DELITOS RELACIONADOS CON INTERNET Y LAS REDES SOCIALES

AUTORES:

CARLOS NARANJO HIDALGO

MARCOS ANTONIO FERNÁNDEZ GARCÍA

DELITOS RELACIONADOS CON INTERNET Y LAS REDES SOCIALES

AUTORES Y EDICIÓN:

© CARLOS NARANJO HIDALGO
Policía Local de Las Cabezas de San Juan (Sevilla)

© MARCOS ANTONIO FERNÁNDEZ GARCÍA
Policía Local de Bormujos (Sevilla)

Registro de la Propiedad Intelectual en Safe Creative **Nº2010185648858**

DELITOS RELACIONADOS CON INTERNET Y LAS REDES SOCIALES

INDICE

PRÓLOGO.

Actualmente nos encontramos como en unos años pasamos de una época donde cualquier documento se plasmaba en un papel (era de la imprenta), a la época actual (era de la informática) donde internet ocupa un papel imprescindible en nuestra sociedad. Desde la llegada de esta era tecnológica se nos presentan grandes posibilidades y a la vez serios problemas de carácter jurídico.

En la actualidad y en la era tecnológica en la que vivimos, cada vez es más común el uso de nuevas herramientas a través de internet, aumentando en la misma proporción el número de usuarios que las utilizan.

Del mismo modo que cada vez más tenemos mayor número de herramientas que nos facilitan la vida (aplicaciones en el móvil, páginas web, etc.), en la misma proporción aumentan las personas que utilizan dichas herramientas para cometer delitos de todo tipo, los cuales vamos a intentar desarrollar y explicar en la presente publicación.

El mayor uso de la telefonía móvil va acompañado del aumento de la ciberdelincuencia dirigida a estos teléfonos inteligentes, afectando en mayor medida a los países emergentes, en los cuales este modo de comunicación es un factor imprescindible del desarrollo. Actualmente, nuestro mundo se ve especialmente afectado por otras maneras de ciberdelincuencia, concretamente el fraude. Los principales países víctimas de suplantación de identidad (phishing) son China, Brasil y Argelia (Forcepoint, 2016). La compañía Symantec comunicó el rápido crecimiento de las actividades ciberdelictivas provocadas a la telefonía móvil, con el incremento del 105% entre los años 2015 y 2016.

Para ello, detallaremos la multitud de los distintos tipos de estafas, acoso, medios de suplantación etc. con los que actualmente nos podemos encontrar.

Como policías locales debemos conocer todos ellos y estar prevenidos en nuestro día a día, para dar un mejor servicio al ciudadano.

1. INTRODUCCIÓN

A través de la presente publicación, profundizaremos en el tema de los distintos tipos de ciberdelincuencia, y lo abordaremos desde el punto de vista policial.

La facilidad de acceder a internet desde edad temprana y comenzar a utilizar las redes sociales, conlleva el hacernos la vida más fácil, pero en igual o mayor proporción nos puede acarrear numerosos problemas ya que el desconocimiento o la falta de pericia nos puede traer numerosos problemas por la falta de seguridad, la privacidad, etc.

De la misma manera debemos insistir en garantizar todas las medidas de seguridad y privacidad, por ello desde que los menores comiencen a usar cualquier tipo de red social, aplicación móvil, página web, etc. debemos enseñarles qué mínimos pasos deben dar para acceder de manera segura, para ello, actualmente existen herramientas para que los padres aumenten la seguridad y protejan la privacidad de estos menores, evitando posibles ataques.

Los menores de edad son unas de las víctimas más vulnerables ante estos tipos de ciberdelitos, es por ello por lo que debemos fomentar la educación entre los más jóvenes para que aprendan a protegerse de estos ataques y todas sus variantes.

El anonimato de las redes sociales y de internet en general, genera aún más indefensión en determinados supuestos. Bajo el anonimato se pueden esconder multitud de personalidades, tales como pederastas, psicópatas, acosadores, obsesos del sexo, así como personas envidiosas y/o vengativas que aprovechan ese anonimato para sus más bajos instintos.

Muchas de las técnicas empleadas actualmente en las redes, son constitutivas de delito y deben ser puestas en conocimiento de la autoridad judicial a la mayor brevedad posible, por ello la importancia de conocer y saber diferenciar cuáles son esas nuevas formas delictivas que han ido apareciendo, para que si en algún momento nos encontramos con un caso parecido, saber qué es lo importante y recopilar la mayor cantidad posible de pruebas, para adjuntarlas a la denuncia.

2. INICIOS DE INTERNET

Los principios de Internet nos llevan a los años 60, en plena guerra fría los Estados Unidos crean una red únicamente militar para prevenir un supuesto caso de ataque ruso y así poder tener acceso a la información militar en cualquier parte del país. En 1969 se creó dicha red: *ARPANET*.

Al inicio, la red contaba con cuatro ordenadores que se dividían entre las distintas universidades del país. A los dos años ya contaban aproximadamente con unos 40 ordenadores conectados. El crecimiento de la red fue tal, que su sistema de comunicación se quedó obsoleto, entonces dos investigadores crearon el Protocolo *TCP/IP*, convirtiéndose en el estándar de comunicaciones dentro de las redes informáticas *(en la actualidad se sigue utilizando)*. La red ARPANET, continuó creciendo y abriéndose al mundo, y cualquier usuario con fines de investigación o académicos podía acceder a ella. Posteriormente, las funciones militares dejaron ARPANET y se fueron a MILNET.

La *National Science Fundation (NSF)* crea una red informática propia denominada *NSFNET*, que posteriormente absorbería a *ARPANET*, lo que crearía una red con objetivos científicos y académicos. La magnitud de cómo se fueron desarrollando las redes fue abismal, creándose nuevas redes de acceso libre que posteriormente se unieron a *NSFNET*, que fueron el comienzo de lo que hoy llamamos *INTERNET, que aún en 1985 era conocida por poca gente.*

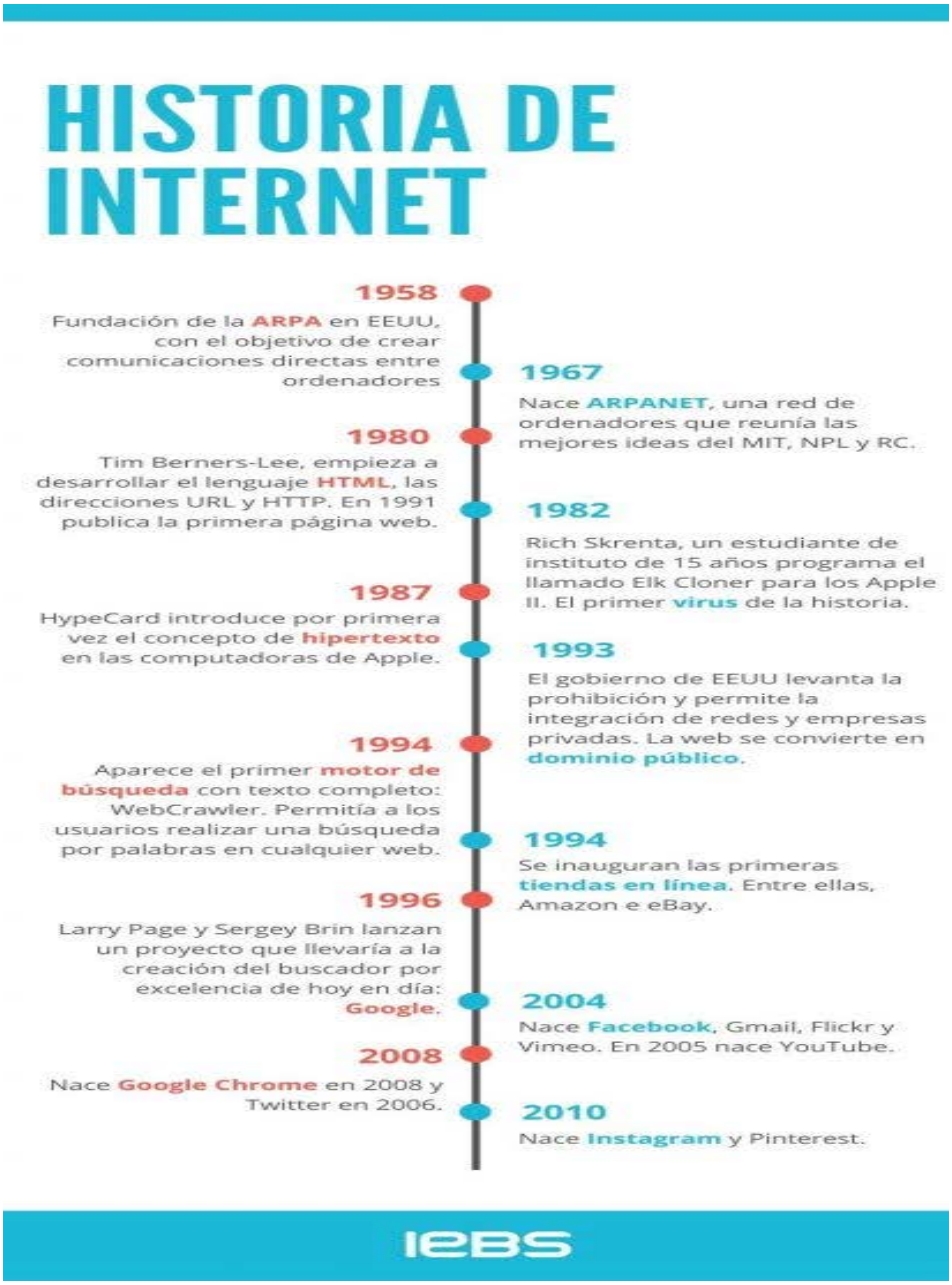
Se fue desarrollando *NSFNET* de tal manera, que sobre el año 1990 ya contaba con alrededor de 100.000 servidores. En 1990 deciden ponerle un nombre al sistema y lo llaman *World Wide Web (WWW)* o telaraña mundial. Los conocidos como “navegadores” o “browsers”, nacieron mediante una fórmula que permitía vincular información en forma lógica y a través de las redes.

En 1992, la gestión de Internet se reforzará con la creación de la (ISOC) Internet Society. Dicho órgano de opinión internacional (sin ánimo de lucro) integrará todas las organizaciones y las empresas implicadas en construir la red, su objetivo sería consensuar las acciones de extensión de Internet. También en 1992, Internet conectaba más de un 1.000.000 de "hosts" (ordenadores que daban acceso a usuarios finales) y enlazaba más de 10.000 redes en 50 países.

En el año 1993 *Marc Andreesen* produjo la versión inicial del navegador *"Mosaic"*, que permitía acceder con más facilidad a la *WWW*.

En 1994, el número de "hosts" conectados era de 3.000.000 y se habían llegado a integrar 25.000 redes de 146 países. Desde entonces, internet empezó a crecer cada vez más rápido que cualquier medio de comunicación, llegando a convertirse en lo que hoy todo el mundo conoce.

A continuación podemos ver un gráfico resumen de la historia de internet:



Fuente: Elena Bello (IEBS). Julio 2020

2.1 PRINCIPIOS DE LOS DELITOS INFORMÁTICOS

Cuando nos referimos a delito informático, cibernético o ciberdelito, nos estamos refiriendo a toda aquella acción antijurídica que se produce en el entorno digital o Internet.

Como consecuencia de la utilización de las nuevas tecnologías en nuestro día a día y debido al gran número de usuarios que tiene, la delincuencia también ha llegado a esa dimensión. Todo ello, debido al anonimato y a los datos de carácter personal que se conservan en dicho entorno digital, los delincuentes han ampliado su zona de ataque y los delitos y amenazas a la seguridad se han incrementado de manera exponencial.

Además de los ataques que tienen como objetivo la destrucción y el dañar activos, sistemas de información u otros sistemas de ordenadores, utilizando para ellos medios electrónicos y/o redes de Internet, es por lo que se producen nuevos delitos contra la propiedad, la identidad y la seguridad de las personas, empresas e incluso instituciones.

Igualmente, también nos podemos encontrar con otras conductas criminales que aunque no pueden tener la consideración de delito, podemos definir como ciberataques o abusos informáticos y que forman parte de la criminalidad informática.

Esa denominada criminalidad informática consiste en la realización de actividades que, aun cumpliendo los requisitos que delimitan el concepto de delito, son llevadas a cabo utilizando para ello un elemento informático.

3. PRINCIPALES CONCEPTOS DE LA CIBERDELINCUENCIA.

Fuente: www.researchgate.net/

3.1. MALWARE

Malware es la abreviatura de las palabras inglesas ***mal****icious soft****ware***, lo que se traduciría al español como **código malicioso**. Estos *malwares* realmente son programas que se diseñan para infiltrarse en otro sistema con la finalidad de dañar o robar información y datos.

Podemos denominar *malware* a los programas que ejecutan acciones no deseadas en un sistema informático, siendo una de las mayores preocupaciones en la seguridad informática.

Tipos de malwares

Ejemplos de *malwares*:

- **Virus**: pueden llegar a eliminar sin autorización ficheros, directorios y datos.
- ***Spyware***: consigue datos sin permiso del usuario (mensajes de correos electrónicos, números de tarjetas de crédito, etc).
- **Gusanos**: se introducen en el sistema y crean copias infinitas de sí mismos, para colapsar la red o el dispositivo, y llegan a bloquear cualquier trabajo adicional.
- **Caballos de troya o troyanos**: cuando se activan o abren, permiten el acceso sin autorización a datos en el ordenador o sistema informático infectado.
- **Bots maliciosos**: están creados para ejecutar acciones las cuales el usuario no ha autorizado.
- ***Adware***: programas que se diseñan para invadir sistemas mediante publicidad no deseada.

Cómo eliminar o prevenir malwares

La forma más eficaz es la instalación de programas que puedan detectarlos como anti-*malwares*, antivirus o anti-*spywares*, con los que se pueda escanear el ordenador de manera regular, previniendo así ataques y manteniendo una protección actualizada.

3.2. PHARMING

El pharming es un tipo de fraude en internet que consiste en **explotar una vulnerabilidad en el software de servidores DNS o equipos de los usuarios,** permitiendo que un atacante consiga redirigir el nombre de dominio a una máquina diferente, permitiendo que el usuario que aparezca en este dominio pueda acceder en su explorador a la web del atacante**.**

Los ordenadores que se conectan a internet tienen una dirección IP única, dicha **IP es un número de 4 octetos (4 grupos de 8 dígitos binarios) de 0 a 255 y separados por un punto (**IP: 165.16.5.210). Estos ataques de pharming se pueden hacer de dos maneras:

- Directamente a los servidores DNS (todos los usuarios serán afectados).

- Atacando a ordenadores concretos (se hace modificando el fichero «hosts», que se encuentra en equipos que funcionen con sistemas Unix o Windows).

3.3. RANSOMWARE

Ransomware es un tipo de componente de software malicioso que utiliza una encriptación para impedir el acceso a sus archivos y de esa manera tomar como rehén a su ordenador. Para poder recuperar el control de su ordenador, es posible que tenga que pagar mucho dinero de rescate.

El ransomware, habitualmente se distribuye mediante emails de phishing que contienen a su vez enlaces a contenido dañino o archivos peligrosos. Los usuarios pueden llegar a descargarlo sin saber cuando visitan páginas web que están infectadas y que instalan software malicioso en su ordenador sin dar su consentimiento. **Tipos de ransomware:**

- **Bloqueadores de Ordenador. I**mpedirán el acceso a la interfaz del ordenador impidiendo que lo pueda usar. Si está infectado aparecerá una pantalla de inicio con el mensaje del autor y unas instrucciones para pagar, que aparecerán cuando arranque el sistema, pueden intentar hacer creer que el rescate ha sido una multa interpuesta por las fuerzas de seguridad.
- **Bloqueadores de Datos. S**on potencialmente más peligrosos que los bloqueadores de ordenador, se conocen como cripto-ransomware, este software logra escanear el ordenador en busca de archivos valiosos y llega a cambiar la extensión por otra que el ordenador no pueda reconocer. Para poder desbloquear sus archivos, el usuario o víctima tendrá que pagar el rescate para poder obtener la clave de desencriptación. Los que están detrás de estos bloqueadores suelen atacar a personas que no realizan copias de seguridad con regularidad de sus archivos importantes.

Otros Tipos de Ransomware: Podemos destacar en los últimos años los siguientes:

- **Scareware** – Habitualmente se esconde tras un software antivirus, pero en lugar de exigir dinero, presiona a las víctimas para que adquieran un software antivirus falso, que repare los errores. Cuando se ha pagado e instalado, el software se convierte en malware y roba la información personal de la víctima.
- **Leakware** – Conocido como doxware, este amenaza a la víctima con publicar su información personal si no paga por el rescate. Se encargan de explotar el hecho de que muchos usuarios almacenan información de carácter íntimo en su ordenador (fotos, vídeos, claves de tarjetas de crédito y documentos personales) y saben que pueden crear en la víctima un estado de pánico.
- **Ransomware Como Servicio (Raas)** – Es un modelo de negocio que está emergiendo y está en auge en la dark web. Los que aspiran a ser hackers pueden llegar a un acuerdo

con terceras personas que desarrollen software para ellos y lo distribuyan rápidamente a las potenciales víctimas. Con esto, el proveedor del RaaS gana un porcentaje y el resto el hacker.

Los 5 ejemplos de ransomware más destructivos:

- WannaCry
- CryptoLocker
- CoinVault
- Bad Rabbit
- NotPetya

Hoy en día, el ransomware también se distribuye a través de las redes sociales y aplicaciones de mensajería instantánea.

3.4. CIBERBULLYNG.

Podemos definir el *ciberbullying* como **el uso de los medios telemáticos (internet, telefonía móvil y videojuegos online) para ejercer el acoso psicológico entre iguales.**

Ciberbullying es una palabra de origen inglés, compuesta por "bullying" que significa acoso e intimidación, y "ciber" que se refiere a su relación con las redes informáticas. Podemos decir que se trata de una nueva variedad de acoso psicológico, que surge entre iguales y únicamente entre niños, estableciéndose por medios telemáticos como el teléfono móvil e internet. Cuando intervienen adultos, se le conoce como ciberacoso.

No hay que confundir ciberbullying con bullying, ya que son dos tipos de acoso diferentes y se puede decir que con pocas similitudes, aunque también es un acoso en el que los compañeros maltratan a otro compañero, pero a diferencia del ciberbullying, este tipo de acoso físico y psicológico se hace en persona sin utilizar medios telemáticos.

Como diferencia del ciberbullying, en el que el anonimato destaca y durante casi todo el tiempo los niños atacados no saben quién les está haciendo daño, es habitual que los niños que realizan bullying terminen utilizando el ciberbullying como otra manera distinta de acosar a sus compañeros.

Las maneras en este tipo de acoso pueden ser muy variadas:

- Subir una foto comprometedora a internet.
- Crear cuentas falsas en redes sociales con el nombre e imagen del niño acosado, y posteriormente usarlas para molestar a los demás compañeros.

La manipulación, exclusión y hostigamiento son algunos ejemplos de las cosas que busca el menor que hace ciberbullying, utilizando para ello las redes sociales, consolas, ordenadores y aplicaciones para teléfono móvil.

En la actualidad hay protocolos establecidos tanto dentro como fuera de la escuela para poder atajar y controlar este tipo de acoso.

3.5. GROOMING

Cuando nos referimos al *"**grooming"*** y, en su evolución digital, el *"**online grooming"*** (acoso y abuso sexual *online*), hablamos de formas delictivas de **acoso** que implican a **una persona adulta que se pone en contacto con un niño, niña o adolescente** con el fin de ganarse poco a poco su confianza **para luego involucrarle en una actividad sexual**.

Este tipo de prácticas tienen distintos niveles de interacción y peligro, pueden ir desde solo hablar de sexo y lograr hacerse con material íntimo, hasta llegar a quedar en persona y mantener un encuentro sexual.

En este proceso, se produce un vínculo de confianza entre víctima y acosador, ya que éste último intenta aislar poco a poco al menor, consiguiendo desprenderlo de su red de apoyo (familiares, profesores, amigos, etc.) llegando incluso a generar un ambiente de intimidad y secretismo.

Sin embargo, en el *"online grooming"* el abusador envía mediante un medio tecnológico, material de contenido sexual al niño o niña. Incluso se suele hacer pasar por menor de edad llegando a adaptar el lenguaje y la forma de expresarse a la edad de la víctima. Se puede considerar una violencia igual de real que la física, pero de la que es mucho más difícil huir.

Fases del "online grooming":

1. **Creación de un vínculo de confianza.** A través de sobornos o engaños, el agresor consigue contactar con la niña o niño y establecer así el vínculo de confianza. Para eso suele fingir otra edad, parecida a la de la víctima. Puede incluso que el abusador haga regalos, empatice a un nivel profundo con los menores haciendo ver que se preocupa por sus problemas y se aproveche de esa información para chantajear posteriormente.
2. **Aislamiento de la víctima.** El agresor intentar separar al menor de familiares, amistades, docentes, etc. para dejarlo desprotegido, por lo que insiste en la necesidad de mantener todo en secreto.
3. **Valoración de los riesgos.** El agresor intenta siempre asegurar su posición, por lo que suele preguntar a la víctima si alguna persona más conoce su relación, así como averiguar si alguien más tiene acceso al dispositivo que utiliza el menor.
4. **Conversaciones sobre sexo.** Cuando logra tener confianza, el abusador comienza a tener conversaciones sexuales de manera regular, buscando que el menor se familiarice con la temática sexual y con el vocabulario.

5. **Peticiones de naturaleza sexual**. El objetivo principal del *"online grooming" es esta fase, en la que el abusador uti*liza las amenazas, la manipulación, el chantaje o la coerción para que el menor le envíe material de contenido sexual, le cuente fantasías sexuales o culmine la relación con un encuentro físico.

Cómo prevenir el grooming, consejos a menores:

- Pedirle que rechace mensajes de tipo sexual y exigir respeto.
- Aconsejar que no publique sus fotos o de sus amigos en sitios públicos.
- Recomendar que use perfiles privados en redes sociales
- Pedirle que no acepte en sus redes sociales a personas que no conozca.
- Explicarle que debe pedir ayuda si se produce una situación de acoso, así como ayudarle a identificar las claves para que no ceda al chantaje.
- Explicarle que debe respetar sus derechos y los de sus amigos y conocidos.

3.6. SEXTING

La palabra sexting procede del inglés formado por "sex" (sexo) y "texting" (escribir mensajes). Se denomina "*sexting"* a la **actividad de enviar fotos, videos o mensajes de contenido sexual y erótico personal a través de dispositivos tecnológicos, utilizando para ello aplicaciones de mensajería instantánea, redes sociales, correo electrónico o cualquier otra herramienta de comunicación**.

El sexting puede ir también unido a otras acciones que también se consideran delitos en el mundo físico, como puede ser el exhibicionismo o la extorsión.

Cualquier cosa que se envíe por internet (whatsApp, telegram, instagram, facebook, email), puede llegar a ser utilizado en contra del usuario, y aún más si se trata de contenido de carácter sexual. Es **ilegal** difundir videos o fotos eróticas o sexuales de otra persona, pudiendo ser un agravante si este contenido pertenece a la pareja, la víctima sea menor de edad o los hechos se hubieran cometido con una finalidad lucrativa.

Es importante saber que **cuando falta el consentimiento, el sexting pasa a ciberacoso sexual,** pudiendo llevarse a cabo de muchas maneras y mediante:

- Envío de mensajes con lenguaje amenazante.
- Publicación de fotos, videos o rumores para deshonrar la reputación de la víctima online.
- Envío de imágenes o vídeos o comentarios a personas del entorno de la víctima denigrándola
- A través del ciberacoso repetido buscando producir miedo.

3.7. SEXTORSION

La “sextorsión” (extorsión sexual), palabra que procede del inglés “*Sextortion”*, es una forma de explotación sexual, en la que una persona es chantajeada, bien con una imagen o con un vídeo de sí misma, desnuda o realizando actos sexuales, que habitualmente ha sido previamente compartida mediante sexting.

El chantaje se suele realizar por Internet (páginas web, aplicaciones, redes sociales, etc.), ya que con esto se asegura cierto grado de anonimato el criminal. Puede ser realizado por conocidos, ex-amantes o personas desconocidas a través de imágenes conseguidas en el contexto de una relación sentimental o de imágenes obtenidas mediante webcams, email, mensajería instantánea, teléfonos u otros dispositivos móviles.

A continuación, la víctima es coaccionada para tener relaciones sexuales, entregar más imágenes eróticas o pornográficas, dinero o cualquier otra contrapartida, bajo la amenaza de difundir dichas imágenes o videos originales si no accede a las exigencias de la persona que la chantajea.

Internet tiene un papel fundamental, ya que facilita el anonimato del delincuente quien además, puede buscar víctimas en cualquier parte del mundo. Aunque el extorsionador pueda ser detenido antes o después de conseguir su objetivo, la víctima se enfrenta a un duro reto: asumir que con un clic la persona que la chantajea podría hacer un daño irreparable a su vida, ya que las imágenes son sencillas de guardar, copiar y distribuir.

La creación de imágenes comprometedoras, tiene dos posibles orígenes**:**

1. El **voluntario y consciente**, en el que el protagonista consiente, participa y genera estas secuencias, aquí nos encontraríamos tres prácticas habituales:

- ✓ Sexting, son comunes las imágenes generadas por el propio protagonista para flirtear o en el seno de una relación para ser enviadas al pretendiente o la pareja usando el teléfono móvil.
- ✓ Exhibiciones voluntarias subidas de tono usando a través de webcam que son grabadas por el receptor.
- ✓ Grabación de prácticas sexuales, en el contexto de una relación de pareja o en un marco grupal privado.

2. El **involuntario**, que se produce cuando terceras personas de manera furtiva toman esas imágenes, sin conocimiento o consentimiento de quien las protagoniza. Se pueden citar algunos ejemplos como:

- ✓ Grabación en lugares de acceso público (encuentro sexual nocturno en la playa, una fiesta en una discoteca donde se celebran concursos atrevidos, locales de intercambio de pareja, etc).
- ✓ Toma de imágenes en un marco privado por parte de la pareja, una broma pesada de unos amigos…

La posesión de las imágenes por el delincuente, en las que el extorsionador puede tener acceso a las imágenes por vías muy diversas:

- ✓ Directamente de la víctima, quien las produce y entrega de manera consciente.
- ✓ Indirectamente por otras personas o en sitios de la Red, sin que la víctima esté al tanto de ello.
- ✓ Realizando una grabación directa, no siendo la víctima consciente.
- ✓ Mediante el robo de las mismas a la propia víctima o a otra persona.

El mejor consejo para no ser víctima de sextorsión es no protagonizar una secuencia o imagen, no obstante, esto puede escapar a nuestra voluntad si, por ejemplo, activan la webcam de nuestro dormitorio y nos graban cambiándonos de ropa. Es por ello, por lo que tenemos que proteger nuestra privacidad e intimidad y la de las personas con las que nos relacionamos, mediante la toma de medidas activas y pasivas de seguridad en nuestro ordenador y teléfono móvil.

3.8. USURPACION DE IDENTIDAD

La "**Suplantación de Identidad**" consiste en el **uso de información personal para hacerse pasar por otra persona con el fin de obtener un beneficio propio**. Habitualmente, este beneficio genera un perjuicio a la persona que sufre dicha suplantación de identidad. En el supuesto de menores, es un factor de riesgo cada vez más frecuente que se produce cuando una persona malintencionada actúa haciéndose pasar por el menor mediante la utilización de diversas técnicas.

Hay que diferenciar entre dos conceptos:

- **Suplantación de identidad**. Consiste en la apropiación de derechos y facultades propias de la persona suplantada (Ej: acceder a la cuenta de una red social).
- **Usurpación de la identidad**. Consiste en que una vez suplantada la identidad se empiece a interactuar como si realmente fuera propietario de esos derechos y facultades (Ej: realizar comentarios o subir fotografías).

El **Pisher** o **delincuente cibernético** mediante el uso de la ingeniera social (Seguridad Informática), suplanta la identidad de una persona o empresa en una aparente comunicación oficial electrónica, como puede ser Email, WhatsApp, Redes Sociales, llamadas telefónicas o SMS.

Ante el aumento del número de estafas o incidentes relacionados con la Suplantación de Identidad, se necesitan métodos de seguridad adicional, por lo que se han creado leyes que castigan este delito y se han hecho campañas de prevención que ayuden a los usuarios con las medidas técnicas de los programas.

Consecuencias de la Suplantación de Identidad:

- **Compras por Internet:** Solo con el número de la tarjeta de crédito, la fecha de caducidad y el nº de seguridad, el **Pisher** puede realizar todas las compras que desee.
- **Aperturas de Cuentas Corrientes:** Utilizan las identidades robadas para abrir nuevas cuentas corrientes y de esa manera poder blanquear dinero en su nombre, lo que crea gravísimos problemas.
- **Daños financieros:** Si ya han obtenido los datos financieros podrían hacer todo lo que quieran con el dinero.
- **Daño en la reputación.**
- **Desgaste físico y psicológico:** Los procesos de este tipo, tardan en resolverse varios años, y muchísimas horas entre juzgados, abogados, etc.

Cómo protegernos de la Suplantación de Identidad. Consejos para evitar el robo de identidad:

1. **No dar información personal.** No compartir datos personales, contraseñas, cuentas corrientes por ningún medio (email, RRSS, etc). Empresas y bancos nunca solicitarán datos por dichos medios.
2. Si hay algún **correo electrónico**, de dudosa veracidad, nunca seleccionar ningún archivo o link incluido en el mismo.
3. Siempre que se **navegue por Internet** y se necesite incluir datos personales para un acceso o registro, asegurarse que se ha entrado en una dirección segura (debe empezar con **https://** y un candado cerrado en la barra de estado del navegador).
4. **No guardar contraseñas en los dispositivos electrónicos.**
5. **Realizar compras seguras:** Si se hacen compras con la tarjeta de crédito por Internet, asegurarse de tener una tarjeta con alerta incluida (muchos bancos ofrecen el envío de SMS o emails cada vez que se registra un movimiento con la tarjeta bancaria).

6. No utilizar **cajeros automáticos** si se observa alguna anomalía en él.
7. **Contratar un seguro.**

Cómo actuar cuando se ha sido víctima de una Suplantación de Identidad.

Las personas que sufren este tipo de delitos, no suelen darse cuenta de que son víctimas de un delito hasta que es demasiado tarde y tienen conocimiento de ello cuando el banco se da cuenta de movimientos sospechosos e irregulares y contacta con la víctima. Por lo cual, las recomendaciones ante la pérdida de algún documento de identidad o tarjeta de crédito es que se sigan las siguientes pautas:

1. **Denuncia:** La mejor arma para presentar antes las deudas y fraudes que el **Pisher** pueda cometer.
2. **Comunicar el robo a la entidad financiera:** Se debe notificar al banco lo antes posible, presentando la denuncia correspondiente para que tomen las medidas oportunas.

3.9. CIBERVIOLENCIA DE GÉNERO

La **ciberviolencia de género** consiste en el acoso que se produce por parte de una persona hacia otra del sexo opuesto, haciendo uso para ello de las nuevas tecnologías y de todas las herramientas que proporciona internet. Tantos redes sociales, como foros, juegos online, chats… suelen ser los lugares más comunes en los que se da este tipo de violencia.

Este tipo de acoso puede ir desde simples comentarios generales en contra del sexo opuesto (Ej. críticas de chicos en juegos online por la posible presencia de chicas) o ataques directos a personas concretas, que atentan contra su libertad e intimidad (control de redes sociales o cualquier otro movimiento que haga en internet).

Esta clase de circunstancia suele producirse habitualmente en parejas que quieren controlar totalmente a la otra persona, aunque también este fenómeno se puede dar entre desconocidos solo por el simple hecho de pertenecer al sexo opuesto. Para diferenciarlo de la violencia de género, las secuelas que presenta este peligro cibernético son mayormente psicológicas y no físicas, puesto que internet permite tanto el contacto como el acoso entre personas desde la distancia. No obstante, la ciberviolencia de género puede trasladarse más allá de la red y agravar aún más las secuelas de las víctimas.

Principales características de la ciberviolencia de género.

Algunas de las características de la ciberviolencia de género pueden manifestarse en internet de varias formas:

- Acceder a las cuentas de la víctima sin permiso.

- Controlar todo tipo de actividad de la víctima tanto en redes sociales o como en páginas de internet.
- Espiar el teléfono móvil o cualquier otro dispositivo.
- Usurpar la identidad de la víctima, haciéndose pasar por la misma en diferentes lugares de la red.
- Prohibir la utilización de diferentes redes sociales y similares a la víctima.
- Prohibir la publicación de contenidos concretos en internet a la víctima.
- El envío de amenazas, insultos o contenido desagradable a la víctima.
- Acosar a la víctima, siguiéndola a través de todos los sitios web que visite regularmente.
- Realizar comentarios ofensivos públicamente contra el sexo opuesto, contra una persona o colectivo en particular.
- El envío de imágenes comprometidas de la víctima, las cuales podrían haber sido enviadas voluntariamente por la misma (sexting).

3.10. SCAM

Al igual que los casos anteriores, el Scam, es otra forma de estafa a través de Internet, en este caso el estafador ofrece un gancho (una herencia ficticia o un supuesto billete de lotería premiado) para el que pide una pequeña cantidad de dinero como adelanto o varias cuotas antes de recibir un gran premio. Los scams, más que en habilidades informáticas, se basan en engaños y técnicas de ingeniería social.

El funcionamiento de este tipo de estafa se realiza de la siguiente manera, dentro de este tipo, la más famosa es la del príncipe nigeriano y sus muchas variantes. Los estafadores envían masivamente un correo electrónico en el que intentan engañar a su destinatario haciéndolo creer que una gran cantidad de dinero se encuentra bloqueada en Nigeria, y que para disponer del mismo debe ser transferida a una cuenta bancaria extranjera. Entonces, ofrecen una comisión al destinatario del correo a cambio de su ayuda para sacar el dinero del país pidiéndole a la víctima que pague una cierta cantidad de dinero por adelantado. Este tipo de estafa también la utilizan para la consecución de donaciones falsas después de un desastre o falsas ONG. Además de estos tipos de scams, tenemos los siguientes:

- Estafas de sitios de citas online.
- Scam de asistencia técnica.

- Smishing. Es un phishing centrado en teléfonos móviles, en el que se envían textos a teléfonos móviles para engañar a su usuario y que este facilite información confidencial del mismo, o también para que acceda a sitios webs falsos y se descarguen una aplicación infectada con un malware.
- Estafas de pago por adelantado
- Scams con lotería

Para poder identificar este tipo de estafa, podemos seguir los siguientes consejos o técnicas y es que todos o casi todos los diferentes tipos de esta estafa tienen en común su carácter urgente. Te informan que tu cuenta bancaria ha sido bloqueada y que debes iniciar sesión inmediatamente utilizando el enlace suministrado, también otra forma es diciendo que una verificación de seguridad ha bloqueado temporalmente el acceso a tu cuenta, antes de pedirte que confirmes tu contraseña para restaurar el acceso, o incluso te pide que descargues una aplicación especial para mejorar la seguridad de la cuenta.

3.11. PORNOGRAFÍA INFORMÁTICA

La pornografía es la filmación, fotografiado y exposición de manera explícita de relaciones sexuales. Si bien es cierto que en algunas ocasiones el término puede emplearse con cierto grado de amplitud, es importante hacer una separación con producciones de tipo erótico; en efecto, en este segundo caso las relaciones sexuales suelen ser sugeridas, pero nunca son explícitas y evidentes. Así, en la pornografía existe una exhibición de la genitalidad y de las relaciones sexuales de manera patente.

Después de esta definición explícita acerca del término pornografía, podemos decir que la pornografía informática es la difusión o exhibición a través de Internet, de filmaciones, fotografías y exposiciones de forma explícita de las relaciones sexuales. En este tipo acciones el hecho delictivo se produce cuando en ese material audiovisual aparecen menores de edad o personas discapacitadas necesitadas de una especial protección, así como cuando esa difusión se hace sin el consentimiento expreso de las personas involucradas en la misma.

3.12. SPAM

El SPAM podría definirse como aquellos mensajes no solicitados, normalmente con contenido de tipo publicitario, que son enviados al usuario de forma masiva. La vía más utilizada es la basada en el correo electrónico pero en la actualidad también se presenta a través de programas de mensajería instantánea o incluso por el teléfono móvil. Entre las características más comunes que presentan los correos no deseados o SPAM, están:

- La dirección del remitente del mensaje no resulta conocida para quien recibe el correo, y lo normal es que sea falsa.
- El mensaje no suele tener dirección “Reply”.
- En el asunto siempre utilizan palabras que llamen la atención del usuario que lo recibe.
- El contenido de estos mensajes es publicitario: anuncios de sitios web, fórmulas para ganar dinero fácilmente, productos milagro, ofertas inmobiliarias, o simplemente listados de productos en venta en promoción.

La mayor parte del spam está escrito en inglés y se origina en Estados Unidos o Asia, pero en España empieza ya a ser común. Como se ha dicho anteriormente el método de distribución más habitual es el correo electrónico, pero en la actualidad existen diversas variantes, cada una de ellas con su propio nombre asociado en función de su canal de distribución:

- Spam: mensaje enviado a través del correo electrónico.
- Spim: mensaje específico para aplicaciones de tipo Mensajería Instantánea (Skype, WhatsApp, etc).
- Spit: spam sobre telefonía IP. La telefonía IP es la telefonía que utiliza Internet como medio de transmisión para realizar llamadas telefónicas.
- Spam SMS: spam destinado a enviarse a teléfonos móviles utilizando para ello los SMS (Short Message Service).

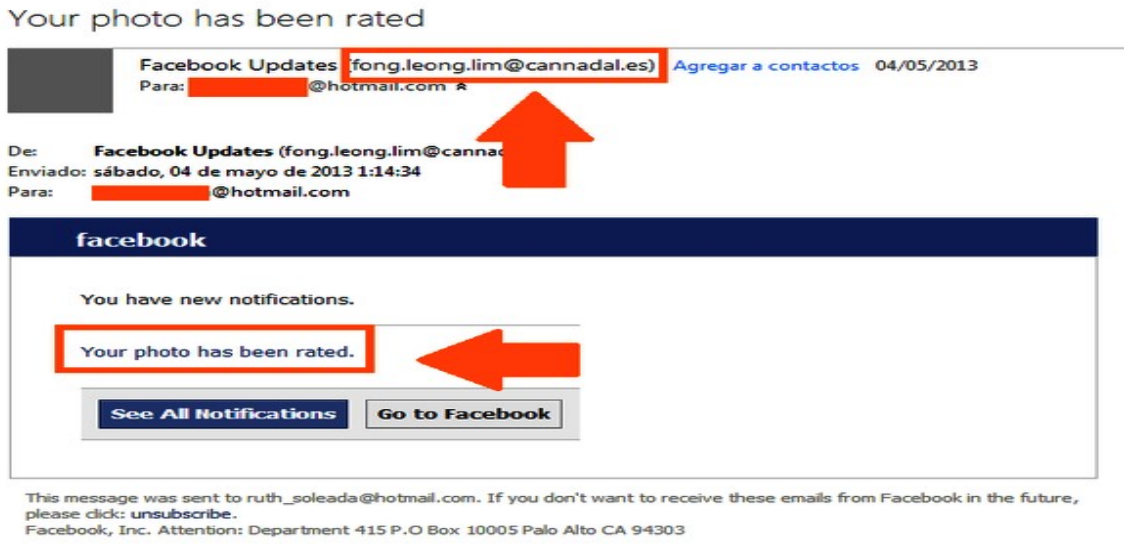
En la actualidad el spam es un fenómeno que va aumentando día a día, y representa un elevado porcentaje del tráfico de correo electrónico total. Además, conforme van surgiendo nuevas soluciones y tecnologías para luchar contra él, los spammers (usuarios maliciosos que se dedican profesionalmente a enviar spam) se vuelven a su vez más sofisticados, y modifican sus técnicas para así poder saltarse las contramedidas desplegadas por los usuarios y conseguir su objetivo, el de inundarle el dispositivo de mensajes que el propio usuario no desea ni ha solicitado.

3.13. PHISHING

El delito de fraude informático o phishing consiste en el envío de correos electrónicos que, aparentando provenir de fuentes fiables, como por ejemplo pueden ser bancos, intentan obtener de manera fraudulenta las claves bancarias y datos confidenciales del usuario, y, a partir de ahí, utilizarlos para realizar algún tipo de fraude.

Para ello, lo más normal es que en el correo electrónico enviado se incluya un enlace que, cuando es pulsado redirecciona al usuario a páginas web falsificadas o se ejecuta un código malicioso sin que el usuario pueda saberlo (malware). De esta forma, el usuario, creyendo estar en un sitio de toda confianza, introduce la información que se le solicita y que, en realidad, va a parar a manos del estafador. Una vez que han obtenido toda la información necesaria de las víctimas,

utilizan esos datos robados para realizar estafas. Por ejemplo, mediante la apertura de nuevas cuentas bancarias usando el nombre de la víctima, o incluso vendiendo los datos robados en el mercado negro.



Ejemplo de phishing utilizando para ello las redes sociales

Existen diferentes formas o métodos de phishing, entre los más usados tenemos:

- Bancos y cajas
- Pasarelas de pago online (Paypal, Mastercard, etc.)
- Redes Sociales (Twitter, Instagram, etc.)
- Páginas de compra/venta y subastas (Wallapop, Amazon, Mil anuncios, etc.)
- Juegos Online
- Soporte técnico y de ayuda de empresas y servicios(Outlook, Apple, Samsung, etc.)
- Servicios de almacenamiento en la nube (Mega, Dropbox, etc.)
- Servicios o empresas públicas
- Servicios de empresas de mensajería
- Falsas ofertas de empleo.

3.14. HACKING

El hacking se podría definir como la búsqueda y explotación de vulnerabilidades de seguridad en sistemas o redes. En otras palabras, el hacking consiste en la detección de vulnerabilidades o agujeros de seguridad, y también engloba la explotación de las mismas. Aquellos que se dedican a este tipo de actividad, se les denomina Hackers y aunque existen muchos tipos los más comunes son:

- *Hackers de sombrero blanco o white hat.* Se les conoce como hackers éticos. Este tipo de personas son contratadas por alguna compañía para la búsqueda de vulnerabilidades de seguridad, para detectarlas, conseguir subsanarlas y que la aplicación sea más segura. Siempre tienen un fin bien intencionado.
- *Hackers de sombrero negro o black hat.* Son hackers malintencionados. Este tipo de hacker al igual que los de sombrero blanco, se dedica a la búsqueda de vulnerabilidades de seguridad, pero en este caso las explotan en su propio beneficio.
- *Hackers de sombrero gris o grey hat*. Estos no están contratados por ninguna compañía, estos hackers trabajan de forma autónoma y no tienen permiso de la compañía o del dueño del producto para realizar esos ataques o búsqueda de vulnerabilidades de seguridad. No tienen malas intenciones, sino que intentan probarse a sí mismos y suelen avisar de que han detectado la vulnerabilidad de seguridad.

3.15. PIRATERÍA INFORMÁTICA

Realmente no existe una definición legal de la piratería de derecho de autor, pero aún así, podemos entender que la misma comprende todo acto de violación del derecho de autor, bien sea mediante la obtención y distribución de copias sin la autorización del autor, o bien, por la comunicación pública y puesta a disposición de los usuarios de contenidos de manera ilegal. Tal circunstancia puede comprender la violación de derechos morales y patrimoniales.

Además de esta definición de piratería, tenemos también aquella definición que considera que el término piratería es un término peyorativo y popular, que fue creado en el SXVII por la industria británica del copyright para referirse a la copia de obras culturales (literarias, audiovisuales, musicales, de software o invenciones) efectuada sin el consentimiento del titular de los derechos de autor o sin autorización legal.

Existen multitud de casusas que “justifican” o explican la existencia de la piratería, pero las más extendidas o importantes son:

- La aparición de fenómenos que han influido para hacer posible la piratería. Por ejemplo, la accesibilidad con respecto a los precios, cualquier persona que desee obtener un producto novedoso y barato puede recurrir a la piratería.
- El desempleo. La piratería está estrechamente relacionada con el desempleo, los bajos ingresos y la accesibilidad en precios.
- Escasa sensibilización del público.
- Alta demanda de bienes culturales.
- Malentendidos sobre la piratería.

- Protección eficaz de la propiedad intelectual y poco respeto a los derechos
- El precio elevado
- Dificultad de acceso a las obras originales.
- Las elevadas ganancias de los piratas

Entre los diferentes tipos de piratería informática tenemos:

- Piratería de usuario final. Se produce cuando una única copia con Licencia de un Software es instalada en varios ordenadores. Otra forma de este tipo de piratería es cuando se utiliza una versión "crackeada" del software.
- Piratería de revendedor. Hablamos de este tipo de piratería cuando un revendedor distribuye copias de un único software a diferentes clientes; también cuando se venden versiones falsificadas de software, imitando embalajes, sellos y documentos del software original.
- Piratería de Internet. Ocurre cuando se pone a disposición de los usuarios una transferencia electrónica de software con derechos de autor en internet para que otros puedan copiarlos y usarlos sin la licencia correspondiente.
- Violación de marca registrada. Esta infracción sucede cuando una empresa no acreditada se presenta como negociante autorizado, técnico, proveedor de soporte o revendedor, o usa indebidamente un nombre de marca registrada.
- Otros tipos de piratería. Otra técnica utilizada por piratas de software es obtener ilegalmente una copia registrada de software. El pirata compra una única copia y la utiliza en varias computadoras. Otra técnica es la compra de software con tarjetas de crédito clonadas o robadas.

3.16. REVENGE PORN

Consiste en la difusión no consentida de imágenes privadas, también conocida como «pornovenganza», es la publicación de contenidos, generalmente imágenes, con contenido sexual explícito o sugerente, sin el consentimiento de la persona que aparece en ellas y que fueron tomadas dentro de un ámbito privado. En este caso las víctimas son principalmente mujeres jóvenes y, en la mayoría de los casos, los instigadores son las ex-parejas u otras personas cuyo objetivo primordial es el de humillar y atacar la reputación de sus víctimas mediante la publicación de esas imágenes de índole sexual.

Durante los últimos años, la proliferación de actividades como el sexting (envío de imágenes y otro tipo de contenido íntimos a través plataformas online) ha provocado un aumento de los casos de Revenge Porn. En España, el Revenge Porn es un delito castigado por la ley, la

Agencia de Protección de Datos recuerda que “amenazar o chantajear con difundir vídeos o grabaciones íntimas de la pareja (fotografías, vídeos o audios) sin su consentimiento puede constituir un delito de violencia de género”. Del mismo modo, cualquier otro que participe en su publicación o los comparta se expone a multas y penas de prisión de tres meses a un año (artículo 197.1 del Código Penal).

De esta manera, si alguien publica fotos íntimas de otra persona estará cometiendo un delito de violencia sexual, ya que aunque no exista ningún tipo de agresión física sí existe un daño psicológico, castigado por la ley.

Cómo protegerse

Aunque parezca una tontería y se vea muy simple, la medida de prevención más simple es no aparecer en fotografías comprometidas. Una vez que un archivo se digitaliza surgen inevitablemente los riesgos derivados del intercambio de datos, de su publicación sin permiso, de robos de dispositivos o de hackeos. Hoy en día todos los móviles, tablets y ordenadores suponen un riesgo, ya que todos están conectados a la red en algún momento y la gran mayoría de ellos no disponen de una protección básica. Si aún así nos decidimos a enviar algún tipo de imagen, conviene que tomemos cierto tipo de medidas de seguridad. Por ejemplo, es aconsejable encriptar tus datos para así dificultar el acceso de terceros.

Otra forma de protegerse es instalando en los dispositivos una solución de seguridad inteligente que proteja de manera eficaz contra posibles intrusiones.

No almacenar imágenes de otras personas desnudas o en ropa interior en tus dispositivos. Tampoco vídeos grabados entre amigos, ni fotos de menores, ni imágenes de antiguas parejas. En el caso de que seamos conocedores de que alguien dispone de imágenes nuestras, asegurarnos de que las eliminan.

Las víctimas de revenge porn además de mujeres jóvenes, son a menudo, jóvenes o adolescentes. Por ello, la comunicación entre padres e hijos es fundamental no sólo para prevenir, sino también para resolver conflictos.

No subir información sensible a ninguna red social, web de contactos o programas de mensajería instantánea. En caso de descubrir que alguien ha enviado imágenes nuestras a cualquiera de estos sitios, tenemos derecho a contactar directamente con el administrador y exigir su inmediata retirada de la web.

3.17. VIRUS INFORMÁTICO

Un virus es un software cuyo objetivo es alterar el funcionamiento normal del ordenador, sin el permiso o el conocimiento del usuario. Los virus, normalmente, sustituyen archivos ejecutables por otros infectados con el código de este. Los virus pueden destruir, de manera intencionada, los datos almacenados en un ordenador, aunque también existen otros más inofensivos, que solo producen molestias. Conocer los diferentes tipos de virus informáticos

existentes es el primer paso para garantizar una protección efectiva. Así, entre los más comunes destacan los siguientes:

- Virus residente. Son los que se alojan en la memoria RAM. Pueden interferir con el funcionamiento normal del sistema, provocando la corrupción de archivos y programas.
- Virus multipartito. Se propaga fácilmente en el sistema informático. Es muy contagioso y realiza acciones no autorizadas en el sistema operativo, en carpetas y otros programas del ordenador.
- Virus de acción directa. Ataca ciertos tipos de archivos, normalmente archivos .exe y .com. Su objetivo es replicar e infectar archivos en carpetas. Normalmente no suelen eliminar archivos ni afectar el rendimiento y la velocidad del equipo. Puede eliminarse de manera fácil con un antivirus.
- Secuestrador del navegador. Este virus infecta el navegador web. De este modo, cada vez que se introduzca un nombre de dominio en la barra de direcciones de Internet, el secuestrador del navegador abrirá varios sitios web falsos que pueden dañar el ordenador.
- Virus de secuencias de comandos web. Este virus vive en ciertos enlaces, anuncios, ubicación de imágenes, videos y diseño de un sitio web.
- Virus de macro. Los virus de macro se dirigen a aplicaciones y software que contienen macros, pueden realizar operaciones que afectan al rendimiento del programa o software.
- Virus de directorio. Se trata del virus más temido ya que cambia las rutas de los archivos.

Aparte de estos virus, existen muchos más como pueden ser los virus polimórficos, los cifrados, los virus que infectan archivos ejecutables o programas, los virus no residentes que se replican a través de módulos, los de tipo spacefiller, los virus FAT o los virus de red. Para evitar una infección de nuestro equipo por cualquiera de estos virus, es importante permanecer al día respecto a las últimas novedades en amenazas de seguridad, instalar las actualizaciones recomendadas en el ordenador, así como un software antivirus que pueda detectar, bloquear y eliminar todo tipo de virus.

3.18. ACCESO INDEBIDO A SISTEMAS

Tal y como su propio nombre indica, se trata del acceso no consentido a los archivos informáticos contenidos en un ordenador o sistema informático de almacenamiento. La publicación en el BOE de la Ley Orgánica 5/2010, de 22 de junio, que entró en vigor el día 23 de diciembre del año 2010, supuso la reforma de la Ley Orgánica 10/1995 que aprobó el vigente Código Penal. Con esta publicación modificaron tres tipos de delitos informáticos: la intrusión informática (art. 197.3 CP), la estafa informática (art. 248 CP) y los daños informáticos (art. 264 CP).

El articulo 197.3 CP en su nueva redacción, regula el llamado "acceso no consentido" o acceso ilícito a sistemas informáticos. De esta forma se castiga: (i) a quien accede a un sistema informático de manera no consentida, independientemente de si lleva a cabo algún tipo de daño en el sistema o algún perjuicio al propietario del equipo; (ii) a quien se mantiene dentro de un sistema informático en contra de la voluntad de quien tiene el legítimo derecho a excluirlo.

3.19. CIBERSTALKING

Con este nombre tenemos un tipo de acoso que se produce utilizando para ello las nuevas tecnologías, en concreto y principalmente Internet. Esta forma de acoso se caracteriza principalmente porque el autor del mismo realiza un exhaustivo seguimiento e investigación de manera constante de la información referente a una persona o empresa. Este tipo de actos son premeditados, repetitivos, obsesivos, y sobre todo, no deseados.

Los cyberstalkers, acceden a chats, foros, redes sociales y demás lugares públicos en la red con el objetivo de encontrar nuevas víctimas y mantener así el acoso sobre ellas. Valiéndose de estas, los acosadores siguen a las personas (víctimas), realizan acusaciones falsas sobre ellas, las amenazan, roban su identidad, pueden incluso llegar al punto de acceder a su información o al equipo en el que la almacenan y provocarle daños para que no puedan hacer uso de la misma. Todo esto, genera en la persona que lo sufre miedo, humillación y le afecta a la autoestima y su seguridad; también, llegado el caso puede llegar a destruir amistades, carreras y empresas. Los objetivos principales de estos cyberstalkers son las personas más vulnerables, es decir, mujeres, niños y grupos minoritarios.

Generalmente el autor de estos hechos suele ser una persona conocida o del entorno cercano a la víctima: un ex, un antiguo amigo, o alguien con motivaciones de odio, venganza, obsesión o control. Una de las dificultades que presenta es que para llevarlo a cabo, el acosador no necesita salir de su casa, sino que se aprovecha de la invisibilidad, el anonimato y distancia que ofrecen las tecnologías, para de ese modo poder actuar sin pensar en las consecuencias.

Aunque es complicado evitar que esto nos ocurra, en la actualidad hay herramientas que nos pueden ayudar a controlar y dar fin a la situación: guardar la información que pueda servirnos como evidencia (chats, correos, capturas de pantalla) y denunciar.

3.20. VISHING

El término vishing proviene de la unión de dos términos: voice y phishing, siendo este último un conocido ataque a través de la suplantación de la identidad de una persona, entidad, etc. (ya visto anteriormente). El vishing se realiza a través de una llamada de teléfono fraudulenta que se realiza con el objetivo de conseguir los datos personales o bancarios de una persona o entidad. Un ataque de vishing consta de dos pasos:

- En el primero nos encontramos con el ataque de "phishing". El ciberdelincuente tiene que haber conseguido previamente información confidencial a través de un correo electrónico o una web fraudulenta. A continuación y para continuar con el ataque necesita la clave SMS o token digital para así poder llevar a cabo y validar la operación.
- En el segundo paso es donde se encarga de obtener dicha clave para finalizar su ataque. Para conseguirla realiza una llamada telefónica a la víctima y se identifica como un trabajador del banco. El objetivo de esta llamada es que el usuario facilite la clave recibida a través de SMS o token digital. Éstos son tan importantes ya que son la clave para poder autorizar transacciones.

4. FACTORES Y TEORÍAS QUE INFLUYEN EN EL FENÓMENO DE LA CIBERDELINCUENCIA.

Para hablar de la criminología, debemos entenderla como un modelo teórico que trata de explicar la delincuencia, así que para razonar la criminalidad analizando el problema, habría que tratarla desde sus causas hasta sus consecuencias.

Esto no quiere decir que por cada delito que se cometa vaya a existir una teoría o que podamos encontrar una teoría aún mayor que pueda calificar todos los delitos, sino que la mayoría de ellas tratan de explicar la mayor parte de delitos, ajustándose a ellos en mayor o menor medida.

La teoría considerada hasta estas fechas como el único modelo que es capaz de explicar la delincuencia en el ciberespacio, es la **teoría de la transición en el espacio** (K.Jaishankar), y para eso se basa en las siguientes premisas:

1. *Las personas que se reprimen de la conducta criminal en el **espacio físico** debido a su estatus tienen una propensión a cometer delitos en el **ciberespacio**.*
2. *La **identidad flexible**, el **anonimato** disociativo, y la **falta** del factor de **disuasión** en el ciberespacio provee a los ciberdelincuentes de los elementos para la elección de cometer cibercrímenes.*
3. *La conducta criminal de los agresores en el ciberespacio es probable que sea **importada** al espacio físico, y también puede, a su vez, ser **exportada** al ciberespacio.*
4. *La aventura intermitente de los agresores en el ciberespacio y la dinámica espacio-temporal natural del ciberespacio provee la oportunidad de **escape** para ellos.*

5. *Los **extraños** se unen en mayor medida en el ciberespacio que en el espacio físico para cometer delitos. Las personas que se asocian en un espacio físico son proclives a que también lo hagan en el ciberespacio.*
6. *Las personas que pertenecen a **sociedades cerradas** tienen mayor probabilidad de cometer delitos que las personas de sociedades abiertas.*
7. *El **conflicto de normas y valores del espacio físico** con las normas y valores del ciberespacio pueden conducir a la comisión de ciberdelitos.*

Estos puntos pretenden explicar la ciberdelincuencia desde diferentes puntos de vista, convirtiéndola así en una teoría **integradora** y como opción a explicar cualquier ejemplo de cibercrimen.

El Triángulo del cibercrimen

Este concepto trata el cibercrimen desde una triple perspectiva**.**

Por una parte tenemos el **efecto criminógeno de la Red,** y esto se debe a las propias características de esta, como puede ser:

- Facilidad de acceso,
- El anonimato o
- El efecto llamada.

A partir de esto último y sabiendo del conocimiento que a nivel general tienen los usuarios de la Red, ésta se ha convertido en un campo perfecto para que surjan nuevas oportunidades delictivas**,** además esto ha provocado que los delitos comunes (estafa) se hayan trasladado a la red.

Igualmente nos encontramos con la escasez de personal capacidad para prevenir y parar la delincuencia en la Red.

Explicación del Control Social

Para prevenir la ciberdelincuencia, hablamos indirectamente de **controles**, o lo que es lo mismo, medios que puedan influir en la realización o no de delitos, es por lo que si existen penas, medidas o agentes de seguridad que persigan y condenen los delitos en el ciberespacio, esto haría que muchos delincuentes se lo pensaran mejor antes de cometer un ilícito, a estas acciones se les denomina **control formal,** desde este punto de vista nos encontramos personal especializado que es capaz de interceptar el virus, y puede llevar a un proceso con pena de multa cuantiosa.

Por otro lado, el **control informal** se refiere a «frenos a la delincuencia» desde otras perspectivas sociales o familiares.

Estos controles son de suma importancia a la hora de su aplicación para prevenir la ciberdelincuencia, siendo el más destacable el **control social informal** para hacer que una persona no llegue a delinquir.

Los principales factores que hacen que los ciberdelincuentes no actúen, serían el **factor humano y la ciberseguridad**, la **preparación** del profesional a cargo de dicha ciberseguridad, las **herramientas** tecnológicas de las que disponga, la **inversión** económica que haga la empresa en ciberseguridad, etc.

Debemos mencionar, que el **error humano** es la causa principal de infracciones de datos y no los ciberdelincuentes en si. En este punto es donde las compañías deben chequear y revisar sus protocolos, porque es ahí donde los expertos analistas destacan la carencia de visibilidad y contexto sobre cómo y dónde se usan los datos: este escenario es el que le ofrece al ciberdelincuente la oportunidad de atacar.

Podemos destacar que el **Factor Humano es la solución de la Ciberseguridad**, ya que habitualmente los mismos humanos pueden ser la línea de defensa más fuerte y poder actuar como medidas de advertencia y choque frente al **ciberespionaje** y los **ciberataques, así que** estudiando el comportamiento humano y analizando los riesgos, se permitiría a los expertos en ciberseguridad identificar con mayor rapidez las anomalías y obtener la máxima información para poder analizar las alertas de actividad de las redes maliciosas.

Si se le da este valor a la **seguridad informática**, le damos mayor importancia al ser humano que está delante de la pantalla y no al ciberdelincuente.

*Según Enrique Domínguez, director de Estrategia de Entelgy Innotec Security, división de ciberseguridad de Entelgy: "***el factor humano** *influye de forma clave en un 80% de los ciberataques", "es por esto que recomendamos a las empresas que vayan más allá de la detección y hagan especial hincapié en concienciar a sus empleados para que se conviertan en cortafuegos ante estos ataques, formándoles en hábitos seguros en el uso de herramientas digitales".*

Para finalizar, debemos tener claro que la seguridad digital tiene dos importantes vertientes, una es el componente técnico y la otra la parte humana, ambas dependen la una de la otra para lograr que nuestros sistemas sean lo más seguros posible.

5. LEGISLACIÓN APLICABLE E IDENTIFICACIÓN DE LOS PRINCIPALES DELITOS QUE SE COMETEN

En este apartado pasamos a identificar y correlacionar cada una de las conductas anteriormente descritas con el correspondiente hecho delictivo y su articulado en nuestro Código Penal.

5.1. TIPIFICACIÓN EN NUESTRO CODIGO PENAL

Según se establece en nuestro Código Penal, los delitos informáticos cometidos normalmente por los ciberdelincuentes son:

- Delitos contra la intimidad: El acoso, el descubrimiento y la revelación de secretos o la vulneración de la intimidad de las personas, invadiendo por ejemplo los correos electrónicos o incluso interceptando el envío de documentos.
- Amenazas
- Alteración, destrucción o los daños de datos, programas o documentos electrónicos ajenos.
- La pornografía infantil y el exhibicionismo, conductas favorecidas por el anonimato que proporciona la red.
- Delitos contra el honor: Las injurias y las calumnias, normalmente cometidas en redes sociales, foros o por correo electrónico.
- Estafa.

En este caso dependiendo de la conducta realizada por el delincuente, estará cometiendo un tipo delictivo u otro, no obstante, los delitos más comúnmente cometidos con este tipo de actividades son:

5.1.1.- Delito de acoso, artículo 172 Ter del CP

Según lo establecido en el artículo 172 ter *"Será castigado con la pena de prisión de tres meses a dos años o multa de seis a veinticuatro meses el que acose a una persona llevando a cabo de forma insistente y reiterada, y sin estar legítimamente autorizado, alguna de las conductas siguientes y, de este modo, altere gravemente el desarrollo de su vida cotidiana:*

1.ª La vigile, la persiga o busque su cercanía física.

2.ª Establezca o intente establecer contacto con ella a través de cualquier medio de comunicación, o por medio de terceras personas.

3.ª Mediante el uso indebido de sus datos personales, adquiera productos o mercancías, o contrate servicios, o haga que terceras personas se pongan en contacto con ella.

4.ª Atente contra su libertad o contra su patrimonio, o contra la libertad o patrimonio de otra persona próxima a ella."

Como podemos ver, en este caso cometerían acoso aquellos que mediante el uso de las nuevas tecnologías, hostigan, coaccionan, y acosan o sus víctimas de manera reiterada e insistente, sin contar con la legítima autorización de la persona acosada. Aquí la conducta del acosador, altera de

manera grave el desarrollo de la vida cotidiana de su víctima, mediante la vigilancia, persecución o incluso dando un paso más allá y buscando el contacto físico con la víctima. Los medios que puede emplear el acosador para llevar a cabo el delito son entre otros:

- Envío de lenguaje amenazante
- Publicación de fotos, videos o rumores para deshonrar la reputación de la víctima

5.1.2.- Delito de descubrimiento y revelación de secreto, sexting artículo 197 del CP

Delito tipificado en el artículo 197.1 y 197.2 del Código Penal, que dice:

"1. El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales, intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.

2. Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero."

En este primer caso, el bien jurídico protegido es la intimidad, un derecho fundamental reconocido en el artículo 18 de la Constitución Española. El sujeto pasivo en estos delitos puede ser cualquier persona física, y también las personas jurídicas. Para diferenciar la conducta típica de la mera indiscreción es necesario que lo comunicado afecte a la esfera de la intimidad que el titular quiere defender.

Existe un tipo específico consistente en la difusión de imágenes o grabaciones obtenidas con anuencia, este se especifica en el punto 7 de este mismo artículo, que dice (art. 197.7 CP) *"Será castigado con una pena de prisión de tres meses a un año o multa de seis a doce meses el que, sin autorización de la persona afectada, difunda, revele o ceda a terceros imágenes o grabaciones audiovisuales de aquélla que hubiera obtenido con su anuencia en un domicilio o en cualquier otro lugar fuera del alcance de la mirada de terceros, cuando la divulgación menoscabe gravemente la intimidad personal de esa persona."*

Este tipo protege la intimidad personal en relación con materiales fotográficos o audiovisuales cuya difusión puede generar un menoscabo grave. La conducta se construye sobre un primer estadio en el que el material se obtiene con consentimiento del afectado y sobre un segundo estadio en el que la difusión se produce sin tal consentimiento. Incluye las conductas de sexting y revenge porn, conceptos ya mencionados en la presente publicación. La acción típica básica consiste en la «difusión», «revelación» o «cesión» de imágenes o grabaciones audiovisuales, a la que se adiciona un elemento subjetivo consistente en la intención de

menoscabar la intimidad ajena. Además prevé una agravación cuando la víctima sea el cónyuge o ex cónyuge del sujeto pasivo o persona que conviva o haya convivido con él o mantenga o haya mantenido una relación análoga.

5.1.3.- Delitos relacionados con la libertad e indemnidad sexual, acoso, abusos y exhibicionismos sexuales artículo 183 ter y 189 del CP

Delito tipificado en el artículo 183 ter del Código Penal, que dice: *"1. El que a través de internet, del teléfono o de cualquier otra tecnología de la información y la comunicación contacte con un menor de dieciséis años y proponga concertar un encuentro con el mismo a fin de cometer cualquiera de los delitos descritos en los artículos 183 y 189, siempre que tal propuesta se acompañe de actos materiales encaminados al acercamiento, será castigado con la pena de uno a tres años de prisión o multa de doce a veinticuatro meses, sin perjuicio de las penas correspondientes a los delitos en su caso cometidos. Las penas se impondrán en su mitad superior cuando el acercamiento se obtenga mediante coacción, intimidación o engaño.*

2. El que a través de internet, del teléfono o de cualquier otra tecnología de la información y la comunicación contacte con un menor de dieciséis años y realice actos dirigidos a embaucarle para que le facilite material pornográfico o le muestre imágenes pornográficas en las que se represente o aparezca un menor, será castigado con una pena de prisión de seis meses a dos años."

Aquí nuestro Código Penal castiga todo acto o intento de contacto directo o personal así como el contacto virtual, todo ello relacionado con las peticiones y contenidos sexuales dirigidos a menores de edad por parte de mayores de edad. Cuando los hechos los realiza mediante intimidación, coacción o engaño aplica las penas previstas en su mitad superior.

En la misma línea nos encontramos con el art. 189 en el cual, en este caso se castigan los actos de exhibición, venta, distribución de material pornográfico en el que intervengan menores de edad

5.1.4.- Delitos contra el honor. Calumnias e Injurias artículos 205 y 208 del CP

Según el artículo 205 de nuestro Código Penal: *"Es calumnia la imputación de un delito hecha con conocimiento de su falsedad o temerario desprecio hacia la verdad."* e injurias según el artículo 208 son *"la acción o expresión que lesionan la dignidad de otra persona, menoscabando su fama o atentando contra su propia estimación."*

Por tanto, cometerán injurias y calumnias todos aquellos que aprovechando el anonimato que ofrecen internet y las redes sociales aprovechen para lesionar la dignidad de otras personas o acusarlos de la comisión de hechos delictivos aun sabiendo de su falsedad. Estos delitos suelen ser cometidos normalmente por exparejas, seguidores envidiosos o incluso antiguas amistades que tras romper relaciones y no terminar de muy buenas maneras, buscan su acto de venganza

mediante publicaciones ofensivas hacia la persona con el fin de menoscabar la reputación de esa persona.

5.1.5.- Delitos contra el Patrimonio y el Orden Socioeconómico. Extorsión, Estafa y Daños artículos 243, 248 y 264 del CP

En cuanto a la Extorsión nuestro Código Penal dispone: *"El que, con ánimo de lucro, obligare a otro, con violencia o intimidación, a realizar u omitir un acto o negocio jurídico en perjuicio de su patrimonio o del de un tercero, será castigado con la pena de prisión de uno a cinco años, sin perjuicio de las que pudieran imponerse por los actos de violencia física realizados."*

En este caso se produce la extorsión cuando a través de Internet el extorsionador exige cantidad económica para que la víctima se la abone a cambio de no difundir imágenes comprometedoras de la víctima, o de no hacer daño a los archivos del ordenador a los que ha accedido de manera fraudulenta utilizando Internet para ello, tal y como hemos visto en los términos y acciones nombrados en el punto anterior (Ransomware, Sextorsión, hacking, piratería informática, acceso indebido a los sistemas, etc.).

En el caso de la estafa utilizando medios informáticos tenemos que el artículo 248 del Código penal considera, entre otros, que son reos de 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 valiéndose de alguna manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro.*

En este caso los actos de los que se valen los ciber delincuentes para la comisión de estafas son el phishing, vishing, scam y hacking entre otros.

Respecto a los daños, nuestro Código Penal dispone en su artículo 264.1 lo siguiente: *"El que por cualquier medio, sin autorización y de manera grave borrase, dañase, deteriorase, alterase, suprimiese o hiciese inaccesibles datos informáticos, programas informáticos o documentos electrónicos ajenos, cuando el resultado producido fuera grave, será castigado con la pena de prisión de seis meses a tres años."* Las acciones más comunes que provocan este tipo de daños y que pueden incurrir en este tipo delictivo son Ransomware, hacking y el acceso indebido a sistemas.

5.1.6.- Delitos contra la usurpación del estado civil. Usurpación de identidad artículo 401 del CP

Delito tipificado en el artículo 401 del Código Penal, que dispone al respecto *"El que usurpare el estado civil de otro será castigado con la pena de prisión de seis meses a tres años."*

En este caso la acción consiste en apropiarse una persona de la identidad de otra, haciéndose pasar por ella para acceder a recursos y beneficios. Este artículo no exige que la suplantación de la identidad tenga que realizarse en perjuicio del suplantado. Tal y como se expuso con anterioridad, uno de los principales fines de los suplantadores es poder conseguir

dinero, préstamos o créditos en nombre de aquellas personas a las que roban la identidad, celebrar contratos, e incluso cometer ilícitos penales, como por ejemplo los delitos de injurias y calumnias que cometa el autor del delito haciéndose pasar por otro. Para evitar ser víctimas de un posible robo de identidad en la red, es necesario que se sigan los consejos anotados en el punto 3.8 de la presente publicación.

6.- BIBLIOGRAFÍA

- Wikipedia
- Derechodelared.com – martaviolat. Criminóloga, Cibercrimen y Ciberseguridad
- Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.
- Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal
- Ley Orgánica 1/2004, de 28 de diciembre, de Medidas de Protección Integral contra la Violencia de Género.
- Ley 13/2007, de 26 de noviembre, de medidas de prevención y protección integral contra la violencia de género.
- https://www.researchgate.net/figure/Figura-2-Fases-de-la-dinamica-de-Ciberabuso-Sexual-Juvenil-CAS-J_fig1_275273999
- https://www.legaltoday.com/practica-juridica/derecho-civil/nuevas-tecnologias-civil
- http://www.catb.org/~esr/faqs/hacker-howto.html
- https://www.tecnologia-informatica.com/pirateria-informatica/
- https://www.pandasecurity.com/es/security-info
- https://www.legalitas.com