call where a computerized voice or VoIP with a professional looking, requires victims (as clients of the bank) confirmation of their bank account by asking them their account number, credit card number, pin number, expiration date of the card or any other important data.
- Apps (Applications): In this section we are going to treat the frauds on the applications downloaded for Tablets or Smartphones, available not only in both official stores as Google Play Store (Android) or App Store (Apple / iOS) but in external pages found through the net. It is an endless source of fraudulent behavior.

This fraud is called false apps, focused on instant messaging applications such as WhatsApp, Telegram or Line, without ignoring generic ones. Other applications that can also be fraud are battery level indicators or flashlights. We can highlight from this generic applications, three particular ones that has had a big impact among users:
- Naked Scanner and Super Jumper X: These applications capture users with the false promise of being able to see anyone in underwear if you scan people using any of these two applications. For this reasons, users, tempted by the desire of invading people’s privacy download any of these applications or both, being subscripted without realizing to premium messaging services. Moreover, these particular applications were more harmful than others because apart from subscribing users to premium services, indicate the user that has to install new applications so if the victim click to download the updates, the application itself links randomly with other fraudulent applications, which send messages that the user’s device warning that it is infected and that an antivirus installation is needed, recommending a particular one that has a cost, which inflates the user's bill.
- Virus Shield: This is the other application with great affection among users. It consists in a "scam app" that promises to protect the user’s Smartphone from any kind of threat, besides of your personal information, consuming little battery. The only thing that this application does is drawing a check mark on a shield (the image of this application) when the victim touches the screen to simulate that the device is protected. This application supposes a waste of four euros to each person that downloads it.
Now it is time to focus on instant messaging applications due to its key role in the different devices in the world for being an essential tool for every user. Cybercriminals in this area use the popular image of the most famous apps to gain the user’s trust and then capture them making totally false but dissuasive promises (such us spy other user’s

conversations or change the application appearance) to make the victim download such applications.

Let us talk now about WhatsApp application:

- Android security breach that allows conversations to be read: WhatsApp saves conversations in the SD card of the device where it is installed, creating a database with the user's conversations and private archives. Some cybercriminals have created a series of applications trying to access this database. Once downloaded and opened on the device this application copy all data, decoding and carrying it to a particular server owned by the cybercriminal and being stored for fraudulent use. Then the scammer may ask for a certain amount of money in exchange of erasing the copied data or uses some personal information such as bank data reflected in some conversation.
- WhatsApp Spy: This scam is based on offering the user the possibility of spying his contact´s conversations, being this a false offer. What the application really does is to create an accumulation of data from the device, to install malware or even to subscribe the victim to Premium SMS services without its knowledge.
- WhatsApp video calls: This fraud is related to the subscription to premium SMS services, consisting of a message received by the user with a link that says "activate video calls" that redirect the victim to a website that tries to impersonate WhatsApp identity, appearing on the phone a series of screens that simulate to be checking the version of the application and looking for new updates. Then the device is said to be outdated, and when the user tries to update is redirected to a fraudulent website where the phone number and the operator is requested, when the victim introduces it, is subscribed to a premium SMS service without knowing it.
- Frauds via browser: This fraud derives from the announcement which was made to report that WhatsApp was going to have website to hold conversations also using a computer. Many users for novelty and not be familiar with the appearance of the web downloaded fraudulent applications on their computers from fraudulent websites without knowing that they were Trojans that allowed the cybercriminals to obtain private information such as bank data to use it fraudulently.
- Double blue checkmark deactivation: This scam derived from the release of a famous update from WhatsApp to verify that the message receiver had read the message. Due to the great problems that came up after this version appearance, many users wanted to downgrade to the previous version of the application. Some cyber criminals took advantage of this to spread through social networks like twitter a new application which once installed would remove the blue double checkmark automatically. What the application really did was to subscribe users who downloaded it to premium services.

- WhatsApp Gold: This fake application was very popular among users, but is quite harmful. It cheats users by offering them an exclusive update, which provides WhatsApp with some functions and services the normal application does not have. When the user types or selects the application, it redirects him to a fraudulent website where he can supposedly enjoy the improvements of the app. This application asks the victim to introduce his phone number and subscribes him to a premium SMS service.
- WhatsApp Locator: The cybercriminal uses the social network Facebook along with WhatsApp application to produce deception in the user, offering a locator to find in Facebook contacts that the user has in WhatsApp. This is not true and the app subscribe the user to a premium messaging service.
- False WhatsApp answering: This fraud was related to a WhatsApp service that did not exist or would exist, but showed quite attractive to the user. It consisted on an email where the user receives a notification saying that he had a voice message in a supposed WhatsApp answering machine, a malware was downloaded when the victim clicked on the download link included in the email. This malware would allow the full availability of the device to cybercriminals with fraudulent objectives.

This scams happened in a similar way in both Line as Telegram, which are two instant messaging applications, but in a less extension because of its less popularity.

Continuing the analysis of this problem, a number of actual cases of fraud are reflected on the Internet with different figures participating in these acts. The punishment is generally insufficient for behaviors like this, that turn to be profitable to the criminal. The first case where a determined amount of money is extracted to an user using the phishing technique is penalized only with three months of prison. The second event, which affects a salesman because after using PayPal in a transaction this tool will remove the money from the sale of a product that supposedly comes in a fraudulent way, being the fact unpunished because it has not reached 400 euros. The third case is a criminal plot that scams a number of users by the already mentioned Nigerian scam, being practically unpunished due to the difficulties proving it, establishing only a period from nine months to a year of prison to certain people. Being in the last case where the criminal promotes a number of products on the website eBay, a victim transfers the money to the scammer's account, who despite of receiving the money does not send anything to the buyer. In this case, the criminal receives a penalty of one year and nine months in prison, with the obligation to compensate the victim with a specific amount of money.

A series of data and aspects to know about Internet fraud can also be provided. Saying that this is a problem which is in constant motion having ups and downs during the months of different years, Internet fraud specially grows in summer months and Fridays and Saturdays of each week. In addition, the appearance of new devices as phones and

tablets have also triggered the growing of these criminal acts since its inception to the present with a big impact in the beginning and more unstable as we come to the current date. We should also focus on the phenomenon of phishing due to its importance. We have to emphasize that the richest countries, as North America and the Asian giants, are the ones that bear the greatest incidence of phishing, since it produces a large economic and social losses in the country which strikes, ensuring a criminal continuity so the profit never ends.

To fight the issue of Internet fraud, many social and legislative measures are held but they sometimes fall short due to companies or governments interests because they take some sort of economic benefit from these behaviors. So if we really want to end this problem, we should carry out joint strategies in a globalized way with the cooperation of all governments and agents involved in this phenomenon with the only motivation of solving the problem and making the citizen's lives safer.

1.- Resumen.

Este trabajo nace con el objetivo de abordar la materia delictual de fraudes dentro del servicio de sobra conocido llamado internet, presentando un análisis tanto histórico como metodológico de todos los fenómenos que han ido apareciendo y existen de fraudes en internet. Este texto se configura por partes, primeramente se muestran conceptos que sirven de sinónimos como son estafa y fraude desde una perspectiva jurídica así como social que nos ayudará a entender mejor el fenómeno. A continuación se expone el delito de fraudes en internet mencionando como se desarrolla de forma general, luego se concreta un poco viendo los fraudes más típicos en internet explicando uno por uno en qué consisten y su metodología. Seguidamente se profundiza en los nuevos tipos de fraudes que podemos encontrarnos hoy día, así como de los diferentes dispositivos con los que podemos incurrir en estos fraudes, telefonía móvil, tablets, etc. Además, se menciona como se encuentra la situación de los fraudes por internet en España en cuanto a regulación penal se refiere y se realiza una comparación internacional del hecho con numerosos países, acompañado con estadísticas que ratifican dicha comparación. Más tarde, se volverá a hacer hincapié en la técnica del phising como elemento fundamental en los fraudes por internet valorando su impacto tanto económico como social, en España y en otros países. Exponiendo finalmente qué medidas se están llevando a cabo para luchar contra el fraude también de forma internacional y en España como se ha ido realizando previamente.

Acabando con una serie de conclusiones que se pueden extraer de todo lo investigado, siendo de gran ayuda tanto la obtención de sentencias de casos reales, como la experiencia compartida por parte de usuarios afectados por esta práctica.

Palabras clave: Phising, Estafa, Fraude, Delito, Datos, Internet, Redes sociales, Engaño.

Abstract.

This project was created with the objective of addressing the fraud within the well-known service called the Internet, presenting both historical and methodological analysis of all phenomena that have appeared of fraud on the Internet.

This text is set by parts, first concepts that serve as synonyms as scam or fraud are shown from a legal and social perspective that will help us to understand this issues. Afterwards, the fraud on the Internet crime is exposed mentioning how it develops in general, then it is specified seeing the most typical internet frauds one by one explaining them are and their methodology.

Then it deepens into new types of fraud that can be found today as well as the different devices that we can incur these frauds with, as mobile phones, tablets, and so on. In addition, it is mentioned how the situation of Internet fraud is in Spain in terms of criminal regulation and an international comparison with many countries is performed, followed by statistics that allow us to make this comparison properly and clearly.

Later, we will emphasize in the phising technique as a key element in Internet fraud assessing its economic and social impact not only in Spain but in other countries.

Finally presenting what measures are being taken to combat fraud both internationally as in Spain comparing it with the ones that has been previously done.

In conclusion, a set of conclusions are extracted from this investigation, being helpful both sentences obtaining real cases as shared experiences by users affected by this practice.

Keywords: Phising, Fraud, Fraudulent, Crime, Data, Internet, Social networks, Deception.

2.-Introducción.

La materia que se presenta a continuación va dirigida a realizar un análisis de las diferentes estafas que nos podemos encontrar por internet desde las más antiguas o tradicionales, a las más novedosas y populares. Mostrando como los delincuentes de esta materia van adaptándose a los cambios de pensamiento y estilo de vida que se producen en la sociedad así como a los avances tecnológicos, para poder seguir perpetrando sus estafas ya que las técnicas clásicas han quedado obsoletas.

Con el crecimiento que han tenido este tipo de conductas delictuales, y por la falta de medios que existen actualmente para realizar un efectivo abordaje sobre este tema. He querido dar una visión del problema tanto desde el territorio español como desde el ámbito global. Debido a que esta delincuencia se desarrolla en uno de los entornos delictuales que más rápido crece, porque ofrece realizar una serie de conductas ilícitas como en este caso las estafas, de forma rápida y desde el anonimato siendo bastante cómodo para el criminal. Además como el sistema legislativo no avanza al mismo ritmo que la tecnología existen muchos vacíos legales donde el principal afectado es el ciudadano. Asimismo decir, que este problema cada vez crece más principalmente por este incremento a tan alto ritmo de la tecnología del que venimos hablando con la aparición de nuevos dispositivos que hace que los ciudadanos se confíen debido al desconocimiento de estos, aprovechando esta situación estos delincuentes.
Por todo esto, me dirijo a hacer un tratamiento de investigación sobre los procesos de fraude en la herramienta internet para observar su comportamiento, puntos en común y obtener una serie de conclusiones que ayudan a paliar en cierta medida este problema.

3. Aspectos conceptuales.

Con el objetivo de esclarecer primeramente los aspectos que vamos a tratar en adelante, expondremos las distintas formas de entender el fraude o estafa tanto desde una perspectiva conceptual como judicial y social.

3.1. Concepto de Fraude.

Observando las regulaciones legales y el pensamiento que tenemos sobre este fenómeno, y adaptándonos al tema que estamos abarcando, podemos establecer un concepto global de fraude. Siendo este el siguiente:
El fraude o estafa es toda práctica que puede ser realizada tanto por una persona como por un grupo de estas, induciendo a error a una persona o grupo de personas mediante engaño suficiente utilizando artificios que pueden ser informáticos o no, con el objetivo de provocar una disposición que produzca un determinado beneficio para la persona que la provoca o para un tercero, y un perjuicio al propietario de la disposición.

Socialmente el entendimiento que un ciudadano medio puede tener de este hecho fraudulento, es la conducta que realizan un grupo de personas (ya que entienden que 2 o más personas pueden hacer más presión sobre la gente dejándose llevar más fácilmente y cayendo en la defraudación) con la intención de engañar a alguien, para sacarle una determinada disposición que le causa un beneficio a los autores y un perjuicio a la persona agraviada.

Desde una perspectiva jurídica establecida en el art.248.C.P. Se establece la estafa como las personas que con ánimo de lucro utilizaren engaño bastante para producir error en otra persona, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno. (Jefatura de estado, 2015)

Haciendo referencia también a la estafa informática en su apartado 2, diciendo que se trata de la conducta realizada por un usuario de la red buscando producir engaño mediante sistemas informáticos, utilizando artimañas como modificación de datos u obtención de datos auténticos por parte de la persona engañada, para conseguir un determinado beneficio.

La diferencia que encontramos entre el fraude informático a través de internet y el fraude común es la siguiente:
- El fraude informático posee un campo de actuación sin límite de expansión, apoyándose en la herramienta internet que le facilita de forma global engañar a una persona, grupo de personas u organización, modificando incorrectamente el resultado de un procesamiento automatizado de datos, propiciando un beneficio ilegítimo a quien lo realiza o a terceros.
- El fraude común es realizado por una persona o grupo de persona en un campo de actuación limitado, que tiene como objetivo provocar error bastante en una persona o grupo de personas haciéndoles pensar que algo es real cuando no lo es, buscando producir un acto de disposición que le produzca un beneficio a él o a ellos o a terceras personas.

4. Exposición del delito.

Tras haber expuesto las diferentes perspectivas de fraude, en este apartado vamos a tratar como se desarrolla el delito de fraude, observando las motivaciones con las que actúa este delincuente, las diferentes formas de defraudar y la metodología que se usa en cada una de las técnicas para perpetrar la conducta ilícita de estafa.

4.1. Desarrollo del delito.

Los delitos de fraude en internet son de motivación enteramente económica, los cuales se realizan utilizando sistemas informáticos, mediante los cuales se intenta producir error en los diferentes usuarios que navegan por la red con diversas motivaciones y actitudes. Para ello se utilizan numerosas metodologías para intentar abarcar a todos los usuarios existentes, buscando llamarles la atención fijándose en sus gustos y

pensamientos, para hacerles caer en la trampa y así poder estafarlos. Estas conductas que mencionamos y que posteriormente analizaremos derivan de la conducta genérica de estafa llamada phising, basada en la técnica de la ingeniería social[1], debido a que se trata de un tipo de ataque aprovecha las debilidades humanas como el descuido o el deseo de cooperación, para obtener las credenciales que les permitan entrar de una forma legal en una red oculta. Pudiendo decir que el estafador se adapta a los intereses y necesidades de su víctima mientras navega por internet, razonando que es lo que le puede interesar para captarlo provocando que de una manera u otra baje la guardia, y así estafarle.

4.2. Tipos de fraude

Antes de hablar específicamente de los tipos delictuales de fraudes en internet hemos de mencionar que los actos delictivos de fraude se pueden dividir en 2 grandes grupos como son el fraude directo y el fraude indirecto:

- Directo: Se trata del tipo de fraude que se realiza sin intermediario, no teniendo interrupciones o desviaciones, donde el estafador se presenta abusando de su situación, confianza o engaño a la víctima ofreciéndole o vendiéndole algo que no se corresponde con la realidad o con lo esperado por la víctima tras oír al defraudador, a cambio de una determinada remuneración económica por tal objeto o servicio. EJ: Compra venta de coches donde el estafador vende un vehículo que lo promociona fabuloso y a primera vista se ve así pero luego con el uso de este la víctima puede comprobar que está en pésimas condiciones.

- Indirecto: Se trata de otra modalidad de fraude que se realiza mediante intermediarios, con algunas interrupciones o desviaciones, en la cual el defraudador no se presenta directamente ante la víctima, sino que se vale de la imagen dada por una determinada empresa, mensaje o correo electrónico, (encontrándose dicho estafador tras esta empresa o mensaje) como medio para producir error en la persona (víctima) para que facilite una serie de datos personales con acceso a sus cuentas dinerarias o para que abone por un determinado objeto o servicio que luego no se llegará a obtener en la realidad. Esta modalidad delictiva es la más popular en los fraudes en internet. Ej: La técnica de phising con correos spam o empresas fantasma constituidas para ofrecer una serie de servicios que nunca se llevarán a cabo con el único objetivo de sacarles dinero a las personas solicitantes de dicho servicios.

[1] Técnica en donde una persona mediante teléfono, correo electrónico, etc. Se hace pasar por otra persona, entidad o compañía dotándole de credibilidad y confianza a ojos del individuo afectado facilitándole a este primer individuo los datos que se le solicitan.

4.2.1 Fraudes informáticos y estafas típicas en internet.

Aquí exponemos delitos que se realizan mediante medios informáticos (como los tres últimos) y los típicos que utilizan internet para promocionar su estafa.

1) Fraudes en la compra-venta o alquiler de vivienda*.*

Este tipo de fraude, consiste en la publicación en la red de una oferta de un inmueble en alquiler o venta, teniendo como rasgo principal el carácter irresistible de su precio. Se lleva a cabo un anuncio atractivo, poniendo un teléfono extranjero y argumentando que la vivienda no se puede visitar debido a que el dueño se encuentra fuera de España y este quiere estar presente en el momento de la visita. Se le insiste al comprador engañado diciéndole que tienen otras ofertas por lo que ha de decidirse lo antes posible y este dejándose llevar por lo atractivo del precio da una señal al supuesto propietario. Resultando al final un fraude donde el supuesto comprador se lleva la cantidad dineraria otorgada por el comprador y este último perdiendo su dinero ya que además no existe tal inmueble. Además existe otro fraude online muy parecido a este anterior donde se anuncia en una web la venta de un inmueble, con una oferta muy competitiva en el mercado para atraer al comprador, este último contacta con el oferente del bien inmueble, transmitiéndole su interés por el bien y el ofertante le dice que no es el único que se ha interesado y que si quiere llevárselo antes que nadie deberá darle una señal cuanto antes, ingresándolo en su número de cuenta. Cuando el comprador realiza la transferencia, no vuelve a saber nada del oferente y conforme investiga descubre que esa casa tiene un propietario distinto del que se la vendía, dándose cuenta que le habían estafado y había perdido su dinero. Otra variante de este fraude se realiza a través de una oferta en internet donde pone a la venta o en alquiler un bien mueble o inmueble, observándose una serie de fotografías que muestran supuestamente la apariencia del bien, se realiza el pago del producto y luego cuando se tiene el bien obtenido resulta que no corresponderse con la realidad que mostraban las fotografías, perdiendo el dinero.

2) Fraudes en compra-venta online al comprador y al vendedor (EBay).

Este fraude metodológicamente hablando es muy parecido a la compra-venta o alquiler de vivienda. Ya que se realizan ofertas de diferentes productos en la web EBay, donde el comprador puede elegir que producto y oferta quiere y le convence más, realizando normalmente una forma de pago electrónica dentro de los 3 días siguientes a la adjudicación del bien donde tras finalizar la transacción puede resultar estafado de forma que pierda el dinero ya sea con un anuncio falso o con un producto notablemente desmejorado a como se ofrecía, una apropiación del dinero por medio de los sistemas

de pago como PayPal, una burda imitación o simplemente no llegándole nada. (Legalitas, 2015)

Volviendo a las formas de pago aparentes en Ebay como son la subasta o cómpralo ya, permitiéndote este último comprar un producto con precio fijo sin esperar a que termine la subasta. Podemos encontrar dentro de las subastas de EBay otra forma de estafar al usuario, mediante distintas metodologías:

- Bid shielding.

  Esta metodología aparece cuando dos delincuentes acuerdan realizar una serie de pujas en una subasta, realizando uno de ellos una puja con una cantidad dineraria desorbitada provocando que los participantes en dicha subasta no puedan igualarla provocando la retirada de los participantes y el otro delincuente realiza una puja sensiblemente menor que la de su cómplice pero superior a la del resto de participantes quedando en segundo lugar en la clasificación de la subasta. Ganando posteriormente el delincuente con la puja desorbitada, pero a la hora de aceptar el objeto este lo rechaza y pasa a manos del segundo estafador que realizó la puja menor, obteniendo el objeto por menor valor. (Theguardian, 2007)

3) Ofertas de trabajo falsas.

Para que esta estafa se desarrolle primeramente el sujeto engañado debe haber ofrecido su currículum en varios sitios de Internet, siendo posible que haya sido observado por los estafadores y recabado sus datos. Consistiendo la estafa en ofrecerle un puesto de trabajo, informándole de un previo pago de una serie de gastos de gestión, con unas condiciones salariales muy buenas que no son reales puesto que el trabajo ni siquiera existirá.

4) Oportunidades de negocio falsas.

Esta estafa es similar al timo de oferta de trabajo falsas. Es consiste en ofrecer grandes rendimientos o trabajos muy rentables, pidiéndose una cantidad dineraria por anticipado en concepto de permisos, compra de material, etc. No llegando nunca ese trabajo ofertado. En las modalidades más modernas de la estafa se llega incluso a crear una página Web con toda la apariencia de ser una auténtica organización que ofrece realmente el negocio o trabajo.

5) Redes piramidales.

Las redes piramidales hace referencia al tipo de estafa piramidal, siendo esta un fraude en la que no existe una actividad o inversión real que la sustente, sino que los beneficios

que los usuarios obtienen provienen del dinero que invierten otros usuarios, normalmente los nuevos, es decir, yendo el dinero que invierten los nuevos a los antiguos inversores. Tales empresas no invierten el dinero como dicen sino que los nuevos sustentan la red de inversión pagando a los antiguos y la empresa en cuestión se queda con una parte.

6) Estafa nigeriana.

La estafa nigeriana o fraude nigeriano, es un fraude muy extendido actualmente a través del correo electrónico. Las estafas de este tipo consisten en mandar un correo electrónico a diversas personas al azar, ilusionando a la víctima sobre una cantidad económica que ha heredado o que una determinada persona tiene pero para sacarla de su país necesita ayuda. Tras esto se le exige a la víctima una determinada cantidad económica para poder acceder a la herencia o ayudar al millonario que luego le recompensará. Adquiriendo los estafadores la cantidad dispensada y haciéndole perder dinero a la víctima. Adquiere su nombre del número de artículo del Código Penal de Nigeria que viola, dado que buena parte del correo electrónico con este tipo de ofertas proviene de Nigeria.

7) Fraudes en la utilización de instrumentos de pago.

El elemento principal que encontramos para que se cometa este fraude, son los instrumentos mediantes los cuales se realiza el pago, como tarjetas de crédito o cuentas online que gestionen la tramitación del dinero como PayPal. Por una parte el usuario de la tarjeta, realiza un pago autorizado y hasta ahí todo bien, pero si luego observa que se han ido realizando una serie de gastos desde su tarjeta sin su autorización lo demandará y su proveedor de servicios de pago deberá comprobar si ha habido alguna irregularidad, pudiéndose dar el caso que si no observa irregularidad el proveedor no reclama y obtiene ese dinero posibilitando que la persona pierda el dinero. En el caso de PayPal una persona puede salir estafada de forma que se introduce el dinero para obtener determinado objeto esto se le hace llegar al vendedor y este envía el objeto, pero PayPal hace una comprobación más tarde del dinero y si observa que hay alguna irregularidad en él se lo queda en cuarentena, hasta que se pueda resolver, dejando a una parte sin cantidad dineraria.

8) Ransomware**.**

Podríamos decir que aquí se plasma una forma de estafa mas novedosa basándose en la infección de sistemas informáticos mediante virus que bloquean el ordenador, sistema

operativo o archivos, exigiendo para su desbloqueo una cantidad dineraria que se debe abonar de diferentes formas para un determinado individuo u organización.

El virus más utilizado para cometer este tipo de fraudes es el llamado Ransomware, tratándose del genérico en esta modalidad de estafas del que se derivan muchos más. Esta técnica realiza el delito de fraude o estafa por internet mediante la publicitación de un programa lícito como reparador de sistemas operativos o recuperador de archivos, del cual una vez el usuario se lo descarga sale el virus ransomware bloqueando el ordenador y pidiendo una cantidad dineraria para su desbloqueo. (Clucley, 2014)
Teniendo en cuenta la generalidad de este tipo de virus, podemos mencionar una serie de subgrupos donde a su vez encontraremos subtipos que derivan de él, continuando con la realización de conductas delictivas del ámbito de fraudes por internet:

- *Winlocker*.
En este grupo se presentan los ransomware de SMS. Este tipo de malware bloquea el sistema exigiendo el envío de un SMS con cierto código a un número de tarificación adicional. (Spyware, 2014)

- *Ransomware de MBR*.
Esta variante del ransomware es de las que más asusta a los usuarios, aunque no es tan complicada de solucionar como otras. Debido a que afecta al arranque principal o maestro, en inglés MBR (*Master Boot Record*) dándole nombre ha dicho ransomware, modificando el registro de forma que se interrumpe el proceso de arranque del disco duro. Imposibilitando que el usuario pueda iniciar el sistema para intentar eliminar la infección. (Crespo, 2012)

- *Cifrado de ficheros*.
Este tipo de ransomware es el más popular de entre estos malware defraudadores. Se dedica a cifrar archivos y carpetas del ordenador del usuario, de forma que queden inaccesibles para este, a menos que realice el pago del rescate exigido. En algunos casos también se bloquea el acceso al sistema. Dentro de este subgrupo encontramos varios subtipos de este ransomware:

- *Teslacrypt*.
Se trata de un tipo de virus que se introduce en el ordenador de diferentes usuarios infectando estos, provocando que se encripten diversos archivos existentes en el ordenar. Principalmente este virus se distribuye por los videojuegos que descargan los

usuarios donde al ejecutarlo se infecta el sistema informático, encriptando numerosos archivos de distinto tipo pero primordialmente partidas guardadas y archivos esenciales de otros videojuegos, utilizando el método de encriptación AES. Además el medio de pago para desencriptar los archivos podrá ser bitcoin o Paypal que aun siendo más peligroso este último para el desarrollo de los hechos por parte del hacker ya que se controla la ruta del dinero, se suele utilizar bastante debido a la mayor popularidad que posee sobre el bitcoin en cuanto a usuarios se refiere. (Risk, 2015)

- *AlphaCrypt*.

Nos encontramos ante el virus sucesor de Teslacrypt, tratándose del mismo tipo de virus entrando por los ordenadores de los usuarios a través de mensajes por correo electrónico o mediante programas, algunos malintencionados como son el Angler Exploit Kit (programa que puede esconderse de la detección de antimalware desarrollando el malware así como el ciclo de la vida del ataque). Como su antecesor se dirige fundamentalmente a jugadores de videojuegos. Su función defraudadora como el Teslacrypt es el bloqueo de los archivos mediante el encriptamiento de estos existentes dentro del ordenador del usuario infectado, donde una vez están todos infectados cambia el fondo de pantalla del escritorio avisando de que si se quiere desbloquear los archivos se han de seguir una serie e instrucciones para transferir mediante bitcoins y por la red Thor una determinada cantidad dineraria. (Risk, 2015)

- *Cryptowall y Cryptolocker*.

Estos virus derivados de las consiguientes derivaciones del virus ransomware como hemos mencionado previamente (Teslacrypt y AlphaCrypt), afecta a usuarios de Windows usando tecnología avanzada de encriptación, encriptando no todo el sistema operativo sino archivos importantes de los ordenadores de los usuarios infectados, pidiendo para su desbloqueo una determinada cantidad dineraria que se abona de forma anónima mediante bitcoins y la red Thor. Esto virus son introducidos en el sistema informático, mediante aplicaciones legítimas encontrándose enmascarados, siendo detectados de forma tardía por los antivirus y son ejecutados por descuidos o confianza excesiva del usuario. Su modus operandi y fin es el mismo pero son diversos tipos de virus que se propagan por diferentes programas lícitos para abarcar distintos tipos de bloqueo de archivos para luego más tarde realizar el chantaje ya mencionado con anterioridad. (Pc risk, 2014)

Tras haber observado estos subgrupos de ransomware, podemos hablar de otros archivos bloqueadores sin encriptación. Los cuales realizan el secuestro del sistema de otra forma pero persiguiendo el mismo fin de remuneración económica, produciéndose una toma de control del sistema sin encriptar los datos. Por regla general, el malware desactiva el administrador de tareas, amurallando el acceso al registro e infecta el fichero EXPLORER.EXE, el cual es muy importante y necesario para encontrar archivos y carpetas en Microsoft Windows, para hacer desaparecer los iconos del escritorio y así impedir que se usen programas. Ya en los casos más sofisticados también impiden arrancar en Modo Seguro. Aun no siendo fácil deshacerse de ellos, al no existir encriptación de datos es posible recuperar el equipo instalando un antivirus.

9) Phising.

Es la forma de defraudar por internet que más se ha repetido a lo de largo de los años. Esta técnica se desarrolla mediante un envío masivo de correos electrónicos mediante spam, que simulan proceder de entidades oficiales normalmente bancarias imitando el mensaje oficial de dichas entidades en el diseño, logotipo, firma, caracteres, etc. A través de este engaño existen 2 formas de extraer los datos de los usuarios/víctimas; Una mediante el envío de correos electrónicos con la misma estructura que los oficiales como hemos mencionado, donde en el mismo correo aparece un formulario a rellenar por el individuo afectado, donde se le pide que deposite una serie de datos personales relacionados con su cuenta bancaria, normalmente a partir de alguna excusa como "debido a un problema con su cuenta bancaria esta ha quedado bloqueada, por favor deposite todos los datos que le requerimos para poder solucionar el problema, gracias." Otra forma de defraudar, se realiza partiendo siempre de la misma base del envío masivo de correos electrónicos con igual estructura, donde la diferencia radica en que cuando el usuario abre el correo recibido, este en vez de mostrarle un formulario donde requerirle datos personales lo redirecciona a una página web que es exactamente igual en apariencia a la de la concreta entidad bancaria por la que el phisher[2] se está haciendo pasar y solicita una serie de datos que normalmente no se hubieran requerido, para que el usuario establezca su datos personales, y poder ser utilizados estos de forma fraudulenta. Esta es la forma más común de expresión de la conducta de phising pero también se puede desarrollar mediante contactos en las redes sociales, enlaces o virus informáticos que permitan el apoderamiento de las claves de acceso y contraseñas de seguridad. Este fraude parte de un origen donde su objetivo final es extraer una

[2] Es un tipo de delincuente que hace o crea sistemas para hacer realizar la conducta delictiva de phising, engañando a personas para obtener información bancaria o personal con la que puedan hacer fraude de algún tipo.

determinada cantidad dineraria de las cuentas bancarias de los usuarios que han engañado extrayéndoles los datos necesarios para la intromisión. En este objetivo final aparece la figura del mulero (el cual se lleva una comisión), los cuales habilitan cuentas corrientes legales abiertas para recibir la transferencia que efectúa el estafador, para que dichos muleros retiren la cantidad transferida de forma inmediata o de ahí la transfieran a cuentas en el extranjero que sean difícilmente detectables por la legislación del país donde se realiza el fraude.

Una vez visto todo esto podemos pasar a realizar una clasificación de conductas fraudulentas que derivan de la técnica del phising:

- Phising Tradicional.

Se hace uso de imágenes y metodologías de entidades u organismos por la que el delincuente se hace pasar, cambiando la dirección a la que se dirigen los datos ingresados por la víctima robando así las credenciales de esta. Teniendo como característica principal este método, que solamente está ligado a un sitio web donde se alojan todos los contenidos del portal falso.

- Phising redirector.

Este es muy parecido al phising tradicional, realizando campañas masivas de envío de correos electrónicos, copiando imágenes y metodologías. Pero se diferencian en que este tipo posee un mayor nivel de complejidad, ya que utiliza por lo menos 2 o más sitios o dominios para perpetuar la estafa, pudiendo destacar el uso de acortadores de URL´s, y la inyección de los conocidos iframes[3]. Aun siendo técnicas distintas tienen en común que utilizan una redirección para reflejar un sitio almacenado en determinado servidor, desde otro servidor. (Paus, 2015)

- Spear phising.

Este es un tipo de phising que va dirigido a grupos reducidos o a determinadas personas. En este caso las víctimas llevan a recibir mensajes personalizados con nombre, apellidos, incluso falsificando direcciones conocidas para crear más empatía hacía el afectado. A la hora de atacar a las entidades u organismos no van a por estas de forma general sino a por sus empleados individualmente y siempre en departamentos alejados

[3] Se trata de una línea de código de programación que permite colocar un elemento HTML dentro de otro objeto HTML principal, es decir, una etiqueta dentro del código de programación para mostrar otro sitio web de forma más pequeña, una ventana dentro de otra ventana.

de conocimientos técnicos de informática, para tener mayor probabilidades de que el usuario caiga en la trampa.

- Whaling.

El whaling es un tipo de phising que tiene como característica principal el objetivo al que se dirige; gerentes, directores o personas importantes dentro de grandes empresas. La técnica es similar a los procedimientos anteriores, con envío de correos electrónicos copiando la apariencia para parecer oficial, sin embargo contiene código maligno que es transferido al ordenador del usuario con el fin de captar información personal, y permitir al remitente asumir el control del sistema intervenido.

Tras haber mencionado una clasificación de conductas derivadas del phising hemos podido comprobar como este ha ido evolucionando, desde el más tradicional obteniendo datos de manera indiscriminada sin ningún tipo de filtro de información afectando a la totalidad de usuarios de internet. Hasta métodos más modernos como los otros tres apartados que hacen referencia a un tipo de phising con objetivos más concretos a la hora de obtener datos, siendo selectivos y no masivos como los anteriores, es decir, poseen la misma forma de ataque pero varía su víctima, no tratándose ya del cliente de un banco o un organismo concreto sino los empleados de estas mismas, así como los objetivos de más alto nivel como pueden ser directores de la empresas u organismos. Con todo esto podemos pasar a hablar de las diferentes fases por las que pasa el phising, es decir, por las fases en que se va desarrollando el phising. Pudiendo definirse estas fases según el instituto nacional de tecnologías como un conjunto de pautas más o menos estable en los ataques realizados por este tipo de delincuentes. Aun así dichas fases pueden variar en cuanto profundidad, extensión y dificultad se refiere, debido a las diferentes formas de enfocar la técnica del phising. Seis son las fases principales que aparecen en todo ataque phising:

- Planificación.

En esta etapa el phisher toma las principales decisiones que va a llevar a cabo, las cuales son: remitente del ataque, como se va a realizar y donde, qué tipo de engaño se va a utilizar, que medios serán necesarios para llevar a cabo la conducta fraudulenta, con qué objetivo se realiza el fraude, etc. Siendo esta primera acción común a todas las conductas de phising analizadas previamente, así como tomar la decisión de realizar el ataque de forma colectiva o en solitario.

Siguiendo con esta fase el delincuente se planteará que tipos de datos desea obtener: cuentas bancarias, nombres de usuario y contraseñas, datos personales de diversa

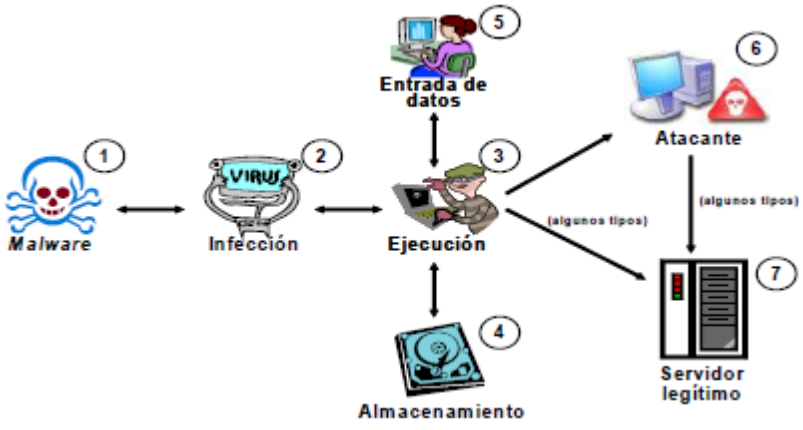
índole, etc. Estando este planteamiento al tipo de fraude que se intenta cometer, ya que como hemos plasmado. Además, El número de agentes implicados así como el lugar que se desea atacar y a quien, a la hora de la realización de las tareas determinan el grado de complejidad del ataque.

- Preparación.

En esta etapa comienzan a aparecer las diferencias entre los diferentes ataques de phising, apreciables en las tareas de creación y consecución de cada uno de los ataques. Aquí estos delincuentes han de conseguir el software, datos de contacto, localizador de los destinos de sus ataques, preparar sus equipos informáticos para el ataque, construir los sitios webs fraudulentos para realizar al estafa y otras muchas tareas siempre teniendo en cuenta las necesidades de cada tipo de delito ya que muchos son diferentes. En caso de que los delincuentes decidan realizar ataques muy específicos dirigidos a personas u organizaciones, han de realizar un envío de correo mucho más elaborado que los que se utilizan en envíos masivos, pudiendo destacar de estos ataques su estudiada segmentación en la búsqueda de objetivos y preparación de la trampa. Con todo esto, decir que los estafadores en la fase de preparación harán sus cábalas, estimando sus costes y beneficios entre elegir un ataque más o menos complejo, conociendo así si su acción es rentable.

- Ataque.

En esta habrá 2 formas diferenciadas de proceder según el objetivo seleccionado, siendo una el servidor de la empresa u organismo objetivo donde realizar el ataque, y otra preparando las trampas para que los usuarios caigan en ellas. Requieren del concurso de las víctimas en los casos de complejidad media o alta, ya que al tratarse de abrir correos electrónicos, enlaces o páginas webs, son acciones necesarias para que el ataque se lleve a cabo. Pudiendo plasmar todo lo explicado mediante un esquema.



- Recolección.

Esta es la fase que consiste en la espera hasta que los usuarios caigan en la trampa creada por phisher, ya sea entrando en el servidor atacado, que respondan al mensaje enviado o visitando la página web fraudulenta. En todas estas conductas es necesaria su ejecución por parte de los usuarios para conseguir los datos necesarios.

- Fase de ejecución del fraude.

En esta fase una vez se ha dado la obtención de datos, se produce la realización de la estafa, ya sea de forma directa o indirecta (vendiendo los datos robados para que otros delincuentes los utilicen para conductas fraudulentas).

- Post-Ataque.

En esta fase tras haber consumado el fraude, el phisher realizará actuaciones destinadas a eliminar las pistas que hayan podido quedar, borrando código maliciosos, de rastros electrónicos, de webs fraudulentas así como borrado de los registros de los motores de búsqueda. Y además de todo esto procederán los delincuentes al lavado (blanqueo) de los beneficios obtenidos de la operación y otros procesos normales en cualquier tipo de robo o fraude.

10) Pharming.

Se trata de una técnica muy parecida al phising, pero digamos más concreta, donde se realiza una suplantación de correos electrónicos o páginas webs, de forma que parezcan idénticas a las originales. El estafador mediante la emisión del correo electrónico redirecciona a través de la modificación del sistema de resolución del nombre del dominio (DNS) a la víctima a la página web suplantada, produciendo que cuando la víctima establezca el dominio de la página a la que quiere acceder le redirecciona a la copia de tal página al engañado para que introduzca ahí sus datos y puedan ser captados por el estafador. (Crespo, 2015)

4.2.2 Diferentes formas de defraudar por internet.

En este apartado de diferentes formas de defraudar por internet, hablaremos de forma general de algunos métodos de defraudación diferentes a los vistos en el apartado anterior y nos centraremos en los fraudes que encontramos en la telefonía móvil en los llamados Smartphones, como dispositivo que más ha evolucionado y popularizado con el paso de los años, debido a que ha simplificado la forma en la que cubrir nuestras necesidades tecnológicas, adaptando un GPS, una cámara de fotos/video, un

ordenador, etc.. Al ser el dispositivo que más ha evolucionado y que más se utiliza entre todas las personas del mundo, los estafadores se adaptan a este movimiento creando nuevos fraudes que se ajusten a las motivaciones de las personas para hacerles caer en el engaño. Por lo tanto los fraudes que nos podemos encontrar en diferentes dispositivos y algunos en concreto en el Smartphone son:

- Fraudes en SMS y llamadas de alta tarificación.

Estos tipos de fraude únicamente se han ido realizando a través de la telefonía móvil, donde en ningún momento han precisado conectarse a páginas webs mediante internet, siendo una herramienta prácticamente inútil en este tipo de estafas. Desarrollándose actos como la llamada recibida por parte de la víctima que al contestar se le cargan en su facturación gastos derivados de esa llamada, o el SMS que recibe la víctima que al abrirlo se activan una serie de emisiones de mensajes hacía el número de dicha víctima con los costes correspondientes por ello, reflejándose en la factura. Además existe otro timo mezcla entre estos 2, donde la víctima recibe un SMS informando de que ha habido una incidencia con su dada de alta (en algún lugar) y que debe de llamar a un número, al cual llama y le redirecciona a otro hasta que la víctima se cansa y deja de llamar, pero ya le han cargado los gastos de esas llamadas.

Actualmente la estafa se desarrola ofreciendo un servicio o un juego por ejemplo que para obtenerlo y bajarlo de internet necesitas introducir tu número de teléfono donde por consiguiente se te enviará un sms diciéndote que el número recibido en tal mensaje se debe introducir en la zona de la página web donde solicita un código, el cual denegará el número diciéndole que no se corresponde, habiéndose suscrito la víctima sin saberlo aún servicio de mensaje Premium donde por cada mensaje recibido le cobrarán una determinada cantidad dineraria.(Osiseguridad, 2012)

- Smishing

Primeramente diremos que el Smishing o Smishing SMS es una variante del popular fraude conocido como phising. En este caso, la actividad fraudulenta de forma general se realiza empleando mensajes de texto (SMS), dirigidos a usuarios del Smartphone receptor intentando convencer a este con reclamos atractivos de que realice una determinada llamada, visite página web fraudulenta, que conteste al SMS recibido y todas aquellas conductas que supongan un coste adicional, realizándose prácticamente de la misma forma que el apartado anterior.

Su objetivo fundamental con estas conductas es robar datos privados y personales, infectando el teléfono móvil con algún virus, para obtener rendimiento económico mediante acceso bancario o cargando una serie de gastos en la factura del teléfono

móvil. Pudiendo ratificar esa conducta con algunos ejemplos que se pueden encontrar: (Osiseguridad, 2013)

- *«Sólo necesitamos tus datos personales, envía un SMS desde tu móvil con la palabra OFERTA al [número] y te pediremos la dirección de tu domicilio. En un plazo de 20 días te enviaremos el Reloj.»*
- *«Tiene un aviso importante. Llame al [número].»*
- *«Envíenos la siguiente documentación copia de su tarjeta de coordenadas y su tarjeta bancaria [banco] y anote también el pin al correo: [correo].»*
- «Estimado cliente, su tarjeta visa ha sido bloqueada por su seguridad. Para desbloquear su tarjeta visite urgente [web] y complete los pasos tiene 24h.»

- Vishing

Este fraude proviene de la unión de dos palabras en inglés, las cuales son voice y phising. Indicando, como muestra su nombre que se trata de una variante del phising realizada a través de un teléfono móvil usando la voz para producir el engaño. Este fraude consiste en el envío de un correo electrónico donde los delincuentes configuran detalles de datos bancarios mediante una llamada gratuita, donde una voz computarizada o VozIP de aspecto profesional, requiere a las víctimas (como clientes de la entidad bancaria) la confirmación de su cuenta bancaria solicitándoles número de cuenta bancaria, número de tarjeta, número de pin, fecha de expiración de la tarjeta o cualquier otro tipo de información importante.

Esto se realiza concretamente, configurando por parte del delincuente un war dialing que consiste en hacer una serie de llamadas automatizadas para comprobar si habían módems conectados y permitían la conexión de otro ordenador, y si los había y se cogía la llamada automáticamente se envía al correo un mensaje donde se informa a la persona engañada que hay un problema con su tarjeta o está siendo usada de forma fraudulenta indicándole que debe llamar a un determinado número gratuito para solucionar el problema donde se le requerirán una serie de datos mencionados previamente pudiendo realizar al estafa.

- Apps (Aplicaciones).

Este fraude que se menciona en este apartado hace referencia a las aplicaciones que los usuarios de Smartphone nos bajamos con tanta facilidad y credulidad de lo que nos ofrecen. Los usuarios en este campo piensan que al tratarse de un teléfono móvil hay menos riesgos que con el ordenador, pensamiento que no es cierto y que estos delincuentes aprovechan para cometer este tipo de fraude mediante las denominada

“Apps Falsas”. Las aplicaciones donde se centrará esta estafa son en las de mensajería instantánea como WhatsApp, Telegram, Line. Las cuales son las más popularizadas y por ello poseen más copias o actualizaciones fraudulentas. Pero no debemos dejar de lado al resto de aplicaciones que podemos encontrar en cualquier tienda online oficial (ej: play store) que también pueden ser fraudes bajo otra apariencia, desde indicadores del nivel de batería, linternas y hasta supuestos rayos infrarrojos para ver a través de la ropa de la personas. Pudiendo destacar varias aplicaciones genéricas de este tipo como son “Escáner desnudo”, “Súper Jumper X”, “Virus Shield”.

- Escáner desnudo y Súper Jumper X.

Son 2 aplicaciones que Captan a los usuarios con la falsa promesa de poder ver a cualquier persona en ropa interior si se le escanea usando alguna de estas 2 aplicaciones. Por ello, promovidos muchos usuarios por las ganas de invadir la intimidad de otras personas se ven seducidos por las funcionalidades que ofrece la aplicación sin pensar en lo fraudulento de sus promesas, provocando que una vez los usuarios se la descarguen estos sean subscritos sin que se den cuenta a servicios de mensajería Premium. Además estas aplicaciones una vez instaladas, indican al usuario que ha de instalar nuevas aplicaciones por lo que este clickea para descargar dichas actualizaciones y la propia aplicación enlaza de manera aleatoria con otras aplicaciones fraudulentas dentro de la tienda google play para ser descargas en el dispositivo del usuario. A continuación estas nuevas aplicaciones intentan engañar al usuario para que compre un antivirus dándole avisos de que el dispositivo está infectado, recomendando la instalación de un determinado antivirus como es Antivirus Pro for Android con un coste para el usuario de 17,24 euros.

-Virus Shield.

El caso de esta aplicación falsa, es bastante conocido porque llego a tener más de 10000 descargas en google play y entre las 3 aplicaciones de pago más populares. El Virus Shield, consiste en una “app estafa”, que promete proteger tu Smartphone de cualquier tipo de amenaza, además de tu información personal y consumiendo poca batería, no siendo realmente así ya que lo único que realiza la aplicación es realizar un tic sobre el escudo (imagen de esta aplicación) al tocar la pantalla para simular que el dispositivo se encuentra protegido, suponiéndole un gasto al usuario de 4 euros por su descarga.

Centrándonos ahora en las aplicaciones de mensajería instantánea que hemos mencionado previamente y partiendo de la base de que estas aplicaciones son las más populares, podemos decir que este tipo de delincuentes aprovechando esto y utilizando

la técnica de la ingeniería social (técnica en la que se basan todos los fraudes en internet) captan a los usuarios para que descarguen estas aplicaciones ofreciéndoles algo atractivo para ellos como prometer que con esas aplicaciones pueden espiar conversaciones de otros usuarios, acceder a funciones aun no disponibles como cambiar la apariencia de la aplicación, etc.
Pasando tras todo esto, a centrarnos primeramente en los fraudes relacionados con la aplicación WhatsApp:

- Fallo de seguridad en Android que permite leer las conversaciones.

Este fraude aparece cuando el hacker Bas Bosschert[4] realizando una de sus numerosas investigaciones descubrió que WhatsApp guarda las conversaciones en la tarjeta sd del dispositivo donde se encuentre instalado en caso de que el dispositivo disponga de dicha tarjeta de memoria, claro está. Por lo que se crea una base datos con nuestras conversaciones y archivos privados. Tras conocerse esto los delincuentes comenzaron a crear herramientas para intentar conseguir esas conversaciones y archivos privados teniendo muchos como objetivo obtener un determinado rendimiento económico, empezando a aparecer aplicaciones falsas que aparentaban ser una cosa que luego no eran para que los usuarios las descargaran y así poder acceder a esa gran base de datos que hemos mencionado. Una vez se abren estas aplicaciones en el dispositivo móvil se copian dichos datos en su totalidad, descifrándolos y llevando los datos a un servidor propiedad del determinado delincuente quedando almacenados para su uso fraudulento. Pidiendo posteriormente una determinada cantidad económica por el borrado de los datos copiados o usando algunos datos personales como bancarios plasmados en alguna conversación. Durante el transcurso de este fenómeno WhatsApp comenzó a mejorar el cifrado de los mensajes y archivos enviados pero aun así no es suficiente ya que estos delincuentes se siguen reinventando para seguir perpetrando esta conducta delictiva. Un ejemplo de este caso sería la aplicación ya eliminada Ballonpop2, la cual se ofrecía para ser descargada en google play store siendo esta un juego en donde había que explotar una serie de globos con un cañón, no encontrándose el problema en su apariencia externa sino en lo que realizaba en segundo plano mientras el usuario jugaba a explotar globos, introduciéndose en los archivos del dispositivo en donde la aplicación estaba instalada y haciendo una copia de estos (fotos, mensajes de voz conversaciones de WhatsApp, etc.) la cual redireccionaba a un

[4] Ingeniero informático de nacionalidad holandesa experto en seguridad que trabaja como director de tecnología en Double Think.

servidor propiedad del estafador, buscando con esto una remuneración económica como hemos mencionado previamente. (Enriquecuartas, 2014)
Esta estafa hoy día aunque se sigue perpetrando no es de las más populares, utilizándose esta intrusión en la vida privada de los usuarios por motivos de investigación. (Alonso, 2013)

- WhatsApp Spy.
Esta estafa se basa en el ofrecimiento al usuario de poder espiar las conversaciones ajenas de los diferentes contactos que se poseen, buscando su captación. Ya que esta no es la auténtica función que realiza la aplicación, sino que realmente lo que suele hacer es acumular datos del dispositivo, instalar malwares o incluso subscribir al usuario a servicios de SMS Premium sin que este sea conocedor total de la práctica. Podemos mencionar que esta modalidad de aplicación espía falsa también se introduce en el ámbito de las redes sociales como Facebook donde se promete hackear las cuentas pudiendo entrar en estas y observar el movimiento de las cuentas ajenas a los usuarios, engañando al usuario realizando posteriormente conductas fraudulentas sobre él. Este fraude en internet en los Smartphones es el claro ejemplo de como el criminal se aprovecha de la inocencia y el deseo de información en este ámbito del usuario el cual no es conocedor de la ilegalidad de esa práctica espía, lo que le tendría que hacer sospechar de descargarse esa determinada aplicación.

- Fraudes vía navegador.
Este fraude deriva del anuncio que se realizó para informar de que WhatsApp iba a tener página web, para poder mantener conversaciones también mediante el ordenador. Ampliando de forma exponencial las probabilidades de estafa, debido a la novedad de dicha página ya que la mayoría de usuarios no son conocedores totalmente de la apariencia de la web, de los servicios que proporciona, posibles fallos de seguridad, etc. Provocando que muchos usuarios descargaran aplicaciones en sus ordenadores de webs fraudulentas sin saber que se trataba de un troyano que permitía al delincuente obtener información confidencial, logrando acceder a datos bancarios de los usuarios.

- Desactivación doble check azul.
Esta estafa aparece también debido a una nueva famosa actualización de esta aplicación (WhatsApp), llamada doble check azul, consistiendo en una confirmación de lectura por parte del receptor al mensaje que había enviado el emisor, observando este último que efectivamente había sido leído el mensaje que había enviado. Al tratarse de una novedad tan polémica en donde muchos usuarios mostraban su rechazo por temas

de privacidad e intimidad. Muchos de estos delincuentes aprovecharon esto para difundir a través de la redes sociales como twitter una nueva aplicación que si la instalabas se quitaba el doble check azul automáticamente. Subscribiendo a los usuarios que descargaban esta aplicación falsa a una serie de servicios Premium.

- WhatsApp Oro.

Este fraude viene motivado por una aplicación que recibe este nombre, es muy conocido debido a que muchos usuarios se vieron afectados por él, informando de su peligrosidad tanto la policía nacional como la guardia civil. Esta aplicación fraudulenta engaña a los usuarios ofreciéndoles una actualización exclusiva, que dota a WhatsApp de unas funciones y servicios que la aplicación normal no posee. Este fraude se promociona mediante las redes sociales como máximo exponente y mediante su ofrecimiento en google play el cual eliminó cuando comenzaron a aparecer los diferentes sucesos de estafa. Cuando el usuario teclea o selecciona la aplicación esta le direcciona a una página web fraudulenta donde para disfrutar supuestamente de las mejoras que le da esta aplicación debe introducir su número de teléfono subscribiéndose así a un servicio de SMS Premium, donde cada SMS recibido cuesta 1,45 euros, hasta un máximo de 36,25 euros mensuales.

- Localizador de WhatsApp.

Este fraude es algo diferente a los demás ya que el delincuente utiliza la red social Facebook junto con la aplicación WhatsApp para producir el engaño en el usuario, ofreciéndole un localizador para encontrar en Facebook los contactos que el usuario posee en WhatsApp. Subscribiéndose el usuario a un falso localizador que le ayudaría a saber dónde se encuentran sus contactos, suscribiéndose realmente a un servicio de envío de SMS Premium, cobrando a la persona afectada 1,45€ por cada mensaje recibido.

- Falsos contestadores de WhatsApp.

Los estafadores en su renovación continua se inventan nuevos servicios de WhatsApp que no existen para seguir engañando al usuario y obtener de ellos un rendimiento económico. Este fraude trata de un correo electrónico que recibe el usuario notificándole que tiene un mensaje de voz en un supuesto contestador de WhatsApp. Siendo este contestador inexistente. Si el usuario pincha en el enlace dispuesto a escuchar el mensaje de voz se le descargará un software malicioso que permitirá la total disposición del dispositivo por parte de los delincuentes con objetivos fraudulentos.

Además, mencionamos como último apunte que la mayoría de descargas fraudulentas se producen en las páginas no oficiales.

Podemos comentar otros puntos en contra de otras aplicaciones de mensajería instantánea, también conocidas pero no tan populares y mundialmente establecidas como WhatsApp, siendo estas Telegram y Line, no habiéndose producido grandes afecciones en forma de estafas para los usuarios bajo el nombre de estas aplicaciones. En el caso de Telegram podemos decir que aun presentándose como una herramienta de mensajería muy segura con aspectos abanderados de dicha seguridad como:
- Cifrado robusto en sus comunicaciones, que las hace indescriptibles en caso de que terceros las intercepten. Incluso interponiendo un reto donde si alguien conseguía descifrar los mensajes que intervenían en una conversación se les otorgaría 200000 dólares.
- Posibilidad de autodestrucción de mensajes por un tiempo determinado.
- Chats secretos con conversaciones seguras entre 2 móviles donde nadie puede ver el contenido de las conversaciones.

Encontramos actuaciones que realiza la aplicación, que de ser usadas de forma fraudulenta pueden hacer mucho daño al usuario, como es poner el número de teléfono como único identificador y almacenar nuestra agenda de contactos en su servidor a un pidiendo autorización. Una estafa que podemos encontrar que también afectó a Telegram entre otros, es la estafa de la app de la cámara de visión nocturna. Esta consistía en que una vez el usuario la descargaba en su dispositivo le contrataba una serie de servicio de mensajería Premium, es decir, a un servicio de SMS Premium. Lo particular de este caso es que accedía a aplicaciones como WhatsApp y en este caso Telegram (que supuestamente es infranqueable) para obtener el número de teléfono del afectado y contratare sin que se diera cuenta dicho servicio de pago. Esto denota que Telegram también posee flaquezas. (Sorivella, 2014)

Con respecto a Line, aun siendo una aplicación con una seguridad muy alta perseverando mucho en la privacidad de sus clientes. Encontramos desventajas no tanto con los posibles fraudes que pueden existir sino más bien con la funcionalidad de cara al usuario. Line presenta tantas opciones de funcionalidad en busca tanto de la expansión del ocio del usuario como de la privacidad, que a veces llega agobiar al usuario al verse un poco perdido con tanta funcionalidad, además posee un alto consumo de RAM así como de batería, algo muy negativo debido a la ya de por si poca duración de estas en los Smartphones. No posee un diseño atractivo dirigido más a

adolescentes que al consumidor medio lo que provoca en parte un rechazo de un sector de la población, ya que por último resulta poco útil en cuanto facilidad de uso, intentando abarcar tantos campos que el usuario en varias ocasiones ya no sabe si está en un servicio de mensajería instantánea o en otro tipo de aplicación. Esta “incomodidad” en cuanto a entendimiento se refiere provoca que los usuarios al menos en España se dirijan a aplicaciones más inseguras, siendo más vulnerables para conductas de estafa o fraude por internet. (OSI, 2014).

En función del sistema operativo que poseamos en nuestro dispositivo móvil accederemos a google play store tienda oficial de apps para Android o a Apps store tienda oficial de aplicaciones para iOS. Siendo este último más seguro que el anterior por una serie de motivos basados en los controles de seguridad que trataremos más adelante.

5.- Casos denunciados de fraudes en internet.

En este apartado se expondrán casos concretos de personas afectadas por este ámbito delictivo en la red, mostrando un pequeño resumen del suceso en donde se puede observar cómo se desarrolló el hecho delictivo y la resolución jurídica que tuvo.

1º **Caso:** En este suceso vamos a exponer un fraude por internet realizado mediante la técnica del phising, apareciendo además la figura del mulero. Sentencia núm. 669/2013.

Una persona logró una serie de datos bancarios personales de su víctima, concretamente de una cuenta corriente perteneciente a dicha víctima, la cual estaba ligada a la empresa donde trabajaba. Más tarde, el acusado empleando los datos personales obtenidos realizó una transferencia ordenada por un desconocido, por importe de 3.124,59 euros de la citada cuenta corriente a una determinada cuenta, de la que el acusado era titular, habiéndola puesto a disposición del ordenante, a sabiendas del carácter fraudulento de la operación, denotando el grado de implicación de este mediante su participación como mulero, logrando así el reo los fondos transferidos.

Tras la valoración de estos hechos, se dictó la sentencia final la cual quedaba así:
Se le impone al acusado una pena de 3 meses de prisión, teniendo en consideración una atenuante por dilaciones indebidas que no recae bajo su responsabilidad.

Observando esta sentencia final, vemos la poca pena que se le impone al reo ante la gravedad del hecho, que incluso siendo su primer delito podría llegar a ser sustituida, quedando prácticamente impune la conducta saliéndole rentable al delincuente. Debiendo ser un poco más severa en un ámbito donde el aumento de pena si podría disuadir la realización de esas conductas. Se sienten seguros tanto por el anonimato con que la realizan así como por la pena tan baja si son capturados. Dejando un sentimiento de desprotección para el afectado.

2º **Caso:** En este caso hablamos del fraude cometido a través del uso de PayPal en una compra-venta por internet en la página EBay.

La víctima de este delito se disponía a efectuar una venta por eBay de un teléfono móvil, que costaba más de 150 euros. Dicho teléfono fue adquirido por un comprador el mismo día puesto a la venta realizándose el pago mediante PayPal. El dinero fue recibido en la cuenta de PAYPAL, ese mismo día y confirmado como pagado. El vendedor al parecerle todo correcto, realizó el envío del teléfono a la dirección que facilitó el comprador. Al día siguiente, el teléfono había sido recogido por el comprador, estableciéndose esto en el informe de seguimiento de correos. Y en ese momento aparece el problema con PayPal, comunicando al vendedor que proceden a retener la cantidad dineraria correspondiente al pago del teléfono, por haber detectado una irregularidad en cuanto a la procedencia de los fondos se refiere. Pidiendo al vendedor (víctima) que envíe toda la documentación posible para acreditar la transacción. Tras esto, PayPal le comunica a la víctima que después de investigar el suceso, han decidido retirarle de la cuenta el importe de la venta y cerrar la investigación, pues según ellos, el comprador ha utilizado para pagar, un dinero que no es suyo. Siendo este suceso sorpresivo para el afectada, optando por llamar al departamento de atención al cliente de PayPal, el cual no es gratis, y tras una larga espera una teleoperadora le dice que no pueden ayudarla porque no existe una política de protección del vendedor, aconsejándole que denuncie por su cuenta. La víctima tras este suceso decide denunciar tanto al comprador como a PayPal por su conducta ilícita, dándose la siguiente resolución judicial:

El comprador no aparece en el juzgado. La víctima tira la toalla por recomendación del juez, ya que como la cantidad defraudada no supera los 300 euros no le pueden hacer nada

En este caso se observa la el vacío de voluntad judicial que existe para paliar estos casos ya que aunque las cantidades dinerarias no sean relevantes, la sensación de inseguridad que deja a los afectados y de impunidad a los autores del hecho, es tal que debería regularse en un capítulo específico esta conducta abarcando mayor campo de actuación ya que no se tratan de fraudes normales, sino que se opera desde un anonimato donde incluso empresas aparentemente serias aprovechan de las diversas artimañas que permite el ciberespacio donde realmente el usuario o posee una gran conocimiento de este mundo ya paralelo o se encuentra totalmente expuesto a los abusos que quieran realizar sobre él, dejando a dicho usuario sin armas y sin enemigo sobre el que proceder. (Ramón, 2012)

3º Caso: En este caso nos encontramos con un fraude en compra-venta online estándar, básico no con lo característico de PayPal si no tradicional. Exponiéndose un resumen del hecho acaecido

La acusada de 19 años de edad, con un determinado Nick en la página web eBay ofreció a través de dicha página web los siguientes lotes:
Un Lote de Móviles Nokia y varios, adjudicándose a una concreta usuaria, por un importe de 107,50 euros. Otro Lote de Nokia n81 Vodafone nuevo a estrenar, adjudicándose a la misma usuaria por un importe de 162,50 euros. Además, de un lote wifi usb zyxel, adjudicándose también a la misma usuaria, por un importe de 43,50 euros.
Dicha usuaria a la cual se le adjudicaron todos esos lotes, con el fin de obtenerlos, procedió a realizar dos ingresos a un determinado número de cuenta facilitada por la vendedora:
Primeramente por importe de 368 euros, que se desglosan en: 323 euros correspondientes al valor de los dos móviles Nokia n81 y 30 euros por liberar los dos aparatos, más 15 euros de gastos de envío. Y seguidamente otro ingreso por importe de 151 euros, que se desglosan en: 107,50 del lote móviles Nokia y varios y 43,50 del lote wifi usb zyxel. Ascendiendo el importe total ingresado en la cuenta citada a 519 euros. Siendo el titular de la cuenta donde se realizaron los ingresos la acusada. Además, la usuario compradora abonó 3 euros en concepto de gastos en cajasol. Resultando finalmente que dicha usuaria no recibe en ningún momento los lotes indicados en el hecho primer ni tampoco la devolución del dinero ingresado en la cuenta de la que es titular la acusada.
Tras valorar estos hechos y analizarlos se realizó la siguiente propuesta de sentencia:
Se condena a la acusada como autora de un delito continuado de estafa, imponiéndose la pena de un año y nueve meses de prisión, con la accesoria de inhabilitación especial

para el ejercicio del derecho de sufragio pasivo durante el tiempo de la condena. Así como indemnizar a la víctima de estos hechos en concepto de responsabilidad civil con 552 euros por el precio pagado y los gastos bancarios. Y todo ello con imposición a la condena de las costas del proceso.

En este suceso, podría decirse que la sanción correspondiente por el hecho ocurrido es bastante justa, ya que aunque la víctima no ha sido estafada por una gran cantidad de dinero (lo justo para ser delito) y sólo no recibiendo los objetos comprados no yendo a mayores, la situación de desamparo en la que se deja la víctima en cuanto a sensación de desprotección se refiere, queda cubierta con la indemnización para recuperar su dinero perdido así como con la pena establecida que es relevante sin exagerar permitiendo una sustitución valorando las circunstancias del autor, asegurando una mejor o mayor reinserción social.

6.- Comparación internacional del hecho.

Después de haber visto como se realizan las diferentes conductas ilícitas de fraude por internet, los diferentes dispositivos que pueden actuar en perpetración del delito, sentencias de casos reales y en general la estructura delictual que crean estos delincuentes, nos disponemos en este apartado a hacer un análisis estadístico del problema en el territorio nacional así como internacional.

6.1. Estadísticas actuales del fenómeno.

En el caso de España podemos extraer los siguientes datos: Las herramientas que más se utilizan en internet son el correo electrónico con un 100%, búsqueda de información y descargas un 75% y el uso de servicios de banca electrónica y las compras online un 50%. Viendo como se da mas uso justamente a las herramientas que más se utilizan para realizar las conductas de estafa hacia los usuarios. Los fraudes por internet poseen altibajos pero siempre con una tendencia de crecimiento, llegando a alcanzar los 20.000 ataques mensuales e incluso superar los 250.000 ataques únicos. En los últimos años se ha aumentado en un 100% el número de sitios web fraudulentos orientados a realizar fraude, siguiendo su aumento con el paso de los años lo que se explica por la sofisticación de los ataques y por el uso de otros medios de comunicación, distintos del correo electrónico, para engañar al usuario. Podemos hablar además de un crecimiento en el número de keyloggers orientados al phishing de en un porcentaje superior al 300%, siendo además del código malicioso que mas producción se registra. Aumentando en estos periodos los ataques de phishing y códigos maliciosos. Un 33,8% de usuarios ha sufrido un perjuicio económico de entre 101 y 500 euros euros por fraude en internet. El

2,9% de los usuarios de Internet en España declaran haber sido objeto de un intento de fraude a través de un mensaje corto recibido en su teléfono móvil (SMS Premium.). Vemos que existen datos que nos muestran que la población sufre ataques de conductas de estafa en gran medida (phishing 41,2%, scam 21,6%, pharming 8,1%, Vishing 4,1%, Smishing 3,7%) pero no la identifican ya que no se ha dado un buen tratamiento de esta problemática por los medios nos sabiendo muy bien en que consisten estos ataques que sufren. Este hecho refuerza la idea necesaria de que se vayan adaptando dichos términos por otros en castellano para un mejor entendimiento del fenómeno delictivo, comenzándose a trabajar sobre eso. Un 73,1% de los usuarios aun habiendo sufrido un intento de phishing al comprar por internet y un 80,2% en la banca online, siguen realizando la conducta no viéndose intimidados sorprendiendo el porcentaje de este último, lo que es bueno para el desarrollo tecnológico debiendo tomar responsabilidades las autoridades e infromar bien de este fenómeno a los usuarios para que no caigan en el engaño. El mayor objetivo del phishing son las entidades bancarias debido a las grandes cantidades económicas que se encuentran reunidas e como demuestran el 82,3% de los usuarios afectados por phishing donde los datos requeridos eran las contraseñas de acceso a su servicio bancario, situándose en un porcentaje bastante menor las compras online 21,5%, las asociaciones o redes sociales 19,5%, de páginas de subastas 18,1% y de servicios de administración electrónica 15,6%.

Pasando a observar los datos que nos ofrece fiscalía con respecto a este delito, vemos la incidencia del delito de estafa infromática en diferentes años bastante recientes:

Año 2012: 64,36% (4.204 casos) de procesos incoados. / Año 2013: 75,30% (5992 casos) de procesos incoados. / Año 2014: 80,59% (9.663 casos) de proceso incoados / Año 2015: 84,39% (17.328 casos).

Aun teniendo en cuenta la gran cifra negra que nos encontramos en esta problemática (pudiendo aumentar los números), hemos de tomar muy en cuenta estas cifras y porcentajes que se nos presentan observando el gran crecimiento que experimenta este fenómeno año tras convirtiéndose en un gran problema a paliar con medidas prácticas efectivas ya que le desarrollo tecnológico va mas rápido que la legislación.

Este crecimiento puede explicarse por el desarrollo de herramientas orientadas a facilitar la actividad de los delincuentes y el cambio de motivación de estos.

Con todo esto, decir que un 22% de usuarios actuales estarían dispuestos a cambiar de entidad financiera en busca de mejoras para la protección de sus datos. Produciendose ese cambio a una nueva entidad de servicio de banca online en un 4% de los usuarios tras haber sufrido un intento de fraude con perjuicio económico, quedándose este porcentaje de cambio en un 1% cuando no ha existido perjuicio económico tras el intento. (Inteco, 2007)

6.2. Abordaje de esta perspectiva en diferentes países

Internacionalmente la conducta ilícita de fraude que mas incidencia tiene es la suplantación de identidad (phishing). Encontrando en Estados Unidos incrementos de 10% al 80%.

En cuanto a la procedencia de la mayoría de los ataques aparecen como principales actores Estados Unidos, la República de Corea y China, aglutinando mas del 50% de los servidores que alojan sitios web de phishing. Pero es En Estados Unidos donde se registra un mayor porcentaje, aun registrando cad año que pasa más la descentralización a otros países.

Estos países de donde sale la conducta defraudatoria de phishing tienen en común es que poseen un mayor nivel de desarrollo económico, ya que esa conducta fraudulenta posee tantas afecciones negativas de gran nivel económico que países con menor riqueza no podrían soportarlo. Ya que tal y como muestran las estadísticas la suplantación de la identidad va dirigda al sector financiero soportando mas del 90% de los ataques. Pudiendo añadir que estos ataques suben relevantemente en los tres últimos días laboralbles concentrándose en el viernes con un porcentaje de 17,2% de mensajes enviados. Intentando que las víctima contesten al correo antes del fin de semana para aumentar el tiempo disponible para la estafa.

En cuanto al ámbito legislativo. Primeramente hablaremos de diferentes países sudamericanos para tener una idea de como se trata a la materia que aquí atañe. Viendo que en Chile se encuentra la ley 19.223 de delitos informáticos protegiendo la información que hay dentro de los medios infromáticos así como la buena práctica con ellos. En Venezuela se encuentra la ley de delitos informáticos de 30 de junio de 2001 con los mismos ámbitos a proteger que la chilenal. En Méjico encontramos en el art.167 fr. VI del código penal federal protección en el ñambito delicitual de fraudes en internet así como el uso fraudulento de datos como en las legislaciones de los otros países mencionados. Colombia también posee regulada esta materia en la ley 1273, regulando los mismos ámbitos que los países sudamericanos ya mencionados. Argentina Ley 26.388 que regula los delitos informáticos protegiendo el daño informático, el acceso a información privada y delitos de pornografía infantil. Hemos mencionar el caso de Uruguay que aprobó en el año 2007 la ley Nº18.237 de expediente electrónico con el objetivo de autorizar la realización de conductas ilícitas para realizar investigaciones, no existinedo un tratamiento específico por la legislación uruguaya en materia de delitos informáticos.

Observando que en estos países menos desarrollados que norte america asia y europa, también existe regulación legal para estos delitos, pero no dbdemos olvidar que su corrupción institucionalizada dificulta mucho que se aplique la ley de forma efectiva.
Lógicamente en Europa, Norteamérica y Ásia, esta regulada esta materia, pero nos encontramos con la problemática de la misma legislación vigente en esos países desde donde se comenten estos hechos delictivos, ya que se recogen unos requisitos diferentes en las diferentes legislaciones dificultando su persecución.Pudiendo decir que en España para considerar determinadas conductas delitos es necesario que se cumpla unos requisitos económicos mínimos fijados de 400 euros, en comparación con otros países como EEUU que para que sea considerado delito la cifra económica se fija en 6000 dólares (5400 euros)Esta diferencia legislativa conlleva que muchos casos queden impunes cuando se realizan desde otros países. Además añadir que países como Reino Unido se presentan como paraísos fiscales para estos delito debido a su secreto y negación a colaborar, encuanto a su persecución se refiere, con documentos o todo tipo de prueba que se le pide en esta materia. (Inteco, 2007)

7.- Impacto del phising

Volvemos a centrarnos en la conducta de phising como conducta que centraliza todas las actuaciones fraudulentas, utilizando esta como media para perpetrar las estafa de otras formas. Por ello cabe destacar dicha conducta de fraude y fijarnos cuál es su impacto tanto social como económico.

7.1.- Impacto económico

La afección que produce el phising en el ámbito económico no sólo afecta al bolsillo concreto de determinados particulares afectados por caer en la trampa, sino que también daña a las empresas. Damnificando con todo esto de forma indirecta a los Estados de los países atacados.
A nivel mundial podemos decir que el daño medio cuantificado que se experimenta por cada fraude exitoso es de 593€. Una cantidad muy elevada si la comparamos con el territorio español en donde 2 de cada 3 fraudes online conllevan un perjuicio menor a los 400€ buscando este delincuente con el código penal anterior no cometer el delito sino la falta en caso de ser descubierto, cosa que ya no sería posible porque se consideraría delito leve debido a la reforma del código penal de 2015.
Haciendo referencia a las estadísticas de países extranjeros del apartado 6, podemos decir que en Estados unidos de forma general se provocó un impacto económico de 1,5 millones de dólares por caso, de ataques mediante suplantación de identidad y en caso de ataques por código malicioso de 2400 dólares. Siguiendo con estados unidos el robo

de información contenidas en un ordenador puede llegar a suponer una pérdida de 90000 dólares, suma extrapolable al ámbito español. Por cada registro de información sustraído produce un sobrecoste para la empresa de 182 dólares, frente a años anteriores donde era de 138 dólares, pudiendo observar el crecimiento al alza de estas conductas delictivas. Además debemos tener en cuenta que cada delito de estafa financiera a perseguir tiene un coste de 20000€.

Concluyendo que el coste total sumando todos los factores intervinientes, para las empresas y consumidores del robo de identidad en 2005 pudo ascender a 56600 millones de dólares. Manteniéndose estable o incluso creciendo con el paso de los años debido al aumento de la aparición de nuevos dispositivos como los Smartphones.

Afecta tanto empresas (credibilidad empresarial los clientes se fian menos, etc.) como particulares. (Inteco, 2007)

7.2.- Impacto social

Tratando la afección social en la que incide la práctica del phising, provoca que se dé un freno en el desarrollo de una economía basada, cada vez más, en las transacciones electrónicas, debido a la desconfianza que se genera en los sistemas de seguridad. Ya que por culpa de esa desconfianza muchos clientes buscan empresas en donde se sientan seguros[5] y un mínimo ataque de esas entidades en las "confían", puede hacer perder a dicha entidad muchos clientes y por lo tanto grandes cantidades dinerarias. Además esto límite bastante el avance tecnológico en diversas materias como hacer la compra sin salir de casa, debido a que los usuarios (68%) desconfían de estas herramientas para dar detalles de sus tarjetas de crédito. En el caso de la banca online pasa igual, no se fían de la seguridad que pueda tener (72%), sólo accederían si tuvieran determinadas garantías de seguridad y privacidad (90%). Siendo esto muy determinante para las entidades financiera ya que la seguridad influye hasta un 65% de los usuarios a la hora de elegir con que banco operar[6]. Además de tener en cuenta el tiempo empleado que dedican estas entidades financieras solventando problemas de seguridad y los ataques que hayan recibido. (Inteco, 2007)

8.- Lucha contra el fraude.

Desde la creación de los primeros sistemas informáticos, se pudo comprobar el gran desarrollo que se realiza en esta materia en poco tiempo, así como el rápido crecimiento

[5] En 2005, un estudio norteamericano mostró que el factor más importante para un usuario en internet es conservar la privacidad de la información transmitida.

[6] Usuarios con cambio efectivo de entidad bancaria tras haber sufrido un intento de fraude. 4% de los usuarios que han sufrido un intento de fraude con perjuicio económico. 1% cuando hay intento de fraude sin perjuicio económico.

que experimentan estas tecnologías. Ya desde los años 50 y la década de los 60, cuando comenzaron los cambios y el crecimiento notorio en esta materia empezaron a observarse la peligrosidad delictual que podían conllevar estos sistemas desde un punto de vista criminológico. Atendiendo a este fenómeno se intentó comenzar a legislar viendo los aspectos comunes que tenían con otras conductas ya sancionables, así como tomando en consideración la posibilidad de la existencia de una gran cifra negra en estas conductas fraudulentas, debido al anonimato que da la red y la difícil detección. Cuando se cometían delitos a través de sistemas informáticos en este caso estafas y se encontraba al autor del hecho, en cuanto a regulación penal se relacionaba el hecho con conductas ya existente en el código estableciéndose penas poco disuasorias o incluso no llegando a sanción penal. Esto exigía una urgente reforma del código penal para adoptar estas modalidades de conductas defraudadoras para adaptándonos a los cambios fruto de la evolución social, pero se hacía complicado debido al carácter transnacional. En España la primera regulación que recogía más expresamente los delitos de estafa mediante medios informáticos fue en 1992 en el art.252.2, pero se trataba de una regulación muy básica que pronto se quedó obsoleta con los avances tecnológicos y los cambios en la forma de defraudar en este ámbito, aplicándose posteriormente una reforma que establecería la regulación que tenemos actualmente, recogida en el código penal en el art.282., donde se sanciona la estafa de la misma forma que la estafa común pero siendo los medios comisivos sistema informáticos, así como sanciona la facilitación de estos medios para la comisión de estos fines a través de ellos como forma de prevención que la práctica sea de fácil acceso para todas las personas. Esto en cuanto a España donde también las F.C.S.E. han recibido formación en esta materia, para adaptarse a estos delincuentes y delitos creando programas de lucha contra estas conductas ilícitas, facilitando el acceso a los ciudadanos a la hora de denunciar estos tipos de hechos.

Internacionalmente se ha tomado una serie de medidas pertinentes en esta materia, basada en la cooperación entre países de todo el mundo ya que es un fenómeno delictual transfronterizo. Creándose por el año 2001 y actualmente vigente, una alianza internacional contra el fraude en internet donde colaboran 12 países entre ellos España, consistiendo el proyecto en la creación de una página web www.econsumer.gov que tiene por objetivo proporcionar información acerca de la protección al consumidor, servir de contacto con las autoridades de protección al usuario y también facilitar un formulario de quejas on-line. Formándose una base de datos de información con todas las quejas que más tarde serán investigadas, además dentro de la propia red hay un apartado para los gobiernos donde mediante una clave privada entran y podrán analizar la base de datos para poder ser investigada de una forma efectiva. (Computing, 2001)

8.1. Formas de evitación y actuación ante el delito de fraude por internet.

Tras la movilización de los gobiernos de distintos países, a través de sus fuerzas y cuerpos de seguridad, así como de la colaboración ciudadana se han expuesto consejos y medidas de prevención, para concienciar a la población sobre los fraudes existentes en internet e intentar que no caigan en ellos mientras navegan por internet. Incluso las propias páginas webs de compra-venta o alquiler de productos o servicios, colabora con la evitación de los fraudes dando la posibilidad de que los usuarios puedan dar puntuaciones de sus transacciones tanto al vendedor como al comprador y dejar comentarios de estos, facilitando que usuarios honrados dejen sus impresiones y propios consejos para que lo próximos usuarios que no deseen ser víctimas o autores de conductas fraudulentas, puedan realizar sus actuaciones tranquilos gracias a las guías para evitar las estafas que han ido depositando los demás usuarios con sus opiniones y votaciones. Un claro ejemplo de esto último es la página web eBay. Otro caso llamativo como el de eBay es el de la página web Nuroa.es que cuenta con una herramienta para comprobar la evolución de los precios de la vivienda en los últimos años que se puede consultar por ciudades e, incluso, por barrios, para saber sobre qué precios nos movemos para nuestros intereses y sospechar de los que disten mucho sobre los que ronda la mayoría.

La fuerzas y cuerpos de seguridad han colaborado por su parte mediante consejos para crear conciencia e influir en las conductas de los cibernautas que deben ser un poco más desconfiados, exactamente con “desconfianza natural”, es decir, ir con pies de plomo no dar por supuesto que un usuario es quien dice ser, desconfiar de los anuncios con precios muy por debajo de las cifras de mercado, fijarnos bien en el link que pinchamos o donde nos introducimos mirando que el nombre de la página web que aparece en la barra de navegación sea el auténtico de donde queremos entrar. Además, en caso de trato entre particulares, la policía recomienda comprobar siempre la existencia del inmueble (solicitar, por ejemplo, una copia de la documentación o un recibo del IBI), utilizar un método de pago seguro y solicitar un breve compromiso de contrato para luego poder acreditar la operación.

Después de mostrar técnicas de prevención de forma general, podemos pasar a centrarnos en prevenciones más particulares focalizadas a prevenir un tipo de delito en concreto como es el caso del phising, que al tratarse del procedimiento principal por el que se desarrolla la conducta delictual de fraudes en internet, debemos dotarle de una atención especial buscando prevenir el desarrollo de su actuación fraudulenta, por ello se recomienda al usuario una serie de pasos.

Por una parte concienciar a los usuarios que nadie “da duros a cuatro pesetas”[7] para que no se produzcan casos como la estafa nigeriana ya vista previamente, así como hacerles pensar si una compañía o entidad financiera requeriría tantos datos personales como DNI, tarjetas de crédito o pin de las tarjetas, por correo electrónico cayendo en la cuenta que esos datos ya lo tienen las propias entidades cuando el usuario se crea una cuenta en dicha entidad o compañía, además muchas compañías se dirigen a sus clientes por nombres de usuario registrado y no dándole la bienvenida directamente sin referirse a nadie en concreto. Aun con esto, si existen dudas llamar siempre telefónicamente al número de atención al cliente de esos organismos para verificar lo lícito de la conducta que se presenta.

En este caso como en muchos otros cuando falla la barrera social del usuario, existen herramientas técnicas como softwares Anti-phising, o una serie de preguntas llamadas preguntas desafío que sólo puede conceder el usuario legítimo y la organización de esa cuenta a la que se desea acceder. También se han realizado técnicas de verificación en páginas webs como la muestra de una serie de imágenes secretas que los usuarios seleccionan por adelantado y sí estas imágenes no aparecen, el sitio no es legítimo.

Podemos seguir mostrando recomendaciones más en concreto con delitos como el fraude de los SMS Premium.

Organizaciones como CEACCU cree que una forma efectiva de enfrentarse a este problema sería exigir la contratación y autorización expresa del servicio, un modelo que ya se aplica en muchos países Europeos. Por otro lado, las distintas operadoras de telefonía también deben tomar decisiones en este sentido y proteger a sus clientes de los servicios de SMS Premium. Un ejemplo de esto sería Movistar que ya se ha puesto manos a la obra y desde hace unos meses, obliga a los proveedores a conseguir una solicitud de alta, firmada por el cliente, y una fotocopia del DNI de todo aquel que quiera suscribirse a sus servicios. De esta forma, evita que a través de algún tipo de engaño, el usuario se suscriba a servicios de SMS Premium que no desea. Aunque en caso de ya ser suscritos a un sistema de mensajería Premium debemos llevar a cabo las siguientes actuaciones:

- Desinstala la app de tu móvil y borra los datos.
- Contacta con tu operadora móvil, explícale lo sucedido y pide que se bloquee cualquier servicio de SMS Premium activo.
- Si ya has detectado cobros en tu factura, anota el NIF y nombre de la

[7] Refrán de origen español que significa que nadie da nada por nada, invitando a desconfiar de las ofertas y de los regalos.

empresa que hace los cobros, y pon una denuncia en consumo, con todos los datos sobre la aplicación.

Con todo esto, también podemos hacer una pequeña diferenciación de las 2 partes afectadas por fraudes o estafas por internet, tanto del vendedor como del comprador. Pero centrándonos en el vendedor, podemos decir que hay numerosos peligros a la hora de ejercer como tal y se han de intentar prevenir como aquí se muestran.

- Cuenta falsa de PayPal*:* Consigues vender un producto o servicio y te encuentras con un correo electrónico de PayPal avisando de la confirmación de que el comprador ha realizado la transferencia correspondiente al pago del producto y servicio, realizando por lo tanto el envío del producto o servicio por parte del vendedor hacia el comprador. Sin embargo, al comprobar su cuenta el vendedor observa que no hay tal transferencia.
  La forma de evitar esto sería entre otras técnicas no fijarnos en el mensaje recibido, ya que puede ser un mensaje duplicado (algo muy común en las conductas de phising). Comprobar siempre bien la dirección del emisor y asegurarte que todo es correcto, dirigiéndote además al sitio de PayPal directamente para comprobar que el ingreso del comprador sea real.

- El cambio**:** En muchas ocasiones ocurre que el vendedor ha enviado un producto en perfecto estado y sin embargo la persona que lo compra acusa a este de recibir un producto falso o en mal estado y debido muchas veces a la política de la web del cliente siempre tiene la razón, se obliga al vendedor a devolver el importe abonado por el comprador y este te deja sin dinero y con el producto. Esto se puede paliar haciendo suya por parte del vendedor la política de no se admiten devoluciones**,** pudiendo prevenirse de los clientes que vayan con intenciones fraudulenta. Por añadido el vendedor puede enviar los productos con un seguro por si durante el envío el producto sufre algún tipo de daño.

- Reembolso forzado**:** El vendedor tras hacer una transacción de un producto comprueba que el pago ha sido realizado y se entrega la mercancía en cuestión, pero más tarde la transacción es revertida ya que nunca se ha realizado el pago, debido a que este se produjo mediante un phising a otros usuarios de PayPal, o solicitando un reintegro del producto ya que nunca lo recibió. Esto se evita actuando si confiar nunca en un pago rápido, siendo preferible un ingreso en efectivo en cuenta que una transferencia que puede ser reinvertida. Realizando

siempre la entrega tal y como se había acordado previamente, pudiendo solicitarle a la persona compradora realizarle una fotografía con el producto por si en algún momento se dijera que no lo llegó a recibir, siempre y el comprador acepte.

Habiendo observado los métodos y técnicas para prevenir la comisión de los fraudes tradicionales por internet que han ido evolucionando partiendo de la misma base, así como los consejos para intentar que el usuario no se convierta en víctima de estos hechos. Podemos ahora mencionar las técnicas tanto para prevenir la caída en estas trampas como para luchar contra modalidades como los ransomware.

Ante esta modalidad de estafa los principales consejos y actuaciones a llevar a cabo una vez se nos presentan, aparecen en la opinión dada por los usuarios afectados por esta práctica así como la opinión de artículos escritos por expertos en la materia, no encontrando recomendaciones específicas ni técnicas de lucha o evitación por parte de las fuerzas y cuerpos de seguridad del estado.

Las recomendaciones más comunes que encontramos van dirigidas a la prevención:

- Instalar parches y actualizaciones del sistema, ya que de forma creciente estos virus se van reinventando día a día para superar las barreras de protección existentes y poder realizar su conducta maliciosa.
- Usar un navegador de internet moderno y actualizado, para asegurarnos de que acepte la instalación de los parches así como las actualizaciones para una protección efectiva.
- Instalar además de los parches y las actualizaciones de Java, Adobe Flash y otras librerías de internet, para impedir que los malware entren por esa vía.
- Tener siempre funcionando en segundo plano un antivirus y un cortafuegos siempre actualizados.
- Cada cierto tiempo como una vez al mes realizar un chequeo del ordenador con algún programa especializado en detectar malware del tipo troyano o gusanos como spyware o anti-malware.
- Como norma general y básica de prevención, no entrar en webs de mala reputación, llenas de publicidad con ventanas emergente, que ofrecen contenido sospechosamente atrayente. Así como a la hora de descargar algún archivo dudoso, antes de usarlo chequearlo con algún antivirus.

Habiendo observado los métodos de prevención comunes, podemos añadir que al tratarse de esta nueva modalidad de fraude por internet mediante malware difíciles de combatir, en donde eres tú mismo el que abres las puertas al ransomware hemos de andar con mucho ojo, siendo muy recomendable realizar periódicas copias de seguridad en un dispositivo de almacenamiento externo al ordenador, para en caso de no poder evitar su intrusión y su afección, formatear el ordenador y empezar desde la copia de seguridad pudiendo recuperar la totalidad o parte de los sistemas afectados por el ataque en el ordenador del usuario.

Después de haber observado las medidas de prevención, pasamos a hablar de las medidas a llevar a cabo una vez no hemos podido prevenir el ataque y estamos infectados, es decir, de las medidas para eliminar el malware, teniendo en cuenta que hay muchas formas de actuación y ransomware que poseen concretas técnicas de eliminación.

Ante el suceso de que un ransomware se haya instalado en el ordenador, primeramente hemos de mantener la calma ya que tenemos la certeza de que los chantajes son falsos, ni la policía ni el FBI han analizado tu ordenador, ni tienes un potente virus que requiere comprar un antídoto. Como hemos mencionado en la prevención es recomendable hacer una copia de seguridad, y en este caso crear un disco de rescate pareciéndose mucho la forma de actuar descargando un fichero ISO, y lo grabas en un CD o DVD grabable con un programa que extraiga ISOs, como por ejemplo CDBurnerXP, o usando un pendrive de alta capacidad, tras esto se introduce el dispositivo externo o el disco y reinicias el ordenador, ya que el antivirus se instalará en memoria antes que el sistema operativo e intentará retomar el control, siendo recomendable arrancarlo en modo seguro. Si nos encontramos que el ransomware que nos ataca no ha encriptado los archivos, tendremos altas probabilidades de recuperar los archivos, sino lo más seguro es que tendremos que formatear.

Estas amenazas además de en los ordenadores también las podemos encontrar en la telefonía móvil dentro de los Smartphone que utilizan como sistema operativo Android, el cual al tratarse de un sistema abierto permite instalar aplicaciones de terceros mediante servicios de descarga alternativos a google play, o incluso de forma manual. Siendo esto aprovechado por los malware no siendo menos por los del tipo ransomware, disfrazándose de apps con algún tipo de gancho invitándote a que lo instales desde google play, consiguiéndose introducir él. Siendo la única forma de recuperarlo sin realizar el pago del rescate es regresar a los valores de fábrica.

Ulteriormente, de hablar de la eliminación de los ransomware una vez infectados los dispositivos en líneas generales, pasamos a concretar qué medidas llevaríamos acabo encontrándonos ante determinados tipos de ransomware.

En el caso de que nuestro ordenador sea infectado con el virus cryptowall u otro específico de encriptación, encriptando una serie de archivos personales debemos tomar una serie de medidas que iremos mencionando paso por paso, partiendo de la base de que para poder encriptar los archivos con el virus, antes has de borrar el archivo original.

- *Paso 1*: Apagar el ordenador cuanto antes nada más observar que estamos infectados, ya que cuanto más tiempo esté encendido más archivos se cifrarán.
- *Paso* 2: Arrancar Windows en modo seguro con funciones de red.
- *Paso* 3: Descargar e instalar un recuperador de archivos borrados iniciando una búsqueda de archivos por extensión, debido a que como hemos dicho previamente antes de encriptar los archivos han tenido que borrar los originales. Durando la búsqueda un par de horas rescatando casi todos los archivos, pero muchos otros no será posible conseguirlos. Se recomienda no haber instalado programas de antispyware porque se reescriben archivos pudiendo perder definitivamente los originales.
- *Paso* 4: Realizar como hemos mencionado en la prevención en general una copia de seguridad o haber pasado la información restaurada por el programa recuperador a un dispositivo o disco externo. Tras esto formatear el ordenador debido a que este tipo de virus es un rootkit el cual se instala en el sistema y es muy difícil de eliminar ya que permite un acceso de privilegio continuo a un determinado ordenador pero que mantiene su presencia activamente oculta al control de los administradores, corrompiendo el funcionamiento normal del sistema operativo u otras aplicaciones, por no hablar que se conecta a tu red e intenta transferir todo lo referente a tu entramado bancario. Y ya con todo esto finalizar el proceso formateando y restaurando los archivos. Aun no recomendando la instalación de programas antispyware debido a que se reescriben archivos, sí que una vez realizado el proceso de eliminación, si es recomendable instalar programas como shunte que puede de eliminar la modalidad de cryptowall 4.0., diciendo que puede porque los programas de infección son en muchas ocasiones específicos para cada ordenador. Si tras reiniciar el ordenador siguen abriéndose las imágenes de CryptoWall, no tendremos que preocuparnos porque el virus habrá sido eliminado, pero no las entradas correspondientes de su menú de inicio (Star-up) que aun siendo

inofensivas son molestas, debiéndose eliminar una por una para que no se abran al iniciar Windows.

Siguiendo con los pasos a dar tras estar infectados por el cryptowall, podemos hablar de otro programa específico encriptador de archivos siendo el cryplocker, funcionando ambos de la misma manera con pequeñas diferencias. Habiendo también forma de actuaciones destinadas a su eliminación:

- Apagar el ordenador y encenderlo en modo seguro o mediante un cd de arranque con antivirus incorporado como hemos dicho previamente.
- Una vez en modo seguro utilizar programas específicos de limpieza para eliminar el virus como Kaspersky rescue disk, el cual limpia el ordenador sin pasar por windows.

- Tras la limpieza recurrir a copias de seguridad para intentar recuperar los máximos archivos posibles, así como utilizando programas de descifrado para intentar recuperar los archivos que se encuentren en esa situación. Y hasta no terminar toda la recuperación no poner nuevos archivos en el ordenador porque puede afectar a los programas recuperadores de archivos provocando que se pierda su rastro.

- Por último, una vez finalizada la recuperación, instalar programas como cryptoprevent que ayudan a imposibilitar la actuación del malware.

Además también debemos tener cuidado con virus adicionales que pueden entrar con estos virus como en el caso de tesla Crypt que además de la intromisión del virus principal se implementan otros adicionales aprovechando la infección realizada por el principal, debiendo protegerse con programas del tipo malwarebytes de estas amenazas adicionales que pueden agravar la situación. Pudiendo comprobar que en este ámbito de los ransomware presentan medidas muy parecidas incluso comunes variando pequeños detalles dependiendo del tipo, en cuanto a prevención y eliminación del problema se refiere.

Otros ámbitos a tener en cuenta son los accesos remotos a un ordenador debiéndose tomar medidas de seguridad adecuadas, no debiéndose realizar ese acceso remoto por vía directa a través de internet ya que nos exponemos ante ataques que intercepten la señal de control apoderándose de dicho control del dispositivo, por ello siempre debemos realizarlo desde una VPN, significando esto Red privada virtual que nos permite realizar una doble identificación, para comprobar que el usuario que entra a

internet para realizar ese determinado control remoto es realmente ese usuario, mediante una identificación con nombre y contraseña normalmente. Pensando además en el gran campo de actuación de los malware y la mala fe de sus creadores también sería buena idea proteger con contraseña la configuración de la solución antimalware para evitar que un atacante la modifique, imposibilitando la detección de archivos o programas maliciosos.

Como he ido plasmando durante este trabajo en el ámbito de internet y de los fraudes existentes en esta comunidad existen muchos intereses contrapuestos así como una mayor tolerancia social sobre estos delitos, no se produce tanto rechazo. Digamos que la sociedad solo reclama ante estos delitos cuando le afecta de primera mano esa vulneración de sus datos personales, copiándolo fotos privadas, datos bancarios, etc. Y no se escandalizan en gran medida cuando le pasa a otro, lo vetan mínimamente y ya cuando una persona con unas ciertas habilidades informáticas a la que se le denominaría hacker consigue vulnerar grandes estructuras de seguridad introduciéndose en lugares gubernamentales por ejemplo, la sociedad en vez condenarlo en muchas ocasiones lo ensalza casi dejando notar que no son capacees de apreciar que esa misma persona que en un momento están ensalzando puede ser el mismo que luego le copie o sustraiga esos datos personales que tanto desean ocultar. por lo que si queremos abordar este tema óptimamente reduciendo las labores delictivas la mejor forma de evitar que se sigan produciendo esos fraudes será primeramente debemos inculcar una conciencia efectiva en la ciudadanía sobre este problema, como mayor elemento de presión que existe en los estados para legislar, por desgracia o por fortuna según por donde se mire, y una vez hayamos conseguido establecer ese rechazo los intereses de los poderes, interpuestos en estos temas serán más difíciles de ocultar por lo que será más difícil para estos delincuentes realizar sus actuaciones fraudulentas, debido a que habrán más actuaciones destinados a pararlos.
(Santiago, 2012)

9.-Conclusiones.

Con todo lo visto a lo largo del trabajo podemos extraer una serie de conclusiones.

- Conclusione objetivas.
  - Primero: Este delito de fraudes por internet se presenta hasta la fecha como inagotable debido a que se encuentra en un campo ilimitado.
  - Segundo: La metodología del delito cambia pero su objetivo final no.
  - Tercero: Cualquier usuario puede ser un estafador, tanto compradores como vendedores.

- Cuarto: Las barreras de seguridad son insuficientes.

- Quinto: Los sujetos activos de estos delitos atacan más a los Smartphones que a los ordenadores por el desconcimiento de peligrosidad de los usuarios en estos dispositivos.

- Conclusiones personales.

- Primero: Cometer el hecho delictivo en internet mediante medios informáticos, otorga una sensación de impunidad al delincuente que le sirve como refuerzo positivo de sus conductas.

- Segundo: Los delincuentes escogen las páginas webs mas conocidos para aprovecharse de su buena fama socialmente hablando, buscando que el usuario este con la guardia y baja y perpetrar la estafa.

- Tercero: Existe una doble vara de medir en cuanto a seguridad Informática se refiere, ya que dependiendo del sistema operativo en el que nos encontremos o del tipo de aplicación que deseemos obtener, habrá mas o menos restricciones en función de intereses.

- Cuarto: Hay que mostrarle al usuario que toda conducta fraudulenta es relevante independientemente del perjuicio creado, ya que estos tipos de delincuentes crean un perjuicio económico moderado para que el usuario no sienta la necesidad de denunciar los hechos y puedan seguir perpetrando ilícitos sin que la policía lleve acabo actuaciones, ayudando a crecer la cifra negra.

- Quinto: Estos tipos de delincuentes actúan pensando en la manera de captar al usuario, así como la forma de presentarse una vez han sido pillados, buscando minimizar su ilícito para que quede impune.

- Sexto: Todos debemos remar en una misma dirección con el único objetivo de acabar con los fraudes en internet, sino es así siempre dejaremos una vía abierta para que se sigan perpetrando estos hechos. Dejando atrás intereses y creando una conciencia efectiva entre los usuarios haciéndoles ver que todo dispositivo con conexión a la herramiento global de internet tiene riesgo de ser violentado por estos hechos tan relevantes como otros.

10.-Bibliografía.

- Jefatura de estado, 2015. Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. [Online] disponiblen:<www.noticias.juridicas.com/base_datos/Penal/lo10-1995.html>

- Cortes generales, 2011. Constitución española, 1978. [Online] disponible en: <www.noticias.juridicas.com/base_datos/Admin/constitucion.html>

- Redacción Computing, 2001. Se crea una alianza contra el fraude en internet. [Online] disponible en: <www.computing.es/negocios/1002409002201/crea-alianza-fraude-internet.1.html>

- Osiseguridad, 2012. Conoce los fraudes utilizados en internet II: Los sms premium. [Online] disponible en: <www.osi.es/es/actualidad/blog/2012/07/05/conoce-los-fraudes-utilizados-en-internet-ii-los-sms-premium.html>

- Theguardian, 2007. Dismay at eBay's unsatisfactory response to 'bid shielding' offences. [Online] disponible en: <https://www.theguardian.com/technology/2007/may/17/newmedia.guardianweeklytechnologysection>

- Legálitas, 2015. Evita las estafas más comunes en Ebay. [Online] disponible en: <www.legalitas.com/actualidad/evita-las-estafas-mas-comunes-en-ebay>

- Ignacio Santiago, 2012. Estafas en internet: Tipos, consejos y dónde y a quién acudir. [Online] disponible en:<www.ignaciosantiago.com/blog/todo-lo-que-tienes-que-saber-sobre-las-estafas-en-internet>

- Los virus, 2016. Ransomwares webs y bancos entre sus últimos objetivos. [Online] disponible en: <www.osvirus.es/ransomwares-webs-y-bancos-entre-sus-ultimos-objetivos/>

- Graham Cluley, 2014. Todo sobre Ransomware: Guía básica y preguntas frecuentes. [Online] disponible en: <www.welivesecurity.com/la-es/2014/06/10/todo-sobre-ransomware-guia-basica-preguntas-frecuentes/>

- PC risk, 2015. Virus Alpha Crypt. [Online] disponible en: <www.pcrisk.es/guias-de-desinfeccion/7793-alpha-crypt-virus>

- Lucas Paus, 2015. 5 tipos de phising en los que no debes caer. [Online] disponible en: <http://www.welivesecurity.com/la-es/2015/05/08/5-tipos-de-phishing>

- Osiseguridad, 2013. Fraudes Online (VII): Smishing, estafa que llega a través de un SMS. [online] disponible en:<https://www.osi.es/es/actualidad/blog/2013/09/09/fraudes-online-vii-smishing-estafa-que-llega-traves-de-un-sms.html>

- Debra Littejohn Shinder, 2003. Prevención y detección de delitos informáticos. Madrid: Anaya Multimedia.

- Alfonso Galán Muñoz, 2005. El fraude y la estafa mediante sistemas informáticos. Valencia: Tirant Lo Blanch.

- Carolina Sanchis Crespo, 2015. Fraude electrónico. Valencia: Tirant Lo Blacnh.

- Alfredo Sneyers, 1990. El fraude y otros delitos informáticos. Madrid: Tecnologías de gerencia y producción.

- Mª. Luz Gutiérrez Francés.1991. Fraude informático y estafa. Madrid: Artegraf.

- Chema Alonso, 2013. Un juego de Android que roba los mensajes de WhatsApp. [Online] disponible en: <http://www.elladodelmal.com/2013/12/un-juego-de-android-que-roba-los.html>

- María González, 2014. ¿Puede una app cualquiera acceder a tu historial de WhatsApp? Sí, según un investigador holandés. [Online] disponible en: <http://www.xatakamovil.com/aplicaciones/puede-una-app-cualquiera-acceder-a-tu-historial-de-whatsapp-si-segun-un-investigador-holandes>

- Enriquecuartas, 2014. WhatsApp para Android permite que hackers lean tus conversaciones. [Online] disponible en: <http://hipertextual.com/archivo/2014/03/whatsapp-android/>

- La Nueva España, 2016 .Ojo con estos mensajes de WhatsApp: son estafas. [Online] disponible en: <http://www.lne.es/vida-y-estilo/tecnologia/2016/04/22/cuidado-mensajes-whatsapp-son-estafas/1915510.html>

- Leticia Sorivella, 2014. Cámara Visión Nocturna: nueva estafa que utiliza apps como WhatsApp o Telegram. [Online] disponible en: <http://www.malavida.com/post/camara-vision-nocturna-nueva-estafa-que-utiliza-apps-como-whatsapp-o-telegram>

- Fran_ramon, 2012. Cuidado con vender por Paypal a usuarios de dudosa reputación. [Online] disponible en: <https://comunidad.ebay.es/t5/Confianza-y-Seguridad-para/Cuidado-con-vender-por-paypal-a-usuarios-de-dudosa-reputaci%C3%B3n/td-p/41232 >.

- OSI, 2014.WhatsApp, Telegram y LINE. ¿Cuál es más segura para chatear? [Online] disponible en:<https://www.osi.es/es/actualidad/blog/2014/05/09/whatsapp-telegram-y-line-cual-es-mas-segura-para-chatear.html>

- Inteco, 2007. Estudio sobre usuarios y entidades públicas y privadas afectadas por la práctica fraudulenta conocida como phishing. [Pdf] disponible en: <https://www.incibe.es/file/rmqBMNKZwCoOKzEyqx15mg>

- Pc risk, 2014. Instrucciones para eliminar el virus cryptowall. [Online] disponible en: <https://www.pcrisk.es/guias-de-desinfeccion/7401-cryptowall-virus>

- Pc risk, 2015. Instrucciones para eliminar el virus Teslacrypt. [Online] disponible en: <https://www.pcrisk.es/guias-de-desinfeccion/7715-teslacrypt-virus>

- Como eliminar virus spyware, 2014. Eliminar winlocker-Como quitar winlocker. [Online] disponible en: <http://eliminarspywarevirus.blogspot.com.es/2014/11/eliminar-winlocker-como-quitar-winlocker.html>

- Adrian Crespo, 2012. Detectado un virus en Windows que reemplaza el MBR del disco duro. [Online] disponible en: <http://www.redeszone.net/2012/04/14/detectado-un-virus-en-windows-que-reemplaza-el-mbr-del-disco-duro/>