Suplantación de la identidad

Esther Núñez Vidal, Carlos Villarroel González, Victoria Cuevas Gil
Universidad Complutense de Madrid

estherfacultad@gmail.com, cvillarroelgonzalez@gmail.com, victoria.cuevas@yahoo.es

Resumen.

Este trabajo pretende aclarar el concepto de suplantación de identidad basándose en el perjuicio para el usuario, las leyes que regulan el delito y la inexistencia de leyes para alguno de los casos, como son los casos electrónicos. La suplantación de identidad es un problema grave para la persona que lo sufre, no solo por la pérdida de derechos sino por el coste personal que supone. El auge de Internet ha propiciado que los modos de sustracción de datos con fines maliciosos hayan florecido y sean cada día más complejos. Se habla pues de términos como phising, spoofing, pharming, etcétera. Todos estos términos están asociados al robo información personal para uso fraudulento y/o acometer diversos delitos con dichas identidades robadas. A lo largo del trabajo se exponen casos reales y las medidas que se deben tomar para evitar que dichas situaciones sucedan. Dichas medidas no son solo de carácter legal sino también de carácter personal, para concienciar a los usuarios de la red de la importancia de hacer un buen uso de los recursos y de la prudencia que se debe tener a la hora de introducir datos en la red.

Palabras clave: Phishing, fraude, spoofing, riesgos, seguridad, prevención.

1 Contexto del trabajo

Este trabajo trata sobre la suplantación de identidad. Se parte de una serie de leyes como por ejemplo la LOPD. Esta ley regula el tratamiento de los datos personales por las empresas. Como no solo la suplantación se identifica con la problemática electrónico, además de la ley anterior, el trabajo se encuadra en un marco legal basado en el Código Penal español. Asimismo, se incluyen recomendaciones creadas a nivel nacional como internacional.

Las formas de suplantar la identidad son múltiples y variadas. Con el paso de los años han ido evolucionando, tanto en técnica como en la tecnología utilizada. A pesar de ser conscientes del peligro que hay, las personas son vulnerables. Con el fin de sensibilizar se expone los casos reales de fraudes conocidos. En particular con correos electrónicos masivos.

El trabajo muestra una serie de medidas que tanto los usuarios ordinarios del los equipos informáticos como los expertos en la materia deberían seguir para evitar en la medida de lo posible los daños causados. Es cierto, que a pesar de todas las medias de seguridad que se introduzcan, los malhechores pueden encontrar una rendija por la que colarse pero, es imprescindible ponérselo lo más difícil posible.

Es significante el caso particular de la suplantación de identidad en Internet ya que no existe una ley que regule este fraude. Los usuarios sufren graves consecuencias y la justicia, en el caso español, no interviene salvo que se incurra en el delito de suplantación *completa* de la identidad no solo de nombre o algunas claves, caso muy habitual.

2 Introducción

Es una realidad que el surgimiento de Internet ha dado lugar a un avance muy importante en el manejo de la información. No obstante hemos de ser conscientes que sus aportaciones no son sólo positivas sino que un uso incorrecto de la misma o no tomar las medidas oportunas puede dar lugar a peligros con consecuencias realmente importantes.

Vivimos en una sociedad en la que imperan las prisas y en la que cada vez se realizan más transacciones electrónicas por su facilidad y comodidad.

Sin embargo, estos cambios de hábitos suponen también un cambio en los malhechores. El timo de la estampita es historia ahora lo que se promueve es la suplantación de la identidad o el robo de la información personal vía Internet. Es necesario concienciar al público en general de las precauciones que deben tener a la hora de usar Internet.

Adicionalmente, dado que internet no se puede estudiar como un único medio, hemos de diferenciar y estudiar de forma separada cada posible servicio. Son múltiples las vías de comunicación que ofrece, y en cada una de ellas cabe un uso malintencionado.

A lo largo de este trabajo se desarrollan las diversas formas de suplantación comenzando por las electrónicas. La suplantación de la identidad tiene múltiples objetivos y finalidades. La naturaleza de tales actos, independientemente de la plataforma y tecnología, son tan antiguos como las propias estafas o suplantaciones físicas de forma que mediante falsificación de documentos acreditativos e incluso el disfraz, fuese posible engañar a quien ofreciese un servicio haciéndose pasar por otra persona, la cuál sería la víctima.

En la informática la suplantación de identidad, se define en conceptos tales como Phishing o Spoofing sobre los que abordará principalmente este apartado 3.1. Dentro del conjunto de Phishing se encuentran peculiaridades como Scam técnica basada en las empresas ficticias, Hoax, mensajes engañosos recibidos en cadena en los correos electrónicos y AFF, fraude por adelanto de pago. Las técnicas de Spoofing requieren un conocimiento de la informática mayor que las anteriores. Por este motivo, las partes en las que se divide este apartado son IP, relativo al protocolo TCP-IP, ARP, mediante el uso de la red Ethernet, DNS, modificación fraudulenta de la IP. También,

entorno a la web hay otros fraudes: utilizar páginas web falsas que engañen al usuario o el envío de correos electrónicos con fines maliciosos.

En todos los casos se trata de una intervención de un tercero, con diversas intenciones, en la comunicación entre dos interlocutores que por lo general son: la víctima o usuario, y la entidad.

Internet nos muestra un amplio abanico de nuevos tipos de amenazas: amenazas tecnológicas como virus, malware, amenazas a la privacidad, grooming, ciberbullying, delitos contra la propiedad intelectual, fraude económico, acceso a contenidos no adecuados, etcétera, a los que hemos de ser capaces de vencer.

Las administraciones han tomado medidas para evitar o al menos minimizar los daños causados por este tipo de fraudes. Sin embargo, no todos los fraudes son delitos e incluso hay fraudes que no son considerados delitos por la ley.

No solo las leyes son un recurso para recuperar la identidad perdida, el dinero sustraído, las cuentas robadas, etcétera, sino también cada uno de los individuos. Es cierto que no todo el mundo posee el mismo nivel de conocimiento y por tanto, hay que explicar desde las medidas más básicas hasta las más sofisticadas. Además se incluyen las normativas que se pueden llegar a utilizar en caso de considerar la suplantación un delito.

Por ejemplo, se introduce información acerca de las medidas previas antes de comenzar la navegación en Internet. La Oficina de Seguridad del Internauta (OSI) es un servicio del Gobierno, concretamente de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información puesto en marcha por el Instituto Nacional de las Tecnologías de la Comunicación (INTECO) para proporcionar información y el soporte necesarios para evitar y resolver los problemas de seguridad que pueden afectarnos al navegar por Internet.

Para realizar trámites seguros, como el acceso a bancos, compras por internet, hemos de verificar la legitimidad del sitio web. La forma más segura es la comprobación del certificado digital y de la firma digital cuya validez es la misma a la firma manuscrita. Como se verá existen diversos certificados digitales según el carácter del mismo. ¿Cómo funciona el DNI digital? La respuesta está totalmente clarificada en este documento.

La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD)[1], y el Real Decreto 1720/2007 de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica, obliga a cualquier empresa que trate información personal (de clientes, proveedores, trabajadores, etc.…), a tomar una serie de medidas documentales y técnicas a los efectos de garantizar que el tratamiento de dicha información, se lleva a cabo con garantías de confidencialidad y seguridad. Esta es una de las leyes que las empresas deben cumplir para el buen tratamiento de los datos personales. Aunque las leyes son efectivas algunas empresas como Skype o FaceBook tienen políticas propias, más restrictivas, del uso de los datos. Se basan fundamentalmente en dar el poder a los usuarios, que deben realizar buenas prácticas de sus datos personales.

1 Ver apartado 4

Un apartado importante es la seguridad de los más pequeños. Es fundamental tratar punto como las redes sociales, en las que se encuadra FaceBook, los video juegos online, chats, foros, etcétera.

Esta problemática aunque no lo parezca es real y está a la orden del día. Por este motivo se incluyen en los diferentes apartados menciones y casos reales que ejemplifican estas situaciones.

Los últimos apartados de este documento se centran en la legislación vigente y recomendaciones de buenas prácticas y las conclusiones sacadas del trabajo realizado.

3 Suplantaciones electrónicas

3.1 Phising

Phishing es un término informático utilizado para denominar el fraude por suplantación de identidad, una técnica de ingeniería social. El origen de la palabra phishing se dice que proviene de la contracción de "password harvesting fishing" (cosecha y pesca de contraseñas); sin embargo, esta explicación es muy probable que sea posterior al propio término. El término phishing procede de la palabra inglesa "fishing" (pesca) haciendo alusión a "picar el anzuelo".

Este término se acuñó por primera vez en 1996, en los casos de intento de apropiación de cuentas de AOL, a pesar de que se había iniciado varios años antes. Se trataba de envío de mensajes instantáneos haciéndose pasar por empleados de AOL, solicitando contraseñas. AOL tomó medidas en el año 1995, y reforzó las mismas en 1997.

No siempre ha sido con fines a priori tan lucrativos, pues también se extendió al MSN Messenger, con la finalidad de hacerse con el control de cuentas. Pero los últimos intentos se han centrado en el caso de la banca, para conseguir acceso y control de las cuentas bancarias de sus clientes.

Las personas que realizan el fraude se denominan *phishers*. Su objetivo es la obtención de información personal confidencial de las víctimas, ya sean cuentas bancarias, contraseñas, números de tarjetas de crédito, etcétera.

El *phisher* actúa de varias formas distintas para conseguir la información: mediante el envío de mensajes de correo electrónico fraudulentos, mensajería instantánea o mediante la utilización de falsos sitios web. En este último caso podemos enmarcar los casos de suplantación de páginas web de entidades bancarias muy utilizados actualmente.

Generalmente en el caso de los correos, el envío masivo, pese a ser buenas falsificaciones y ser aparentemente veraces, no suele ser muy efectivo pues llega a personas que no tienen ninguna relación con la entidad que es falsificada. Por ello, otra forma más efectiva es relacionar por cualquier método de ingeniería o

investigación a cada posible víctima con una entidad que será falsificada, ya sea cliente o empleado. En este caso la probabilidad de éxito es mucho mayor, pues está dirigida y es más creíble. Este caso se denomina *spear phishing.*

3.1.1 Scam

En el caso de que el objetivo final, tras conseguir los datos personales, sea económico, un *phisher* cauto no ingresará directamente el dinero en su cuenta, por ello utilizará esta técnica

Este tipo de fraude consiste en que empresas ficticias realizan la captación de personas mediante diversas vías como chats, foros, notificaciones vía correo electrónico, anuncios en periódicos e incluso difusión en webs; donde ofrecen puestos de trabajo con excelentes ventajas y cuyas condiciones se resumen en disponer de un ordenador y ser titular de una cuenta bancaria. Las personas que aceptan este tipo de empleos reciben el nombre de "muleros" y desconocen el carácter ilícito de sus acciones que consiste en el blanqueo de dinero obtenido a través del *phishing.*

A continuación, mostramos un ejemplo de un correo electrónico para la captación de personal y el relato de una víctima de *scam*[2]*:*

Subject: EMPLEO

La compañía de comercio internacional MARIA F. FINANCE GROUP busca a una persona respetable para ocupar el cargo de correo financiero el trabajo en casa usando el internet.
Exigencias: edad. 21-50 años, despierto, comunicativo, cumplidor, con conciencia del deber, listo para aprender en el proceso del trabajo. La educación especial no es necesaria. El salario se basa en la realización de las obligaciones [1000-4000 USD por la semana].
El trabajo le llevar. 1-2 horas cada día y Usted puede combinar su trabajo principal con el trabajo en nuestro mercado. Además Usted podrá ganar dinero a partir del primer día.
Si Usted está listo[a] para ganar más dinero hoy día, no tiene más que comunicarse con nosotros por correo electrónico!
Reciba la información complementaria y comience su trabajo HOY!
Atte,
Maria F., staff manager
MARIA F. FINANCE GROUP
Contact e-mail: MFGrp@xxx.com

A continuación se expone el caso de una víctima de scam.
José Luis ha recibido una citación judicial en la que le indican que ha de ir acompañado de un abogado. La víctima cuenta como le ocurrió el engaño; "Recibí en mi correo electrónico una oferta de trabajo que después de preguntarles varias veces si era fiable, me convencieron y acepté el trabajo que consistía en que ellos me mandaban una cantidad de dinero a mi cuenta del BBVA, en este caso me mandaron 1950 euros y luego siguiendo sus instrucciones yo tendría que sacar y reenviar a

[2] http://www.trucoswindows.net/article402.html

donde ellos me dijeran por medio de MoneyGram (incluso me llamaron por teléfono para decirme que ya tenía el dinero y lo que tenía que hacer) y quedándome yo con el 5% del dinero, (en este caso mandé el dinero a Letonia a un señor llamado Artun Safin), hasta ahí todo correcto pero al cabo de dos días me llamó la directora de mi banco diciéndome que la estaban reclamando del Banco de Valencia una cantidad de 1950 euros de un señor llamado Francisco de Alicante y que no sabían como había salido de su cuenta y había ido a parar a la mía, a partir de ahí ya me di cuenta de que todo era una estafa, pero ya era tarde, llamé inmediatamente a MoneyGram para retener el dinero pero el tal Artur Safin ya lo había cobrado, fui al BBVA a hablar con la directora y me aconsejó que lo denunciara, cosa que hice, pero por la noche me llamó a mi casa Francisco pidiéndome el dinero y yo le dije que era tarde que ya no lo tenía, que yo sólo tenía mi correspondiente 5%. Al cabo de unos días recibí una carta certificada del Banco de Valencia diciendo que enviara el dinero a un número de cuenta que me ponían y en caso de no hacerlo me lo reclamarían por vía judicial"[1]

Atendiendo a los casos de *scam* que se han denunciado podemos apuntar que en los casos más graves, se ha producido la prisión provisional incondicional, exigiendo para la puesta en libertad, fianzas de hasta 6000 euros.

En cuanto al proceso penal, éste puede terminar o bien en un sobreseimiento en la fase de instrucción por inexistencia de pruebas suficientes de la culpabilidad del imputado, o bien, acaban en condena por un delito de estafa del artículo 248 del código penal, castigado con la pena de prisión de seis meses a tres años.

Artículo 248.

1.- Cometen estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno.

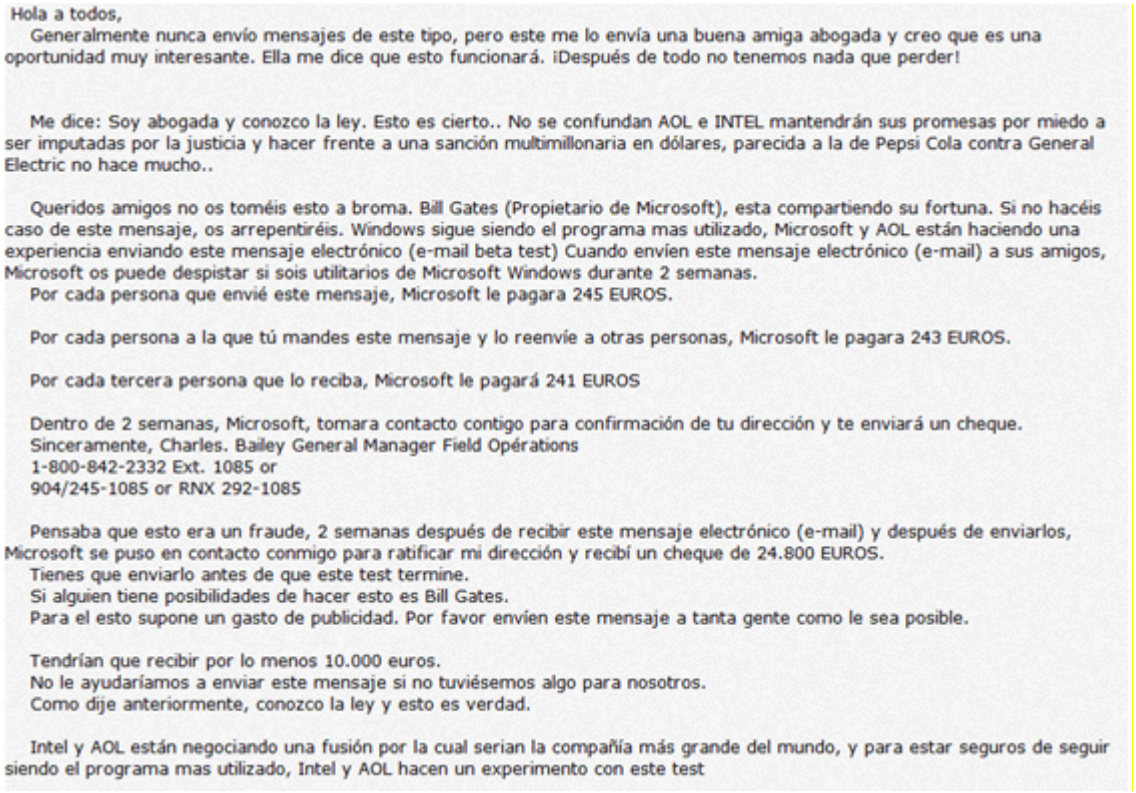
2.- También se consideran reos de estafa los que, con ánimo de lucro, y ***valiéndose de alguna manipulación informática o artificio semejante*** *consigan la transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero.*

3.1.2 Hoax

Estos mensajes engañosos o bulos, se distribuyen en cadena. Abarcan diferentes temas, como por ejemplo desgracias, cadenas de solidaridad, falsas advertencias de virus informáticos… y todos ellos se caracterizan por atemorizar al destinatario si no continúa con la cadena de mensajes, no están firmados e incluso algunos referencian los nombres de grandes compañías. Los objetivos de este tipo de fraude son conseguir direcciones de correo electrónico, colapsar servidores, colapsar las LAN[3], alimentar el ego del autor, generación de temor, etcétera.

Ejemplo de correo electrónico en cadena[4]:

3 Redes de área local.
4 http://www.microsoft.com/spain/seguridad/articulos/hoaxes.mspx



Hola a todos,
Generalmente nunca envío mensajes de este tipo, pero este me lo envía una buena amiga abogada y creo que es una oportunidad muy interesante. Ella me dice que esto funcionará. ¡Después de todo no tenemos nada que perder!

Me dice: Soy abogada y conozco la ley. Esto es cierto.. No se confundan AOL e INTEL mantendrán sus promesas por miedo a ser imputadas por la justicia y hacer frente a una sanción multimillonaria en dólares, parecida a la de Pepsi Cola contra General Electric no hace mucho..

Queridos amigos no os toméis esto a broma. Bill Gates (Propietario de Microsoft), esta compartiendo su fortuna. Si no hacéis caso de este mensaje, os arrepentiréis. Windows sigue siendo el programa mas utilizado, Microsoft y AOL están haciendo una experiencia enviando este mensaje electrónico (e-mail beta test) Cuando envíen este mensaje electrónico (e-mail) a sus amigos, Microsoft os puede despistar si sois utilitarios de Microsoft Windows durante 2 semanas.
Por cada persona que envié este mensaje, Microsoft le pagara 245 EUROS.

Por cada persona a la que tú mandes este mensaje y lo reenvíe a otras personas, Microsoft le pagara 243 EUROS.

Por cada tercera persona que lo reciba, Microsoft le pagará 241 EUROS

Dentro de 2 semanas, Microsoft, tomara contacto contigo para confirmación de tu dirección y te enviará un cheque.
Sinceramente, Charles. Bailey General Manager Field Opérations
1-800-842-2332 Ext. 1085 or
904/245-1085 or RNX 292-1085

Pensaba que esto era un fraude, 2 semanas después de recibir este mensaje electrónico (e-mail) y después de enviarlos, Microsoft se puso en contacto conmigo para ratificar mi dirección y recibí un cheque de 24.800 EUROS.
Tienes que enviarlo antes de que este test termine.
Si alguien tiene posibilidades de hacer esto es Bill Gates.
Para el esto supone un gasto de publicidad. Por favor envíen este mensaje a tanta gente como le sea posible.

Tendrían que recibir por lo menos 10.000 euros.
No le ayudaríamos a enviar este mensaje si no tuviésemos algo para nosotros.
Como dije anteriormente, conozco la ley y esto es verdad.

Intel y AOL están negociando una fusión por la cual serian la compañía más grande del mundo, y para estar seguros de seguir siendo el programa mas utilizado, Intel y AOL hacen un experimento con este test

3.1.3 AFF

El fraude por adelanto de pago (AFF Advance Fee Fraud) o Fraude 419 es conocido también por el fraude de la lotería y constituye una de las formas de amenaza de delito telemático más peligrosas y con mayor crecimiento. Se trata de un crimen en el que se engaña a la víctima para que pague una cantidad de dinero por adelantado para recibir un regalo a un premio en metálico. Normalmente los delincuentes simulan páginas de compañías de prestigio para dar más credibilidad y autenticidad a sus mensajes de correo electrónico.

3.2 Spoofing

A diferencia del *phishing*, el *spoofing* también se trata de una suplantación de identidad, pero en la cual no se requiere por lo general de un engaño previo a la víctima o a la entidad. Adicionalmente, los motivos del mismo pueden ser muy variados, desde la estafa a la investigación.

Como se ha dicho, normalmente no usa el engaño, por lo que la actuación de forma general es básicamente técnica, menos picaresca y fraudulenta. Por ello suele requerir siempre de unos conocimientos muy avanzados.

3.2.1 IP

En este caso, la suplantación de identidad se inicia en el *host* [5] que va a realizar la suplantación, mediante el envío de paquetes de cualquier protocolo bajo TCP.

Consiste en la modificación de tales paquetes, de forma que la dirección de origen no es la real, sino la de quien se va a suplantar (modificación del remitente). De esta forma el *host* que es suplantado recibe los paquetes de respuesta sin haberlos solicitado.

Tiene ciertas desventajas iniciales, como es el hecho de que el *host* víctima puede cortar la conexión o que los *routers* actuales no admiten paquetes cuyos remitentes no corresponden con los que administra en su red, lo cual acotaría el engaño a la red gestionada por un *router*.

3.2.2 ARP

Esta suplantación trabaja en una red Ethernet conmutada[6] la cual no está pensada para este tipo de validación.

Se basa en el envío de mensajes ARP falsos de forma que, la tabla de ARP que contiene la asociación de la MAC[7] y la IP[8] de la víctima, se cambie por la MAC del atacante y la antigua IP de la víctima.

De esta forma, todos los paquetes que la máquina víctima iba a recibir ahora son recibidos por la máquina atacante. Es entonces cuando el atacante decide si simplemente espía a la víctima reenviando los paquetes (ataque pasivo o escucha), los modifica (ataque activo) o simplemente le incomunica asociando una dirección MAC inexistente.

3.2.3 DNS

También llamado *pharming*, se trata del cambio de la relación de un nombre de un dominio por una IP falsa. Este ataque se realiza si el servidor DNS no es muy seguro, o si confía en otros que si son inseguros. Por otro lado, una vez se haya realizado el cambio, otros servidores DNS que se fíen de este, podrán añadir a sus cachés la dirección falsa, denominándose *DNS poisoning*.

3.2.4 Web

Suplanta la dirección real a una página falsa que encaminará hacia otras páginas auténticas que recolectarán información de la víctima. Esta página falsa actuará a modo de *proxy* (intermediario), de forma que recolectará toda la información de la

5 En este caso, un host es una única dirección IP que normalmente se corresponde con un ordenador.

6 Una red conmutada se basa en la unión de otras subredes mediante un Switch, elemento que las interconecta de forma lógica, redireccionando mensajes y almacenando una tabla con cada uno de los elementos de la red. Los basados en Hubs, son interconexiones más sencillas y carecen de tablas.

7 Dirección de un ordenador a nivel de red local.

8 Dirección de una interfaz de un computador para toda la red.

comunicación de la víctima pudiendo modificarla o recolectarla. Esto la hace muy difícil de detectar y de protegerse contra ella.

En este caso se requiere de un primer engaño para hacer que la víctima visite la página falsa y no la verdadera. Pero a diferencia del *phishing*, no suplanta realmente la página original, sino que se coloca en medio de la conversación.

3.2.5 Mail

En este caso con cualquier servidor sencillo de SMTP (protocolo de correos electrónicos), se envían correos con un remitente falso. Las intenciones pueden ser variadas, como complemento para phising, o simplemente para distribuir bulos.

Igualmente, sería sencillo para protegerse mediante firma digital, o revisando la dirección IP del remitente para reconocer si es la IP de la entidad auténtica que lo envía o es otra dirección IP.

3.3 Medidas de prevención.

Una de las medidas más radicales es la destrucción de toda la información que sea sensible con el fin de evitar el robo de nuestra información. Pero como buenas prácticas se deben mantener los documentos personales y confidenciales en un lugar seguro, es decir, que no estén en el directorio compartido o en una red local. Asimismo, nunca se deben mandar datos confidenciales por medio de un correo electrónico. La comprobación de las cuentas bancarias es importante pero se deben tomar ciertas precauciones ya que existen muchas páginas que imitan a las de los bancos con el único fin de obtener de forma fraudulenta tu usuario y contraseña. Asimismo, los bancos jamás piden por correo electrónico ningún dato personal, por lo tanto, nunca se deben responder a los correos de los bancos si piden dichos datos. Y si aún así, se produce un robo de información lo que se debe es acudir directamente a la entidad financiera y si es necesario a la policía.

Según la OSI[9] *"La prevención es la mejor receta para evitar ser víctima de las amenazas que circulan por la red. Invertir un poco de tiempo en interiorizar unos sencillos hábitos en el uso de los servicios, y configurar los sistemas para que sean seguros, nos ahorrará tiempo y disgustos en el futuro."* [1]

Desde la Oficina de Seguridad del Internauta recomiendan seguir unas buenas prácticas sobre el uso de los servicios que proporciona Internet.

3.3.1 Navegación

Uno de los principales usos de Internet es la búsqueda de información mediante la navegación. Para poder realizar una navegación segura hemos de tener en cuenta una serie de factores:

Pasos previos a la navegación.

[9] http://www.osi.es/econf/Protegete/

- Hemos de asegurarnos que nuestro sistema sea robusto y esté preparado para combatir posibles ataques desde la web. Para ello, dispondremos de una versión actualizada de antivirus, firewall.
- Configurar varias cuentas de usuario en nuestro sistema, tendremos una cuenta de usuario limitada para la navegación ya que si se produjese una invasión durante la misma, el invasor tendría los mismos permisos que el usuario de navegación por lo que en ningún caso se ha de realizar con una cuenta de administrador.
- Limitar el uso de ciertas funcionalidades Java y Javascript[10]. Ambos lenguajes en ocasiones son aprovechados maliciosamente para propagar virus en el sistema.
- Bloqueo de las ventanas emergentes.
- Configurar las cookies. Éstas pueden contener información sobre los hábitos de navegación, información entre visitas que pueden ser utilizados por terceras personas de forma maliciosa y afectar nuestra privacidad.

Durante la navegación.

- Hemos de actuar con cautela, no todos los datos que encontramos en la web han de ser ciertos. Hemos de contrastar la información que obtenemos con fuentes alternativas. Podemos hacer uso de analizadores de Url's.
- Descargar la información de páginas de confianza y analizarla mediante antivirus.

3.3.2 Trámites en línea

Una de las maneras de evitar la suplantación de identidad por Internet es ser propietario de un Certificado Digital. Gracias a él se podrá realizar transacciones electrónicas en varios dominios. Es de gran utilidad en el mundo empresarial ya que este certificado permite firmar digitalmente documentos electrónicos , como por ejemplo, correos, ofertas y pedidos, facturas, calidad, actas, cartas, etcétera. Es decir, protege la información transmitida.

Asimismo, dicho certificado ayuda a realizar trámites vía Internet con organismos oficiales. Como ejemplo práctico, se fomenta el uso del Certificado Digital para trámites con Formación en el Empleo, la Agencia Tributaria Estatal, el Ministerio de Trabajo, la Seguridad Social, etcétera.

Un certificado digital es un DNI único, unipersonal e intransferible. Está avalado por una autoridad de certificación: "*entidad de confianza, responsable de emitir y revocar los certificados digitales o certificados, utilizados en la firma electrónica, para lo cual se emplea la criptografía de clave pública"*[11]. Al fin y al cabo, es un sistema de seguridad cuyo objetivo es establecer confianza en las transacciones electrónicas y evita la suplantación de identidad. Para ello debe garantizar la identidad de las partes implicadas en la transacción, debe asegurar la integridad de la

10 Generalmente, cualquier página con un mínimo de dinamicidad incorpora este lenguaje que es interpretado por el navegador de internet.

11 http://es.wikipedia.org/wiki/Autoridad_de_certificaci%C3%B3n

transacción, es decir, la no manipulación del paquete emitido por un tercero ajeno al envío, y que los implicados en la transacción no puedan negar que realmente son ellos lo que han realizado la operación. En general, los certificados garantizan la identidad del emisor, el no repudio de origen, la integridad y confidencialidad del contenido.

Un punto realmente importante del certificado digital es su validez. Legamente es exactamente igual que una firma manuscrita. Y, por lo tanto, tiene los mismos deberes y las mismas responsabilidades.

Actualmente existen varios tipos de certificados digitales que emiten la Fábrica Nacional de Moneda y Timbre y las Cámaras de Comercio. En primer lugar, hay certificados de carácter personal que acreditan la identidad del titular. En segundo lugar están los certificados de persona jurídica que identifica una empresa o sociedad. En tercer lugar, existe un certificado de perteneciente a empresa y de representante de la empresa que acredita la vinculación con la empresa y los poderes de representación de la empresa respectivamente. Además hay dos tipos de certificados técnicos: certificado de servidor de seguros relativo a los servicios web y el certificado de firma de código que garantiza la autoría de las aplicaciones informáticas.

El DNI electrónico surge como respuesta a la adaptabilidad al mundo digital en el que vivimos. Utilizado para realizar todo tipo de operaciones a través de la red como transacciones con entidades bancarias, administraciones públicas, etcétera mediante la autentificación de nuestra identidad ya que asegura de forma inequívoca que el titular del dni ha sido quién ha realizado la operación.

La ley aplicable a la firma electrónica es:

- Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos. Sistemas de firma electrónica para las relaciones entre los ciudadanos y las administraciones públicas.
- Ley 59/2003 de firma electrónica.
- Real Decreto 1553/2005, de 23 de diciembre, donde se regula la expedición del DNI y sus certificados de firma electrónica.

La suplantación de identidad digital comenzó con los fraudes de tarjetas y ha continuado con la banca online. Esta situación ha sido producida por dos factores: el aumento de transacciones bancarias por la red y la impunidad de los ladrones frente a estos hechos delictivos. Las leyes dirigidas a evitar este tipo de fraudes y a omitir la responsabilidad del cliente del banco está poco desarrollada y, en general, se aboga por las buenas prácticas bancarias basadas en el principio de equidad, proporcionalidad y justo equilibrio de las contraprestaciones tras el fraude. Es más, la suplantación de personalidad como tal no aparece en el Código Penal español, que en 1995 eliminó el antiguo delito de uso público de nombre supuesto. Actualmente solo se castigan la usurpación de estado civil: suplantación completa de la identidad no solo de nombre o algunas claves.

Los mayores casos de robo bancario tienen que ver con la averiguación de las claves y transferencias a cuentas ajenas al titular, en particular, al extranjero. Este

hecho hace difícil la recuperación del dinero robado. Además de la suplantación de la identidad en este sector nos encontramos el uso fraudulento de tarjetas de crédito.

Tanto a nivel comunitario como a nivel nacional existen diversas normativas aplicables para estos dos casos. Para la normativa comunitaria nos encontramos con: Recomendación 88/590/CEE, de la Comisión, de 17 de noviembre y Recomendación 97/489/CE, de la Comisión, de 30 de julio de 1997.

Y en ámbito nacional se pueden citar las siguientes normativas: Código de Buena Conducta de la Banca Europea y la Ley 7/1996, de 15 de enero de Ordenación del Comercio Minorista.

Como podemos ver estas leyes son muy efectivas para la problemática de las tarjetas de crédito, sin embargo, para la banco online la situación difiere ligeramente. En primer lugar, porque la normativa es inexistente. Y, en segundo lugar, porque los contratos entre el banco y el cliente responsabilizan al titular de la cuenta de todos los eventos que puedan sufrir. Es decir, al contrario que en las tarjetas donde hay un límite de dinero que puede ser defraudado, el cliente de la banca online debe acarrear con todos los problemas causados por la suplantación de identidad. Es decir, que todas las consecuencias del uso indebido de su firma digital recaen sobre el titular de la cuenta. Para que un cliente pueda reclamar ante un fraude de este tipo debe:

- Acreditar la información ofrecida sobre el conocimiento del compromiso y riesgo asumido en la contratación del servicio banca online.
- Acreditar el conocimiento del uno adecuado y la custodia de las claves. Es decir, asegurarse que se está trabajando sobre la URL del banco y no sobre una similar y potencialmente maliciosa.
- Realizar una diligencia para la gestión de la recuperación del dinero perdido.

En los casos de robo de cuentas de correo electrónico se aplica el artículo 197 del Código Penal español si se produce el acceso a una cuenta de correo ajena sin el consentimiento del titular. Este artículo no solo se refiera a la intercepción de los mensajes sino también a toda información de carácter personal que pudiera haber en las libretas de direcciones de dicho correo. Según el código penal se pueden cumplir hasta siete años de prisión en aquellos datos especialmente protegidos como pudieran ser los datos de las creencias religiosas, salud origen racial, datos de menores, etcétera.

Si el robo de cuentas de correo se realiza para apoderarse, utilizar o modificar datos reservados estamos ante un delito de revelación de secretos. Pero si además, se borra información el delito se considera delito de daños informáticos y está castigado con hasta 3 años de prisión por el artículo 264, 2 del Código Penal español.

Uno de los mayores peligros de la sustracción de las cuentas de correo o de datos personales es la incursión en delitos por parte de los ladrones y que la justicia los impute al titular real de la cuenta. Para evitar este problema es pertinente presentar una denuncia ante las Fuerzas y Cuerpos de Seguridad del Estado que solicitarán al Poder Judicial tomar las medidas oportunas sobre el proveedor de servicios para impedir la continuación de fraudes.

Skype es una aplicación para comunicarse por Internet dirigida tanto por particulares como empresas. Dichas comunicaciones deben de ser seguras, tanto para unos como para los otros. Así pues uno de los objetivos primordiales es mantenerse a salvo de los hackers. Y, especialmente ponen hincapié en la prevención de la falsificación de la identidad obtenida mediante engaños a los usuarios de Skype. Esta aplicación emite un certificado digital como los explicados anteriormente en el cual se establece la identidad del usuario y posee las siguientes características: Ser emitido por una autoridad que pueda revocar el certificado en cualquier momento. Ser difícil de falsificar. Contener un aval de la autoridad que lo emite; en este caso, Skype. Gracias a este certificado todos los usuarios puede comprobar si el interlocutor es fiable o no. Skype insiste en la importancia de mantener la identidad para garantizar la seguridad en las comunicaciones, por eso, realiza diversos cifrados en las comunicaciones, uno de los más comunes es el cifrado por clave pública. Skype trata de asegurar la privacidad del usuario y la integridad de los datos intercambiados.

3.3.3 Correo electrónico

Es una de las formas de comunicación más utilizadas en la actualidad y por tanto un medio muy atractivo para la propagación de virus, mensajes fraudulentos, spam, etcétera. Para evitar minimizar los riesgos hemos de hacer uso de antispam, limitar la difusión de nuestra cuenta de correo, eliminar mensajes sospechosos de remitentes desconocidos, no reenviar mensajes masivos.

3.3.4 Redes sociales

Las redes sociales son una fuente de sustracción de información importante y gracias a ellas y aplicando la llamada ingeniería social, se pueden obtener muchos datos personales que después se utilizarán de forma fraudulenta.

Esta nueva forma de relacionarse con otras personas tiene, por tanto, muchos riesgos. De la misma forma que en la vida real somos precavidos cuando conocemos nuevos amigos, hemos de actuar de igual modo en las relaciones vía web.

El principal inconveniente de este nuevo medio de relacionarse es la falta de privacidad. Es importante hacer una diferencia entre los términos privacidad y seguridad.

"La privacidad en la red consiste en la habilidad de cada individuo de controlar que información revela uno mismo en el conjunto de Internet, y controlar quien puede acceder a ella". [12]

"La seguridad se centra en la confianza de que esas decisiones son respetadas, mediante por ejemplo, la correcta protección de los datos personales almacenados".

Como usuarios hemos de adoptar una serie de medidas para evitar que nuestra información personal sea utilizada por ciberdelicuentes de forma fraudulenta. Para ello, antes de utilizar cualquier servicio de una red social, leeremos sus políticas de privacidad y condiciones de uso. Hemos de ser nosotros los que determinemos nuestro perfil y los límites de nuestra privacidad, grupo de personas que acceden a

[12] http://www.osi.es/econf/ABC_Seguridad/Privacidad/

nuestro perfil, etcétera para protegernos de posibles robos de identidad; en especial los adolescentes que no son conscientes del alcance que puede llegar a tener la publicación de documentos, fotos e información personal en la web.

La publicación de los contenidos es responsabilidad de la persona que los publica, por ejemplo, no se puede publicar fotos de otras personas sin su consentimiento, por lo que es muy importante conocer la legislación existente al respecto para comprender qué derechos y responsabilidades tenemos en la red. Actualmente las leyes más importantes son la LOPD (Ley Orgánica de Protección de datos) y la LPI (Ley de Propiedad Intelectual).

Como ejemplo de red social está FaceBook cuya política de privacidad ha sido modificada recientemente. Cuando un usuario se quiere dar de alta en la red necesita únicamente introducir nombre de usuario, dirección electrónica y una clave de acceso. Posteriormente se puede rellenar el perfil personal y, seleccionar qué información se quiere compartir y con quién.

Facebook se compromete a no vender, publicar o entregar a terceros ninguna información privada introducida por los usuarios de Facebook bajo ningún propósito, excepto cuando la ley así lo exija. Aún así como ya hemos comentado, el responsable de la publicación o no de información siempre es el usuario y es el que tiene siempre la última palabra sobre sus datos.

3.3.5 P2P

Las ventajas de estas redes, velocidad y facilidad de intercambio de contenidos son utilizados para la propagación de virus. Hemos de pasar el antivirus a todos los archivos que nos descarguemos, controlar en todo momento las carpetas que compartimos con el resto de usuarios, extensión de los ficheros, etcétera. En este apartado hemos de prestar especial atención a la compartición y descarga de programas de ordenador que incluyan los juegos de consolas y PC ya que la Ley de Propiedad Intelectual no contempla el derecho de copia privada por lo que conlleva multas elevadas.

3.3.6 Juegos en línea

Esta modalidad de juego a través de la red resulta muy atractiva tanto a los jugadores como a los ciberdelicuentes por lo que tenemos que tomar precauciones que en gran medida son las mismas que las del correo electrónico y las redes sociales. Podríamos añadir el poner especial atención al software del juego, hemos de utilizar el programa oficial del juego y asegurarnos también que los pluggins que nos descarguemos sean realmente oficiales.

3.3.7 Menores protegidos

Este colectivo es realmente vulnerable a todos los riesgos que hemos explicado anteriormente por lo que hemos de extremar las precauciones cuando hagan uso de la web. Hemos de realizar filtros personalizados respecto a las páginas que pueden visitar mediante el uso del control parental utilizando productos como Microsoft Protección Infantil o Naomi que es un programa de filtrado de contenidos gratuitos y en español. Actualmente no tiene soporte pero sigue siendo funcional.

Existen otro tipo de herramientas para poder llevar un control sobre el uso del equipo y el historial de navegación del equipo. De esta forma, los padres y educadores pueden llevar un seguimiento de la navegación por la web.

En varios sitios web dedicados a la enseñanza de las ventajas de la utilización de internet mediante el uso de buenas prácticas, proporcionan guías para llevarlo a cabo enfocadas tanto a padres y educadores como a los propios adolescentes. Incluso utilizan el juego como una herramienta más para acercar a los menores el uso responsable de la web y enseñar los posibles riesgos a los que se han de enfrentar como el ciberbullying y grooming. Ejemplos:

- **Secukid**: juego de inteligencia para terminales de telefonía móvil dirigido a todos los públicos, especialmente a niños y adolescentes a partir de 11 años.
- **TriviRal**: consiste en un trivial para poner a prueba nuestros conocimientos de seguridad relacionados con los virus, troyanos, spyware, etcétera. Se puede jugar de forma individual o por grupos de hasta 4 personas.

Microsoft España en colaboración con protégeles.com proporciona unas directrices para el uso de Internet de los niños según su edad. Así establece un nivel de configuración alto nivel para los menores de 10 años. Aconsejando que en todo momento un adulto esté con ellos mientras utilizan la web y establezcan unas reglas claras de uso. Un nivel de configuración medio entre 11 y 14 años donde se permita que utilicen la web por sí solos pero en todo momento se llevará un seguimiento del mismo y finalmente una configuración de bajo nivel de 15 a 18 años donde se establecerán también normas sobre el uso de internet y se tratará que la conexión a Internet se haga en una zona abierta y no en los dormitorios de los menores. En todos los casos hacer uso de alias para no desvelar información personal.

3.3.8 Móviles

Hemos de tomar las mismas medidas que en el caso de los ordenadores ya que son dispositivos que almacenan información muy personal. Hemos de proteger el móvil mediante el uso de contraseñas (PIN), apuntar el número identificativo del teléfono (IMEI) para utilizarlo en caso de pérdida del mismo para bloquearlo y ser cautos en el uso del bluetooth.

4. Legislación

La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), y el Real Decreto 1720/2007 de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica, obliga a cualquier empresa que trate información personal (de clientes, proveedores, trabajadores, etcétera), a tomar una serie de medidas documentales y técnicas a los efectos de garantizar que el tratamiento de dicha información, se lleva a cabo con garantías de confidencialidad y seguridad.

Artículo 1. *Objeto.*	*La presente Ley Orgánica tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar.*

Artículo 3. *Definiciones.*	*A los efectos de la presente Ley Orgánica se entenderá por:* *Datos de carácter personal: cualquier información concerniente a personas físicas identificadas o identificables.* *Fichero: todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.* *Tratamiento de datos: operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.* *Responsable del fichero o tratamiento: persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento.* *Afectado o interesado: persona física titular de los datos que sean objeto del tratamiento a que se refiere el apartado c) del presente artículo.* *Procedimiento de disociación: todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable.* *Encargado del tratamiento: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento.* *Consentimiento del interesado: toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.* *Cesión o comunicación de datos: toda revelación de datos realizada a una persona distinta del interesado. …*

Tanto a nivel comunitario como a nivel nacional existen diversas normativas aplicables para estos dos casos. Para la normativa comunitaria nos encontramos con:

- Recomendación 88/590/CEE, de la Comisión, de 17 de noviembre, relativa a los sistemas de pago y, en particular, a las relaciones entre titulares y emisores de tarjetas.
- Recomendación 97/489/CE, de la Comisión, de 30 de julio de 1997, relativa a las transacciones efectuadas mediante instrumentos electrónicos de pago, en particular las relaciones entre emisores y titulares de tales instrumentos.
- Y en ámbito nacional se pueden citar las siguientes normativas:
- Código de Buena Conducta de la Banca Europea con respecto a los sistemas de pago mediante tarjeta, de 14 de noviembre de 1990, adaptación de la Recomendación 88/590/CEE. Limita la responsabilidad del titular de la tarjeta a 150 euros siempre que no haya habido una negligencia en la custodia

- Ley 7/1996, de 15 de enero de Ordenación del Comercio Minorista, particularmente en su artículo 46-1º, reformado por la Ley 47/2002 de 19 de diciembre.

5. Conclusiones

En este trabajo hemos pretendido presentar la problemática causada por la suplantación de identidad centrando nuestros casos en las vías electrónicas. La suplantación de identidad no es un concepto nuevo y sus orígenes no están en Internet. Desde los tiempos más tempranos de la historia se pueden ver cambios de identidad para conseguir beneficios propios en perjuicio de otros. Al igual que la sociedad se ha ido sofisticando, así lo ha hecho el robo de la identidad.

Hablamos pues de la suplantación de la identidad como obtención de los datos personales y el uso fraudulento de los mismos. Dicho perjuicio puede ser moral, personal, económico, etcétera. Los casos de suplantación de identidad como se ha visto en el apartado 3.1 suponen grandes perjuicios para los afectados. Desde la pérdida de credibilidad a nivel profesional o personal, a la falta de fondos económicos debido a la pérdida del efectivo de las cuentas bancarias o por la imposibilidad de conseguir nuevos fondos al estar incluido en cuentas de morosos.

Las leyes no son suficientes para contener esta problemática. Así pues, con el fin de evitar estos inconvenientes es necesario tener una serie de precauciones. La más importante de todas es la desconfianza en las “gangas” obtenidas por Internet: nadie regala nada. Toda la información personal que se dé en la red debe estar controlada. En el caso de las entidades económicas nunca solicitarán datos por esta vía, y, en caso de las redes sociales, hay que tener cuidado con qué personas son las que pueden ver tus datos personales. Un descuido en la seguridad de los mismos puede acarrear grandes problemas.

6. Bibliografía

Las consultas a las referencias de la bibliografía se han realizado en febrero del 2010.

1. La enciclopedia libre Wikipedia, http://es.wikipedia.org/wiki/Wikipedia:Portada.
2. Skype: http://www.ecostecnologicos.com/index.php?option=com_content&view=article&id=53:identidad-digital-y-cifrado-en-skype&catid=3:newsflash
3. FaceBook: http://facebook.corank.com/legal/privacy.html
4. Certificado Digital: http://camaragipuzkoa.com/secciones/servicios/tecnologias-certificacion.php
5. Ley: http://www.elnotario.com/egest/noticia.php?id=1220&seccion_ver=3
6. Microsoft: http://www.microsoft.com/spain/protect/default.mspx
7. Cómo proteger : http://www.protegeatushijos.com/
8. Juegos educativos trivial: http://www.navegacionsegura.es/
9. Telefonía Móvil: http://www.secukid.es/
10. Spoofing: http://www.lcu.com.ar/spoofing/

11. Recomendación 88/590/CEE, de la Comisión, de 17 de noviembre, relativa a los sistemas de pago y, en particular, a las relaciones entre titulares y emisores de tarjetas.
12. Recomendación 97/489/CE, de la Comisión, de 30 de julio de 1997, relativa a las transacciones efectuadas mediante instrumentos electrónicos de pago, en particular las relaciones entre emisores y titulares de tales instrumentos.
13. Código de Buena Conducta de la Banca Europea con respecto a los sistemas de pago mediante tarjeta, de 14 de noviembre de 1990, adaptación de la Recomendación 88/590/CEE. Limita la responsabilidad del titular de la tarjeta a 150 euros siempre que no haya habido una negligencia en la custodia
14. Ley 7/1996, de 15 de enero de Ordenación del Comercio Minorista, particularmente en su artículo 46-1º, reformado por la Ley 47/2002 de 19 de diciembre.
15. La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), y el Real Decreto 1720/2007 de 21 de diciembre