Parte IV
Delitos informáticos

Siempre que se habla de los delitos cometidos a través de Internet se dice lo mismo: la red de redes no ha creado nuevas tipologías de delitos. Estos son los mismos de siempre. Lo que ha cambiado son las herramientas mediante los que se cometen, así como la complejidad de su investigación. Hoy en día, gracias a Internet, es posible sufrir un delito en Girona, cometido por un autor que reside en China y que ha accedido a datos confidenciales que la víctima tenía almacenados en un servidor de Estados Unidos. Un ejemplo de algo que parece tan rebuscado es el robo de nuestras credenciales como vendedor en Ebay, por ejemplo. O de nuestra contraseña de acceso a Facebook. ¡Así de sencillo!

Aunar todas estas circunstancias en una investigación, con diferentes nacionalidades y legislaciones; con diferentes organismos policiales y judiciales implicados y con políticas más o menos colaboradoras con la investigación de los mismos es algo a lo que todo investigador de la red se enfrenta, y su solución es aún la gran asignatura pendiente de Internet. Desde el punto de vista policial quizás la situación sea algo más sencilla, ya que el objetivo final es el de informar a la autoridad judicial de dónde están los datos y a quién hay que pedírselos para identificar al autor del delito informático, quedando en manos judiciales la "pelea burocrática" para realizar esos trámites. Es por ello que otra cosa que ha traído Internet a la investigación policial es la falta de inmediatez a la hora de detener a los autores de un delito. Incluso más, la no detención de los autores por encontrarse generalmente estos fuera del país, dejando en manos de autoridades de otros estados la persecución de los delitos investigados, cosa que se realiza mediante organismos policiales internaciones como Interpol o Europol y, a nivel judicial, mediante las correspondiente comisiones rogatorias. En resumen: En el investigador de delitos informáticos se genera un cierto grado de frustración. Es por ello que la labor informativa a los ciudadanos, siempre necesaria para evitar todo tipo de delitos, sea en los de este tipo quizás más necesaria y una de las acciones policiales más directa en los delitos informáticos más comunes, aunque en los delitos cometidos fuera de la red, los habituales hasta ahora, haya sido siempre algo muy secundario.

Pues bien, en esta sección vamos a analizar los delitos informáticos más comunes, siempre teniendo en cuenta que este es un curso básico y que debido a ello, es totalmente imposible abarcarlos todos, pues los más complicados requieren de conocimientos, técnicas y programas informáticos que por su complejidad, quedan muy lejos de éste nivel.

En la mayoría de estos delitos veremos que no se utilizan herramientas informáticas sofisticadas, como pudieran ser virus, sniffers o conocimientos avanzados de vulnerabilidades, sino que casi todo ellos se comenten mediante el engaño y la simulación, técnicas utilizadas desde el principio de los tiempos para estafar y que en el ámbito de los hackers informáticos son conocidas como *"ingeniería social"*.

9. Ingeniería social

En el campo de la seguridad informática, ingeniería social es la habilidad para conseguir información confidencial a través de la manipulación de usuarios legítimos.

El principio que sustenta la ingeniería social es el que en cualquier sistema, en lo referente a la seguridad, "los usuarios son el eslabón débil". En la práctica, un ingeniero social usará comúnmente el teléfono o Internet para engañar a la gente, fingiendo ser, por ejemplo, un empleado de algún banco o alguna otra empresa, un compañero de trabajo, un técnico o un cliente. Vía Internet o la web se usa, adicionalmente, el envío de solicitudes de renovación de permisos de acceso a páginas web o correos electrónicos falsos que solicitan estos datos confidenciales, e incluso las famosas "cadenas", llegando así a revelar información sensible, o a violar las políticas de seguridad típicas. Con este método, los ingenieros sociales aprovechan la tendencia natural de la gente a reaccionar de manera predecible en ciertas situaciones, -por ejemplo proporcionando detalles financieros a un aparentemente empleado de un banco- en lugar de tener que encontrar agujeros de seguridad en los sistemas informáticos.

Quizá el ataque más simple pero muy efectivo sea engañar a un usuario llevándolo a pensar que un administrador del sistema esta solicitando una contraseña para varios propósitos legítimos. Los usuarios de sistemas de Internet frecuentemente reciben mensajes que solicitan contraseñas o información de tarjetas de crédito, con el motivo de "crear una cuenta", "reactivar una configuración", u otra operación benigna; a este

tipo de ataques se los llama phishing (pesca) y lo veremos con más detalle a continuación.

La principal defensa contra la ingeniería social es educar y entrenar a los usuarios en el uso de políticas de seguridad y asegurarse de que estas sean seguidas.

Uno de los ingenieros sociales más famosos de los últimos tiempos es Kevin Mitnick. Según su opinión, la ingenier´ıa social se basa en estos cuatro principios:

1. Todos queremos ayudar.
2. El primer movimiento es siempre de confianza hacia el otro.
3. No nos gusta decir No.
4. A todos nos gusta que nos alaben.

Explotando estos principios es posible conseguir información confidencial y utilizarla posteriormente contra su legítimo dueño.

10. Los delitos informáticos más comunes

Los delitos informáticos más usuales con los siguientes:

- Estafas.
- Amenazas.
- Insultos.
- Abusos sexuales a menores (grooming).
- Pedofilia.
- Suplantación de identidad.
- Contra la propiedad intelectual.
- Daños y revelación de secretos.

10.1. Estafas.

10.1.1. Phishing

Consiste en la obtención, mediante engaño, de las contraseñas de acceso a servicios de la banca online o a cuentas de vendedores de productos, como por ejemplo, de Ebay. Los datos de acceso se consiguen mediante el envío masivo de correos, utilizando técnicas de Spam, simulando un mensaje de una determinada entidad. Estos mensajes remiten a un servidor que simula la web del servicio que se quiere suplantar. La v´ıctima introduce sus datos de acceso, que son capturados por el estafador.

Las ”cibermulas” Una vez con los datos de acceso a una cuenta corriente online, el estafador puede realizar transferencias, pero si lo hace a una cuenta que esté a su nombre, quedará inmediatamente identificado como el receptor del dinero “robado” a través de Internet. ¿Cómo soluciona éste problema? Busca colaboradores que se ofrezcan a recibir el dinero robado en sus cuentas, para posteriormente, enviárselo a él mediante Wester Unión. Pero ¿quién pude ofrecerse para esto, si quedaría inmediatamente identificado como el receptor del dinero? Pues mucha gente... ¡engañada, claro!

Igual que el estafador envía millones de correos electrónicos simulando ser una entidad bancaria, a la espera de que algún incauto “pique” y facilite sus datos de conexión, hace lo mismo simulando ser una multinacional extranjera que carece de oficinas en España y solicitando personas que cómodamente, dedicando muy poco tiempo a la semana, quieran trabajar para ella y así poder ganas mucho dinero con el tan manido “trabaje desde casa”. Todo aquel que “pica” en estas ofertas recibe información sobre la supuesta multinacional, que le envía muchos certificados y contratos, y que lo único que necesita del solicitante del trabajo es que disponga de una cuenta corriente donde recibir el dinero de os clientes en España para remitirlo inmediatamente a sus oficinas centrales.

Los "trabajadores" que envían sus cuentas, enseguida reciben varias transferencias que deben de reenviar en el mismo día de su recepción, tras quedarse dicho trabajador con el 10 % del dinero recibido, siempre por Wester Unión. A los pocos días estas "cibermulas" son imputadas por la policía como colaboradores necesarios en la comisión de un delito de estafa, ya que son las únicas identificadas por el banco y han colaborado en el robo del dine- ro, haciéndolo desaparecer. ¿Cómo? El destinatario del dinero que se envía por Wester Unión no queda identificado ya que este sistema de envío de dinero, ideado para remitir pequeñas cantidades de dinero (hasta 3000 ⇛) sin necesidad de documentos de identidad, solamente requiere que se sepa el nombre y la cantidad justa de dinero que se ha enviado para que éste se entregado a su destinatario. Es decir, es posible enviar 3000⇛ a "Perico el de los palotes" a la oficina de Londres y cualquier persona que sepa que en el día de hoy se ha enviado este dinero a nombre de este perico solamente tiene que pedirlo en dicha oficina para que se lo entreguen sin más trámites, y sin necesidad de que el receptor se identifique. ¡Dinero desaparecido!

Figura 8: Texto remitido en un correo para Phishing. Siempre llama la atención su mala redacción.

10.1.2. Phishing-car

Estafa similar al phishing, pero en esta ocasión especializada en la compra-venta de vehículos.

En la venta: Consiste en el pago con un cheque superior a la cantidad pedida por el vehículo. El vendedor debe de enviar la diferencia al estafador. Para ello siempre se alega que es un cheque de empresa, o un presupuesto ya cerrado que se pagó por adelantado y que si el vendedor acepta, pueden repartirse la diferencia entre ambos. Para ello, inmediatamente a la recepción del cheque, el vendedor, por Wester Unión, debe de hacerle llegar la comprador su parte de esa diferencia. Con el tiempo, se descubre que el cheque es falso. Un ejemplo:

El comprador, residente en el extranjero, necesita que, por exigencias de la ley, el vendedor realice un depósito de 3000 ⇛ (por Wester Unión) para poder sacar del país la cantidad pedida por el vendedor por el coche. O por ser el comprador representante de una empresa, que le dado un cheque por 12000 ⇛ para la compra de un vehículo, está dispuesto a enviárselo al vendedor, que puso su coche a la venta en Internet por 8000⇛, si éste le envía por Wester Unión la cantidad de 2000 ⇛ (los otros 2000 de la diferencia son "de regalo" para el vendedor).

En la compra: La víctima debe de enviar el dinero por Wester Unión al supuesto vendedor, quien previamente le ha hecho llegar a la víctima un documento justificativo de una falsa empresa aseguradora que garantiza que el vehículo está en su poder y le será entregado al comprador en el momento en que el vendedor reciba el dinero. Además, se le facilita una página web y un número de tiket de seguimiento, mediante el que puede saber en todo momento en qué lugar se encuentra el coche comprado. La página web de la empresa aseguradora ha sido creada por el propio estafador y desaparecerá a los pocos días.

En estos tipos de delitos, el estafador no se suele conformar con el primer envío de dinero que recibe de la víctima. Es frecuente que, ante las reclamaciones de falta de información por parte del comprador, se le conteste que hay problemas aduaneros y que debe de pagar 3000⇛ más (siempre por Wester Unión) para desmovilizar en coche de la frontera, etc. etc.

10.2. Distribución de pornografía infantil.

La paidofilia o pedofilia es la inclinación sexual por parte de adultos a sentir una atracción primaria hacia niños.

Se considera "paidofilia" etimológicamente más correcto que "pedofilia", si bien esta segunda forma es más usada. En el lenguaje común, pedófilos son considerados aquellos que abusan sexualmente de niños.

El término "pedofilia" se ha visto confundido con el término "pederastia". A pesar de que etimológicamente significan lo mismo (ya que ambas se basan en paidós: "niño" o "adolescente"), la pedofilia no se refiere al abuso sexual, sino a la mera tendencia sexual o atracción de un hombre adulto hacia un menor. La pederestia sería el abuso sexual de estos menores.

Los "pedófilos" han encontrado en Internet un medio excelente para localizar y compartir imágenes y vídeos con contenidos sexuales de su agrado, existiendo una gran comunidad en la red. Debido a ello ha surgido el negocio de la pedofilia. En determinados países del Este, Sudamérica y Asia se están grabando películas e imágenes (donde se viola de forma sistemática a decenas de niños y niñas) que son ofertadas por la red. Finalmente, existen movimientos sociales que defienden el amor libre entre niños y adultos (ej. NAMBLA) que han encontrado en Internet un medio para darse a conocer y distribuir su propaganda.

En España, la simple tenencia de material de contenido pedófilo es un delito. Generalmente este material se distribuye mediante programas de descarga que utilizan la red Edonkey 2000, es decir, programas P2P (emule, Ares, Mldonkey, etc.) y su investigación es complicada. En la actualidad existe programas policiales especialmente dedicados a la investigación de estos delitos, los cuales quedan, debido a su complejidad, fuera de este curso, ya que se necesitan conocimientos bastante más avanzados que los que requiere un curso básico como este.

10.3. Abusos sexuales de menores: Grooming

El grooming de niños por Internet (o simplemente grooming) consiste en acciones deliberadas por parte de un/a adulto/a de cara a establecer lazos de amistad con un niño o niña en Internet, con el objetivo de obtener una satisfacción sexual mediante imágenes eróticas o pornográficas del menor o incluso como preparación para un encuentro sexual, posiblemente por medio de abusos.

En inglés, para diferenciarlo del significado original relativo al acicalado de animales se suelen utilizar los términos *child grooming* o *internet grooming*.

10.3.1. El proceso de grooming

El grooming habitualmente es un proceso que puede durar semanas o incluso meses, y que suele pasar por las siguientes fases, de manera más o menos rápida según diversas circunstancias:

Figura 9: Grooming de menores.

1. El adulto procede a elaborar lazos emocionales (de amistad) con el/la menor, normalmente simulando ser otro niño o niña.
2. El adulto va obteniendo datos personales y de contacto del/a menor.
3. Utilizando tácticas como la seducción, la provocación, el envío de imágenes de contenido pornográfico, consigue finalmente que el/la menor se desnude o realice actos de naturaleza sexual frente a la webcam o envíe fotografías de igual tipo.
4. Entonces se inicia el ciber-acoso, chantajeando a la víctima para obtener cada vez más material pornográfico o tener un encuentro físico con el/la menor para abusar sexualmente de él/ella.

10.4. Suplantación de identidad.

Aunque "suplantación de identidad" es utilizado también como término similar al phishing, al ser la finalidad de éste la de obtener los datos identificativos del titular de una cuenta bancaria y "suplantar" su identidad a la hora de realizar una transferencia, la suplantación de identidad no está limitada solamente a esto. Existen otras forma de suplantar la identidad de las personas a través de Internet:

- Para hacerse pasar por otra persona en las redes sociales (facebook, twitter, identi.ca...) y desprestigiarla, obtener contactos, acceder a sus amigos, concretar falsas citas en su nombre, etc.
- Suplantar páginas web o atribuirse la autoría de un producto, obra artística, musical, etc.
- Acceder a información conficencial de una persona o empresa...

10.5. Contra la propiedad intelectual.

La propiedad intelectual es un derecho patrimonial de carácter exclusivo que otorga el Estado por un tiempo determinado para usar o explotar en forma industrial y comercial las invenciones o innovaciones, tales como un producto técnicamente nuevo, una mejora a una máquina o aparato, un diseño original para hacer más útil o atractivo un producto o un proceso de fabricación novedoso; también tiene que ver con la capacidad creativa de la mente: las invenciones, las obras literarias y artísticas, los símbolos, los nombres, las imágenes y privilegios.

La propiedad intelectual se clasifica en dos categor´ıas:

Propiedad industrial: Incluye las invenciones, marcas, patentes, dibujos y modelos industriales, as´ı como indicaciones geográficas de origen.

Derechos de autor: Las obras literarias y art´ısticas, es decir, se refieren a los derechos que tienen los artistas sobre sus obras, los derechos de los intérpretes sobre sus ejecuciones e interpretaciones, los derechos de los autores de fonogramas sobre sus grabaciones y los derechos de las empresas de radiodifusión sobre sus programas, tanto de radio como de televisión.

Estos derechos son defendidos por un amplio grupo de asociaciones que constantemente denuncian que son vulnerados en Internet, al existir una distribución libre y sin control de libros electrónicos, programas informáticos, música y películas que tienen sus derechos reservados. Aquí, al igual que en los de pedofilia, las redes P2P (eMule, Ares, etc.) son las más utilizadas y debido a su complejidad, tal y como se dijo en el otro caso, queda fueran de este curso.

10.6. Daños y revelación de secretos.

La información, a pesar de ser un bien intangible, está protegida por el marco legal, por lo que la acción de destrucción o alteración de datos, programas o cualquier otro tipo de información digital se considerada un delito de daños.

La información en su formato digital, contabilidad, las bases de datos, la facturación de una empresa, su listado de clientes, el estado de cuentas de una entidad financiera... todo ello configura un nuevo activo patrimonial que está protegido por la Ley. El delito de daños ocurre cuando, rompiendo contraseñas, aprovechando vulnerabilidades o utilizando de forma ilegal las propias contraseñas de acceso, se accede a un servidor u otro tipo de ordenador y se destruyen todos o parte de los datos que contiene.

la revelación de secretos ocurriría cuando estos datos fueran copiados y utilizados en provecho del delincuente.

Es por ello que dentro de esta sección se cometen muchos delitos que el investigador debería de valorar antes de comenzar su actuación. No es lo mismo que se acceda aprovechando una vulnerabilidad a los servidores de una gran empresa, a que se le robe el fichero de clientes de su ordenador personal a un autónomo que solamente utiliza una simple hoja de cálculo para almacenar esos datos. En el primer caso se necesita de un complicadísimo análisis forense que suele realizarse por expertos y en el segundo puede deberse simplemente a que la v´ıctima tiene una carpeta compartida y la red wifi de su domicilio abierta, por lo que cualquiera que haya accedido a la misma ha podido copiar el archivo. Una vez más hay que recordar que esto es un curso básico.

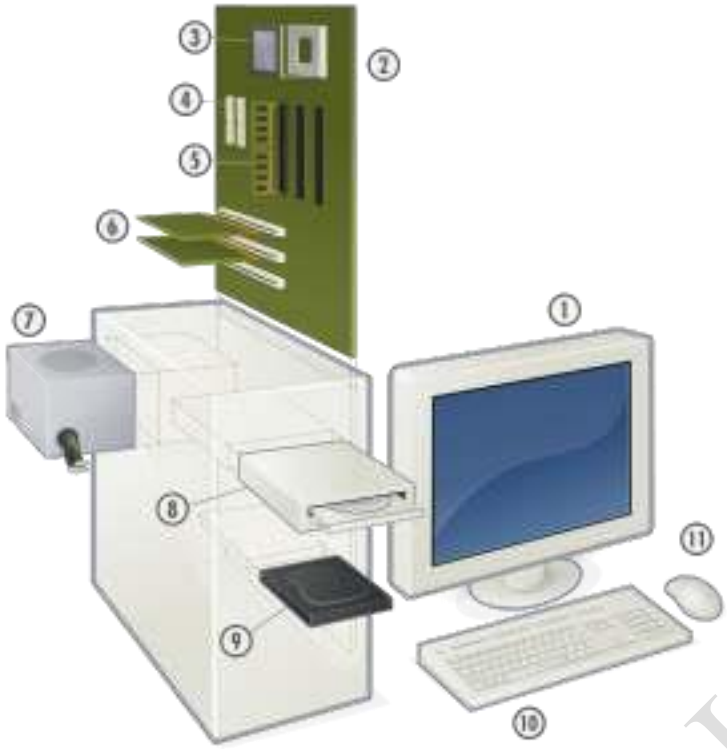

Figura 10: Vista expandida de una computadora personal. 1: Monitor 2: Placa base 3: Procesador 4: Puertos ATA 5: Memoria principal (RAM) 6: Placas de expansión 7: Fuente de alimentación 8: Unidad de almacenamiento óptico 9: Disco duro, Unidad de estado sólido 10: Teclado 11: Ratón

Parte V
Obtención de datos probatorios

En esta parte nos centraremos en qué datos son de interés a la hora de tener que investigar cualquier tipo de delito y en cómo aportarlos correctamente en cualquier informe o diligencia.

11. Intervención de hardware

11.1. Qué es hardware

Hardware es como se denomina a todas las partes f´ısicas y tangibles de una computadora: sus componentes eléctricos, electrónicos, electromecánicos y mecánicos; sus cables o cajas, periféricos de todo tipo y cualquier otro elemento físico involucrado; contrariamente al soporte lógico e intangible que es llamado software.

Un sistema informático se compone de una unidad central de procesamiento (CPU), encargada de procesar los datos, uno o varios periféricos de entrada, los que permiten el ingreso de la información y uno o varios periféricos de salida, los que posibilitan dar salida (normalmente en forma visual o auditiva) a los datos.

11.2. Tipos de hardware

Una de las formas de clasificar el Hardware es en dos categorías: por un lado, el ”básico”, que abarca el conjunto de componentes indispensables necesarios para otorgar la funcionalidad m´ınima a una computadora, y por otro lado, el ”Hardware complementario”, que, como su nombre indica, es el utilizado para realizar