EL PHISHING

TRABAJO FINAL DE GRADO.
GRADO EN CRIMINOLOGÍA Y SEGURIDAD

ALUMNO: **Mayra Sheila Mariana Leguizamón**
TUTOR: **Manuel Mollar Villanueva**

ÍNDICE

Extended Summary

Phishing is a crime under international field. It comes from several years ago. The word comes from a report by Jerry Felix and Chris Hauk called: “Security System: The prospect of a Hacker “, where they discussed how to impersonate a trusted company. But the phishing as such stems from the company AOL, a company that provides Internet services. It was chosen for such attacks because of its fame and the number of Internet users who are connected to it. That’s why it was the focus of the phishers. First, they marketed pirate software and constituted WAREZ community. Then they began to open accounts at AOL with fake and regenerated credit cards to trick the users. The security system managers of AOL saw what was happening and created AOHell to avoid this problem.

The origin of the word “Phishing” comes from fishing. It identifies with this word because the intent of this scam is "fish" internet users to relieve sensitive information. It is trying that the users catch the "bait" and provide this private data. There is also another reason why the word is written with “ph” and not with “F”: It’s because the first hackers were known as “phreaks”. It comes from the word phreaking which means study, understanding and learning of new technologies. Both “Hacker” and “Phreaker”, were always linked and therefore the use of “PH" is to identify these attacks with these communities.

You can define phishing as the process by which a person is contacted by email or phone by someone who pretends to be a legitimate institution to get private data, such as bank details, passwords, etc. ... Then this information obtained fraudulently it is used to access the personal accounts of the victims and cause economic loss or identity theft. Currently the most widely used form of phishing is sending mass e-mail in order to deceive the victim and providing personal data to the "phisher". Although this is not the only form of phishing. In the last few years this activity has been improved and it’s increasingly more difficult to detect a fake mail. Besides the techniques have improved considerably and each day there are more and better than the first methods. The most sophisticated are using fake websites, installation of Trojans, key-loggers, screen-loggers, sending SMS messages, phone calls etc.

They can be classified according to the modus operandi, it means the way phishers use to get this information or depending on the data they are looking to obtain. Therefore with this classification we distinguished for example banking phishing or phishing in social networks. Currently they are counting more than 10,000 forms of phishing.
The most commonly cited definition is provided by the APWG and has undergone several expansions and modifications as the very evolution of Phishing:

“Phishing is a criminal mechanism employing both social engineering and technical subterfuge to steal consumers’ personal identity data and financial account credentials. Social engineering schemes use spoofed e-mails purporting to be from legitimate businesses and agencies, designed to lead consumers to counterfeit websites that trick recipients into divulging financial data such as usernames and passwords. Technical subterfuge schemes plant crime ware onto PCs to steal credentials directly, often using systems to intercept consumers online account user names and passwords -- and to corrupt local navigational infrastructures to misdirect consumers to counterfeit websites (or authentic websites through phisher-controlled proxies used to monitor and intercept consumers’ keystrokes).

In recent years, the term phishing has become increasingly important due to the large economic losses and the great social impact it causes to companies and users. Besides their techniques have progressed and improved over the years, but also the methods for its prevention. It is a problem of international scope and the countries that are victims of these attacks must work together to have all necessary information about the evolution of phishing and be able to fight successfully.

What differentiates this type of computer crime with the same type are four key points:
1) Social Engineering: phishing somehow interacts with people and takes advantage of its weakness to make the attack more easily.

2) Automation: advances in communications and techniques are used by phishers to send massively emails to the future victims.

3) Electronic communication: it’s the means used to commit these attacks, especially used internet.

4) Impersonation: as we have seen above, for an attack of this nature is necessary for the criminal, impersonates a legitimate company or entity

Phishing also has a number of stages for its commission:

1) Planning phase: As its name suggests, is the stage where the scammer prepares his attack: he decides who will be his victim, which is the method he will use, which agency or company he will supplant, seeking with this attack, the means he will use ... This is a stage, it could be "common" to all phishing attacks.

2) Preparation phase: Generally there are not much difference between the three types of phishing, depending on the complexity and involvement, but there are differences in the way of carrying out the attack, that is, for their creation and achievement. This is because the offender according to the type of information he wants to achieve, he must use different means, specifically, taking into account the needs of each offense.

3) Attack Phase: Here according the type of phishing has been chosen, the tasks will be different. If we talk about a phishing with a low participation of the victim, as an attack to the server, the main task will be to carry out this attack with the necessary means. If we talk about the other two types of attack, the preparation would be to prepare the different traps for the victim.

4) Data collection phase: As already explained, there are three types of phishing. Therefore, if it is a medium or high collaboration of the victim will have to wait for it to enter their confidential data in order to obtain them. If it is an attack on the server, the main task is to run the malware to get this information.

5) Implementation phase fraud: At this stage, once the phisher has the data and achieved his objective, he use this information for personal gain or he sells this information to interested persons so that they carry out the crime.

6) Post-attack phase: At this point, the phisher seeks to eliminate all traces that could then incriminate him of this crime. It means that if we talk about a banking phishing, the scammer will then proceed to the commission of another crime: money laundering or similar.

To learn more about phishing it is necessary to know that there are different types considering the modus operandi or the means to attack. In the first case we found the deceptive phishing, malware based phishing, DNS or pharming, phishing content injection, man in the middle phishing and search engine phishing. According to the second classification it could be bank phishing, social networks, online payment gateways, pages buy / sell auctions, online games, support and

assistance to businesses and services, cloud storage, services and public companies, services messaging and false job offers.

Talking about the economic impact of phishing we can say like this crime it's new, there is little data on their impact. What can be said is that worldwide per attack there is an average economic loss of 593 €. In the case of Spain, these scams have less loss, being less than 400 € per attack. This is because here is set the limit to make it crime. Therefore, phishers make them more profitable over the lower of phishing attacks to one that is more gain but is crime.
As shown, phishing gains are not of great importance, but each attack is multiplied produced (in Spain about 1500 a year) by the amount obtained can understand the dimension of the problem.

About the social impact of phishing it is important to know that damage to a company which supplants its identity is quite considerable. This is because confidence in users of these companies is decreasing, causing losses to the company. It affects the general user when make online operations, especially transactions and transfers of money.
Statistical data determined that 68% of users make purchases on the Internet for fear of being scammed.
Of all phishing attacks committed, 82% of these are made for obtain bank details and get money, and 21.5% were attacks committed for information on companies buying and selling online.

After analyzing all the information we obtained the following conclusions:

1. Over recent years, technology has advanced considerably. There have been improvements in almost all sectors and in the field of internet these changes were successful. But it was not all benefits. With increasing technology also they increased the ways to commit phishing and methods used are becoming more reliable and credible. It is easier to trick the victim with the new techniques employed. The advancement of technology has become a tool for criminals to commit crimes. Therefore, the distrust of users increases and all progress made in this area are paralyzed.
2. Anyone can be a victim of phishing and the victim could be individual or collective. For this reason it is necessary to campaign against phishing. It is important that Internet users know what this type of crime and know easily identifiable offering real data and statistics on it. This will be achieved raise public awareness about the real dimension of these attacks.
3. Phishing is a problem around the world. It is not a problem only of Spain or any particular country, it is a global one. Therefore, cooperation between countries is very important. It is necessary that the information and data on this crime is shared with the all countries to keep everyone up to date on the developments of the crime and then battle against this

attack. Every day are born more types of phishing, unknown to many countries. If this information is shared, it will be easier to prevent these scams from occurring.

4. In terms of evolution, many studies find that has reached its maximum evolution while another's believe it is a phenomenon that has yet to evolve. Considering its evolution in recent years, probably in the future will increase even more techniques and phishing will be growing. It is therefore important to keep as much information as possible to be prepared in the future

Resumen:

En este trabajo se definirá el fenómeno actual del Phishing, un delito poco conocido pero con gran impacto tanto económico como social. Además, se explicarán los tipos de phishing según el modus operandi o según el medio o servicio que ataquen. Por otra parte, se comentará la forma de combatirlo y las medidas necesarias que un usuario debe tomar para no ser una futura víctima y cuáles deben tomar las empresas para que no suplanten su identidad. Seguidamente se hablará de este delito en el código penal español, en que artículos se regula y demás leyes que lo contienen. En cuanto al ámbito internacional, se nombraran los medios utilizados para evitar estos ataques y la forma en que los países colaboran entre sí para que todos estén actualizados e informados de las últimas novedades y evolución del mismo. En el área práctica se demostrará como se producen ataques Phishing tanto en bancos como en las redes sociales. En el primer ejemplo se tratará el tema de las mulas e intermediarios y su responsabilidad penal. En el segundo ejemplo, se muestra lo fácil y sencillo que es realizarlo y que está al alcance de cualquier usuario de internet por medio de una página web. También, acorde con toda la investigación, se comparará información del impacto del phishing en el mundo, haciendo hincapié en España; todo ello acompañado de gráficos que muestran su evolución. Dicho contenido va encabezado por la historia del nacimiento de este delito y el origen de su nombre.

Palabras clave:

Phishing, Phisher, Estafa, Fraude, Delito, Dinero, Mulas, Bancos, Redes sociales, Ataques online, Internet, WWW, Antivirus, Antiphishing, Origen

Abstract:

In this paper, the real phenomenon of phishing will be defined, a crime little known but with great social and economic impact. Also, will be explained types of phishing according to the modus operandi or according to the means or service that's attack. On the other hand, will be discussed

how to combat it and the necessary measures that a user should take to not be a future victim and which should take companies for that the phisher not supplant their identity. Then will be talk about this crime in the Spanish penal code, where this crime is regulated and other laws regulating this offense. On the international level, we will say the means used to prevent this attacks and the way the countries are working together to keep everyone updated and informed of the latest developments and evolution of phishing. In the practice area, it will be shown how a phishing attack occur both in banks and in social networks. In the first example, the issue of mules and intermediary and their criminal responsibility will be discussed. In the second example, we will show how easy and simple it's to do and that is available to any user via a web page. Also, according to all the research, the impact of the phishing in the world will be compared, emphasizing Spain; all accompanied by graphs showing phishing progress. That content is led by the story of the birth of this crime and the origin of its name

Keywords

Phishing, Phisher , Fraud, Crime , Money, Mules , banks , social networks , online attacks , Internet , WWW , Antivirus, Anti-phishing , Origin

1. HISTORIA DEL PHISHING:

La primera vez que se oyó hablar del Phishing fue en el año 1987 en una conferencia dónde Jerry Félix[1] y Chris Hauck hicieron referencia al término a causa de un documento titulado *"Sistema de Seguridad: La perspectiva de un Hacker*". Aquí se pretendía discutir un método sobre el cual una persona pudiera imitar un organismo o entidad de confianza. Pero el primer uso del término como tal, se produjo en la compañía AOL[2]. Esta empresa es proveedora de servicios de internet que tiene su sede en New York. Su popularidad fue en aumento y millones de personas se conectaban a esta red. Por este motivo fue el punto de ataque de los phishers, que en primer lugar comercializaban software pirata, constituyendo así, la comunidad WAREZ[3]. Esta fue la que comenzó con los ataques de phishing. Antes del año 1995 era muy sencilla la apertura de una de estas cuentas utilizando números de tarjeta falsos o regeneradas. Creaban un algoritmo donde se creaban números de cuenta totalmente falsos y aleatorios. Esto trajo como consecuencia una gran pérdida económica para AOL. La empresa al percatarse de esta situación tomó medidas drásticas. Además creo AOHell para la lucha contra estas estafas.

1.1. *ORIGEN DE LA PALABRA PHISHING*

El origen de la palabra Phishing proviene del término fishing que significa pescar. Se identifica con esta palabra porque la intención de esta estafa es "pescar" a usuarios de internet para que releven información susceptible. Es decir intentan que cojan el "anzuelo" y ofrezcan estos datos.

Pero también hay razones por las cuales se utiliza el vocablo "ph" para referirnos al término y no la "F". Esto es debido a que los primeros hackers eran conocidos como phreaks. Proviene de la palabra phreaking que es el estudio, comprensión y aprendizaje de las nuevas tecnologías. Tanto el término Hacker como Phreaker siempre han estado relacionados y están estrechamente vinculados y por tanto el uso de la "PH" es para identificar estos ataques con estas comunidades.

[1] http://www.brighthub.com/internet/security-privacy/articles/82116.aspx
[2] Proveedor estadounidense de medios y servicios de acceso a internet.
[3] Comunidad que distribuye material bajo copyright vulnerando los derechos de autor.

2. ¿QUÉ ES EL PHISHING?:

Se puede definir al phishing como el proceso por el cual una persona es contactada por email o por teléfono por alguien que simula ser una institución legítima para obtener datos privados, tales como datos bancarios, contraseñas, datos personales etc... Luego esta información obtenida de forma fraudulenta es utilizada para acceder a las cuentas personales de las víctimas y causar pérdidas económicas o suplantación de identidad.

Actualmente la forma de phishing más utilizada es el envío masivo de correo electrónico con la finalidad de engañar a la víctima y que proporcione sus datos personales al "phisher". Aunque esta no es la única forma de phishing. En los últimos años esta actividad ha ido mejorando y cada vez es más difícil detectar un correo falso. Además las técnicas han ido mejorando considerablemente y cada día hay más y mejores. Las más sofisticadas son el uso de sitios web falsos, instalación de troyanos, key-loggers, screen-loggers, envío de mensajes SMS, llamadas telefónicas etc...

Además del Phishing, hay más formas de estafas por internet, como el Pharming que es un ataque al servidor DNS[4] y re direcciona el tráfico legítimo a una web falsificada. El Vishing es el ataque por el cual el usuario recibe un correo electrónico donde se le indica que llame a un número de teléfono. Al hacerlo se le pedirán datos personales. El Smishing es similar al anterior pero el método es por medio de SMS

Se pueden clasificar según el modus operandi, o sea la forma que utilizan para obtener esta información o una clasificación según los datos que buscan obtener. Por tanto con esta última clasificación distinguimos por ejemplo el phishing bancario o el phishing de redes sociales. Actualmente se han contando más de 10.000 formas de phishing.

La definición más citada es la que proporciona el APWG[5] y ha sufrido varias ampliaciones y modificaciones según la evolución misma del Phishing:

[4] Sistema de nombre de dominio.
[5] Anti-Phishing working group www.antiphishing.org

“Los ataques de phishing recurren a formas de ingeniería social y subterfugios técnicos para robar los datos de identificación personal de consumidores y las credenciales de cuentas financieras. Los ardides de ingeniería social se basan en correos electrónicos engañosos que conducen a los consumidores a sitios web falsos diseñados para estafar a los destinatarios para que divulguen datos financieros tales como números de tarjetas de crédito, nombres de usuario de cuentas, contraseñas y números de la seguridad social. Apropiándose de nombres comerciales de bancos, distribuidores y compañías de tarjetas de crédito, los phishers a menudo convencen a los destinatarios para que respondan. Los subterfugios técnicos implican la instalación de crimeware en ordenadores personales para robar las credenciales directamente, habitualmente utilizando troyanos que captan las pulsaciones de teclado”.

En los últimos años la palabra phishing ha ido cobrando relevancia e importancia debido a las grandes pérdidas económicas que ha causado. Y también debido a que sus técnicas y su calidad ha mejorado notablemente y cada vez es más alto el número de personas que son víctimas de esta estafa.

El phishing consiste en la suplantación de identidad de una empresa o entidad bancaria para que la víctima crea que la empresa legitima contacta con ella y necesita los datos personales de la misma. La víctima al creer que es un email/ llamada de la empresa o entidad de forma legítima proporciona esta información privada, sin darse cuenta que está siendo víctima de una estafa cometida por medios electrónicos.

Este método funciona muy bien porque la persona no piensa que puede tratarse de un fraude y ofrece sin pensarlo estos datos. Estos datos luego son utilizados para causarle un perjuicio.

Datos que se obtienen del phishing. [6]

Tal como se observa en la imagen anterior, el phishing intenta captar diferentes tipos de información, entre ellas, destacamos la información personal (dirección de correo, número de documento de identidad, datos de contacto...), la información financiera (número de tarjetas de crédito, números de cuentas, información sobre el banco...) y datos sobre credenciales de acceso (redes sociales, cuentas de correo...).

2.1. *¿CÓMO SE REALIZA?*

Mediante una técnica denominada Password Harvesting[7], el phishing intenta recopilar contraseñas de los usuarios de internet.

Para conseguir su objetivo, en primer lugar, comienzan enviando correos electrónicos suplantando la imagen de una empresa u organización conocida que aporta la confianza necesaria. El email contiene un enlace falsificado donde mediante el uso del engaño consiguen que el usuario entre en él. Una vez en la página a la cual dirige el enlace, se solicita a la persona que introduzca sus datos personales. Lo común en estos emails es el uso del factor miedo, por ejemplo se le

[6] www.pcworld.com.mx
[7] Cosecha y pesca de contraseñas

comunica al usuario de determinado banco que vuelva a otorgar sus datos personales para que no se le caduque el servicio. Este, al confiar en el email, los otorga y ahí es cuando pasa a ser víctima del Phishing. Es una de las técnicas más utilizadas porque las webs que falsifican son muy similares a las originales y legítimas y el phisher utiliza la imagen corporativa de la empresa en los emails para que sean más fiables.

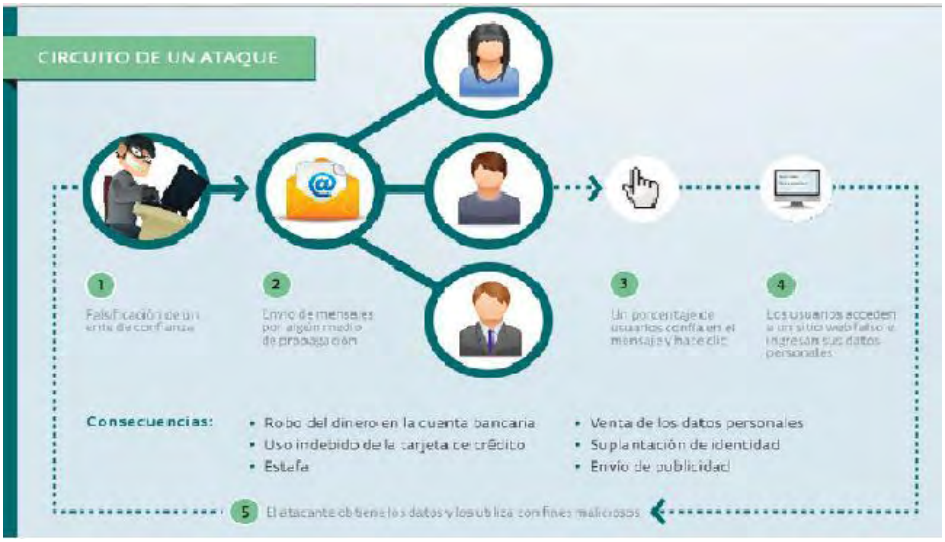
Lo que diferencia este tipo de delito informático de los demás son cuatro puntos básicos:

1) Ingeniería social: ya que el phishing interactúa de alguna forma con las personas y se aprovecha de su debilidad para poder cometer el ataque con mayor facilidad.

2) Automatización: los avances de las comunicaciones y sus técnicas, son utilizados por los phishers para conseguir enviar correos de forma masiva.

3) Comunicación electrónica: es el medio que utilizan para cometer estos ataques, especialmente internet.

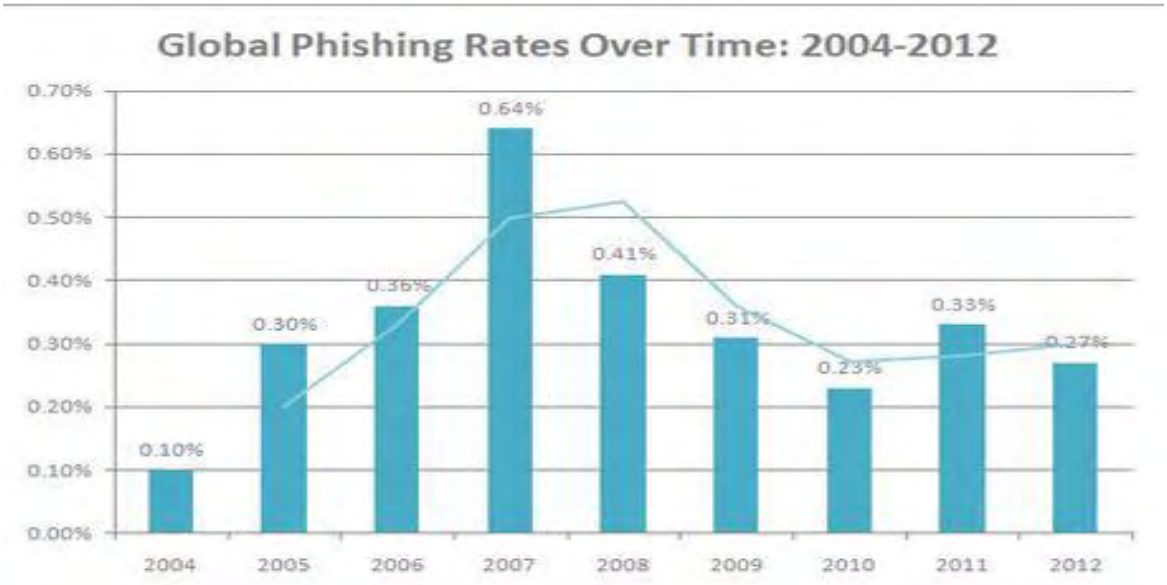
4) Suplantación: como ya se vio anteriormente, para realizar un ataque de estas características es necesario que el delincuente suplante la identidad de una empresa o entidad legítima.



Como se observa en la imagen se ve un circuito de phishing. [8]

[8] www.pcworld.com.mx

2.2 EVOLUCIÓN DEL PHISHING



Como se observa en el gráfico, es un fenómeno que está en continua evolución que se va adaptando a la actualidad.[9]

Los primeros casos conocidos de phishing surgen como un fraude de ingeniería social en el cual suplantan la identidad de un organismo conocido y por el cual solicitan a los usuarios de internet por medio de un email simple que proporcionen sus datos, creyendo estos últimos que todo es legítimo.

Pero esto se va difundiendo y poco a poco los usuarios sospechan cada vez más de este tipo de correo electrónico, y el phishing deja de ser efectivo. Por tanto los estafadores amplían las técnicas utilizadas. Esta vez en los mismos correos electrónico añaden un enlace que les conduce a una página web fraudulenta, que es igual a la original. En esta página web falsa recopilan los datos del usuario. El phishing vuelve a ser rentable. Esta técnica ha ido avanzando. Las páginas web cada vez son más parecidas a las legítimas, tienen menos errores y los links tienen pocas diferencias al original. Incluso a veces aparecen ventanas emergentes en donde no se aprecia ninguna dirección web.

El phishing sigue evolucionando constantemente. Ahora cambia el medio por el cual cometen la estafa: los SMS pasan a formar parte del phishing que en este caso se conoce como "SMISHING". Los objetivos de esta estafa han ido evolucionando. Al principio solo buscaban

[9] http://es.paperblog.com/phishing-teoria-deteccion-y-actuacion-1672901/

datos bancarios, en la actualidad buscan todo tipo de información.

Por otra parte, a medida que el phishing y sus técnicas van avanzando, las medidas para combatirlo también van aumentando.

Una de las últimas evoluciones del phishing, es en el envió de mensajes más personales y por ende más creíbles para el usuario.

Simultáneamente van apareciendo variantes de esta estafa, por ejemplo el “wishing” o “whale phishing” que se dirige a personas o pequeños grupos y siguen un criterio determinado (como altos funcionarios de gobierno).

El “spear phishing” es otra de las variantes que consiste en que el estafador realiza un trabajo previo, donde averigua datos de personas o entidades que le aportan confianza a la futura víctima, como un compañero de trabajo por ejemplo. Este ha sido un avance muy grande porque de esta forma la persona que recibe el e-mail y observa que es de una persona de confianza, no tiene sospechas de que pueda ser víctima de una estafa.

Por otra parte, el phishing también utiliza otras formas para expandir spyware (programas espías) y malware (virus, troyanos...) como el “hishing” o el último en descubrirse “blow pish” que es una combinación de criptografía con virus informáticos o códigos maliciosos.

2.3 FASES DEL PHISHING

Debido a la evolución tan fuerte en estos últimos años del Phishing, diversos estudios determinan diferentes etapas que se que llevan a cabo para ejecutar este delito. Si se conocen estas etapas puede prevenirse y evitar estos ataques. También es importante saber que cada una de estas etapas puede variar de un ataque a otro dependiendo de su dificultad, del método empleado, de la complejidad y de la participación de la víctima. Podemos distinguir, pues, seis etapas diferentes:

1) Fase de planificación:

Como bien dice su nombre, es la etapa donde el estafador prepara su ataque: decide quien será su víctima, cual es el método que utilizará, a que organismo o empresa va a suplantar, que busca con este ataque, que medios utilizara... Esta es una etapa, se podría decir “común” a todos los

ataques phishing. El phisher es aquí donde toma una de las decisiones más importantes: si el ataque va a ser realizado de forma individual o de forma colectiva. Según esta decisión, el atacante también se planteará cuáles son los datos que desea conseguir: si son contraseñas de redes sociales, números de tarjetas bancarias, si quiere conseguir datos personales…

Aquí también es importante conocer el tipo de complejidad y la participación que va a tener la víctima. Todo esto está directamente relacionado a los tipos de phishing. Una vez tomadas todas estas decisiones, el delincuente verá de que medios dispone y como conseguir su objetivo. Teniendo en cuenta estas decisiones podemos distinguir tres tipos de phishing: → Alta complejidad/ Baja colaboración (por ejemplo el ataque al servidor DNS) víctima, → Media complejidad/ Media colaboración (malware) y → Baja complejidad/ Alta colaboración víctima (correo electrónico). En estos tres tipos de phishing se pueden encajar los definidos en el punto 7 de este documento.

2) Fase de preparación:

En general no hay mucha diferencia entre los tres tipos de phishing según la complejidad y la participación, pero sí que hay diferencias en la manera de llevar a cabo el ataque, es decir, para su creación y consecución. Esto es así porque el delincuente según el tipo de información que quiera conseguir, tendrá que utilizar medios diferentes, es decir, teniendo en cuenta las necesidades de cada delito. Por ejemplo si hablamos de un destinatario individual, el correo electrónico que se le envía tiene que estar mucho más elaborado, mucho más preparado y personalizado ya que la víctima es más concreta. Si se tratara de destinatarios colectivos, al ser un envío masivo no hace falta que el correo que se les envía sea tan personal.

Un ejemplo de ataque más personalizado es uno realizado en el año 2007 en España donde se suplanto la identidad de la Agencia Tributaria, utilizando exactamente el mismo logotipo de esta. Aquí se le comunicaba al usuario que tenía una devolución tributaria pendiente, y mediante un link falso les dirigía a una página web fraudulenta. Una vez en esta página web, se les pedía que rellenaran un formulario donde exigían sus datos bancarios.

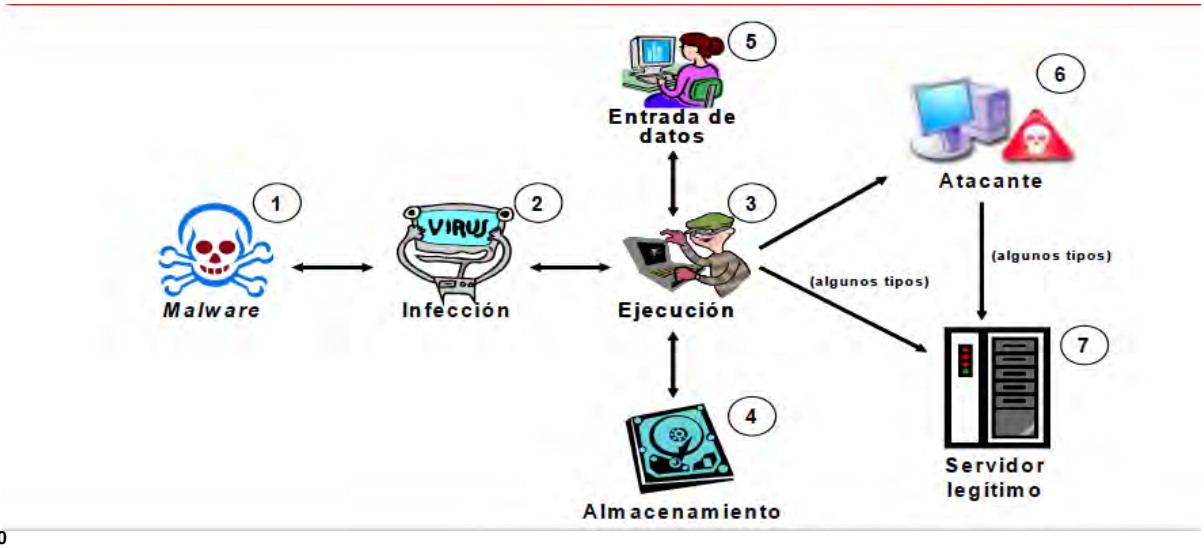
3) Fase de ataque:

Una vez enviados estos correos, aquellos tipos de phishing que necesitan la participación de la víctima de una forma alta o media, van a tener éxito una vez estas caigan en la trampa, como abriendo el link fraudulento y dar sus datos personales.

Aquí según el tipo de phishing que se haya elegido, las tareas serán diferentes. Si hablamos de un phishing con baja participación de la víctima, como un ataque al servidor, la tarea fundamental

será llevar a cabo este ataque con los medios necesarios. Si hablamos de los otros dos tipos de ataque, la preparación consistirá en preparar las diferentes trampas para la víctima.

En esta fase, es interesante conocer cómo se realiza un ataque phishing por medio de un malware. Es decir, lo que sería la "anatomía del phishing". Aquí distinguimos siete elementos esenciales que son: el malware en sí, la infección, la ejecución, la entrada de datos, el atacante y el servidor legítimo. Hay dos puntos de infección importantes: el momento de la propia infección, es decir cuando el malware entra en el sistema sin necesidad de ejecutarlo y cuando se ejecuta el código malicioso.



[10]

4) Fase de recogida de datos:

Como ya se explicó, hay tres tipos de phishing. Por tanto, si se trata de una media o alta colaboración de la víctima habrá que esperar a que ésta ingrese sus datos confidenciales para así poder obtenerlos. Si se trata de un ataque al servidor, la tarea fundamental es ejecutar el malware para conseguir esta información. El gráfico siguiente explica esta fase según el tipo de phishing:

	Agentes	Tareas
Alta complejidad Baja participación	• *Phisher* y colaboradores • Empresa atacada • Víctimas	• A la espera de los datos • Ejecución de código malicioso
Media complejidad Media/Alta participación	• *Phisher* y colaboradores • Víctimas • Empresa suplantada (si existe)	• A la espera de datos (aplicaciones autónomas y *Phishing* de motor de búsqueda) • Ejecución de códigos maliciosos para la consecución de datos (robo de datos, *pharming*)
Baja complejidad Alta participación	• *Phisher* y colaboradores • Víctimas • Empresa suplantada	• A la espera de datos (vía respuesta correo electrónico o visita a la web fraudulenta)

[10] Imágenes proporcionada por INTECO

5) Fase de ejecución del fraude:

En esta fase, una vez que el phisher tiene los datos y consiguió su objetivo, los utiliza para beneficio propio o vende esta información a personas interesadas para que estos efectúen el delito.

6) Fase de post-ataque:

En este punto, el phisher tiene como objetivo, eliminar todo rastro que pudiera luego inculparle de este delito. Cabe decir, que si hablamos de un phishing bancario, el estafador luego procederá a la comisión de otro delito: el blanqueo de capitales o similares.

3. TIPOS DE PHISHING:

3.1 SEGÚN EL SERVICIO QUE ATAQUEN:

BANCOS Y CAJAS:

Aquí el objetivo es robar el pin secreto, el número de tarjeta de crédito y datos análogos con el fin de lucrarse económicamente. Al poseer el atacante estos datos puede utilizarlos para realizar transferencias a otra cuenta, realizar compras y pagos por internet, retirar dinero de la cuenta. Consecuencia de esto es una gran pérdida económica para la víctima. Las excusas utilizadas son varias: a la posible víctima se le envía un correo con un enlace donde se le solicitan los datos porque su cuenta bancaria fue bloqueada por motivos de seguridad, o por un cambio de normativa en el banco, por ejemplo. Los bancos más conocidos que han sido falsificados son ING Direct, Bankia, Banco Popular...

PASARELAS DE PAGO ONLINE:

La intención es igual que cuando se habla de bancos, obtener los datos bancarios. Las excusas que utilizan los estafadores son varias, por ejemplo que se produjo un cierre de sesión del usuario incorrecto o que se detectó una posible intrusión en sus sistemas de seguridad. Las empresas a las cuales afectan son Paypal, Mastercard...

REDES SOCIALES:

Aquí lo que se pretende es claro: suplantar la identidad u obtener información sensible y privada del usuario de redes sociales. Las redes afectadas más comunes son Facebook, Twitter, Tuenti, Instagram... El método empleado aquí es comunicarle a la víctima que se le etiqueto en una foto,

o que alguien le envía una solicitud de amistad, o por motivos de seguridad es necesario que envié sus claves. Este tipo de Phishing es cada vez más utilizado porque hoy en día las personas se comunican por este tipo de redes, el uso de las mismas va aumentando y cada vez es más común que sufran estos ataques. En la actualidad lo raro no es ser usuario de la red social, al contrario, es no serlo. Por tanto, el aumento del uso de las mismas hace que sea un blanco fácil para los Phishers.

PÁGINAS DE COMPRA/VENTA Y SUBASTAS:

La pretensión del estafador en este tipo de phishing es obtener las cuentas de usuario de las víctimas y estafar económicamente al mismo. Las excusas típicas utilizadas para captar la atención del usuario son que se observan movimientos sospechosos, problemas con la cuenta de usuario.... Las empresas que sufren estos ataques son Amazon o EBay. Hay que tener en cuenta que actualmente las personas utilizan cada vez más este tipo de servicios para la compra venta. Antes no era un punto de atención de los phishers porque el uso de estas redes no estaba extendido. Hoy en día, el uso de las mismas es bastante extenso.

JUEGOS ONLINE:

En este medio los motivos son varios: robar la identidad, robar los datos bancarios, los datos privados y suplantación de identidad. Los juegos online comunes suplantados por ejemplo es el World Warcraft. Las excusas son parecidas a las anteriores. Todas destinadas a engañar al usuario.

SOPORTE TÉCNICO Y DE AYUDA DE EMPRESAS Y SERVICIO:

Un ejemplo muy común es el phishing a Apple. Aquí el objetivo es robar la cuenta al usuario, por ejemplo el ID del AppStore para poder hacer compras con la identidad y cuenta bancaria de otra persona. Se suelen suplantar empresas como Outlook, Gmail... etc.

ALMACENAMIENTO EN LA NUBE:

Las empresas que ofrecen este servicio de almacenamiento son Google Drive, Dropbox....Lo que se pretende conseguir son los datos privados, documentos, fotografías que el usuario almaceno en estas páginas web. Una vez obtenidos estos datos, el estafador puede cometer varios delitos relacionados.

SERVICIOS O EMPRESAS PÚBLICAS:

Es un tipo de Phishing que simula ser por ejemplo, la policía nacional, o la Agencia Tributaria y por esto su riesgo. El phisher intenta infectar el ordenador de la persona y así obtener los distintos datos para su beneficio. Una de las excusas utilizadas más comunes, es cuando intentan avisar al

usuario de una posible multa y es necesario obtener sus datos.

SERVICIOS DE MENSAJERÍA:

Esta estafa es menos común. Aquí se utilizan empresas proveedoras de correo y mensajería para efectuar el phishing y así conseguir información privada del usuario. Por ejemplo la víctima recibe un email de la empresa DHL informándole que ha recibido un paquete y le solicita sus datos.

FALSAS OFERTAS DE EMPLEO:

Aquí hay diferentes tipos de oferta falsa que implican phishing para engañar al usuario y conseguir sus datos y a continuación usarlos con fines fraudulentos. Estas son:

- Trabajar desde casa haciendo tareas manuales: se piden sus datos y una cantidad de dinero para guardarle el puesto de trabajo.
- Oferta de trabajo, llama e infórmate: aquí se le pide a la víctima que llame a un determinado número de teléfono y aporte sus datos.
- ¡Empieza a trabajar! Solo tienes que aportar tus datos personales: muy fácil, la víctima ofrece fotografías de su documentación personal y ahí es cuando comenzarían a trabajar. Pero lo único que buscan es obtener información confidencial.
- Infórmate sobre un puesto de trabajo aquí: lo que hacen es poner un anuncio con un enlace ficticio. Cuando la víctima entra en ese enlace, se le instala malware o rellenan formularios con información susceptible.
- Transferencias bancarias: es el trabajo de mula o intermediario que utiliza el phishing bancario.

3.2 SEGÚN EL MODUS OPERANDI

PHISHING ENGAÑOSO- DECEPTIVE PHISHING:

Esta sería la forma en la que se originó el phishing (AOL). Su procedimiento es sencillo: consiste en el envío masivo de correos electrónicos en donde se suplanta una identidad legítima. En este email se piden unos datos por medio de un enlace ficticio y manipulado. Los motivos utilizados para engañar al usuario son varios como la existencia de algún problema en la cuenta bancaria del usuario.

La finalidad de esto es que la víctima ingrese sus datos en la página web a la cual dirige el enlace y así obtener esta información que luego puede ser utilizada por el phisher de forma fraudulenta,

como realizar compras o suplantar la identidad.

Existen diferentes variantes sobre el phishing engañoso. Una de ellas es la instalación de software malicioso en el ordenador del usuario por medio de mensajes.

Hay unos rasgos comunes entre los tipos de phishing. El primero es la suplantación de sitios con buena reputación para así, conseguir la fiabilidad que necesitan. Otro rasgo es que utilizan la página web como cebo y utilizan todo tipo de artimañas para evitar ser descubiertos.
Aquí se ve claramente como el phishing utiliza la ingeniería social, porque de algún modo u otro, necesita la "colaboración" de la víctima. Si esta no "cae" en la trampa, el ataque de phishing no tiene éxito alguno.

Dentro de este tipo de estafa también destacamos el "vishing" y el "smishing"
Por su parte el Vishing es una forma de phishing que utiliza como herramienta principal el teléfono. Resulta muy rentable ya que las personas actualmente tienen plena confianza en el uso del mismo y porque las empresas legítimas también utilizan este medio. Esta técnica utiliza un software llamado "war dialeys" que desde un ordenador realiza las llamadas telefónicas. Cuando la víctima descuelga el teléfono se le intenta convencer de que visite una página web para que confirme sus datos o incluso le piden sus datos personales en la misma llamada.

El smishing por su parte, también es una técnica de phishing pero en este caso utiliza los SMS para que la víctima caiga en la trampa. El primer caso de este estilo que se conoce fue en Pekín. A partir de este entonces el método ha ido evolucionado, donde en cada SMS se le avisa a la víctima que se le ha dado de alta en un servicio de pago y se le comunica que para darse de baja debe visitar determinada página web. Si la víctima accede a esta web se le instalara un software para capturar sus datos. El problema que se observa de este método es su elevado coste, aunque se conoce algún caso donde los estafadores hacen que el SMS corra a cargo de otra persona. Esto es un indicio de cómo se está haciendo cada vez más común su uso.

SOFWARE MALICIOSO- MALWARE BASED PHISHING:

Este tipo de estafa implica la instalación de software malicioso en el ordenador de la víctima. Su propagación depende tanto de la ingeniería social y de la explotación de la vulnerabilidad del sistema. En el primer caso se necesita la acción de la víctima para que el ataque pueda dar lugar, por ejemplo que abra el archivo adjunto de algún correo electrónico y así el malware se le pueda instalar en el ordenador. En el segundo de los casos, el usuario tiene muy poca implicación. Es decir, aunque en muchas ocasiones es por parte del usuario la instalación de un malware, en muchos otros casos se pueden instalar debido a algún fallo en el sistema de seguridad del equipo.

Independientemente de cual sea el método utilizado hay diferentes técnicas y utilización de diferentes programas para conseguir el robo de datos.

→ Estos son:

- *Key-loggers y Screen-loggers:* los key-loggers son programas que se utilizan para grabar y registrar las pulsaciones que se hacen en el teclado. Esto suele ponerse en marcha cuando el usuario ingrese en una página web que este registrada en este programa, tales como entidades bancarias. A partir de ese momento, el programa graba todo lo que se teclea en el ordenador y lo envía al phisher. Esto ha evolucionado tanto que incluso a veces graban los movimientos que se realizan con el ratón. Los screen-loggers por su parte, tienen la misma función pero capturan imágenes que luego envían al atacante.

- *Secuestradores de sesión (session hijackers):* estas aplicaciones actúan cuando el usuario ha accedido alguna vez a alguna web registrada por el software. O sea que no roba datos, sino que su actuación comienza cuando la víctima ya ha accedido a su cuenta. Esto se puede realizar instalando el software malicioso en el ordenador del usuario o mediante la técnica “men in the middle”.

- *Troyanos web:* los troyanos son programas maliciosos que aparecen en forma de ventanas emergentes inesperadamente sobre la pantalla de validación de páginas web legítimas, con el fin de obtener datos privados. Lo importante aquí es que hacen creer al usuario que están en una web legítima pero realmente no es así y estos por tanto introducen sus datos. Esta información se le envía al phisher.

- *Ataques de re configuración de sistema (system reconfiguration attacks):* este tipo de estafa se realiza a través de la modificación de los parámetros de configuración del ordenador de la víctima. Una de las técnicas es modificar el nombre de dominio. Otra forma es la instalación de proxys a través del cual se canaliza tanto la información que entra como la que sale. Esta técnica también es conocida como “men in the middle”.

- *Robo de datos (Data theft):* por otra parte es importante también hablar de la existencia de códigos maliciosos que se instalan en el ordenador y su finalidad es enviar esta información que recaban al atacante.

DNS O “PHARMING”:

Aquí se incluyen las técnicas que se basan en la interferencia del proceso de búsqueda del nombre de dominio. Esta es una de las técnicas de mayor peligro porque tienen poca colaboración del usuario y parece todo más real.

INTRODUCCIÓN DE CONTENIDOS- CONTENT INJECTION PHISHING:

Esta técnica consiste en introducir contenido malicioso en un sitio web legítimo. Esto puede hacerse mediante diferentes modalidades como redirigir al usuario a otra página web o la instalación de algún tipo de malware en el ordenador. Dentro de esta técnica hay tres modalidades:

- Asaltar al servidor legítimo que aprovechan cualquier vulnerabilidad.
- Introducción de contenido maliciosos al sitio web legítimo mediante lo que se conoce como “cross site scripting”. Aquí se aprovecha alguna vulnerabilidad para introducir datos sin ningún tipo de validación.
- Aprovechamiento de una vulnerabilidad SQL. Así consiguen la provocación de la ejecución de comandos de bases de datos de un servidor remoto que conlleve la filtración de datos privados y confidenciales. Se produce por una ausencia de los filtros adecuados, igual que en el caso anterior.

TÉCNICA DEL INTERMEDIARIO- MAN IN THE MIDDLE PHISHING:

Se encuentra muchas veces introducido como un tipo de phishing pero en verdad es una técnica más. Aquí el phisher se posiciona entre el ordenador del usuario y el sitio web legítimo. Así puede leer, modificar y obtener la información que entra y sale del ordenador. Puede obtener todos los datos que desee con el fin de robar cuentas bancarias o el secuestro de la sesión.

MOTOR DE BÚSQUEDA- SEARCH ENGINE PHISHING:

Es como en el caso anterior, un tipo de técnica utilizada por los phishers que consiste en la creación de páginas web donde se ofrecen servicios o productos falsos. Las introducen en los índices de los motores de búsqueda y una vez que el usuario realiza algún tipo de compra, está proporcionando información privada. Normalmente este tipo de ofertas, tienen precios muy buenos y muy bajos para que los usuarios de internet caigan en la trampa más fácilmente.

4. **¿CÓMO PROTEGERSE DE ESTOS ATAQUES?**

→ Lo más importante y destacable es que jamás se otorgue información susceptible, privada e intimida a través del correo electrónico, llamada telefónica o mensaje SMS. Se puede estar seguro de que las entidades y organismos no solicitaran esta información utilizando estos medios. Estas empresas ya disponen de los datos del usuario y en cualquier caso, sería el propio usuario el que solicite esta información al organismo.

Cuando desee visitar algún sitio web, es más seguro teclear la dirección URL en la barra de direcciones y no abrirla por enlaces que se le envíen al correo o medios análogos. Las empresas bancarias disponen certificados de seguridad y cifrados y por tanto son medios seguros.

Si el correo electrónico es de alguien de confianza que le solicita los datos privados, es mejor cerciorarse de que es totalmente legítimo. Muchas veces los phishers utilizan este método para obtener mejores resultados. La víctima al ver que es alguien de su confianza aporta los datos que se le solicitan por medio del enlace. Si en el correo, hay adjunto un documento, probablemente sea un virus y desee infectar el ordenador. Para no caer en la estafa, se debe estar seguro siempre de con quien se está contactando.

→ Si usted tiene duda sobre la fiabilidad del enlace, no cliclee y evite entrar en él. Si desea acceder a la web, mejor cliclee usted mismo el enlace en la barra de direcciones, cerciorándose de que escribe correctamente el enlace. Esto es recomendable porque en ocasiones los enlaces falsificados solo tienen una o dos letras de diferencia.

→ Por último y más importante, si una persona cree ser víctima del phishing, es necesario que cambie todos los datos privados a la mayor brevedad posible.

Todas las personas que utilizan internet, especialmente el correo electrónico, corren el riesgo de ser víctimas de una estafa.

Para un phisher es muy rentable realizar este tipo de ataques. Envían correos masivos a millones de personas diariamente. Un pequeño porcentaje de estos usuarios caen en la estafa, con la consecuencia de un perjuicio económico para él y un beneficio para el phisher. Por este motivo, este tipo de malware continuará y seguirá avanzando. Lo importante es que los usuarios de internet también avancen y estén preparados.

→ Como hemos visto, el phishing no solo se puede realizar por correo electrónico, sino también mediante llamadas telefónicas. Por eso es importante saber identificar una llamada falsa. Puede parecer legítima pero el código de área puede modificarse. Por eso hay que estar seguros de donde proviene la llamada.

→ Protección a través de un software: los antivirus deben ajustarse y actualizarse a menudo para evitar este tipo de ataque

11

5. IMPACTO DEL PHISHING

Si el phishing no tuviera ningún tipo de impacto, no serviría de nada utilizar esta técnica para conseguir beneficios. Este tipo de delito tiene tanto impactos económicos como sociales. Cabe decir que el impacto económico puede ser tanto a un particular (cuando le roban sus claves de acceso a sus cuentas bancarias personales) o a una empresa, mientras que sobretodo el impacto social se produce en las empresas porque sus clientes pierden la confianza en la misma, empiezan a tener menos fiabilidad.

5.1 IMPACTO ECONÓMICO

Es importante saber que ya que estamos hablando de un delito relativamente nuevo, hay pocas estadísticas sobre su impacto, si bien se puede decir que por cada fraude exitoso, la

[11] https://www.infospyware.com/articulos/que-es-el-phishing/

pérdida económica a nivel mundial tiene una media de 593€[12]. En España estos fraudes no tienen tanto beneficio, siendo la media inferior a los 400€. Esto es así por un motivo: según el código penal español, para que una estafa pueda ser concebida como un delito, lo defraudado debe superar los 400€, en caso contrario, se estaría hablando de una falta. Por tanto, a los estafadores les es más rentable cometer más ataques phishing de menor ganancia económica pero que sea constitutivo de falta y no de delito.

En EE.UU, un estudio determina que las pérdidas económicas por este delito son mayores que cualquier otro tipo de fraude, rozando los 1,5 millones de dólares, mientras que por otros delitos son pérdidas que rondan los 2400 dólares. Por tanto llegamos a la conclusión de que a pesar de que los ataques por virus son más dañinos porque llegan a una colectividad mayor, el impacto económico por phishing es considerablemente mayor.

En nuestro país, el impacto también es bastante considerable. Se han analizado los datos obtenidos en los últimos años ofrecidos por diferentes instituciones, tales como INTECO[13] o INE[14] y se llega a la conclusión de que este tipo de ataque ha pasado de 293 ataques anuales a 1.184.

Como se ve, cada fraude no tiene una gran ganancia. Pero si se multiplica la ganancia de cada fraude con todos aquellos exitosos al año, se puede entender la dimensión del problema.

5.2 IMPACTO SOCIAL

Principalmente el phishing afecta a la confianza de los usuarios en realizar operaciones en internet, sobretodo en realizar transferencias o transacciones. El phishing es un fenómeno en aumento, al igual que la tecnología, pero ambos aumentan a la misma velocidad y por tanto la confianza de los usuarios de internet para realizar diferentes operaciones va disminuyendo. El miedo de ser una víctima de phishing se nota sobre todo en las plataformas de compra y venta online. Cada vez más personas tienen menos fiabilidad a los sistemas de seguridad en la red. Según diferentes estudios, una de las cuestiones que más interesa a un usuario es su privacidad. Se siente más seguro en páginas web que conoce y que le aportan mayor fiabilidad y tranquilidad. Una cantidad importante de usuarios, rondando el 68%, determina que no realiza compras por internet por temor a ser estafado. Otros usuarios que no utilizan las bancas electrónicas explican

[12] Datos obtenidos por estudios de INTECO.
[13] En la actualidad conocida como INCIBE
[14] Instituto Nacional de estadística

que lo harían si éstas tuvieran sistemas de seguridad más fiables.

Además por otra parte, la desconfianza que crea en los usuarios que una empresa sea suplantada frena el uso de las mismas plataformas. La pérdida de seguridad de los usuarios en una empresa le causa perjuicios ya que su imagen pública se ve dañada y por tanto, cada vez menos usuarios confiaran en ellas.
Un dato importante obtenido mediante estudios de instituciones dedicadas a la prevención del phishing, es que el 82% de estos ataques son realizados para obtener datos bancarios. Mientras que el 21,5% corresponde a ataques para conocer datos sobre empresas de compra y venta online.

6. AGENTES AFECTADOS

Cualquier persona individual o formando parte de una empresa o institución se puede ser víctima del phishing. Independientemente de cual sea la víctima, todos ellos pueden ser atacados en un mismo nivel de un modo u otro. Todos son susceptibles de convertirse en las próximas víctimas de un phisher.

- *ENTIDADES FINANCIERAS Y EMPRESAS PRESTADORAS DE SERVICIOS*: uno de los puntos principales aquí para prevenir el phishing, es la seguridad en las transacciones de dinero que se producen en estas páginas, por ejemplo, EBay. Por tanto, para los usuarios, es importante la seguridad y las medidas que estas páginas web utilizan. Actualmente muchas de ellas compiten en cual tiene mejores niveles de seguridad, y esto es una ventaja. El usuario optará por aquellos sitios web que le ofrezcan más fiabilidad. Es una forma también de que estas entidades se actualicen y propongan medidas preventivas para evitar el fraude. Una de las instituciones que mejores medidas ofrece es la APWG. Esta web explica que es el phishing y formas para combatirlo. Actualiza diariamente datos y estadísticas sobre esta estafa e informa de nuevos modelos de phishing. Otra entidad muy importante es el Foro Abuses, donde su principal función es evitar que se produzcan delitos informáticos y lo más destacable es que participa con otras instituciones a nivel europeo.

- *BANCOS, CAJAS DE AHORRO.* Si bien no es la única víctima del phishing, si es la que más ataques recibe. Estas empresas son conscientes de los diferentes delitos informáticos que intentan causar pérdidas económicas a sus usuarios. Están actualizados con la mayor tecnología posible y si ocurre algún tipo de estafa, intentan

reparar el daño. Para evitar este tipo de ataques, los bancos también informan a sus usuarios de determinadas medidas que ellos mismos tendrán que tener en cuenta para evitar ser una víctima, además de las medidas que ellos mismos proponen. Dos de las medidas más importantes es la contratación de empresas de seguridad y la creación de un grupo interno de seguridad informática donde se investigan supuestas páginas web fraudulentas y con código malicioso.

- *USUARIO INDIVIDUAL*: al contrario de las víctimas anteriores, aquí no suplantan su identidad sino que intentan obtener sus datos confidenciales para luego utilizarlos a su conveniencia. Por tanto, es importante que un usuario de internet sea consciente de los daños que puede producir internet si no se conocen los diferentes delios existentes y no se toman las medidas adecuadas, por ejemplo en determinadas ocasiones es preciso utilizar contraseñas de un solo uso, que caducan una vez utilizadas y complica la ejecución exitosa del fraude del phisher.

7- EJEMPLOS

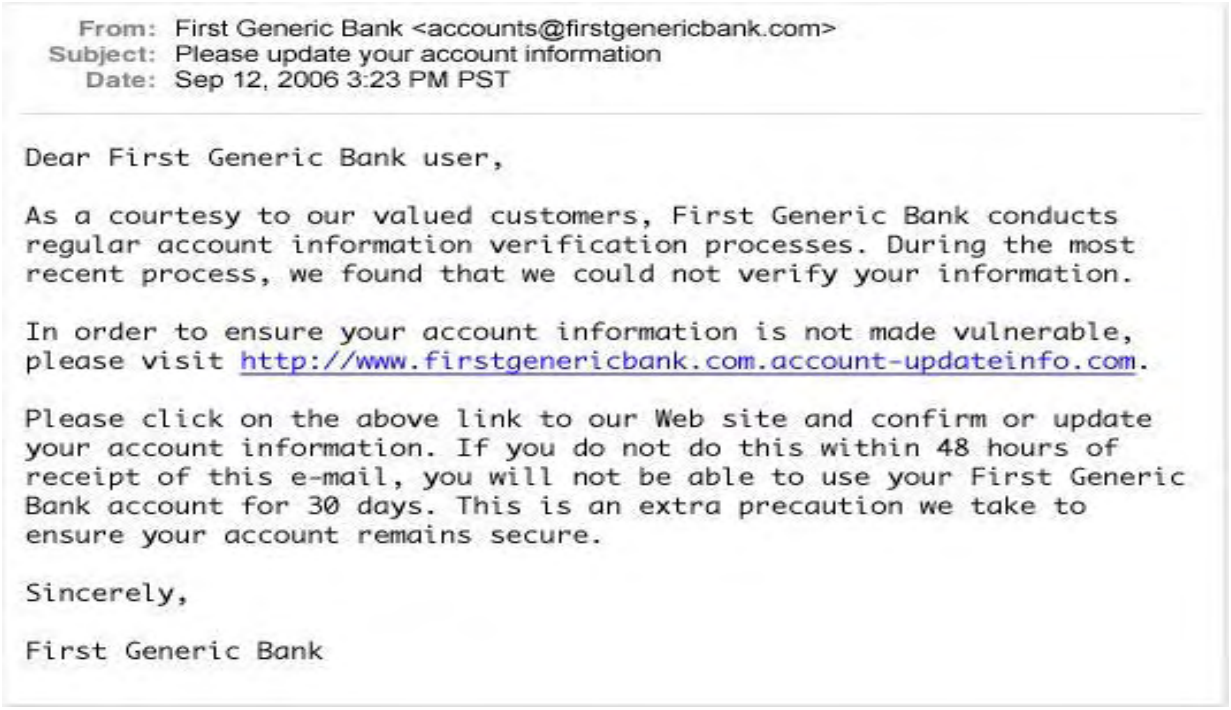
A continuación expondremos dos tipos de phishing muy comunes. El primero de ellos es uno de los más importantes ya que afecta tanto a la entidad bancaria que suplanta como a la persona de la cual obtiene los datos privados. Además en este tipo de phishing es importante destacar que para los phishers obtener luego el dinero de las cuentas bancarias supone contactar con una tercera persona que actuará como el intermediario o mula. Esta persona estará la mayoría de las veces engañada. En el caso del phishing en redes sociales, es una práctica para demostrar que hoy en día el phishing está al alcance de cualquier usuario de internet. Solo hace falta investigar un poco para conocer cómo realizar esta estafa y usurpar la identidad de una persona. En este último caso los phishers no suelen obtener beneficios económicos, pero su finalidad principal es simular que es la persona dueña de la red social para humillarla y ridiculizarla o conocer más datos privados de la misma.

7.1 PHISHING BANCARIO

En el siguiente ejemplo, se verá cómo funciona un ataque Phishing desde la recepción del correo electrónico:

→ En primer lugar, la persona recibe este email en la bandeja “Correo electrónico no deseado” al no pasar los filtros de seguridad del correo electrónico. Si pasan los filtros lo encontraremos en la bandeja de entrada.

El email que podemos encontrar, típico en estafas bancarias es el siguiente:



From: First Generic Bank <accounts@firstgenericbank.com>
Subject: Please update your account information
Date: Sep 12, 2006 3:23 PM PST

Dear First Generic Bank user,

As a courtesy to our valued customers, First Generic Bank conducts regular account information verification processes. During the most recent process, we found that we could not verify your information.

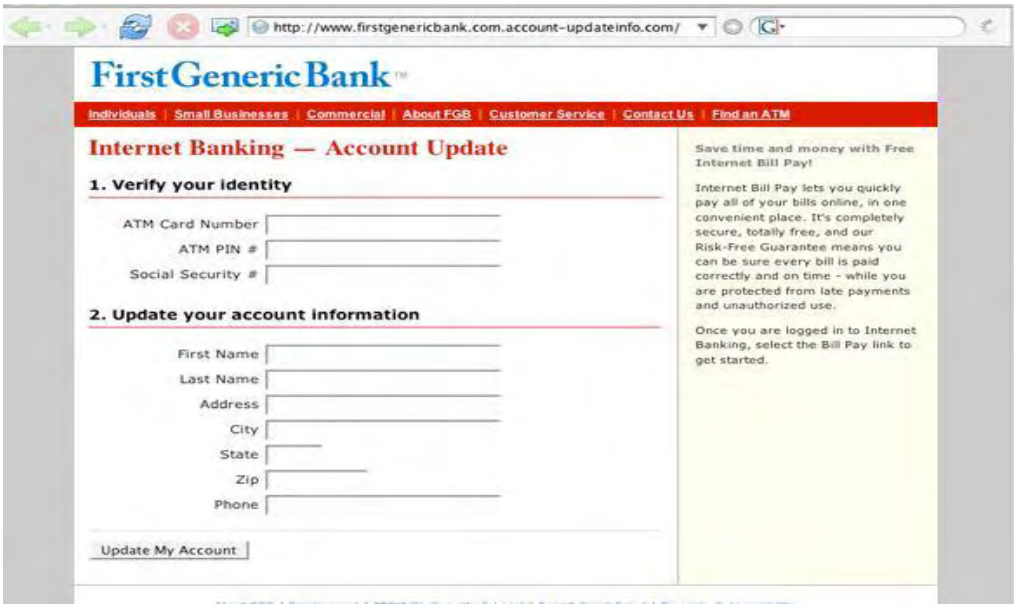
In order to ensure your account information is not made vulnerable, please visit http://www.firstgenericbank.com.account-updateinfo.com.

Please click on the above link to our Web site and confirm or update your account information. If you do not do this within 48 hours of receipt of this e-mail, you will not be able to use your First Generic Bank account for 30 days. This is an extra precaution we take to ensure your account remains secure.

Sincerely,

First Generic Bank

El link de este correo electrónico, le dirige a una página falsificada que simular ser la web



legítima del banco. A partir de ahora todos los datos que el usuario introduzca en esta página serán registrados y utilizados por el phisher para su propio beneficio.

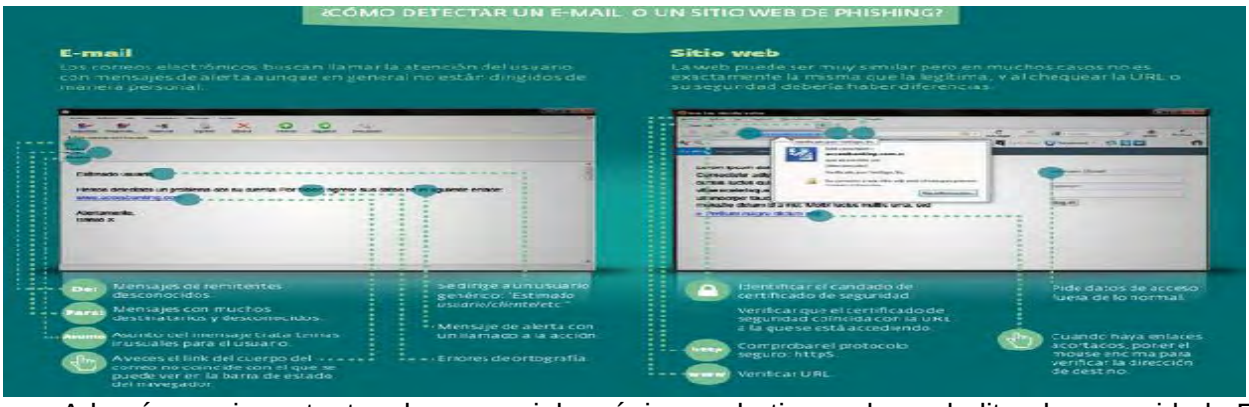
Para distinguir un **correo phishing** de uno legítimo podemos observar varias características:

La primera de ellos, es que los emails fraudulentos contienen un saludo genérico para ahorrar tiempo, tal como vemos en el ejemplo que utiliza “First Generic Bank User”. Así se ahorran de escribir todos los nombres en diferentes correos electrónicos de uno en uno.

El uso de vínculos forjados, es decir, aunque en el enlace se vea el nombre de la institución, del banco en este caso, no significa que el enlace sea real y fiable.

Por otra parte, los sitios donde es seguro entrar, van acompañados de una “s”: https
Esta “s” significa seguridad.
Otra forma común para saber si es un enlace falso, es que siempre requieren que se les otorgue información personal susceptible. Y además suelen ser mensajes que parecen urgentes, es decir, donde la información es requerida cuanto antes.
Otro punto es que los remitentes desconocidos, o que el mensaje tenga muchos remitentes y que además también sean desconocidos.
Por tanto, para no ser víctima de esta estafa, es importante ver y seguir todos estos consejos.

Para distinguir una **página web phishing** podemos mirar la resolución. Una página fraudulenta suele tener poca resolución ya que se crean con rapidez y tienen una corta utilidad. Las direcciones web que suelen empezar con una dirección IP, suelen ser Phisher.



Además es importante observar si la página web tiene el candadito de seguridad. En muchas ocasiones se solicitan datos de acceso fuera de lo normal. [15]

[15] www.pcworld.com

7.1.1 RECOMENDACIONES

Para el sector financiero, tan proclive a estos ataques y anualmente el que más ataques phishing recibe, según estudios, se pueden dar una serie de recomendaciones importantes, tanto generales como específicas.

En las generales distinguimos:

1) *Aunar esfuerzos*: un aspecto importante para la prevención de este delito, es contar con el apoyo de otras instituciones y con empresas destinadas a la seguridad informática y las FCSE. Esto es mejor así porque si cada empresa financiera denuncia aisladamente un caso de phishing, combatirlo será mucho más complicado que recopilar todos estos datos en conjunto y así poder llegar a mejores conclusiones. Por tanto es imprescindible la existencia de una cooperación entre las fuerzas y cuerpos de seguridad y las bancas electrónicas para poder unificar los ataques y descubrir su origen.

2) *Actuaciones globales*: claro está que no se puede solucionar un problema desde el punto de vista de la banca o del usuario afectado. Combatir el phishing va mucho más lejos. Se necesita la cooperación de cuerpos especializados, no solo la entidad financiera o el usuario, sino por ejemplo, una empresa proveedora de telecomunicaciones que pueda reconocer cuales son las páginas web sospechosas y así implantar medidas para evitar que alguien navegue por ella.

3) *Uso de mecanismos preventivos*: el usuario también debe tener los medios necesarios, como antivirus o herramientas antiphishing. Y obviamente que estén actualizados a los avances de estos delitos.

Por otra parte **dentro de las medidas específicas** distinguimos:

1. *Autenticación de dos factores*: son medidas de seguridad fuerte que el usuario tiene derecho a recibir por parte de su banca electrónica, tales como:

- *Tarjeta de coordenadas*: se trata de una tarjeta que dispone un usuario con una clave dinámica, lo que complica los ataques. Y es requerida para hacer

transacciones de dinero. Cada vez que el usuario quiera realizar una transferencia tendrá que disponer de esta clave que cada vez será aleatoria. Es bastante exitosa frente a los ataques phishing.

- Token de seguridad: este permite la identificación del usuario. Pero tiene algunos inconvenientes como la incomodidad del usuario o su alto coste.

2) *Tarjetas de crédito:* existe la creencia que el uso de las tarjetas de crédito tiene menos fiabilidad que las bancas electrónicas. Esto no es del todo así, ya que los métodos de seguridad de las tarjetas de crédito llevan utilizándose hace muchos años y cuentan con bastante seguridad. Por ejemplo si se utiliza una tarjeta en un cajero automático, cualquier movimiento de fondos extraño será detectado ya sea por la cantidad extraída o por la ubicación. Inmediatamente se pondrán en contacto con el usuario para confirmar que es él quien está realizando estos movimientos.

3) *Implementar reglas lógicas y de comportamiento*: aquí se memorizan pautas de actuación del usuario, permitiendo establecer ante caos fraudulentos diferentes alarmas.

4) *Avisos al móvil por SMS*: esta medida tiene mucho éxito entre los usuarios ya que cada vez que se haga una transferencia o un pago, se le avisará al usuario vía SMS. Por tanto siempre tendrá el conocimiento de que está pasando en su cuenta. Es un método que funciona muy bien hoy en día debido a la dependencia de los usuarios a su teléfono móvil.

7.1.2 EL INTERMEDIARIO O MULA

En el phishing bancario, una de las cuestiones más importantes es como puede conseguir el estafador extraer el dinero de las cuentas bancarias sin ser descubierto.

Principalmente, los phisher se basan en técnicas de ingeniería social para conseguir la participación de una tercera persona y así, conseguir el dinero de la cuenta. Esta misma técnica es utilizada también para obtener estos datos bancarios. La ingeniería social significa que la víctima colabora para que se pueda realizar la estafa.

La palabra mula no es nueva, sino que proviene del término anglosajón “money mule” que

significa que una persona realiza transferencias de dinero el cual se obtuvo de forma ilegal en un mismo país a otro donde suele vivir el estafador.

Para conseguir la participación del intermediario, también conocido como “mula”, el estafador le ofrece un puesto de trabajo desde casa, por ejemplo, en actividades administrativas. Uno de los requisitos es que el intermediario resida en el mismo país que la víctima. Por tanto, la mula realiza transferencias bancarias de una cuenta a otra (es decir, de la cuenta de la víctima a su cuenta), sin tener mayor problema y con rapidez. Una vez obtiene este dinero, realiza una transferencia al phisher que le ofrece una identidad falsa y que suele ubicarse en países del Este y por eso es difícil su condena, por medio de moneygram o similar, quedándose él mismo una pequeña retribución. Este intermediario, no sabe que está siendo partícipe de una actividad ilícita.

El intermediario suele caer en esta trampa porque en muchas ocasiones, no tiene un trabajo estable y se encuentra en una situación de necesidad y al ofrecerle esta oferta laboral, acepta sin pensarlo. Con este método, es muy fácil ocultar la identidad del phisher. El solo se encarga de obtener los datos bancarios mediante esta técnica fraudulenta, pero luego la persona que tiene el trabajo de realizar estas transacciones es una tercera persona a la cual engaña.

7.1.2.1 PUNIBILIDAD

Cuando la víctima es consciente de las realizaciones de estas transferencias, la primera persona acusada es el intermediario o mula. Este último no sabe que la actividad que estuvo realizando formaba parte de una estafa planificada por el phisher. El problema aquí se plantea para determinar si la mula puede ser culpable o no de estas acciones. El código penal español determina que para que una acción pueda ser constitutiva de delito, tiene que concurrir dolo o imprudencia. En estos casos, el dolo o intención no existe. La persona no es consciente de que está cometiendo un delito. Pero por lo general, los tribunales españoles determinan que estas ofertas de trabajo tan bien remuneradas deberían llamar la atención del intermediario y este averiguar si realmente es un trabajo lícito. Por tanto, se considera que esta ignorancia deliberada no exime a la mula de la condena penal, y suelen ser condenados por cooperación necesaria o coautoría. Este tipo de condenas suele ser muy criticada ya que no se personaliza y estudia cada caso concreto, no se determina si el intermediario puede ser o no consciente de que se trata de un delito según sus capacidades y además algunos juristas opinan que el intermediario también es víctima del estafador. Pero por lo general, en España se condena la figura del intermediario y en algunas ocasiones, suelen ser bastante duros en las condenas. Se les suele condenar por

delitos de blanqueamiento de dinero y receptación o estafas. Actualmente en España, hay muy pocas sentencias absolutorias a las mulas en los caso de phishing.
Un ejemplo de una sentencia condenatoria en un caso de intermediario lo muestra la sentencia de la Audiencia Provincial de las Islas Baleares 264/2012.

Actualmente, como el fenómeno de las mulas está en aumento, se creó una página web (http://www.bobbear.co.uk/) donde se exhiben diferentes ofertas de trabajo falsas para captar nuevas mulas.

7.2 PHISHING REDES SOCIALES

El phishing es un método que día a día avanza y se aplica con más frecuencia. Además del phishing bancario, uno de los más importantes a causa de las grandes pérdidas económicas que causan a la víctima, también encontramos el phishing en las redes sociales, como Facebook, Hotmail...

Actualmente la mayoría de personas, sobre todo jóvenes, están conectados a estas redes prácticamente cada día y por ello existen muchas formas de usurpar la personalidad de un usuario.

A continuación se mostrará una técnica utilizada para conseguir las contraseñas de las redes sociales mediante el envío de un xploit[16] al correo electrónico. En este caso la red social que intentaremos usurpar es Facebook.[17]

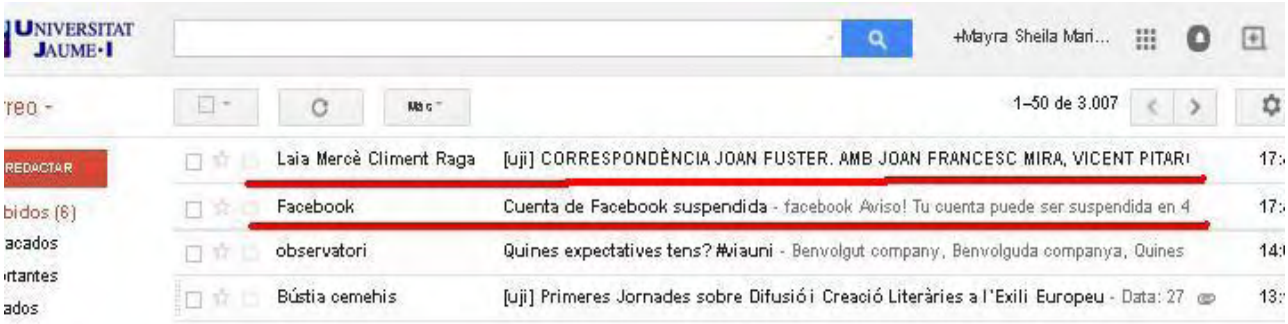
- Lo primero que se hizo fue buscar una página de internet que tuviera lanzador de xploits gratuitos. Esta página es www.lanzadorx.com[18]. Aquí se puede observar como hay diferentes métodos de engaños para las diferentes redes sociales.

[16] Pieza de software utilizada con el fin de aprovechar una vulnerabilidad de un sistema de información y así conseguir un comportamiento no deseado del mismo.
[17] Red social utilizada por una gran cantidad de usuarios hoy en día.
[18] Esta página web permite el envío de varios tipos de xploits en diferentes redes sociales.

Lo primero que hay que hacer es registrarse en la página con un usuario y una contraseña. Una vez visionados los métodos de engaño (invitación, cuenta bloqueada, etiquetado o conectar Facebook), se elige uno de ellos para enviar a la víctima. Para que el xploit llegue a la bandeja de entrada, la misma página recomienda que el email falso que utilicemos sea de Gmail o de Hotmail. De esta forma se asegura que el xploit tenga más probabilidades de visibilidad por la víctima.

Por ello, se creó un email en Hotmail asegurar que el engaño sea más creíble. Nuestro email es faceibookservice@hotmail.com. Este correo electrónico va a ser el utilizado para engañar a nuestra víctima. Una vez elegido el método y teniendo nuestro propio correo electrónico falso, procedemos a enviar el correo al usuario de Facebook.

Por tanto, si estos pasos se realizaron correctamente, la víctima vería en su bandeja de entrada de correo electrónico un email procedente de Facebook.



Al abrir el email, se ve un enlace que nos redirige a una página “real” de Facebook para que se arregle el error.

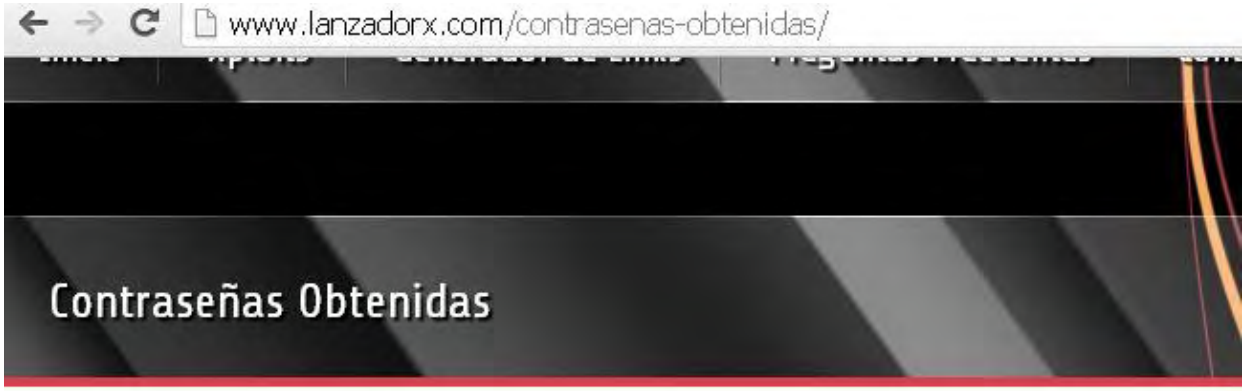
Este enlace fraudulento, nos redirige a una página idéntica a la original de la red social, pero la

verdad es que es una página trampa que una vez coloquemos correctamente nuestra contraseña (ya que no permite que pongamos mal la contraseña de Facebook), se envía a la página de donde proviene el xploit.

Aquí es importante observar que en la barra de direcciones aunque la página parezca totalmente fiable, el enlace es INCORRECTO. Pero es un detalle tan mínimo que las víctimas no suelen identificar.

Una vez colocada nuestra contraseña, se nos redirige a la página oficial de Facebook donde nos pide nuevamente nuestro usuario y contraseña y por tanto el usuario no sospecha que acaba de ser víctima del phishing.

Nuestra contraseña ya está en manos del phisher.



Eliminar	Comprobar	Revelar	Email	Password	Servidor
Eliminar	Comprobar	Revelar	al225916@uji.es	******a*******	Facebook

Como se puede observar, el Phishing está en las manos de cualquier usuario. Eso sí, también hemos encontrado algunos inconvenientes para esta forma. Uno de ellos es que si se quiere usurpar la identidad de una persona concreta, se necesita saber el email de la misma, y esperar a que caiga en la trampa. No es un método que asegure tener éxito al 100%. Además en esta página concreta, aunque el envío de los xploits es totalmente gratuito, el desvelar la contraseña no lo es. Otro inconveniente es que para que llegue a la bandeja de entrada, se tiene que hacer una cuenta falsa en Hotmail y Gmail, porque su lanzador no asegura que llegue a esta bandeja y en cambio llegue a la bandeja de Spam.

Aun así, es una técnica con xploits que funciona y hoy en día su uso se está extendiendo.

8- ¿CÓMO SE DENUNCIA?

Teniendo en cuenta que el Phishing es un tipo de estafa, se puede denunciar al órgano competente para su posterior investigación.

Además, la Asociación de Internautas creo un medio por el cual los usuarios de internet pueden denunciar este tipo de correo phishing. El motivo por el que se creo es erradicar las posibles estafas por medio del phishing.

8.1- EL PHISHING EN EL CÓDIGO PENAL ESPAÑOL

En el código penal español no existe una regulación específica para los delitos informáticos. Aun así, podemos encontrar tipificaciones dentro de los siguientes apartados:

-*Delitos de naturaleza económica:* estos son los que afectan patrimonialmente a una persona, o le causan algún perjuicio económico. Aquí el delito más común, es la estafa informática. Está regulada en el artículo 248 del CP y diferencia dos tipos: los que utilizan ingeniería social pura y los que utilizan un código malicioso (malware) o de intrusión en sistemas de información. El primero es donde incluiríamos el Phishing.

Además se establece también una pena para los daños informáticos, reflejados en el artículo 264.2 del CP.

No solo se encuentran tipificaciones para el phishing, sino que a lo largo del código penal encontramos que también se castiga el delito contra la propiedad intelectual, delitos de empresa...

Un delito que nos interesa es el de falsedades documentales (en este caso falsificación de soporte informático) para prestar apoyo a las diferentes transacciones económicas.

Por otro lado, el spam también está penado por nuestro código penal. Aquí también cabe el phishing o el fraude nigeriano cuando el spam tiene como finalidad el fraude u otros fines delictivos, como dañar la reputación de una persona.

Situándonos en este delito (spam) y la relación con el phishing se puede decir que hay una relación directa porque el enviar correos masivos de forma fraudulenta puede ser una forma de captación bastante eficiente. Un dato importante es conocer que el porcentaje de correo electrónico no deseado que utiliza el phishing es bastante bajo en comparación de los otros fines del spam.

8.1.1. REFORMA CÓDIGO PENAL

El 30 de Marzo se publicó en el BOE una nueva reforma del código penal español que afecta a los delitos informáticos, entre muchas otras cosas. Este tema es de interés ya que, como se dijo a lo largo del documento, el phishing es uno de estos delitos. Esta reforma que afecta directamente al phishing, es la modificación del artículo 197, en sus apartados 1 y 2 y los nuevos artículos

implementados 197 bis y ter, dónde se tipifica el black hacking, craking y técnicas de acceso no consentido. En estos se castiga la producción y la adquisición para el uso, importe o facilitación a terceros, programas informáticos para cometer delitos con ellos, y que además proporcione contraseñas de ordenador o códigos de acceso. El espionaje es también añadido a esta sección al igual que el sabotaje.

8.2 LEGISLACIÓN APLICABLE A DELITOS INFORMÁTICOS

- **Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995**, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

- **Directiva 97/66/CE del Parlamento Europeo y del Consejo, de 15 de diciembre de 1997,** relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones. (Derogada por la Directiva 2002/58/CE).

- **Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002,** relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas. (Directiva sobre la privacidad y las comunicaciones electrónicas):

- **Directiva 2006/24/CE del Parlamento Europeo y del Consejo de 15 de marzo de 2006** sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE.

- **Constitución Española de 1978 en su artículo 18. 4** donde se establece que *"La Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".*

- **Ley Orgánica 1/1982, de 5 de mayo**, de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar, y a la Propia Imagen.

- **Ley 34/2002, de 11 de julio** de Servicios de la Sociedad de la Información y Comercio

Electrónico (LSSI-CE).

- **Ley 32/2003, de 3 de noviembre**, General de Telecomunicaciones.

- **Ley Orgánica 5/1992, de 29 de octubre**, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal. (LORTAD, vigente hasta el 14 de enero de 2000).

- **Ley Orgánica 15/1999 de Protección de Datos, de 13 de diciembre (LOPD)** y el **Reglamento de Medidas de Seguridad (RMS).**

- **Código Penal, (CP), aprobado mediante Ley Orgánica 10/1995, de 23 de noviembre.**

8.3 UNIDADES DE PERSECUCIÓN DEL PHISHING

Como hemos visto, el phishing y en general los delitos informáticos están en continua evolución. Hoy en día las denuncias contra estos delitos son una gran mayoría y cada día son más las víctimas de estos delitos. Por tanto, hubo la necesidad de crear cuerpos especializados en estos temas para conseguir disminuir el número de ataques en la red y que los usuarios puedan navegar con mayor tranquilidad. No es un trabajo fácil. Se necesita de tiempo y sobretodo colaboración entre las diferentes unidades para compartir información y así actuar conjuntamente. A lo largo de los años se han ido creando cuerpos especiales tanto a nivel nacional como internacional. Los delitos informáticos no son un problema que solo ocurre en España, sino que es un tema grave a nivel mundial. La gran mayoría de los países tienen medios adecuados para erradicar estos delitos y una de las mejores opciones es trabajar con otros países en conjunto. A continuación se señalan los grupos especializados tanto a nivel nacional como internacional:

- **NIVEL NACIONAL:**
  - **BRIGADA DE INVESTIGACIÓN TECNOLOGICA DE LA POLICÍA NACIONAL:** se trata de una unidad especializada del cuerpo nacional de policía donde se investiga el delito, el delincuente y las diferentes pruebas para valorarlas y ponerlas a disposición judicial. Por tanto se necesita una información constantemente actualizada y que diferentes instituciones colaboren con ella para obtener estos datos. Por ejemplo, colabora con policías de otros países. Su ámbito de actuación se basa en todo tipo de delito informático.
  - **GRUPO DE DELITOS TELEMÁTICOS DE LA GUARDÍA CIVIL:** esta unidad no es nueva, sino que existe hace varios años. Su base consiste en la investigación de

delitos que utilizan la red para llevarse a cabo. Tal y como avanzan las medidas para evitar la comisión de estos delitos, también avanza la tecnología y era necesario un grupo especializado que investigara cada tipo de delito individualmente y creara formas y medios para prevenirlo y combatirlo. Ofrece consejos para los usuarios de internet y advierte de todas las formas delictivas conocidas hasta el momento. Una de sus grandes mejoras es que facilitan un enlace para que las víctimas de estos fraudes puedan denunciar de forma directa.

    - **POLICÍAS AUTONÓMICAS:** tanto los Mossos d'escuadra como la Ertzaina tienen cuerpos especializados en estos delitos.
    - **AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS:** su función principal es velar porque se cumpla la Ley Orgánica De Protección de Datos de carácter personal.

- **NIVEL INTERNACIONAL**
    - **EUROPOL:** es una organización europea que pretende la colaboración de todos los países miembros de la unión para prevenir y luchar contra el crimen informático. Actúa por medio de los ELOs, recopilando información sobre los diferentes delitos e intercambiándola entre los diferentes países. Además crea análisis y estadísticas de los delitos para que todos los países miembros sean conocedores de ellos.
    - **INTERPOL:** esta unidad por su parte, creó 4 grupos especializados en delitos informáticos y su finalidad es estar al corriente de todas las actualizaciones y avances de estos fraudes.
    - **G-8:** es un grupo integrado por los países más ricos del mundo que crearon a su vez un subgrupo sobre delitos de alta tecnología. Aquí se muestran diferentes protocolos de participación de los países y diferentes colaboraciones con empresas privadas para la evitación de estos delitos.

9- MITOS DEL PHISHING

En el pasado, todos los artículos que hacían referencia al phishing, lo hacían informando de cómo evitarlo. Pero en la actualidad, con todas las mejoras que han ido adoptando es muy complicado, incluso para una persona especializada, distinguir cuando se está hablando de una estafa phishing a una página o correo electrónico legítimo. Por esto han surgido varios mitos del phishing:

1) Las estafas phishing contienen errores ortográficos y no parecen emails fiables.

→ Esto ocurría con anterioridad, pero al ir avanzando la tecnología estos errores se fueron reparando.

2) Comprobar la línea del navegador para ver a que página web nos está dirigiendo el correo electrónico fraudulento.

→ El uso de códigos sofisticados hacen que en la línea del navegador se vea la URL deseada por el phisher.

3) Corroborar la URL mientras estas en la página web.

→ Algunos enlaces contienen dominios que parecen reales pero no lo son.

4) Comprobar que el link es seguro, que es “https”.

→ Un certificado de seguridad no es muy costoso y además pueden utilizarse en otros países. Por tanto, ya existen muchas web phishing que son “seguras”.

10- FUTURO DEL PHISHING

Si se tiene en cuenta cómo ha ido evolucionando el Phishing en los últimos años, se cree que un nuevo tipo de Phishing surgirá pronto.

Por fortuna, las empresas bancarias están tomando las medidas necesarias para que los usuarios del banco se sientan seguros con la banca online y así poder evitar estafas phishing y otro tipo de delitos informáticos. Por ejemplo no solo requerirán un usuario y una contraseña, sino que se aporten más datos.

Cuantos más métodos de autenticación en bancas y redes existan más segura se volverá la red y los fraudes electrónicos y los phishing comenzarán a reducir. Pero de todas formas es necesario que los usuarios sigan las directrices para su seguridad establecidas, que no clicleen en links que parezcan ser ilegítimos y que sobretodo no aporten datos por medio de estos enlaces.

También el número de estafas aumentará con el paso del tiempo, así como los usuarios que desconozcan el phishing y sean víctima de él.

11- CONCLUSIONES

- **PRIMERA**: El avance de los medios informáticos y de la tecnología trajo consigo grandes ventajas en la vida de la población. Estos avances facilitan la realización de cosas cotidianas y es muy favorable en muchos aspectos en la vida de una persona. Pero no todo trajo beneficios. Estos avances también facilitan que los delitos comunes se trasladen a las redes. Como es el caso que hemos tratado: el PHISHING. Como hemos visto es un tipo de estafa pero que se produce en la red. Al cobrar tanta importancia en los últimos años el uso de internet, se abrieron las puertas para que también sea un medio donde se pueden cometer diferentes delitos. Podríamos decir pues, que todas estas ventajas que nos trajo la evolución, también tiene su parte negativa, y es que en internet y en la red se producen casi tantos delitos como en la vida real. Incluso muchos de ellos con mayores pérdidas económicas. El avance de la tecnología se convirtió en una herramienta para los delincuentes para poder perpetrar los delitos. Como hemos podido comprobar en los datos ofrecidos en este documento, el phishing va en aumento, como casi todos los delitos informáticos. Las cifras demuestran que a pesar de todos los intentos para erradicarlo, el phishing crece día a día. Como ya hemos dicho, el impacto que produce este delito es bastante considerable, tanto en la economía como en el ámbito social. Genera desconfianza en los usuarios y poca fiabilidad en usar medios electrónicos, lo que a su vez produce un freno en la evolución de la economía digital. Todos esos avances que se consiguieron, con delitos de este tipo se quedan paralizados.
- **SEGUNDA:** Como ya hemos visto, las víctimas del phishing corresponden a un ámbito bastante amplio donde nos encontramos con personas individuales, como empresas o instituciones. No se centra en un tipo de víctima en concreto, sino que todos pueden ser víctimas del phishing. Por tanto es necesario que se implementen medidas de lucha contra el fraude en España. Este delito va en aumento, como se ve en los últimos años que nacieron el smishing y el vishing, y es muy importante evitar la comisión de los mismos. Una forma que hoy en día poco se ve por España pero puede resultar muy exitosa, es la realización de campañas de prevención contra el phishing. Advertir a la población de la existencia de este delito, que conozcan cuales son los riesgos de navegar por internet. Es necesario cambiarles un poco el pensamiento. Muchas personas hoy en día creen que todo lo que ven por internet tiene máxima credibilidad, y por ello en determinadas ocasiones no son conscientes de que pueden estar siendo víctimas de un fraude. Una medida que daría resultados positivos y reduciría las víctimas de estas estafas, es pues, darles a conocer al usuario datos reales sobre el phishing.
- **TERCERA**: Para combatir el phishing, es necesaria una colaboración global e

internacional. Este delito evoluciona de forma diferente en cada país. Si todos colaboran entre sí, se pueden conocer todos los tipos de phishing existentes y combatirlos con mayor eficacia. Cada país debería aportar toda la información necesaria para llegar a una conclusión conjunta que ofrezca resultados positivos. El impacto económico del phishing es bastante elevado, causa pérdidas de dinero en los países y esto es algo lo suficientemente negativo para que todos colaboren entre sí. Por tanto, la creación de legislación y directivas que traten el tema es primordial. La poca legislación existente deja espacios en blanco y muchos de estos delitos quedan totalmente impunes. Esto es así, porque el ataque se produce en un país pero los beneficios van a otros. Al no haber legislación que regule estos temas, el phishing va en aumento y los phishers se consideran inmunes. Ese sentimiento les lleva a seguir cometiendo estafas y mejorando sus técnicas.

- **CUARTA**: Pocos son los estudios reales que se conocen sobre el phishing en España. Si se ofrecieran estos datos, se sabría por dónde ir. Que hacer para combatir el phishing en números reales. Sería recomendable que las diferentes instituciones colaboraran entre ellas para ofrecer datos y propongan medidas según esta información.
- **QUINTA**: En cuanto a la evolución del phishing, muchas personas están de acuerdo en que llegó a su máxima evolución mientras que otro gran porcentaje considera que esto está recién empezando. Y de acuerdo con esta última idea, si tenemos en cuenta la evolución del mismo en los últimos años, es bastante probable que en los años que nos preceden las técnicas vayan aumentando considerablemente. Es más, los phishers cada día son más profesionales, utilizando esta técnica incluso en grupos u organizaciones criminales. Últimamente los emails eran más personalizados. Lo que queda es estar lo suficientemente preparados en un futuro para conocer estos ataques y su evolución y poder solucionarlo.
- **SEXTA**: El phishing es un fenómeno actual y real. Utilizan la ingeniería social y por tanto es importante la concienciación del usuario.

12- REFERENCIAS BIBLIOGRAFICAS.

BRIGHT HUB, *http://www.brighthub.com/internet/security-privacy/articles/82116.aspx*

DELITOS, *http://www.delitosinformaticos.com/03/2012//fraudes/informacion-sobre-phishing-ofertas-_de-trabajo-falsas-y-blanqueo-de-capitales*

EL ECONOMISTA, *http://www.eleconomista.es/CanalPDA/2014/50021/por-que-es-rentable-el-phishing-y-como-funciona/*

GREEN VIEW DATA, *http://www.greenviewdata.com/documents/white_papers/phishing_past_present_future.pdf*

INFOSPYWARE, *http://www.infospyware.com/articulos/que-es-el-phishing/*

INTECO, *Estudio sobre usuarios y entidades públicas y privadas afectadas por la práctica fraudulenta conocida como phishing, Octubre 2007*.

NOSOMOSDELITO, *http://nosomosdelito.net/sites/default/files/public_files/documentos/estudio_completo_cp.pdf*

ONGUARDONLINE, *https://www.onguardonline.gov/phishing*

OSI, *https://www.osi.es/es/actualidad/blog/2014/04/11/aprendiendo-identificar-los-10-phishing-mas-utilizados-por-ciberdelincuen*

REVISTA SEGURIDAD, *http://revista.seguridad.unam.mx/numero-02/pescando-informaci%C3%B3n-phishing*

SEGU INFO, *http://www.segu-info.com.ar/malware/phishing.htm*

PHISHING, *http://www.phishing.org/what-is-phishing/*

PHISHTANK, *https://www.phishtank.com/what_is_phishing.php*

WEBOPEDIA, *http://www.webopedia.com/TERM/P/phishing.html*