universidad de león

FACULTAD DE DERECHO
UNIVERSIDAD DE LEÓN
CURSO 2021/2022

FRAUDE INFORMÁTICO: PHISHING

COMPUTER FRAUD: PHISHING

MÁSTER EN DERECHO DE LA CIBERSEGURIDAD Y ENTORNO DIGITAL

AUTOR: D. MIGUEL ZOÉ ESPINOSA PÉREZ

TUTORA: PROF. MARÍA ANUNCIACIÓN TRAPERO BARREALES

ÍNDICE

ÍNDICE DE ABREVIATURAS

Art./s :	Artículo/s.
Coord/S:	Coordinador/es
CP:	Código Penal
Dir./s:	Director/es
Ed/s.:	Editor/es
INCIBE:	Instituto Nacional de Ciberseguridad de España
LSSICE:	Ley 34/2002 Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
NFT-	Token no fungible
Núm.:	Número
RGPD:	Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)
SAP:	Sentencia de la Audiencia Provincial
STS	Sentencia del Tribunal Supremo
Secc:	Sección
TIC:	Tecnologías de la Información y la Comunicación

RESUMEN

Este trabajo trata sobre el Phishing y la respuesta del Derecho penal frente a este comportamiento defraudatorio. Con carácter previo se dan unas breves nociones sobre el Phishing simple, medio y avanzado, con especial atención a los supuestos que han aparecido durante la pandemia del coronavirus, así como unas nociones básicas y simplificadas de los malware más frecuentes. Con esta explicación previa se entra a analizar la respuesta penal frente al fraude informático, el art. 248.2 CP, un precepto penal que se ha incorporado a este texto punitivo desde el año 1995 (es decir, antes de que se aprobara el principal texto internacional en la prevención de ciberdelitos, el Convenio del Consejo de Europa sobre cibercriminalidad).

La competitividad y la competencia en el sector económico abren la puerta a la posibilidad de comisión de este delito por la persona jurídica, al compartir los elementos de fácil elaboración, eficiencia, bajo coste, etc. Debe plantearse que una persona jurídica puede auxiliarse de acciones delictuosas con el fin de ganar posición en el mercado o en su defecto hacer perder posición a sus competidores.

PALABRAS CLAVE, Phishing, malware, manipulación informática, transferencia no consentida, activo patrimonial, patrimonio, perjuicio, ánimo de lucro, mulero.

KEYWORDS, Phishing, malware, computer manipulation, non-consensual transfer, patrimonial asset, patrimony, prejudice, profit motive, muleteer.

ABSTRACT

This work deals with Phishing and the criminal law response to this fraudulent behavior. Beforehand, brief notions on simple, medium and advanced Phishing are given, with special attention to the assumptions that have appeared during the coronavirus pandemic, as well as some basic and simplified notions of the most frequent malware. With this previous explanation, the criminal response to computer fraud is analyzed, art. 248.2 CP, a criminal precept that has been incorporated into this punitive text since 1995 (that is, before the main international text on cybercrime prevention, the Council of Europe Convention on cybercrime, was approved).

Competitiveness and competition in the economic sector open the door to the possibility of committing this crime by the legal person, by sharing the elements of easy preparation, efficiency, low cost, etc. It should be considered that a legal entity can take advantage of criminal actions in order to gain a position in the market or, failing that, make its competitors lose position.

OBJETO DEL TRABAJO

La principal finalidad del presente trabajo consiste en analizar y explicara qué se entiende por el fraude informático-Phishing tipificado en el art. 248.2 del CP.

Para alcanzar este principal objetivo, con carácter complementario se han de fijar los siguientes objetivos específicos y particulares:

En primer lugar, explicar de manera sucinta qué es el Phishing, su aparición como modalidad defraudatoria y las distintas clases o fases en su forma comisiva, evolucionadas al mismo tiempo que se han ido produciendo cambios y evolución en la utilización de las TIC y de las medidas de seguridad.

En segundo lugar, analizar de manera simplificada los distintos malware que pueden ser utilizados en la comisión de un Phishing, que servirán para dar contenido a uno de los elementos típicos del delito de estafa informática, la manipulación informática o la utilización de un artificio semejante.

En tercer lugar, explicar el bien jurídico que se pretende proteger a través del delito de fraude informático del art. 248.2 CP, al ser el objeto de protección el principal y más importante elemento que ha de servir de guía en la interpretación del tipo penal.

En cuarto lugar, estudiar el sujeto activo del fraude informático, en concreto, por un lado, el autor de este delito, pero visto el comentario desde el plano criminológico (pues desde el punto de vista jurídico-penal se trata de un delito común, lo que no plantea especiales problemas interpretativos, al margen de la propia discusión dogmática sobre el concepto de autoría) y, por otro lado, la intervención de los llamados muleros en esta modalidad delictiva, generando el problema de si han de ser castigados o no y, en caso afirmativo, de qué manera han de serlo.

En quinto lugar, interpretar los restantes elementos típicos del delito de estafa informática, que ocupan el lugar de la tradicional estafa; utilizar engaño bastante para producir engaño en otro de la estafa tradicional se cambia por valerse de una manipulación informática o artificio semejante; inducir al sujeto engañado a realizar el acto dispositivo aquí se convierte en conseguir la transferencia no consentida de un activo patrimonial. Y, elementos que sí son idénticos a la estafa común o tradicional, en perjuicio de una persona, el dolo y el ánimo de lucro.

En sexto lugar, realizar un estudio de otros aspectos de interés en la estafa informática, como es el relativo a las penas (porque en el art. 248.2 CP no se establece la pena aplicable, así que

ha de valorarse la aplicabilidad o no de lo dispuesto en los arts. 249 y 250 CP) y la responsabilidad penal de las personas jurídicas en el delito de estafa informática.

METODOLOGÍA

El Derecho es una ciencia social, y como tal, puede y debe ser objeto de investigación. En concreto se trata de la denominada "investigación jurídica"; "investigar" significa buscar datos, de manera ordenada y sistemática, para obtener conocimientos nuevos o para encontrar aplicaciones nuevas a los conocimientos existentes. Por otra parte, la investigación jurídica es una actividad indispensable para buscar soluciones a algún problema jurídico o para tratar de encontrar explicaciones que nos permitan entender mejor la ciencia del derecho. Por "investigar" en Derecho debemos entender

también el conjunto de actividades tendentes a la identificación, individualización, clasificación y registro de las fuentes de conocimiento de lo jurídico; la investigación jurídica persigue identificar y caracterizar al objeto de conocimiento denominado derecho, y que en general los conocimientos jurídicos generalizados y válidos construyen el destino de la ciencia del derecho.

En una investigación relacionada con el Derecho, ocupa un lugar destacado la interpretación de las normas jurídicas que regulan una determinada materia o institución; como métodos interpretativos de las normas jurídicas cabe mencionar el literal, el histórico, el sistemático y el teleológico-valorativo. En este trabajo se pretende interpretar normas jurídico-penales, lo que significa que el método literal o gramatical tiene un peso importante como límite en la labor hermenéutica, como derivación directa del principio de legalidad. En una materia tan relacionada con los avances tecnológicos, como es el de los ciberdelitos, es preciso tener más que nunca presentes los límites que fija este principio en la labor de interpretación sobre el sentido y alcance de una determinada figura delictiva.

Para completar este apartado se van a mencionar de manera sucinta los pasos desarrollados en la realización del presente trabajo:

➢ Elección del tutor y del tema sobre el que versa el trabajo. El primer paso consistió en la elección del tutor mediante la elección por parte del alumno de distintas opciones por orden de preferencia. En mi caso, elegí a la profesora María Anunciación Trapero Barrales; tras una primera reunión con ella donde establecí determinados esquemas sobre cuestiones básicas a la hora de citar, buscar bibliografía y organizar el trabajo, decidí elegir el tema relativo al delito de Fraude informático-Phishing, al considerarlo de gran interés debido al gran impacto actual provocado por un mundo interconectado, masificado y post pandemia. Además de ello, al estudiar simultáneamente el grado en informática, fui relacionando conceptos y habilidades

técnicas que me permitían comprender desde otra perspectiva los documentos técnicos y así poder traspasarlos al lenguaje legal con mayor facilidad.

➢ Reunión con distintos especialistas del mundo de la ciberseguridad y el personal del área de Derecho Penal. La parte normativa fue perfeccionada paso a paso a través de reuniones y consultas en el área de Derecho Penal; la parte técnica fue auxiliada de mis prácticas en INCIBE y sobre todo por la colaboración de APWG (Grupo de Trabajo Anti-Phishing) en representación Zoriana Dmytryshyna Director of Institutional Relations.

➢ Recopilación de fuentes bibliográficas: Tras la elección definitiva del tema se fijaron una serie de pautas por parte de la tutora destinadas a fijar una guía sobre cómo iniciar y estructurar el trabajo y cómo citar. El siguiente paso consistió en la búsqueda de bibliografía (manuales, comentarios, artículos científicos, capítulos de libro, monografías, jurisprudencia), que me permitieran obtener comprensión global sobre el tema objeto del trabajo.

➢ Análisis de la información obtenida y valoración crítica. Seguidamente, se procedió a la búsqueda de información específica de cada uno de los puntos sobre los que versaba el índice. De este modo, se obtuvieron y fueron leídos diversos manuales, monografías y libros en general, localizados en la Biblioteca de la Universidad de León (en su mayoría en el área de Derecho Penal). También fueron de gran ayuda medios electrónicos como revistas electrónicas, además de bases de datos como Aranzadi o Tirant Lo Blanch, que permitieron la lectura online de libros y artículos de revistas.

➢ Redacción y corrección del trabajo. Tras leer, estructurar e interpretar la información, se procedió a la redacción del trabajo, intentado explicar y sintetizar cada apartado de la forma más clara posible. Durante la redacción del mismo se han llevado a cabo diversas correcciones por parte de la tutora, en las cuales se me indicaba cuáles eran los aspectos del trabajo que debían ser susceptibles de mejora, cambio o corrección. Después de tener en cuenta todas las apreciaciones realizadas, le remití el texto completo, que fue objeto de una última revisión y corrección final. Tras tomar en consideración las últimas instrucciones dadas, procedí a trasladar de nuevo el trabajo íntegro a la profesora, quien, por fin, emitió el visto bueno.

➢ El sistema de citas utilizado en la elaboración del trabajo es el que me ha indicado la tutora del trabajo.

I. INTRODUCCIÓN

Como se va a explicar en este trabajo, el *Phishing* es una modalidad de estafa informática, proceso aquel donde el *Phisher* contacta mediante vía electrónica a una potencial víctima desde una cuenta incierta, "suplantando" a una entidad de institución legítima, reclamando datos personales[1] de acceso a cuentas a sus titulares, engañosamente y mediante reclamo; una vez conseguidas son accedidas haciendo una transferencia no consentida de cualquier activo patrimonial desde ella, disponiendo de bienes o servicios valuables para su beneficio personal[2] o de un tercero. O, tomando como definición la que aparece en el art. 248.2 a) CP, el sujeto activo, valiéndose de una manipulación informática o de un artificio semejante, y actuando con ánimo de lucro, consigue una transferencia no consentida de cualquier activo patrimonial en perjuicio de un tercero[3].

El ciberdelito de *Phishing* (Password Harvesting Fishing) procede del inglés de la acción de pescar y, en este caso, pescar o cosechar[4] (mediante correos enviados masiva o exclusivamente dependiendo del tipo de *Phishing*) datos de identificación o autenticación, que responderán en una base de datos de un servicio como usuarios y contraseñas.

El *Phishing* es un ciberdelito que utiliza el fraude, el engaño, es el timo en versión moderna, para manipular al destinatario de este engaño[5]; el coste económico y el riesgo de este proceso es mínimo[6], lo que resulta un claro aliciente para los potenciales sujetos activos.

La primera referencia al término *Phishing* se escuchó a mediados de la década de los noventa en un blog cibernético de *crackers* que tenían como objetivo intervenir los correos de trabajadores en la empresa America Online (AOL) y robar la identidad de la cuenta. Los mensajes (las maniobras engañosas) contenían diferentes excusas como la verificación de la cuenta o corroborar la dirección de facturación[7].

---

[1] ÁLVAREZ LEÓN*, Tópicos de Política Criminal 2. Ciencia y Tecnología,* 2021, 17, 18.
[2] VELASCO NÚÑEZ/SANCHÍS CRESPO, *Delincuencia Informática Tipos Delictivos e Investigación Con jurisprudencia tras la reforma procesal y penal de 2015,* 2019, 31.
[3]GUÉREZ TRICARICO, en: MOLINA FERNANDEZ (coord.), *Memento práctico penal,* 2021, 1356.
[4] SERRANO FERRER, *Derecho Penal y Nuevas Tecnologías,* 2021, 85.
[5] ABADÍAS SELMA/FERNÁNDEZ ALBESA/LEAL RUIZ, *Ciberdelincuencia,* 2021, 242.
[6] Comparte, por tanto, los rasgos de los ciberdelitos puros. Véase DE LA CUESTA ARZAMENDI/PEREZ MACHÍO, en: DE LA CUESTA ARZAMENDI (dir.)/DE LA MATA BARRANCO(coord.), *Derecho Penal Informático,* 2010, 109.
[7] ÁLVAREZ LEÓN, *Tópicos de Política Criminal 2. Ciencia y Tecnología,* 2021, 17.

El *speach* o cuerpo[8] del *Phishing* es aquel texto inmerso en el medio de comunicación (SMS, voz o correo electrónico) fabricado por el *Phisher*, auxiliado por la lógica, la ingeniería social, psicología que busca la persuasión y convencimiento de la víctima por medio de un reclamo al simular la identidad de un ente responsable del servicio o un superior jerárquico. Los *Phisher* utilizan la urgencia humana[9] y contextos sociales determinados[10] para aumentar las probabilidades de consumación del delito.

En cuanto a su forma comisiva, está en constante evolución; los primeros *Phishing* nacieron como un correo simple a través del cual, los autores del mismo, buscaban la obtención de datos personales, datos de acceso o datos que permitieran la inferencia de contraseñas. Posteriormente los servicios de la red han implementaron como medida de seguridad las famosas "preguntas secretas"[11], las cuales por medio de acontecimientos personales permiten identificar inequívocamente al usuario o reducir el número de posibles acertadores, debido a que las preguntas son de carácter personal. Esta circunstancia obligó a cambiar el objeto del *Phishing,* de una búsqueda de datos simples a datos de autenticación[12]. En la actualidad nos encontramos con mecanismos de autenticación más engorrosos, complejos y seguros, en el

---

[8] INCIBE, *Temáticas Phising* [en línea].[10/05/2022].[https://www.incibe.es/protege-tu-empresa/tematicas/phishing].

[9] Sobre urgencia humana: "la conducta humana ante situaciones de emergencia establece que, durante este proceso de percepción y evaluación, se produce paralelamente la vivencia a nivel emocional de la situación por parte del sujeto. En estos casos veremos cómo se puede llegar a un grado de excitación emocional que inhabilita a las personas para tomar decisiones que pueden bloquear el procesamiento de información y ejecutar conductas de forma adecuada". FIDALGO VEGA, *NTP 390: La conducta humana ante situaciones de emergencia: análisis de proceso en la conducta individual.* [en línea]. [03/07/2022].[https://www.insst.es/documents/94886/326853/ntp_390.pdf/967860c0-87f3-4cb8-8421-6e3a8583a941?version=1.0&t=1614698481311 *].*

[10] sobre contexto social: "el contexto social, que es construido por las características de los usuarios que se comunican en entornos virtuales y su percepción del entorno comunicativo virtual; la comunicación virtual, es decir, los atributos, aplicaciones y percepciones del lenguaje usado en el entorno virtual; y la interactividad, que consiste en esas actividades cooperativas y los estilos de comunicación usados por los usuarios de la comunicación mediada por ordenadora". PEREZ-MATEO SUBIRÁ, *La Dimensión Social en el Proceso de Aprendizaje Colaborativo Virtual: El caso de la OUC*, 2010 [en línea] [03/07/2022]. [https://www.tdx.cat/bitstream/handle/10803/37113/tesi_mperezmateo-1.pdf].

[11] Sobre recomendaciones de preguntas secretas: "considerar la seguridad de sus preguntas (y respuestas) secretas, ya que mientras sigan siendo utilizadas como método de restitución de cuentas, permiten el acceso sin necesidad de conocer la contraseña". PAGNOTTA SANABRIA. *Noti_infosegura: ¿Cuáles son las preguntas de seguridad de la información más adecuadas según Google?* [en línea] [03/07/2022]. [https://www.uv.mx/infosegura/general/noti_google-4/].

[12] Sobre los términos el acceso lógico, identificación y autenticación *"Acceso lógico***.** Se trata del procedimiento que permite introducir, modificar, suprimir, consultar los datos y registros presentes en un sistema mediante un acceso autorizado./ *Identificación***.** Es el medio por el cual un usuario proporciona una identidad reclamada por el sistema./ *Autenticación.* Se trata del medio que permite establecer la validez de una solicitud formulada para acceder a un sistema. Este mecanismo es precedido por una identificación que permite hacerse reconocer por el sistema. Esto puede ser en forma de contraseña, identificación PIN*"*. CARPENTIER, *La seguridad informática en la PYME.* [en línea] [10/05/2022]. [https://www.ediciones-eni.com/open/mediabook.aspx?idR=cbc5b457b60ff38bb7e4e6f90df31bec].

momento actual la transición de nuevas medidas de seguridad, como la autenticación de dos pasos[13], identificación por datos biométricos (huellas dactilares, voz, iris, rostro, forma de caminar, etc.)[14] y, en un futuro próximo, utilizaremos los datos genéticos y neuro-datos[15] en los servicios de comunicación (Facebook, Whatsapp, Instagram, etc.), lo que supone protección y blindaje a usuarios, implicando consecuentemente también nuevos retos al creador de *Phishing*.

El *Phishing simple* [16]es aquel en el cual el *phisher* elabora un correo simple, pudiendo ser absurdo o poco elaborado, con un nivel mínimo de ingeniería social, incluso sin esta, donde regularmente no lleva una investigación mínima del sujeto-presa potencial. Ejemplo de ellos son aquellos comunicados (correos, llamadas, SMS) por medios tradicionales que ocupan un lenguaje básico, inexacto, incluso mal traducido en el cual exigen los datos bancarios/servicios a un sujeto que ni siquiera tiene una cuenta en aquella entidad o servicio reclamado. Esto se debe a que la gran mayoría de *phisher* apuestan por la cantidad y no la calidad respecto de la poca importancia de la eficacia, puesto que no elabora mensajes acertados; los *Phisher* simples compran bases de datos con N número de correos sin verificar, sin autenticar el origen y existencia de los mismos, ni mucho menos la existencia de una relación que favorezca su propósito ilícito.

El *Phishing medio* por lo general está elaborado en el seno de un grupo delictivo, el cual está claramente organizado con el objetivo de sumar esfuerzos y así, ayudados de Malware e ingeniería social, aumentan su nivel de eficiencia. El grupo criminal realiza designación de roles y funciones determinadas a cada integrante, dentro de las más importantes encontramos: *creador del Malware* y, en su defecto, si no cuentan con un integrante con habilidades de programación que permitan el desarrollo, optarán por comprar a un tercero el Malware, encontramos un *analista de base de datos,* un *redactor* encargado de elegir el lenguaje, la

---

[13] Sobre la autenticación de dos pasos "La autenticación en dos pasos es combinar dos métodos de autenticación de índole diferente, es decir, combinar el «algo que sabemos» con el «algo que tenemos». También podemos combinar «algo que somos», con «algo que tenemos»" ESPINOSA, *Mejora la seguridad de tus cuentas con la autenticación en dos pasos.* [en línea] [10/05/2022]. [https://www.redeszone.net/tutoriales/seguridad/autenticacion-dos-pasos/].

[14] Datos biométricos: datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos. Art. 4.14 RGPD.

[15] En la Ley 21383 Senado de la República de Chile de 24 de noviembre de 2021 se da una definición de dato neuronal: la información obtenida de la actividad de las neuronas que contiene una representación de la actividad cerebral. Consulta 10/04/2022[en línea]. [https://www.senado.cl/proteccion-de-los-neuroderechos-a-un-paso-de-pasar-a-segundo-tramite]. Véase también https://www.bcn.cl/leychile/navegar?idNorma=1166983&idParte=10278855&idVersion=2021-10-25).

[16] Clasificación de Phishing simple, medio y avanzado, son de elaboración propia.

redacción del *speach* y el diseño del mensaje, y un *Ingeniero social* capaz de determinar el momento y modo adecuado del envío. Por último, encontramos un *operador,* el encargado de recibir las contraseñas, posteriormente utilizarlas para ingresar al servicio y, finalmente, realizar una transferencia (monetaria o de contenido, dependiendo del servicio) a una cuenta tercera ajena de la víctima.

Pero el phishing medio también puede ser realizado por un solo sujeto, auxiliado de programas automatizados para realizar las funciones de los roles anteriormente mencionados.

El *Phishing avanzado*, es el que contiene un grado elevado de ingeniería social, malware y además es auxiliado de otras modalidades de fraude: vishing, smishing[17], Qrishing, etc. Este

[17] sobre Phishing/Vishing/Smishing: "Phishing- es el nombre dado en inglés a una estafa mediante la cual los defraudadores envían mensajes de tipo spam o pop-up para "pescar" información personal y financiera engañando a las víctimas inadvertidas. Mediante el texto del mensaje electrónico es posible que se le solicite que "actualice", "valide" o "confirme" la información de su cuenta, y que, en caso de no hacerlo, podría enfrentar graves consecuencias. El correo lo dirige a una página de Internet que parece legítima, pero no lo es. El propósito es hacer que la persona envíe la información para robarla. Vishing-Es una práctica criminal fraudulenta en donde se hace uso del Protocolo Voz sobre IP (VoIP) y la ingeniería social para engañar a personas y obtener información delicada como puede ser información financiera o información útil para el robo de identidad. El término es una combinación del inglés "voice" (voz) y phishing. Sea sospechoso de cualquier mensaje que usted reciba que venga de University Credit Union que le pida que proporcione sus datos personales o de su cuenta. Phishing-Smishing es un término informático para denominar un nuevo tipo de delito o actividad criminal usando técnicas de ingeniería social empleado mensajes de texto dirigidos a los usuarios de telefonía móvil. Es otra manera que utilizan los ladrones para robar números de tarjeta de crédito o débito por teléfono. Sea sospechoso de cualquier mensaje que usted reciba en el cual pretende ser de University Credit Union y le solicite sus datos confidenciales. Las víctimas de Smishing reciben mensajes SMS con líneas similares a éste: "Estamos confirmando que se ha dado de alta para un servicio de citas. Se le cobrará 2 dólares al día a menos que cancele su petición de número de cuenta, número de tarjeta de crédito o número de seguro social." en; UNIVERSITY CREDIT UNION: *Phishing/Vishing/Smishing.* en línea]- [05/07/2022]. [https://ucumiami.org/es/education-3/phishing-vishing-smishing#:~:text=Es%20una%20pr%C3%A1ctica%20criminal%20fraudulenta,%22%20(voz)%20y%20phishing.].

tipo de Phishing, por su complejidad, es frecuentemente utilizado para ayudar la comisión de un APT[18] o ransomware[19].

las características del Phishing avanzado son:

- Realizar un análisis previo y profundo del objeto/víctima del *Phishing*,

[18] Sobre ATP y sus características: Como el nombre "avanzado" lo sugiere, una amenaza avanzada persistente (APT) utiliza técnicas de hackeo continuas, clandestinas y avanzadas para acceder a un sistema y permanecer allí durante un tiempo prolongado, con consecuencias potencialmente destructivas. Objetivos prioritarios. Debido al nivel de esfuerzo necesario para llevar a cabo un ataque de este tipo, las APT suelen asociarse con objetivos de alto valor, como países y grandes corporaciones, con el objetivo de robar información durante un largo período de tiempo, en lugar de simplemente "adentrarse" y salir rápido, como hacen muchos *hackers* de sombrero negro durante ciberataques de bajo nivel. Las APT suponen un método de ataque que debería estar en el radar de las empresas de todo el mundo. Sin embargo, esto no significa que las pequeñas y medianas empresas puedan pasar por alto este tipo de ataque. Los atacantes de APT utilizan cada vez más a las empresas más pequeñas que conforman la cadena de suministros de su objetivo final como una forma de acceder a las grandes organizaciones. Por ejemplo, utilizan a tales empresas como trampolines ya que, normalmente, cuentan con menos protección. Un ataque en constante evolución. El propósito global de un ataque de APT es obtener acceso continuo al sistema. Los *hackers* lo logran en una serie de etapas. Etapa 1: obtener acceso Al igual que un ladrón fuerza una puerta con una palanqueta, para insertar malware en una red objetivo, los cibercriminales suelen obtener acceso a través de una red, un archivo infectado, el correo electrónico basura o la vulnerabilidad de una aplicación. Etapa 2: infiltrarse Los cibercriminales implantan malware que permite crear una red de puertas traseras y túneles utilizados para desplazarse por los sistemas de manera desapercibida. A menudo, el malware emplea técnicas como reescribir el código para ayudar a los *hackers* a ocultar sus rastros. Etapa 3: intensificar el acceso Una vez dentro, los *hackers* utilizan técnicas como el quebrantamiento de contraseñas para acceder a los derechos de administrador, aumentar el control sobre el sistema y obtener mayores niveles de acceso. Etapa 4: desplazamiento horizontal. Con un mayor nivel de incursión dentro del sistema gracias a los derechos de administrador, los *hackers* pueden moverse por este a voluntad. También pueden intentar acceder a otros servidores y a otras partes seguras de la red. Etapa 5: mirar, aprender y permanecer. Desde el interior del sistema, los *hackers* obtienen una completa comprensión de su funcionamiento y sus vulnerabilidades, lo que les permite hacer uso de la información que desean. Los *hackers* pueden intentar mantener este proceso en funcionamiento, posiblemente de manera indefinida, o retirarse después de cumplir un objetivo específico. A menudo, dejan una puerta abierta para acceder al sistema de nuevo en el futuro. El factor humano. Debido a que la ciberseguridad corporativa tiende a ser más avanzada que la de los usuarios particulares, los métodos de ataque a menudo requieren la participación activa de alguien en el interior para lograr el momento crucial e importantísimo de la "palanqueta". Sin embargo, esto no significa que el personal participe a sabiendas en el ataque. Por lo general, esto implica un atacante que despliega una amplia gama de técnicas de ingeniería social, como el "whaling" o el "spear phishing". Una amenaza persistente. El principal peligro de los ataques de APT es que incluso cuando se descubren y la amenaza inmediata pareciera haber desaparecido, los *hackers* podrían tener varias puertas traseras abiertas que les permitan regresar cuando lo deseen. Además, muchas ciberdefensas tradicionales, como los *firewalls* y antivirus, no siempre pueden proteger contra estos tipos de ataques. Para maximizar las posibilidades de una defensa continua exitosa, se debe implementar una combinación de varias medidas, que van desde soluciones de seguridad avanzadas como Kaspersky Enterprise Security, hasta una fuerza de trabajo capacitada y con conocimiento en técnicas de ingeniería social. En: KASPERSKY, *¿Qué es una amenaza avanzada persistente (APT)?*[en línea]. [05/07/2022]. [https://latam.kaspersky.com/resource-center/definitions/advanced-persistent-threats].

[19] Sobre el el *ransomware;* es una extorsión que se realiza a través de un *malware* que se introduce en los equipos de las empresas: ordenadores, portátiles y dispositivos móviles. Este software malicioso «secuestra» la información de la empresa, impidiendo el acceso a la misma generalmente cifrándola, y solicitando un rescate (en inglés *ransom*) a cambio de su liberación. En las empresas causa pérdidas temporales o permanentes de información, interrumpe la actividad normal, ocasiona pérdidas económicas y daños de reputación. Este tipo de ataque está creciendo de forma exponencial debido a que es muy rentable para los delincuentes: cada vez hay más dispositivos «secuestrables»; es más fácil «secuestrar» la información debido a los avances de la criptografía; los ciberdelincuentes pueden ocultar su actividad para lanzar ataques masivos; al utilizar sistemas de pago anónimo internacionales es más difícil el seguimiento del delito. En: INCIBE, *Ayuda ransomware* [en línea]. [05/07/2022]. [https://www.incibe.es/protege-tu-empresa/herramientas/servicio-antiransomware].

- Utilización de metodologías científicas como la psicología, sociología, informática, sistemas, ingeniería social, ciberseguridad, recursos humanos, administración, política meteorológica, arquitectónica, etc.
- Creación de un vector de ataque, partiendo de la identificación de amenazas potenciales, posteriormente explotando vulnerabilidades.

Como ejemplo de *Phishing* avanzados encontramos[20]:

El spear-Phishing, el fraude a CO o cualquier ataque híbrido (presencial y remoto) a una persona jurídica[21].

Un phishing ayudado de *pharming*[22] que posteriormente al robo de datos con características de autenticidad o autenticación permiten el desplazamiento de una cuenta o suscripción que contiene el respaldo de datos sensibles, que posteriormente pueden ser o no encriptados, pero de ser divulgados generarán perjuicios al sujeto pasivo.

Un sujeto víctima de un robo tradicional, despojado de su Smartphone, que está protegido por un código de seguridad y una cuenta asignada al dispositivo que genera un bloqueo, haciéndolo inaccesible a sus funciones básicas, al imposibilitar revender el dispositivo libreado, los ladrones se ven orillados a sacar provecho revendiendolo para usar piezas (display, bocinas, sensores, etc.) en el mercado negro, ante esto el ciberdelincuente realiza un phishing en coordinación con un *smishing* y un *vishing* con intenciones de liberar el

---

[20] DE LA CUESTA ARZAMENDI/PÉREZ MACHÍO, en: DE LA CUESTA ARZAMENDI (dir.)/DE LA MATA BARRANCO (coord.), *Derecho Penal Informático,* 2010, 109.

[21] Sobre el spear Phishing o fraude al CO: El spear phishing es una estafa de correo electrónico o comunicaciones dirigida a personas, organizaciones o empresas específicas. Aunque su objetivo a menudo es robar datos para fines maliciosos, los cibercriminales también pueden tratar de instalar malware en la computadora de la víctima. Funciona así: llega un correo electrónico, aparentemente de una fuente confiable, que dirige al destinatario incauto a un sitio web falso con gran cantidad de malware. A menudo, estos correos electrónicos utilizan tácticas inteligentes para captar la atención de las víctimas. Por ejemplo, el FBI advirtió de estafas de spear phishing que involucraban correos electrónicos supuestamente procedentes del Centro Nacional para Menores Desaparecidos y Explotados. En: KASPERSKY.*¿Qué es el spear phishing?* [en línea]. [05/07/2022]. [https://latam.kaspersky.com/resource-center/definitions/spear-phishing].

[22] Sobre el Pharming: El pharming, una combinación de los términos "phishing" y "pharming", es un tipo de cibercrimen muy semejante al phishing, en el que el tráfico de un sitio web es manipulado para permitir el robo de información confidencial. El pharming aprovecha los principios con los que funciona la navegación por Internet, es decir, la necesidad de convertir una secuencia de letras para formar una dirección de Internet, como www.google.com, en una dirección IP por parte de un servidor DNS para establecer la conexión. El exploit ataca este proceso de dos maneras. En primer lugar, un hacker puede instalar un virus o un troyano en la computadora de un usuario que cambia el archivo de hosts de la computadora para dirigir el tráfico fuera de su objetivo previsto, hacia un sitio web falso. En segundo lugar, el hacker puede envenenar un servidor DNS para que los usuarios visiten el sitio falso sin darse cuenta. Los sitios web falsos se pueden utilizar para instalar virus o troyanos en la computadora del usuario, o pueden ser un intento de recopilar información personal y financiera para usarla en el robo de identidad. En. KASPERSKY.*¿Qué es el pharming y cómo evitarlo?[*en línea]. [05/07/2022]. [https://latam.kaspersky.com/resource-center/definitions/pharming].

dispositivo y poder elevar el precio de venta, desbloqueado el mismo posee la capacidad de duplicar el contenido de las aplicaciones y decide ciber-extorsionar al ya robado y defraudado.

Otra clasificación tipológica de Phishing podría ser la establecida en los ciberejercicios de Diciembre 2021 por parte de INCIBE CERT- referente a los ataques dirigidos en contexto de un escenario simple:

Phishing - Nivel I – Básico.

Este es el nivel básico de phishing que se ha implementado y hace referencia al acceso a una URL acortada que previamente se ha enviado por correo electrónico.

Ni el dominio ni el contenido del propio correo han de levantar alertas al no tener contenido malicioso en ambos casos.

Se emplea trazabilidad detectando los accesos y posteriormente se insertan en base de datos. El acceso a la URL es personalizado para cada una de ellas y es así cómo se efectúa la trazabilidad. Los datos que se guardan son los siguientes.

- Día y hora.
- IP origen.
- Empleado que ha hecho clic en el enlace (trazabilidad personalizada).
- Empresa objetivo (trazabilidad personalizada).

La imagen que verá la persona que acceda a la web es una “landing page” de una empresa de promociones de productos.

Phishing - Nivel II – Medio.

El segundo nivel phishing que se ha implementado emplea las mismas características que el nivel básico añadiendo un formulario de inscripción a una supuesta promoción para captar la atención del empleado, evidenciando así el envío de datos explícito y de forma activa por parte del empleado.

- Datos del formulario a rellenar
- Activación del código de promoción.

Phishing - Nivel III – Avanzado.

El tercer nivel de phishing que se ha implementado adjunta un fichero malicioso con una macro que descarga un “payload” convenientemente ofuscado/cifrado para evadir posibles medidas de seguridad. El documento WORD/EXCEL informa del catálogo de productos canjeables. La macro estará usando alguna herramienta y/o técnica de la siguiente lista de repositorios.

- https://github.com/S3cur3T
- https://github.com/outflanknl
- https://github.com/DidierStevens/DidierStevensSuite/
- https://github.com/mgeeky/VisualB
- https://outflank.nl/blog/2019/04/17

Las acciones “maliciosas” se ocupan, como en el escenario complejo, de recoger datos del entorno del usuario, guardarlo en C:\Windows\Tasks\” y enviarlo a un servidor remoto.

Los *malwares* utilizados en el *Phishing* suelen ser fáciles de elaborar y actualizar, hoy en día son más elaborados en nivel de ejecución los contenidos en un QRshing frente al primer *malware* llamado *Creeper*[23]. Los QRshing tuvieron un auge durante la pandemia y pos pandemia por ser la medida adoptada y aprobada por los gobiernos y el sector sanitario como medida de acceso a información sin necesidad de un contacto físico; el procesamiento lo realiza la cámara de un dispositivo, la cual escanea una imagen estructurada en sectores, que remiten al escaneador a una dirección previamente almacenada que identifica al código QR. Es una de las medidas utilizada para respetar la famosa sana distancia y pretendía evitar el contagio por contacto, siendo ideal para identificar, llenar formularios y realizar servicios, pero también es ideal para defraudar, toda vez que la víctima al ser direccionadas mediante el escaneo de este código salta las medidas culturales que poco a poco la sociedad adquiere[24]. Al

---

[23] Sobre el primer virus y el primer antivirus: desarrollado por Robert Thomas Morris que atacaba a las conocidas IBM 360. Simplemente mostraba de forma periódica el siguiente mensaje: "I'm a creeper... catch me if you can!" (soy una enredadera, cójame si pueden). Fue aquí donde podríamos decir que apareció el primer antivirus conocido como Reaper (segadora) el cual elimina a Creeper. En: PRIETO ÁLVAREZ/PAN CONCHEIRO, *Virus Informáticos,* [en línea]. [10/05/2022]. [http://sabia.tic.udc.es/docencia/ssi/old/2006-2007/docs/trabajos/08%20-%20Virus%20Informaticos.pdf].

[24] Sobre medidas culturales de seguridad para identificar el Phishing: Comprobar la ortografía y redacción Verificar que la cuenta es original. Muchos de los correos de phishing contienen errores ortográficos y de redacción no son propios de entidades debido al uso de traductores automatizados. Debemos comprobar que el email coincide con la empresa que nos envía el correo. Generalmente utilizan dominios públicos o que se parecen al que sería el correo oficial. Revisar la URL: Los enlaces del correo deben ser comprobados antes de hacer clic, podemos colocar el cursor del ratón sobre el hipertexto para ver la URL a la que nos redirige. No descargar archivos adjuntos bajo ningún concepto descargar los archivos adjuntos del email si no podemos confirmar que se trata de un mensaje legítimo. En: INCIBE_OSI, *Aprendiendo a identificar* [en línea]. [10/05/2022].[https://www.osi.es/sites/default/files/docs/guia_fraudes/guia-fraudes-online.pdf].

entrar QR el usuario es conducido a una página web falsa o web sin medidas de seguridad que permite al ciberdelincuente ejecutar un ataque como: extraer información confidencial, instalar códigos maliciosos en el dispositivo, entre otros. Se trata de una modalidad relativamente nueva de phishing, si bien el uso de Qr no es nuevo, pues nace en 1994, esta variante de Fraude informático fue creada a raíz de su implementación en sectores comercial y sanitarios[25].

II. MALWARE

Es un software catalogado malo por la intencionalidad, no por errores de diseño, puesto que se ha creado con la finalidad de realizar una actividad perniciosa para la información o sistema que alberga. Es todo software que, de forma malintencionada, pretende acceder, modificar, o eliminar información; y, en general, el propósito del malware es afectar la confidencialidad, disponibilidad, integridad de un sistema informático. A título ejemplificativo, cabe citar, entre otros[26], los troyanos, gusanos, software espía, scareware[27] y ransomware (este último ya mencionado en la introducción).

- *Gusanos y virus:* un virus informático es un malware que, cuando es ejecutado, infecta a otro software del mismo sistema y puede saltar a otros sistemas, este se replica mutando y puede ser transportado por un correo electrónico; suele llevar una carga añadida de otro malware. Los gusanos son erróneamente catalogados como malware, estos solo se auto replican, no necesitan alterar archivos, su finalidad original es afectar la comunicación en la red, pero este puede ser utilizado para transportar otro tipo de malware.

- *Los Rootkits* son softwares que modifican el sistema operativo, engañan al sistema para evitar ser detectados por programas antimalware, puesto que el sistema operativo los asume como software lícito o procesos del sistema operativo.

---

[25] PARIS BALLEZA, *QRshing: conoce los riesgos de la nueva estafa*. [en línea] [10/05/2022]. [https://es.linkedin.com/pulse/qrshing-conoce-los-riesgos-de-la-nueva-estafa-paris-balleza?trk=articles_directory].

[26] Para más detalles, véase, por todos, CÁMARA ARROYO/CANO CARRILLO/GARCÍA RUIZ/GIL GIL (coord.)/HERNÁNDEZ BERLINCHES (coord.)/MARTÍN FERNÁNDEZ/PASTOR VARGAS/ROBLES GÓMEZ/TOBARRA ABAD, *Cibercriminalidad,* 2019, 59 ss.

[27] Sobre el scareware: es un software malicioso que engaña a los usuarios de computadora para que visiten sitios web infestados de malware. También conocido como software engañoso, software de escáner malicioso o scareware, el scareware suele aparecer como ventanas emergentes. En: KASPERSKY, *¿Qué es el scareware?* Definición y explicación. [en línea]. [https://latam.kaspersky.com/resource-center/definitions/scareware].

- *Los troyanos* son un software capaz de engañar al usuario introduciendo un código dañino en un programa aparentemente inocente que, posteriormente, podrá borrar, robar, cifrar información o instalar otro software para convertir el ordenador en un Bot.

- *Las Backdoors* son un malware que explota vulnerabilidades en los procedimientos de autenticación, estableciendo conexiones no autorizadas con los sistemas y permitiendo la entrada de otros malwares y atacantes.

- *Los Keyloggers* son malwares que se utilizan para la obtención de credenciales mediante el monitoreo indiscriminado de pulsaciones en las teclas, posteriormente el malware procede a almacenar dichas pulsaciones en un fichero y, finalmente, remitir ese fichero a un tercero.

- *Los stealers* son un malware semejante a los keyloggers, con la peculiaridad de que son capaces de analizar el software y así captar la información del usuario, contraseña, cuentas de correo o bancarias, para remitir posteriormente a un tercero.

- *El spyware* es un programa espía que se suele instalar en el sistema, recopila información de una computadora y después transmite esta información a una entidad externa sin consentimiento[28].

III. LA EFICACIA DEL PHISHING

Se debe atender a varios factores[29]: la masividad de intentos que tienen a su disposición los *Phisher*, la facilidad de mantener en disposición las URL, los anonimizadores y la ingeniería social.

1-Mantener en disposición las URL

[28] CÁMARA ARROYO/CANO CARRILLO/GARCÍA RUIZ/GIL GIL (coord.)/HERNÁNDEZ BERLINCHES (coord.)/MARTÍN FERNÁNDEZ/PASTOR VARGAS/ROBLES GÓMEZ/TOBARRA ABAD, *Cibercriminalidad,* 2019, 61-66.

[29] Otro factor que ayuda al Phishing puede ser la brecha digital, que hace referencia a la desigualdad en el acceso, uso o impacto de las TIC entre grupos sociales. Estos grupos se suelen determinar en base a criterios económicos, geográficos, de género, de edad o culturales. En: Fundación BBVA – Ivie N.º 29/2018. [en liena].[05/07/2022].[https://www.fbbva.es/wp-content/uploads/2018/10/FBBVA_Esenciales_29.pdf].

Desde el comienzo del *phishing*, los atacantes han creado páginas web simples que redirigen a los usuarios a otra URL[30] que contiene el formulario de *phishing* real. Lo hacen por varias razones.

En caso de que su sitio de *phishing* se cierre, simplemente pueden cambiar el destino de la redirección para que apunte a otro sitio de *phishing*. Esto significa que todos los que reciban un correo electrónico con el enlace de redireccionamiento y hagan clic en él, terminarán en un sitio de *phishing*.

El software de bloqueo de URL solo puede bloquear las URL que contienen una página de *phishing* visible. Según el software utilizado y como recopilan sus datos de *phishing*, es posible que solo las URL de *phishing* visibles estén en la lista negra y permitan que las URL de redireccionamiento se filtren. Cuando la página de *phishing* visible finalmente es bloqueada por los filtros de *phishing* del navegador web, los atacantes pueden cambiar la redirección nuevamente y continuar con su estafa.

PhishLabs ha detectado algunas formas avanzadas de usar funciones de redirección a través de programas PHP. En los programas de muestra recuperados, los atacantes han ampliado la funcionalidad para redirigir a los usuarios a uno de varios sitios de *phishing* y verificar primero si esos sitios de *phishing* todavía están disponibles[31].

2-Anonimizadores

El servicio de anonimato actúa como un filtro de seguridad entre tu navegador y el sitio Web que deseas visitar. Te conectas al anonimizador, introduces el URL al que deseas ir, entonces este se adentra en la Red en busca de la página que deseas ver y te la muestra. Si posteriormente vas siguiendo enlaces de una página a otra, se presentarán asimismo a través del anonimato[32].

---

[30] Sobre el funcionamiento de las URL creadas para el Phishing; El sesenta y cinco por ciento de los nombres de dominio registrados de forma malintencionada se utilizan para *phishing* dentro de los cinco días posteriores al registro. Los nuevos dominios de nivel superior introducidos desde 2014 representan el 9 % de todos los nombres de dominio registrados, pero el 18 % de los nombres de dominio son utilizados para el phishing. Alrededor del 9% del phishing ocurre en un pequeño conjunto de proveedores que ofrecen servicios de subdominio.[en línea]. [25/052022]. [https://apwg.org/phishing-landscape-2020-a-study-of-the-scope-and-distribution-of-phishing/].

[31] STACY Shelley, *Advancement in Phishing Redictor Script.* [en línea]. [25/052022]. [https://www.phishlabs.com/blog/advancements-in-phishing-redirector-scripts/].

[32] MOSQUERA, *Anonimizadores*. [en línea] [03/06/2022]. https://es.scribd.com/doc/230334053/Anonimizadores].

Los *Phisher* utilizan los anonimizadores Proxy, VPN, TOR, I2P, los cuales entorpecen u ocultan al transmisor y al del mensaje mediante técnicas de cifrado, saltos de Nodos, túneles de cifrado, enrutamiento tipo "cebolla" y tipo "Ajo".

3- Ingeniería social

Cobra relevante importancia al ser esta ciencia la implicada en la mayoría de los *Phishings*, en mayor o menor medida, pero el 99% de los Phishing actuales aplican un mínimo del mal llamado arte, disciplina de manipular psicológicamente a las personas en la realización de acciones divulgación de información sensible[33]. También cobra relevancia entre la doctrina pues, a la poca seguridad en los Smartphones y demás sistemas se suma el uso de los Malwares, con la finalidad de consumar la Transferencia del activo patrimonial. Esta alianza de herramientas e ingeniería social crearán una especie de carrera del gato y el ratón[34].

La ingeniería social es una recopilación de habilidades que, cuando se unen, componen ingenio, es el arte, es la ciencia que utiliza las fuerzas del orden público y las relaciones interpersonales, con el fin de maniobrar, manipular al ser humano a ejercer una acción que puede ser o no lo más conveniente para el objetivo[35].

Todos somos un poco de ingenieros sociales en el desarrollo de nuestras profesiones, y, sobre esto, Chris Nickerson dice que la verdadera ingeniería social no consiste en creer el papel, sino que, durante ese momento, eres esa persona "eres ese papel, ésa es tu vida". El objetivo de la ingeniería social es y se basa en generar confianza plena de las personas para después engañarlas, manipularlas, sin que estas sospechen de ser timadas, usando la persuasión, puesto que las personas padecen las mismas debilidades dentro y fuera del sistema informático o de la red de trabajo, al final, el ser humano se desenvuelve dentro de diferentes grupos sociales de una manera, u otra, dependiendo del entorno existirán reglas de conducta diferentes que lo limitan, pero la esencia personal jamás se modifica, solo la forma de expresión corporal y verbal de las ideas. Las técnicas conocidas vigentes desde los inicios de la humanidad solo fueron "adaptadas" al nuevo entorno, cumplimentadas con el aprovechamiento, para su

---

[33] ANDRÉ MORALES, *Ingeniería Social, 5.* [en línea]. [https://cybercamp.es/cybercamp2014/attachments/multimedia/CyberCamp_IngenieriaSocial.pdf].

[34] GRIS, *Hackers, Crakers, e Ingeniería Social,* 102 [en línea]. [03/06/2022] [https://pdflife.one/download/4660813-hackers-crackers-e-ingenieria-social].

[35] HADNAGY, *Ingeniería Social, el Arte del Hacking personal,* 2011, 36, 67.

explotación, de cualidades propias del ser humano; ingenuidad, inocencia, ambición, morbo, etc. Este arte de engañar puede ser utilizado por cualquiera[36].

Distintos tipos de ingenieros sociales:

- **Hackers**: Los proveedores de software van logrando crear software cada vez más "blindado" o más difícil de forzar.
- **Probadores de seguridad:** Estos profesionales aprenden y utilizan las técnicas de los *hackers* para ayudar a garantizar la seguridad de sus clientes.
- **Espías:** Para los espías la ingeniería social es un modo de vida.
- **Ladrones de identidad:** El robo de identidad es el uso de datos como el nombre de una persona, números de cuentas bancarias, direcciones, fechas de nacimiento y números de la seguridad social.
- **Agentes de recursos humanos:** son expertos no solo en leer a las personas sino también en comprender qué es lo que motiva a la gente.
- **Vendedores:** al descubrir cuáles son las necesidades de la gente para después tratar de satisfacerla.
- **Gobierno:** utilizan la ingeniería social para controlar el mensaje que envían y a las personas que gobiernan.[37]

Capacidades de un ingeniero social.

1. Capacidad de examinación de grandes volúmenes de información, a manera de buscar el mayor impacto y aprovechamiento de su uso.
2. Capacidad de cuestionamiento. Replanteamiento de las preguntas que dieron origen a la información recopilada y analizada.
3. Identificación de fallos y aprovechamiento de vulnerabilidades personales y funcionales.
4. Desarrollador de modelos de comunicación interpersonal, verbal y no verbal. [38]

Los modelos de comunicación cobran relevancia en el análisis de un *Phisher* que usa la ingeniería social, pues este proceso definirá la efectividad del *Phishing*. El problema de la efectividad: la medición de la carga manipulante se mide en correlación de la efectividad del mensaje recibido. Pero, ¿afecta a la conducta? Es importante recordar este último punto. La

[36] BORGHELLO, *El Arma Infalible: La Ingeniería Social,* 2, 3. [en línea]. [03/06/2022] [https://p303.zlibcdn.com/dtoken/dfdbdbc908ca3791794e6fd56ed0d675].
[37] HADNAGY, *Ingeniería Social el Arte del Hacking personal,* 2011, 44-48.
[38] HADNAGY, *Ingeniería Social el Arte del Hacking personal,* 2011, 55- 81.

meta absoluta del ingeniero social es crear la conducta que se desea. El *Phisher*, respecto al modelo, comprenderá y dominará:

- Una fuente de información, que produce un mensaje.
- Un transmisor, que codifica el mensaje en señales.
- Un canal, por el que las señales se adaptan para la transmisión.
- Un receptor, que "decodifica" (reconstruye) el mensaje de la señal.
- Un destino, donde llega el mensaje.
- Propiedades formales de los signos y los símbolos.
- Las relaciones entre los signos/expresiones y sus usuarios.
- Las relaciones entre los signos y los símbolos y lo que representan.

El modelo de comunicación debe ser preciso a manera de lograr credibilidad, explotar los rasgos de rol, lograr que el blanco asuma el rol desviando la atención del pensamiento sistemático de la víctima, eliminando el procesamiento de resolución de problemas de manera sistemática, anulando momentáneamente las reglas de la lógica y dominar al sujeto de manera emocional explotando el miedo y la reactancia[39].

Al desarrollar un *Phishing* se toma en cuenta.

- La fuente: Es el origen de la información que analiza e interpreta el ingeniero social, por ejemplo, una base de datos, perfiles web, historiales médicos.
- El canal: Es la forma de envío (correo electrónico, mensaje de texto, llamada. etc)
- El mensaje: Probablemente, la parte más importante del mensaje (pretexting), redactado de forma adecuada, tomando en cuenta el idioma, la formalidad, la presión y la urgencia que desea comunicar al receptor en el supuesto de ser dirigido a una persona o receptores en el caso de ser masivo.
- El receptor o receptores: Este es el objetivo (víctima).
- La retroalimentación: ¿Qué quiere que hagan después de transmitirles correctamente la comunicación? (aportación de datos)[40].

---

[39] ANTOKOLETZ HUERTA, *Ingeniería social,*. 17-25. [en línea]. [03/06/2022]. [https://www.researchgate.net/publication/327285308_Ingenieria_Social].

[40] HADNAGY, *Ingeniería Social el Arte del Hacking personal,* 2011, 83 ss.

IV. ESTAFA INFORMÁTICA

1. Consideraciones generales

El *Phishing* es un delito informático cometido a distancia, instantáneo en el tiempo[41] y generalmente en masa[42]. También es conocido como un delito para cometer otros, que guardan relación con la informática; este es el medio para cometer el delito, que ha sufrido cambios exponenciales debido a las nuevas formas de comunicación, los nuevos intereses, la accesibilidad a la red, la desubicación y los nuevos grupos sociales[43].

El *Phishing* es un ciberdelito en sentido impropio o sentido amplio, por ser aquel en donde el uso de las TIC son el medio comisivo para atentar contra otros bienes jurídicos individuales; las TIC presentan un protagonismo esencial en el mismo, por ser el medio comisivo y porque, además, se utilizan para su ejecución las funciones propias del ordenador: el procesamiento, la transmisión y automatización de datos y la utilización de programas para tales fines[44].

---

[41] Desde el punto de vista jurídico-penal, se diferencia entre delitos instantáneos y delitos permanentes y de estado. Sobre delito instantáneo: Es el que se consuma en un momento, el que no puede prolongarse en el tiempo. Para determinar ese carácter, es preciso atenerse al verbo, con el que la figura respectiva define la conducta o el resultado típico. La forma o el modo de ejecución del delito tiene poco significado para esta distinción, ya que la prolongación en el tiempo del proceso ejecutivo no es lo que importa, sino el tiempo de la consumación.
ENCICLOPEDIA JURÍDICA, *Delito instantáneo*. [04/07/2022]. [en línea]. [http://www.enciclopedia-juridica.com/d/delito-instant%C3%A1neo/delito-instant%C3%A1neo.htm].

[42] En Derecho Penal se cuenta con la clasificación de delito masa: es aquel que afecta a los intereses difusos de una generalidad o "masa" indeterminada de individuos. El CP lo distingue del delito continuado por tratarse de infracciones contra el patrimonio, con notoria gravedad y que perjudican a una pluralidad de personas. "Masa" en el sentido técnico-penal equivale a público en general o consumidores, y para ser víctimas de un fraude concreto, debe existir un número elevado de perjudicados (todos los que contribuyen a una obra caritativa fraudulenta; los que adquirieron bonos o sellos de sociedades que ofrecían pingües beneficios, que no era tales, etc). Su regulación aparece en el art. 74.2 segundo inciso CP. LA LEY, *Guías jurídicas: Delito en masa* [04/07/2022]. [en línea]. [https://guiasjuridicas.wolterskluwer.es/Content/Documento.aspx?params=H4sIAAAAAAAEAMtMSbF1jTAAAUMjI3NDtbLUouLM_DxbIwMDCwNzAwuQQGZapUt-ckhlQaptWmJOcSoAenxOMTUAAAA=WKE#I58].

[43] VELASCO NÚÑEZ, *Delitos Tecnológicos,* 2021, 30.

[44]Los ciberdelitos en sentido amplio: El cibercrimen hace referencia a que la modalidad comisiva del delito consiste en el abuso de las TIC. Ello permite catalogar como tales a una gran variedad de conductas cuyo ataque implica a los más variados bienes jurídicos . i. Nuevas tipologías de ataque a viejos bienes jurídicos. En esta categoría vamos incluir aquellos comportamientos que constituyen nuevas modalidades de ataque a bienes jurídicos y que ha sido necesario tipificar de manera expresa, pues de lo contrario el hecho resultaba típico. Es posible que la nueva modalidad delictiva encuentre similitudes con los delitos presidentes que podían cometer fuera de las TI, pero no encaja exactamente en la definición. en; CÁMARA ARROYO/CANO CARRILLO/GARCÍA RUIZ/GIL GIL (coord.)/HERNÁNDEZ BERLINCHES (coord.)/MARTÍN FERNÁNDEZ/PASTOR VARGAS/ROBLES GÓMEZ/TOBARRA ABAD, *Cibercriminalidad,* 2019, 158-165.
Los aspectos que permiten distinguir los delitos comunes o informáticos en sentido amplio de los cibercrímenes es, precisamente, que los objetos digitales son al mismo tiempo medios virtuales (ámbitos) inherentes de ejecución del delito y el objeto final sobre el que se ejecuta la acción cibercriminal.93 POSADA MAYA. *El cibercrimen y sus efectos en la teoría de la tipicidad: de una realidad física a una realidad virtual. 93.*

Otra parte de la doctrina encuadra al *Phishing* simple dentro de los delitos informáticos en sentido estricto[45] o lato, bajo el razonamiento de constituir una alteración de datos[46].

Una de las cuestiones que se han planteado a la hora de realizar el presente trabajo ha sido si el *Phishing* simple es en realidad o no una estafa informática del art. 248.2 CP. O dicho de otra manera, si no se tratará simplemente del delito de estafa del art. 348.1 CP. La cuestión se plantea debido a la conceptualización que el *Phishing* simple es solo una estafa sociológica a través de internet y las TIC, pues precisan del engaño bastante a otro ser humano, mediante reclamos de ingeniería social, que produzca en la víctima un error tal que le lleve a realizar un acto de disposición de contenido económico en su perjuicio o en perjuicio de un tercero, y solo en casos donde añada *malware* o links este se considerara manipulación informática[47]. [48]Como lo expone el apartado respectivo de "Ingeniería social" esta es metódica, y por lo

---

[10/07/2022]. [en linea]. [file:///home/chronos/u-ab4b79542e3553828d070ffa3039bf9e8e20557b/MyFiles/Downloads/Dialnet-ElCibercrimenYSusEfectosEnLaTeoriaDeLaTipicidad-6074006.pdf].

El concepto de cibercrimen (o ciberdelitos) en sentido amplio, abarca tanto delitos comunes que se ejecutan a través de medios informáticos, como nuevos delitos, cuya ejecución sólo es posible gracias a la existencia de dichos medios. Esto implica que la respuesta a este tipo de criminalidad apele tanto a la legislación general como a leyes especialmente diseñadas para combatirla, sin perjuicio de que se critique la inadecuación de la legislación basada en la jurisdicción estatal para perseguir un fenómeno de alcance global. *CAVADA HERRERA. Cibercrimen y delito informático: Definiciones en legislación internacional, nacional y extranjera. 6. [10/07/2022]. [en linea]. [https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/29012/2/Definicion_y_regulacion_de_cibercrimen_y_delito_informatico_JPC_edit.pdf].*

los delitos informáticos en sentido amplio o, lo que es lo mismo, de los delitos tradicionales cometidos a través de computadoras y, muy especialmente, de internet (v. gr., extorsión o difusión de pornografía infantil), amerita una investigación específica, a propósito del delito tradicional de que se trate.MAYER LUX.*Elementos criminológicos para el análisis jurídico-penal de los delitos informáticos.* [10/07/2022]. [en línea].[https://www.redalyc.org/journal/197/19758807005/html/].

[45] Los cibercrímenes en sentido estricto vendrán a proteger un nuevo bien jurídico que algunos concretan en la seguridad informática, y otros, siguiendo más literalmente la redacción del convenio de Budapest en la en la confidencialidad, integridad y la disponibilidad (o funcionalidad de los sistemas informáticos Se trata de un bien jurídico colectivo antepuesto, es decir, una barrera que adelanta la protección de otros bienes jurídicos individuales, o incluso, en este caso, también supraindividuales, pues la protección de los propios sistemas informáticos, su confidencialidad, su integridad y funcionalidades, viene a adelantar la protección de bienes como la intimidad del patrimonio, pero también de otros como la propiedad intelectual la fe pública el libre mercado la seguridad del Estado y otros muchos intereses públicos tal y como viene el manifiesto de la directiva 2000/13 / 40 UE del Parlamento Europeo , de 12 de agosto de 2013, relativa a los ataques contra sistemas de información de seguridad del Estado. Pero a la vez tienen dimensión positiva, al garantizar las condiciones en las que pueden desarrollar esos otros bienes jurídicos en el ámbito de las TIC. en; CÁMARA ARROYO/CANO CARRILLO/GARCÍA RUIZ/GIL GIL (coord.)/HERNÁNDEZ BERLINCHES (coord.)/MARTÍN FERNÁNDEZ/PASTOR VARGAS/ROBLES GÓMEZ/TOBARRA ABAD, *Cibercriminalidad,* 2019, 158-165.

ciberdelitos en sentido estricto únicamente aquellas conductas en las que el Código Penal haga específica alusión a la afectación o utilización de sistemas informáticos o los que presenten una modalidad de comisión habitual a través de las TIC. CANO TERUEL *Ciberdelincuencia en el Código Penal. [10/07/2022].[en linea].[https://cibercrim.com/ciberdelincuencia-en-el-codigo-penal/].*

[46] VELASCO NÚÑEZ, *Delitos Tecnológicos,* 2021, 23.

[47] Se plantea esta cuestión VELASCO NÚÑEZ, *Delitos Tecnológicos,* 2021, 41, 42, 46, 47, 49.

[48] VELASCO NÚÑEZ, *Delitos Tecnológicos,* 2021, 41, 42, 46, 47, 49.

tanto organizada, requiere de un análisis y estudio previo profundo, por lo cual el implementarla da sustento que el *Phishing* simple, que sin necesidad de auxiliarse de un malware puede consumarse de la misma manera y con la misma eficacia de los Phishing medios y avanzados.

La estafa informática en su variante *Phishing*, aparece regulada en el art. 248.2 CP; puede ser clasificada tomando en consideración varios criterios, tales como *el bien jurídico, la intencionalidad* y por su relación con el *medio informático.*

Por el bien jurídico

A la vista de la ubicación sistemática de esta figura delictiva, el patrimonio es el bien jurídico que se persigue proteger y, por tanto, el que se afecta con el Phishing; esta nueva modalidad de ataque (art. 248.2 CP) contiene similitudes con la estafa tradicional preexistente (art. 248.1 CP) donde los elementos de engaño bastante y error son sustituidos por la manipulación informática[49].

Por la intencionalidad

Como se deduce de lo explicado en el párrafo anterior, es la motivación económica[50]. Los sujetos activos del *Phishing* tendrán siempre la intención de lucrarse por medio del desplazamiento de bienes cuantificables. El delito de estafa informática requiere de ánimo de lucro. Pero, el autor luego puede tener otras motivaciones adicionales, como podría ser, el cumplimiento de un reto intelectual, práctica muy común en las iniciaciones o procesos de incorporación a grupos criminales, consiste en una evaluación de las habilidades del candidato, donde el grupo criminal le presenta un blanco a batir, pudiendo ser una empresa, partido político, secretaría de estado etc. al aprobar, es aceptado dentro del grupo criminal.

El objeto del ataque dependerá de la misión del grupo criminal, si es tendente a hacer Hacktivismo buscando la obtención de información que pueda ser utilizada en nota amarilla de índole política o si el grupo criminal es tendente al lucro, busca dinero o bienes valuables en dinero. El objeto del grupo criminal puede ser establecido por un contrato, el grupo al exponer servicios en sitios web dentro de la Deep web y Dark web, ofrece un catálogo de posibles prestaciones, medio de pago y garantía de entrega del servicio. Por financiación de

---

[49] CÁMARA ARROYO/CANO CARRILLO/GARCÍA RUIZ/GIL GIL (coord.)/HERNÁNDEZ BERLINCHES (coord.)/MARTÍN FERNÁNDEZ/PASTOR VARGAS/ROBLES GÓMEZ/TOBARRA ABAD, *Cibercriminalidad,* 2019, 157.

[50] VELASCO NÚÑEZ, *Delitos Tecnológicos*, 2021, 24.

un estado, respetando el mando e indicaciones del financiador su objeto puede ser; de espionaje, sabotaje, robo o destrucción de datos, etc. Objeto por venganza, miembros de grupos criminales que al conocer una organización desde dentro, ante el recelo y desprecio por la finalización de su relación laboral quedaron inconformes y buscan, utilizando credenciales de antiguos compañeros o valiéndose de vulnerabilidades conocidas, entrar al sistema, robar datos para venderlos a competidores y, aumentando el daño a la organización, deciden realizar un ransomware[51].

Por su relación con el medio informático

El delito de estafa precede al nacimiento de internet y las TIC, pero al incursionar estas en la vida cotidiana de los ciudadanos, en la banca y en el gobierno, los actores empezaron a asistirse de las Tic para la realización de estafas, esta clasificación es conocida como "computer assisted Crimes".

2. Fases del Phishing

A continuación se van a explicar las fases de realización del Phising, desde un plano "fáctico", esto es, ajeno a su explicación desde planteamientos jurídico-penales, para posteriormente conocer el alcance de la protección de los usuarios frente a comportamientos engañosos a través del Derecho penal[52].

1-Averiguación de datos que responden a contraseñas de cuentas que utiliza la víctima, donde se utilizan técnicas de ingeniería social como el envío masivo de correos haciéndose pasar por una entidad bancaria, un prestador de servicios[53] o un proveedor de servicios de pago[54].

2-Acceso a la cuenta cuya contraseña se ha obtenido ilícitamente.

---

[51] CÁMARA ARROYO/CANO CARRILLO/GARCÍA RUIZ/GIL GIL (coord.)/HERNÁNDEZ BERLINCHES (coord.)/MARTÍN FERNÁNDEZ/PASTOR VARGAS/ROBLES GÓMEZ/TOBARRA ABAD, *Cibercriminalidad,* 2019, 157.

[52] Sobre las distintas fases del *Phishing*, *Memento Experto Ciberseguridad,* 2021, 275.

[53] Concepto sobre prestador de servicios Art. 2 LSSICE: persona física o jurídica que proporciona un servicio de la sociedad de la información", teniendo la consideración de servicios de la sociedad de la información los servicios prestados normalmente a título oneroso, a distancia, por vía electrónica y a petición individual del destinatario.

[54] Los servicios de pago, regulados en el art 1 del Real Decreto-ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera, son: Los servicios que permiten el ingreso de efectivo en una cuenta de pago y todas las operaciones necesarias para la gestión de una cuenta de pago; los servicios que permiten la retirada de efectivo de una cuenta de pago y todas las operaciones necesarias para la gestión de una cuenta de pago; la ejecución de operaciones de pago, incluida la transferencia de fondos, a través de una cuenta de pago en el proveedor de servicios de pago del usuario u otro proveedor de servicios de pago; la ejecución de operaciones de pago cuando los fondos estén cubiertos por una línea de crédito abierta para un usuario de servicios de pago; la emisión de instrumentos de pago o adquisición de operaciones de pago; el envío de dinero; los servicios de iniciación de pagos; los servicios de información sobre cuentas.

3-Realización de transferencias de datos o servicios cuantificables en dinero que suponen un perjuicio patrimonial a un tercero.

4-Receptación del dinero, bien o servicio, y, en caso de que intervengan muleros, este realizará una posterior remisión a otra u otras personas.

Tras estas consideraciones previas sobre el *Phishing*, es momento de entrar a explicar con cierto detalle los elementos típicos del art. 248.2 CP.

3. El bien jurídico protegido

El art. 248.2 CP está ubicado dentro del Capítulo dedicado a las estafas, en el Título XIII del Libro II CP relativo a los delitos contra el patrimonio y el orden socioeconómico.

De esta ubicación sistemática se deduce que el objeto de protección es el patrimonio.[55]

---

[55] el bien jurídico protegido en general es la información, pero está considerada en diferentes formas, ya sea como un valor económico, como uno valor intrínseco de la persona, por su fluidez y tráfico jurídico, y finalmente por los sistemas que la procesan o automatizan; los mismos que se equiparan a los bienes jurídicos protegidos tradicionales tales como: € EL PATRIMONIO, en el caso de la amplia gama de fraudes informáticos y las manipulaciones de datos que da a lugar. ACURIO DEL PINO. *Delitos Informáticos: Generalidades.20.* [10/07/2022]. [en linea]. [https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf].
La afectación de bienes jurídicos propia del fraude informático se identifica, en todos los casos, con la vulneración del patrimonio de la víctima. MAYER LUX/ OLIVER CALDERÓN. *El delito de fraude informático: Concepto y delimitación.* [10/07/2022]. [en linea]. [file:///home/chronos/u-ab4b79542e3553828d070ffa3039bf9e8e20557b/MyFiles/Downloads/mcoloma,+Gestor_a+de+la+revista,+mayer.pdf].
El tipo penal de la estafa protege el patrimonio. En los casos de Phishing si hay un pequeño engaño inicial al incitar a la víctima a dar sus claves personales, pero una vez obtenidos los datos sensibles no es necesario más contacto entre ambos. En esta segunda fase no existe engaño ni error como tal que motive alguna variación en el patrimonio de la víctima. GONZALEZ SUÁREZ. Fraudes en internet y estafa informática.[10/07/2022]. [en linea].
[https://digibuo.uniovi.es/dspace/bitstream/handle/10651/27824/TFM_Gonzalez%20Suarez%2C%20Marcos.pdf?sequence=3&isAllowed=y].
En cuanto bien jurídico protegido, podemos decir que es el patrimonio ajeno, ya sea en sus distintos elementos que lo integran, como bienes muebles, inmuebles o derechos, etcétera. Además de ello se puede mencionar que también se ve afectada la buena fe, tomada como la que debe tener todo contratante o sujeto en el tráfico jurídico, puesto que se elimina o se cambia la esperanza que lo adquirido o lo supuestamente pactado no corresponde a la realidad. Teniendo la estafa un contenido patrimonial, que no permite castigar la frustración de expectativas derivadas del tráfico jurídico económico, pero que no perjudican económicamente nadie en concreto, trascendiendo los derechos patrimoniales individuales a los derechos lesionados de los consumidores. Sin embargo es recomendable señalar que las tasas el delito patrimonial por excelencia, es el nombre siguiendo el tipo penal la protección de la propiedad, ni la posesión o título de crédito, sino que por el contrario patrimonio de una persona valores económicos, todo esto como expresión del desarrollo de la personalidad. DEVIA GONZALEZ. *Delito Informatico: Estafa informática del articulo 248.2 del Codigo Penal.* 247-269 [10/07/2022]. [en linea].

La mayoría de los ciberdelitos están motivados por el lucro, el enriquecimiento a costa de la depreciación de otro, por ello debemos entender que el patrimonio en el Phishing debe ser interpretado de manera amplia, no solo aquel patrimonio inmerso en cuentas bancarias, si bien es el objeto principal de la mayoría, también debemos considerar bienes o servicios que son valuables que, de perderse, suponen un decrecimiento del patrimonio de la víctima[56].

Una vez fijado el bien jurídico protegido por el delito de estafa informática, se ha de tener presente que, sobre el concepto de patrimonio, no hay acuerdo interpretativo; sobre este particular se utilizan diferentes conceptos de patrimonio, lo que repercute en la mayor o menor amplitud aplicativa de los delitos ubicados en el Título XIII:

- Concepto jurídico. El conjunto de los derechos subjetivos patrimoniales. Esta conceptualización no entiende dentro del patrimonio las posiciones que poseen valor económico, como las ganancias y clientela, pero si formarán parte del patrimonio aquellos derechos subjetivos patrimoniales carentes de valor económico, una carta personal, por valor de apreciación del propietario.

- Concepto económico. Es el conjunto de bienes de valor económico de una persona, determinado por los criterios del valor que tiene el bien o posición de poder en el mercado y el valor de utilidad que posee ese bien para su titular.

- Concepto mixto jurídico-económico. Conjunto de bienes de valor económico que gozan de apariencia jurídica. No entran dentro del patrimonio los bienes carentes de valor económico por el mero afecto del propietario, tampoco los bienes carentes de apariencia jurídica[57].

El patrimonio es un conjunto de derechos y obligaciones referibles a cosas u objetos, materiales e inmateriales, que tienen un valor económico y que deben de ser valorables en dinero, como mínimo un valor estimable[58]. En sentido amplio, siguiendo la concepción mixta jurídico-económica del patrimonio, de esta forma de entender el bien jurídico se derivan una serie de rasgos o consecuencias como las siguientes:

[https://idus.us.es/bitstream/handle/11441/75625/Tesis%20Edmundo%20Devia%20Completa%20Final%2031%20Mayo%202017.pdf?sequence=1&isAllowed=y]·

[56] MATA Y MARTÍN, *Delincuencia Informática y Derecho Penal,* 2001, 46.

[57] RAGUÉS i VALLÉS en; AYALA GÓMEZ/ORTIZ DE URBINA GIMENO (coord.), *Memento penal económico y de la empresa*, 2016, 413-415.

[58] Art. 23.2 REGLAMENTO (CE) 1186/2009 DEL CONSEJO, de 16 de noviembre de 2009, sobre el valor estimable: «mercancías sin valor estimable» se entenderá las mercancías cuyo valor intrínseco no supere los 150 EUR en total por envío.

1. El objeto material de un delito patrimonial sólo pueden serlo aquellos bienes dotados de valor económico.

2. Para ser sujeto pasivo no basta con la simple relación física con la cosa, se requiere que esté relacionada con ella en virtud de una relación protegida por el ordenamiento jurídico.

3. Por perjuicio patrimonial hay que entender toda disminución, económicamente evaluable, del acervo patrimonial que, jurídicamente, corresponde a una persona[59].

El contenido del patrimonio está compuesto por obligaciones, no solo por derechos, reales o no; la propiedad es uno de estos derechos, al igual que la posesión, pero, claro está, hay más derechos que forman parte del patrimonio. Partiendo de este bien jurídico genérico o global, a través de las diferentes figuras delictivas que se engloban en el Título XIII se pueden proteger determinados aspectos o derechos que se engloban en él. En el caso del Phishing, este es un delito que se dirige sobre elementos integrantes del patrimonio total, sin concretarse en uno. El patrimonio está compuesto por relaciones jurídicas que tienen valor económico, sin perjuicio de que algunas de esas relaciones tengan también incidencia en ámbitos socio económico[60] la cartera de clientes, o socios, relaciones comerciales, alianzas estratégicas de mercado.

Un ejemplo de un Phishing que afecta al patrimonio de relaciones jurídicas es un correo Phishing de nivel medio, donde adquieren datos de acceso con la intención de robar los datos de una cuenta no bancaria, buscan la cuenta de un servicio (cuenta de sistema operativo de respaldo correo electrónico) mediante la cual sustraen información sensible de su cartera de clientes, para después extorsionar y solicitar el pago en bitcoin con la promesa de no divulgar a los contactos.

En resumen el patrimonio digital comprenderá, por la gran cantidad de operaciones financieras, depósitos de fondo, tráfico económico[61] y no económico (tráfico de datos en redes sociales) todo tipo de activos, tanto materiales como inmateriales, muebles o inmueble, tangibles o intangibles, así como los documentos o instrumentos que acrediten la propiedad de dichos activos o un derecho sobre los mismos, bienes que en todo caso han de ser susceptibles

---

[59] MUÑOZ CONDE, *Derecho penal. Parte Especial*, 23ª, 2021, 367 [10/05/2022]. [https://biblioteca-tirant-com.unileon.idm.oclc.org/cloudLibrary/ebook/show/9788413979076].

[60] MUÑOZ CONDE, *Derecho penal. Parte Especial,* 23ª, 2021, 368 [10/05/2022]. [https://biblioteca-tirant-com.unileon.idm.oclc.org/cloudLibrary/ebook/show/978841397907].

[61] FLORES PRADA, *Criminalidad Informática aspectos sustantivos y procesales,* 2012, 286 [10/05/2022]. [https://biblioteca-tirant-com.unileon.idm.oclc.org/cloudLibrary/ebook/show/978849033570].

de una valoración económica y, por lo tanto, idóneos para ser incorporados al tráfico mercantil o económico, así como al patrimonio[62].

4. El sujeto activo

Desde el análisis dogmático, la explicación del sujeto activo del delito de estafa informática es relativamente sencilla; nos encontramos ante un delito común, que puede cometerlo por tanto cualquier persona. No se requiere de una cualidad o circunstancia especial para la realización del hecho a título de autor. Más adelante se retomará la cuestión del sujeto activo, explicado desde la perspectiva jurídico-penal.

Mayor interés puede tener el análisis del sujeto activo desde el plano criminológico. El *phisher* es un ciberdelincuente de cuello blanco[63], el autor del fraude informático denominado Phishing posee características generales y, a medida que se va profesionalizando respecto a la elaboración de *Phishings* de nivel medio o avanzado, va adquiriendo rasgos específicos. Al principio se encuentra en el estándar de la versatilidad, un *Phisher* novato lo puede ser cualquiera con un dominio mínimo de las TIC, un consumidor medio es capaz de cometer un *Phishing* simple al poseer las capacidades técnicas de nivel de usuario si tiene habilidades digitales trabajadas y está sumamente familiarizado con el uso de las TIC. La elaboración de *Phishing* medio ya requiere de conocimientos técnicos avanzados; respecto de los usuarios medios, el Phisher novato, en búsqueda de elevar su eficiencia y, por tanto, sus ganancias, o buscando el ingreso en un grupo criminal, se verá impulsado a adquirir conocimientos. Dentro de una organización criminal se refuerza la cadena criminológica, donde los *Phisher* veteranos y competentes, de manera análoga a una universidad, transmiten el conocimiento y técnicas, haciendo crecer cualitativamente a los integrantes nuevos y así se mantienen actualizados los procesos[64], la actualización del *modus operandi*[65]: la implementación de *malware* nuevo, la mejora del *speach* (contenido del correo electrónico) y el análisis del

---

[62] *REBOLLO VARGAS, en; GARCIA ARÁN (Dir.)La delincuencia económica Prevenir y Sancionar, 2015, 145 [10/05/2022]. [https://biblioteca-tirant-com.unileon.idm.oclc.org/cloudLibrary/ebook/show/9788490536667].*

[63] VELASCO NÚÑEZ/SANCHÍS CRESPO, *Delincuencia Informática Tipos Delictivos e Investigación. Con jurisprudencia tras la reforma procesal y penal de 2015,* 2019, 24.

[64] MATA Y MARTÍN, *Delincuencia Informática y Derecho Penal,* 2001, 25.

[65] CÁMARA ARROYO/CANO CARRILLO/GARCÍA RUIZ/GIL GIL (coord.)/HERNÁNDEZ BERLINCHES (coord.)/MARTÍN FERNÁNDEZ/PASTOR VARGAS/ROBLES GÓMEZ/TOBARRA ABAD, *Cibercriminalidad,* 2019, 88.

blanco potencial. Dicho con otras palabras, es esta retroalimentación la que permite que un ciberdelincuente novato pase de cometer un *phishing* simple a uno medio y posteriormente a uno avanzado en poco tiempo.

Los tipos y perfiles de los ciberataques son diversos y pueden ser abordados y analizados desde diversas ópticas[66]. Prevalece el predominio masculino, con un coeficiente intelectual medio y sujeto joven con fines de lucro inmediatos[67]. El crecimiento de los ciberdelincuentes es propiciado por las misma características del Internet y las TIC, la accesibilidad es un elemento a destacar, toda vez que mediante una búsqueda en simple, en un motor de búsqueda o una red social, permite a los usuarios ingresar, participar, investigar y adiestrarse en foros relacionados con ciber crímenes, hackers, etc., mismos que son administrados y controlados por grupos criminales, *emugers* o ciber bandas; estos reclutan soldados rasos y son los mismos grupos los que impulsan por medio de pago a los generadores de malware que posteriormente venderán a las personas que, por diversas razones, fundamentalmente por falta de conocimientos y preparación, son incapaces de programarlos. Este círculo vicioso es alimentado por otra característica permitida en el ciberespacio; la anonimización[68] lo que aumenta las dificultades para la averiguación y persecución de *Phishings*[69].

El *phisher*, aquel que realiza la manipulación informática[70] puede caber en múltiples categorías, al ser un delito muy amplio, pues abarca supuestos de manipulación muy simples, pero también casos de actuaciones muy complejas y sofisticadas, por tanto se extiende sobre un elenco de supuestos atendiendo a los mínimos y máximos requerimientos técnicos y económicos: podrá ser un sujeto desestructurado[71] o con un escaso nivel económico; por lo general no tendrá relación interpersonal[72] con la víctima; puede tener conexión con una organización criminal o no; cualquier individuo medio con una conexión a internet también

---

[66] CUEVAS RUIZ, *El papel de la Ciberseguridad en el proceso de la transformación digital en México,* 8. [en línea] [20/05/2022]. [https://centrodeestudios.ift.org.mx/documentos/publicaciones/2021/1er_Sem_JLCR_El_papel_de_la_Ciberseguridad_en_el_proceso_de_la_transformaci%c3%b3n_digital_en_M%c3%a9xico.pdf].

[67] DE LA CUESTA ARZAMENDI/PÉREZ MACHÍO, en: DE LA CUESTA ARZAMENDI (dir.)/DE LA MATA BARRANCO (coord.), *Derecho Penal Informático,* 2010, 100.

[68] Sobre la anonimización: es la facultad de desprenderse de una identidad física y ejecutar actos ilícitos de manera impune.

[69] MATA Y MARTÍN, *Delincuencia Informática y Derecho Penal,* 2001, 24, 26.

[70] SANCHÍS CRESPO, *Fraude electrónico su gestión penal y civil,* 2015, 95. [10/05/2022]. [https://biblioteca-tirant-com.unileon.idm.oclc.org/cloudLibrary/ebook/show/9788490865576].

[71] VELASCO NÚÑEZ/SANCHÍS CRESPO, *Delincuencia Informática Tipos Delictivos e Investigación Con jurisprudencia tras la reforma procesal y penal de 2015*, 2019, 24.

[72] FLORES PRADA, *Criminalidad Informática aspectos sustantivos y procesales,* 2012, 200 [10/05/2022]. [https://biblioteca-tirant-com.unileon.idm.oclc.org/cloudLibrary/ebook/show/978849033570].

puede desarrollar un *phishing*, solo requiere el conocimiento necesario para utilizar la herramienta.

La desubicación, el anonimato, la masividad de procesamiento y los nuevos canales de comunicación nuevamente cobran importancia al permitir atacar a nacionales o extranjeros (elemento internacional)[73], usuarios categorizados dentro de la brecha digital, adultos mayores y menores desde la distancia.

Se pueden diferenciar dos clases dentro del sujeto activo, experto e inexperto; y, a su vez, cuatro subclases para los inexpertos:

Los inexpertos, desde un menor de edad de 14-18 años y hasta 34 años; serán divididos en cuatro subgrupos; 1. los *Script kiddie*[74] caracterizados por la falta de habilidades técnicas, sociabilidad o madurez. 2. Y, en sentido opuesto, el nativo digital[75], por su mayor acceso, facilidad y control de esta clase de tecnologías. 3. Las personas que tienen conocimientos por encima del promedio. 4. El autodidacta, interesado en elevar su conocimiento del funcionamiento de las redes y computadoras, con conocimientos por encima del promedio[76].

---

[73] VELASCO NÚÑEZ, *Delitos Tecnológicos,* 2021, 30.

[74]Sobre los Script Kiddie: Un script kiddie es un término despectivo utilizado para referirse a hackers no serios que se cree que rechazan los principios éticos de los hackers profesionales, que incluyen la búsqueda del conocimiento, el respeto por las habilidades y un motivo de autoeducación. Script kiddies atrajo a la mayoría de los métodos de pirateo para ganar rápidamente sus habilidades de pirateo. No piensan demasiado o dedican tiempo a adquirir conocimientos de informática, pero se educan de manera rápida para aprender solo lo mínimo. Los niños de script pueden usar programas de pirateo escritos por otros hackers porque a menudo carecen de las habilidades para escribir los suyos. Intentan atacar redes y sistemas informáticos y destrozar sitios web. Aunque se consideran inexpertos e inmaduros, los niños de script pueden infligir tanto daño informático como los piratas informáticos profesionales y pueden estar sujetos a cargos criminales similares a los de sus homólogos más viejos y más inteligentes. Los niños de script ejecutan sus técnicas informáticas maliciosas simplemente por la emoción de ello, y para presumir ante sus compañeros sobre su destreza informática. Debido a que los kiddies de guiones son hackers profesionales, o simplemente porque carecen de habilidades técnicas, a menudo dejan evidencia de su trabajo. THEASTROLOGYPAGE. *Definición - ¿Qué significa Script Kiddie?*[en línea]-[05/07/2022]. [https://es.theastrologypage.com/script-kiddie].

[75] VELASCO NÚÑEZ/SANCHÍS CRESPO, *Delincuencia Informática Tipos Delictivos e Investigación Con jurisprudencia tras la reforma procesal y penal de 2015*, 2019, 29, 50.

[76] CÁMARA ARROYO/CANO CARRILLO/GARCÍA RUIZ/GIL GIL (coord.)/HERNÁNDEZ BERLINCHES (coord.)/MARTÍN FERNÁNDEZ/PASTOR VARGAS/ROBLES GÓMEZ/TOBARRA ABAD, *Cibercriminalidad,* 2019, 88-96, 104-105.

Experto cualificado en informática[77], también llamado adepto virtual, es un hacker, es un phisher que puede compartir características de comisión con un Sniffer[78], un banquero, Donmainer, viruckers[79], traficante de armas, espías informáticos[80].

Retomando la explicación del sujeto activo del delito de estafa informática, para esta explicación conviene tomar en consideración la redacción del art. 248.2 letras a) y b) CP:

En la letra a) se castiga al sujeto que consigue la transferencia no consentida de un activo patrimonial. Para lograr este objetivo tiene que valerse de una manipulación informática o de un artificio semejante. Autor será la persona que, a través de esa manipulación, consigue que el tercero realice un acto que implica el desplazamiento patrimonial en su perjuicio o en el de otro[81].

Pero el sujeto activo se describe de manera más amplia, a través de lo estipulado en el segundo párrafo del art. 248 CP: asimila y fija idéntica pena al fabricante, facilitador, introductor o incluso poseedor de programas específicamente, esto es, que no tengan un posible doble uso lícito, destinados o creados para estafar. Imponiendo la misma sanción a la mera detentación de software que no tiene otra finalidad que la de estafar con la estafa misma,

---

[77] Sobre experto cualificado: aquel que se encarga de apoyar de manera especializada los sistemas operativos y aplicaciones de distintos servidores tecnológicos. Lo cual logra a través de la observación, conservación y arreglo de los mismos, de forma controlada. EUROINNOVA. *Técnico en informática definición. [05/07/2022]*[en línea]. [https://www.euroinnova.edu.es/blog/tecnico-en-informatica-definicion#:~:text=Para%20hablar%20del%20t%C3%A9cnico%20en,los%20mismos%2C%20de%20forma%20controlada*]*.

[78] Sobre un snifer: aquel que controla un programa que monitoriza la circulación de datos a través de una red y que está encargado de buscar cadenas numéricas o de caracteres que pueden utilizarse con fines de gestión, totalmente inofensivos, o con otros que pueden resultar peligrosos para la seguridad de una red. En: BLOG:INTERDOMINIOS, *Sniffer, la nueva amenaza aumenta cada día su importancia.* [en línea]. [05/07/2022]. [https://blog.interdominios.com/sniffer-la-amenaza-que-va-cobrando-mas-importancia/].

[79] Sobre los Viruckers: Los viruckers son creadores de virus. Su principal objetivo es introducir un virus informático en un sistema para destruirlo, alterarlo o inutilizarlo. Les gusta actuar de forma individual, por lo que no existe un sentimiento de comunidad. Son un grupo altamente peligroso y con una gran difusión. No disponen de ningún tipo de código ético. FANJUL FERNÁNDEZ, en: APARICIO ORDAZ (coord.), *Conceptualización, evolución y clasificación del ciberdelito empresarial*, 2018, 106 [en línea]. [05/07/2022]. [https://es.eserp.com/wp-content/uploads/2019/09/conceptualizacion-evolucion-y-clasificacion-del-ciberdelito-empresarial.pdf].

[80] CÁMARA ARROYO/CANO CARRILLO/GARCÍA RUIZ/GIL GIL (coord.)/HERNÁNDEZ BERLINCHES (coord.)/MARTÍN FERNÁNDEZ/PASTOR VARGAS/ROBLES GÓMEZ/TOBARRA ABAD, *Cibercriminalidad,* 2019, 99-104.

[81] Identificación de un autor en el art 248.2: en materia de comunicaciones electrónicas, se ha admitido como indicios probatorios el hecho de que la dirección IP utilizada en una concreta conducta antijurídica se correspondiera con el domicilio de un pariente del acusado y no de éste mismo; la geolocalización del terminal móvil del acusado en las inmediaciones del lugar de los hechos y en horas próximas a su comisión; el uso de pseudónimos (nicknames) en diversas redes sociales; así como informes periciales lingüísticos para determinar la autoría de un correo electrónico o un SMS. En: CRESPO SANCHÍS, *Fraude electrónico su gestión penal y civil*, 2015, 88. [10/05/2022]. [https://biblioteca-tirant-com.unileon.idm.oclc.org/cloudLibrary/ebook/show/9788490865576].

aunque no haya habido tiempo de desarrollarla, en la doble consideración de que la finalidad sin alternativa legal de su posesión supone y equivale a la consumación misma ante la imposibilidad de otro uso lícito y porque esta es la única manera de penar a los programadores, creadores e inventores de software estafador que normalmente venden anónimamente para que otros se bajen de Internet. Estos difícilmente pueden ser sorprendidos de otra manera con esa parte tan estratégica en la confección del delito sin la cual no habría infracción, dado que estas acciones suelen realizarse masivamente a través de estructuras criminales organizadas en las que, atomizando la acción penal, cada componente aporta a la cadena delictiva[82]. El alcance de esta modalidad deberá establecerse a través del bien jurídico protegido, haciendo una interpretación del fin de protección de la norma.

A través de esta modalidad se están castigando realmente conductas de preparación de las estafas informáticas, ya que el legislador pretende su castigo, y con la misma pena, sin necesidad de probar que se han usado, entendiendo que el software tendrá el único y específico fin de defraudar[83]; demostrada esta finalidad delictiva, se estarían penando actos que, planteados desde otros delitos diferentes, no pasarían de ser considerados meramente preparatorios o a más, de tentativa[84], por ejemplo, en el art. 197 bis CP: la posesión o tenencia de programas informáticos o claves preordenadas al hacking sólo es considerado como acto preparatorio. La razón es que un *virucker* será el principal difusor del programa informático (*malware*), siendo un experto cualificado que contribuye directa o por medio de un grupo criminal a proporcionar a los inexpertos *scripts kiddies* las mencionadas herramientas (*malwares*). La redacción del segundo párrafo parece la manera teórica más efectiva de atacar la cadena criminológica[85].

4. 1. Los muleros

Son llamados mulas, ciber mulas, receptores o Phisher-mule[86], aquellas personas que completan la fase de agotamiento del delito al realizar la conducta. Aquella persona que pone

---

[82] VELASCO NÚÑEZ/SANCHÍS CRESPO. *Delincuencia Informática Tipos Delictivos e Investigación Con jurisprudencia tras la reforma procesal y penal de 2015,* 2019, 29, 30.
[83]GUÉREZ TRICARICO, en: MOLINA FERNÁNDEZ (coord.), *Memento práctico penal,* 2021, 1356.
[84] MUÑOZ CONDE, *Derecho penal. Parte Especial,* 23ª, 2021, 415 [10/05/2022]. [https://biblioteca-tirant-com.unileon.idm.oclc.org/cloudLibrary/ebook/show/978841397907].
[85] VELASCO NÚÑEZ, *Delitos Tecnológicos,* 2021, 43, 49.
[86] GUÉREZ TRICARICO, en: MOLINA FERNÁNDEZ (coord.), *Memento práctico penal,* 2021, 1556.

su cuenta bancaria a servicio de los autores del *phishing* o fraude. El mulero es captado a través de internet, normalmente a través de un correo electrónico recibe un encargo, negocio o una supuesta oferta de trabajo a cambio de una cantidad económica o comisión. El trabajo del «mulero» consiste en facilitar los datos de una cuenta bancaria a su nombre y recibir en la misma una transferencia o cantidad de dinero que el autor del fraude ha obtenido, a través de una manipulación informática, de la cuenta de un perjudicado o víctima. Y, a su vez, el mulero debe transferir definitivamente esa cantidad, descontada la comisión pactada, a las cuentas que le indique el defraudador, que son cuentas de terceras personas desconocidas que se encuentran en paraísos fiscales o en países que no han firmado el Convenio de Cibercriminalidad, con los que no existe posibilidad real de extradición[87]. Los famosos *muleros* regularmente son atraídos a la cadena delictiva por las organizaciones delictivas (y por lo general no pertenecen a estas) mediante simulación de una oferta de trabajo, a manera de abrir o utilizar la propia cuenta bancaria para recibir el producto de la estafa, dificultado, de esta manera, el descubrimiento de los criminales[88].

Los muleros suponen un problema a la hora de calificar el grado de su intervención en la estafa informática.

Para un sector doctrinal se está ante un supuesto de coautoría[89]. Para otro sector doctrinal se trata de una intervención cooperador necesario, pues su actividad es relevante y esencial, pero está la falta de cooperación decisiva[90]. Aunque no tiene control ni dominio del hecho, tendrá el mulero en todo caso un dominio negativo de la fase de agotamiento toda vez que sin su participación el plan del autor se detendría[91].

---

[87] CRESPO SANCHÍS, *Fraude electrónico su gestión penal y civil,* 2015, 99. [https://biblioteca-tirant-com.unileon.idm.oclc.org/cloudLibrary/ebook/show/9788490865576].

[88] CÁMARA ARROYO/CANO CARRILLO/GARCÍA RUIZ/GIL GIL (coord.)/HERNÁNDEZ BERLINCHES (coord.)/MARTÍN FERNÁNDEZ/PASTOR VARGAS/ROBLES GÓMEZ/TOBARRA ABAD, *Cibercriminalidad,* 2019, 249.

[89] Obviamente, para resolver la cuestión sobre la calificación jurídico-penal del mulero es presupuesto previo decidir qué teoría se va a mantener en materia de autoría (y participación). Esta es una cuestión que no puede ser analizada en este trabajo, por razones de espacio. La tesis planteada en el texto se ha defendido atendiendo a la teoría del dominio del hecho, según la cual es autor quien tiene el control del hecho, se suerte que domina la acción, controla su desarrollo y en su caso es quien puede interrumpirlo a su voluntad, lo que engloba la definición del art. 28 CP en cuanto se incluye al autor, al coautor en su caso y al autor mediato No cabe duda, al margen de la calificación del tipo delictivo como estafa o blanqueo, que el conocimiento previo de la trama o el acuerdo previo a la actividad de transferencia se torna en un elemento a menudo decisivo para configurar al intermediario como autor. En: CRESPO SANCHÍS, *Fraude electrónico su gestión penal y civil,* 2015, 10-25. [https://biblioteca-tirant-com.unileon.idm.oclc.org/cloudLibrary/ebook/show/9788490865576].

[90] VELASCO NÚÑEZ/SANCHÍS CRESPO, *Delincuencia Informática Tipos Delictivos e Investigación Con jurisprudencia tras la reforma procesal y penal de 2015,* 2019, 33-36.

[91] MUÑOZ CONDE/GARCÍA ARÁN, *Derecho penal. Parte General,* 10ª, 2019, 223 [10/05/2022]. [https://biblioteca-tirant-com.unileon.idm.oclc.org/cloudLibrary/ebook/show/978841313940].

Para determinar la calificación se debe atender a lo siguiente:

- Casos en los que el «mulero» sabe y quiere colaborar en una operación fraudulenta (dolo directo).
- Casos en los que el «mulero» presenta la probabilidad de estar colaborando en una operación fraudulenta y no hace nada para evitarlo, siendo para él indiferente el origen del dinero que recibe (dolo eventual).
- Casos en los que el «mulero» no sabe que colabora en una operación fraudulenta, pero podía y debía haberlo sabido si hubiera observado la diligencia o deber de cuidado que es exigible a una persona media (imprudencia).
- Y otros supuestos de desconocimiento de los hechos en los que no concurre dolo ni imprudencia[92].

La responsabilidad penal del mulero, si se lleva al ámbito de la participación, se va a admitir indiscutiblemente en los supuestos en los que actúa dolosamente, sea a título de dolo directo o dolo eventual; más controvertido es el supuesto de actuación imprudente, pues ello plantea la cuestión debatida con carácter general de si es punible o no en el Derecho penal español la participación imprudente.

Como cooperador necesario lo encontramos en lo expuesto en la Sentencia del Juzgado de lo Penal de Alicante núm. 296/2013, de 13 de septiembre. En esta sentencia justifican y califican al imputado como cooperador necesario toda vez que el sujeto “no niega la realidad de las transferencias recibidas". Sin embargo, alega que desconocía la procedencia ilícita de dicho dinero, y si bien es cierto que no le pareció normal que le pagaran por realizar algo tan sencillo como es recibir dinero en su cuenta, sacarlo, y enviarlo al extranjero, insiste en que desconocía el origen del dinero y no pensó que pudiera tratarse de una estafa informática”, hace esta explicación frente al argumento del Ministerio fiscal que alega que los depósitos supondrían, cuando menos, generar en el acusado una sospecha razonable. Sin embargo, de lo que no existe prueba, ni siquiera a título indiciario, es de que el acusado conociera que el dinero procedía de la comisión de un fraude, de una estafa, pues también era razonable que pensara en otras alternativas, como sería la posible comisión de un delito de blanqueo de capitales. En este mismo orden de ideas la SAP de Santa Cruz de Tenerife núm. 353/2016, de

[92] CRESPO SANCHÍS, *Fraude electrónico su gestión penal y civil,* 2015, 103. [https://biblioteca-tirant-com.unileon.idm.oclc.org/cloudLibrary/ebook/show/9788490865576].

7 noviembre, argumenta que sin el actuar de la condenada los hechos constitutivos del delito de estafa informática, no hubieran tenido lugar, siendo su conducta esencial para la comisión del mismo.

Lo expuesto en la SAP de Toledo de núm.882/2016. de 5 de octubre. analiza también este tema. En ella se expone que los acusados muleros recibieron en sus cuentas bancarias cantidades dinerarias que posteriormente eran reenviadas a cambio de una comisión porcentual de las mismas a personas desconocidas que, a través de empresas supuestas, les habían contratado para eso. La sentencia revoca y absuelve a los acusados porque considera que no existe prueba alguna de que los muleros, por mucho que abran una cuenta bancaria (donde personas desconocidas les dicen que les van a enviar dinero de origen desconocido para reenvialo después, una vez descontada su comisión), están colaborando y ni siquiera sepan de la ilícita procedencia del dinero, ni que tengan la voluntad ni concierto con la actuación defraudatoria origen del envío dinerario. La Sala considera que no obran con dolo necesario en las estafas, ni siquiera a título eventual, pues su participación en la cadena fue ser un mero instrumento, una víctima de los verdaderos estafadores. También atendiendo a las circunstancias sociales, la sala establece que los acusados eran personas en paro y sin especial cualificación, que buscaron trabajo por internet, y aportaron a la causa un contrato online y los e-mails que intercambiaron con los estafadores[93].

La jurisprudencia considera una tercera opción de castigo para el mulero; el blanqueo de capitales del art 301 CP, cometido con dolo eventual si el mulero prevé y cuenta con la posibilidad de que el dinero recibido tenga origen delictivo, o imprudente[94], si ignora el origen ilícito de los bienes por haber incumplido con el deber objetivo de cuidado. Sobre este particular, atendiendo a la imprudencia grave del mulero, la STS núm. 556/2015 de 2 octubre, condena por delitos de estafa informática y blanqueo de capitales. También se recurre al delito de blanqueo de capitales imprudente (en su modalidad de delito continuado) para castigar al mulero en la SAP Badajoz núm. 19/2017, de 31 de enero.

Otra clase de mulero es el Schipper; se denomina así a la persona que brinda su domicilio y credenciales ante las empresas de paquetería y, posteriormente, envía los paquetes de bienes

[93] VELASCO NÚÑEZ, *Delitos Tecnológicos,* 2021, 50-56.
[94] VELASCO NÚÑEZ/SANCHÍS CRESPO, *Delincuencia Informática Tipos Delictivos e Investigación Con jurisprudencia tras la reforma procesal y penal de 2015,* 2019, 32.

físicos, paquetes o mercancía comprados por internet usando una cuenta corriente fruto de un Phishing[95].

Pueden recibir su comisión en especie o en dinero, en especie bajo acuerdo pactado en quedarse con uno de los paquetes recibidos, o en dinero una vez que realiza el reenvío a un tercero, este último se encarga de vender los paquetes, y sobre el monto total de la venta le paga un porcentaje, este supuesto requiere de una confianza y comunicación por encima de las modalidades típicas bancarias y por lo tanto supone relación cercana al Phisher.

5. Manipulación informática

Definir en un solo enunciado las múltiples ideas de la manipulación informática es imposible; además, y su complemento típico, el artificio semejante, resulta de suma complejidad e indeterminación. Debido a la existencia de múltiples variantes de Phishing, cada una de ellas utiliza diferentes medios de comunicación, diferente malware y mayor o menor medida de ingeniería social, así que debemos plantear que el concepto de manipulación informática o artificio semejante debe ser interpretado de forma amplia, pues esta tiene múltiples definiciones.

La manipulación informática podría existir en cualquier etapa del procesamiento automatizado de datos y además podrán existir varias manipulaciones diferentes en el tiempo[96]. Es la alteración, la modificación de programas y/o datos, así como de equipos informáticos, reconectando las definiciones de amenaza, vulnerabilidad, vector de ataque y ataque. La manipulación es aquella característica que recae en la amenaza, esta se desplaza en el elemento objetivo del tipo[97]:

- En una amenaza humana su correspondiente manipulación sería la ingeniería social
- En una amenaza de red su correspondiente manipulación informática sería un malware Sniffing y un Spoofing.

---

[95] CÁMARA ARROYO/CANO CARRILLO/GARCÍA RUIZ/GIL GIL (coord.)/HERNÁNDEZ BERLINCHES (coord.)/MARTÍN FERNÁNDEZ/PASTOR VARGAS/ROBLES GÓMEZ/TOBARRA ABAD, *Cibercriminalidad,* 2019, 250.

[96] CÁMARA ARROYO/CANO CARRILLO/GARCÍA RUIZ/GIL GIL (coord.)/HERNÁNDEZ BERLINCHES (coord.)/MARTÍN FERNÁNDEZ/PASTOR VARGAS/ROBLES GÓMEZ/TOBARRA ABAD, *Cibercriminalidad,* 2019, 250

[97] GUÉREZ TRICARICO, en: MOLINA FERNÁNDEZ (coord.), *Memento práctico penal,* 2021, 1355.

- En una amenaza de software una manipulación informática sería un malware específico a ese software que sea únicamente destinado al fraude informático.

El fraude informático por lo general ataca dos de tres amenazas, aun cuando podría valer solo una para la consumación del delito; el *Phisher* aumenta su eficacia sumando diferentes técnicas de manipulación[98].

Se puede entender por manipulación informática o artificio semejante aquella acción donde la máquina informática o mecánica actúa a impulsos y en beneficio de una persona ilegítima para administrar, esta técnica consiste en la alteración de los elementos físicos o puede consistir en la alteración de elementos de programación, que generen una modificación de los comandos de programación. También es considerada la indebida utilización de datos y la utilización de los mismos de forma contraria al deber, así como la introducción de datos falsos[99].

Es de importancia señalar que en la estafa informática el *error* y *engaño bastante* (elementos de la estafa) son suplantados como elementos objetivos por los de manipulación o *artificio semejante.* Teniendo una configuración propia, esta no respondería a la estructura tradicional[100].

1-Enfoque temporal

- La manipulación informática puede producirse de cualquier forma, en el mismo programa o en cualquier etapa del procesamiento automatizado de datos[101], y desde cualquier lugar. Por ejemplo: *Backdoors, stealers*.

- La manipulación informática puede producirse en la fase de input[102] u output, cuando se actúa en los datos sobre los que opera el programa. Por ejemplo: *Keyloggers, spyware.*

- La manipulación informática puede ser en el programa mediante modificación de las instrucciones, alterando o eliminando algunos pasos o introduciendo partes nuevas en el mismo. Por ejemplo: Troyanos, *Backdoors*[103].

---

[98] CÁMARA ARROYO/CANO CARRILLO/GARCÍA RUIZ/GIL GIL (coord.)/HERNÁNDEZ BERLINCHES (coord.)/MARTÍN FERNÁNDEZ/PASTOR VARGAS/ROBLES GÓMEZ/TOBARRA ABAD, *Cibercriminalidad,* 2019 18, 19.
[99] SERRANO FERRER, *Derecho Penal y Nuevas Tecnologías*, 2021, 85.
[100] Véase, con más detalles, VELASCO NÚÑEZ, *Delitos Tecnológicos,* 2021, 41, 42, 46, 47, 49.
[101] MATA Y MARTÍN, *Delincuencia Informática y Derecho Penal,* 2001, 48, 49.
[102] ALONSO/LASCURAÍN SÁNCHEZ/RODRÍGUEZ MOURULLO, en: CREMADES/FERNÁNDEZ ORDÓÑEZ/ILLESCAS (coords.), *Régimen Jurídico de Internet*, 2002, 290.
[103] MATA Y MARTÍN, *Delincuencia Informática y Derecho Penal,* 2001, 51.

- Puede consistir en la alteración de elementos físicos de la máquina, de aquellos que permite su programación, o por la introducción de datos falsos de entrada y salida[104].

Sobre el procesamiento de datos que realiza un programa será una forma de manipulación identificarse mendazmente, introducir datos en el sistema que no corresponden con la realidad ha de ser considerado también bajo la conducta de manipulación informática a que se refiere el tipo de la estafa del art 248.2 CP[105].

6. Transferencia no consentida

Es el resultado del delito. La transferencia no consentida es el elemento del tipo que determina la consumación del acto, que se consigue a través de la manipulación informática o el artificio semejante. La transferencia está interrelacionada con el perjuicio patrimonial[106].

La transferencia no consentida supone el traspaso de un activo de un patrimonio a otro, y constituye un resultado material intermedio que puede o no significar todavía la lesión del bien jurídico, dependiendo de si implica o no simultáneamente el perjuicio de tercero; el traspaso no necesariamente debe producirse por medios electrónicos, pero dada la naturaleza del delito esta es la forma más habitual[107].

Caracterizada por:

- No ser consentida por la persona que tenga facultades para ello. (Víctima)
- Será objeto de un activo patrimonial susceptible de ser transferido.
- y que el perjuicio sea a persona distinta del autor del delito.

El legislador hace un **adelantamiento consumativo** al no exigir la definitiva apropiación del bien; el delito se consuma con la mera transferencia, en atención a la especial potencia depredadora de este delito en relación con la masividad de los Phishing, siendo el caso que,

---

[104] GUÉREZ TRICARICO, en: MOLINA FERNÁNDEZ (coord.), *Memento práctico penal,* 2021, 355.
[105] CRESPO SANCHÍS, *Fraude electrónico su gestión penal y civil,* 2015, 38 [10/05/2022]. [https://biblioteca-tirant-com.unileon.idm.oclc.org/cloudLibrary/ebook/show/978849086557].
[106] MATA Y MARTÍN, *Delincuencia Informática y Derecho Penal,* 2001, 37.
[107] FARALDO CABANA, *Eguzkilore* 21 (2007), 38.

ante una transferencia no autorizada el banco o responsable del servicio logra detener que los autores se apropien del bien no constituye tentativa, sino consumación[108].

7. El perjuicio patrimonial

El perjuicio es el menoscabo del patrimonio de titular del mismo o de aquel que tiene facultades de administración sobre el patrimonio; al existir diversas concepciones de patrimonio, tal como se ha comentado anteriormente, entendiéndolo desde la concepción mixta jurídico-económica; las unidades de valor económico con apariencia jurídica, permitirán constatar el perjuicio patrimonial al reflejar estados, un estado previo a la transferencia y un estado posterior a la transferencia, reflejando una diferencia negativa entre el primero y el segundo[109].

Será aquella consecuencia de enriquecimiento[110] injusto del Phisher, generado por la transferencia no consentida resultado de la manipulación informática, existiendo una relación de causa y efecto, enriquecimiento del autor/decremento en la víctima.

---

[108] No será considerado Phishing+Pharming el falseamiento de página para obtención de claves con la finalidad de vender las claves obtenidas: será un delito de revelación de secretos del art 197.2 CP. CRESPO SANCHÍS, *Fraude electrónico su gestión penal y civil*, 2015, 97. [10/05/2022]. [https://biblioteca-tirant-com.unileon.idm.oclc.org/cloudLibrary/ebook/show/9788490865576].

[109]RAGUÉS i VALLÉS en: AYALA GÓMEZ/ORTIZ DE URBINA GIMENO (coords.), *Memento penal económico y de la empresa*, 2016, 420, 427.

[110] Sobre el enriquecimiento; beneficio patrimonial ilícito para el autor del delito o para un tercero, consecuencia del perjuicio que se produce en el patrimonio lesionado por la acción dolosa. MUÑOZ CONDE, *Derecho penal. Parte Especial,* 23ª, 2021, 371 [10/05/2022]. [https://biblioteca-tirant-com.unileon.idm.oclc.org/cloudLibrary/ebook/show/978841397907].

Para establecer el importe del perjuicio patrimonial (pues tiene importancia para determinar la concreta pena que ha de aplicarse en la estafa informática), se atenderá al valor del mercado de la cosa[111], bien o servicio defraudado[112].

8. El dolo

El delito de estafa informática tiene que cometerse con dolo. La actuación dolosa significa que el sujeto tiene que conocer y querer realizar los elementos objetivos del tipo penal.

Indiscutiblemente se castigará al sujeto que actúa con dolo directo, sea en la modalidad de dolo directo de primer grado, sea en la modalidad de dolo directo de segundo grado[113].

Más problemática es la admisión de la estafa informática cometida con dolo eventual; esta modalidad dolosa consiste en que el sujeto que actúa piensa en la posibilidad de ocurrencia de un daño a consecuencia de la actuación, y no obstante, pese a saber que cabe esa posibilidad, aun cuando directamente no la quiera, acepta el riesgo y persiste en cometer los actos

---

[111] Los efectos del engaño y el acto de disposición patrimonial se traducen en un perjuicio causado a una víctima, que puede ser el sujeto objeto del engaño o un tercero, por tanto el perjuicio puede ser propio o ajeno. Lo fundamental es que perjuicio debe ser cuantificable económicamente. GONZALEZ SUÁREZ. Fraudes en internet y estafa informática.[10/07/2022]. [en linea]. [https://digibuo.uniovi.es/dspace/bitstream/handle/10651/27824/TFM_Gonzalez%20Suarez%2C%20Marcos.pdf?sequence=3&isAllowed=y].
Para determinar el perjuicio se tiene que partir de alguna cosa estimable económicamente que puede ser incluido en el patrimonio y si recibe protección jurídica, por ello la expectativa solo futuros, así la venta de un negocio, la estimación económica de la clientela (que se asegura mediante datos falsos de ser te gran consideración), o bien, mediante información falsa asegura que fruto del negocio ser asistente, cuando esté está de antemano condenada al fracaso. en cuanto ha habido una contraprestación estimada equivalente que implique una disminución del patrimonio de la víctima perjudicado haciendo hincapié que es algo totalmente distinto cuando existe una estimación subjetiva de la víctima, pues tocar perjudicar el patrimonio, no, que no pueden valorarse económicamente. En este sentido entonces, cuando hablamos de patrimonio, y con la idea qué ha sido perjudicado, peldaño el mismo debemos entender que tiene que ser valorable económicamente, y no tomando estándares morales que solo pueden ser valorados, en todo caso de forma civil. Ahora bien, una vez que ha ocurrido este perjuicio la posterior reparación del mismo no hace que desaparezca el delito, porque en este caso solo estaríamos de alguna manera entrando a sede civil. DEVIA GONZALEZ. *Delito Informático: Estafa informática del artículo 248.2 del Código Penal.* 247-269 [10/07/2022]. [en linea]. [https://idus.us.es/bitstream/handle/11441/75625/Tesis%20Edmundo%20Devia%20Completa%20Final%2031%20Mayo%202017.pdf?sequence=1&isAllowed=y]·

[112] MUÑOZ CONDE, *Derecho penal. Parte Especial,* 23ª, 2021, 414-420 [10/05/2022]. [https://biblioteca-tirant-com.unileon.idm.oclc.org/cloudLibrary/ebook/show/978841397907].

[113] BREL PEDREÑO, en: SANCHIS CESPO (dir.), *Fraude Electrónico su gestión penal y civil,* 2015, 23, 24. [en línea]. [06/07/2022].[https://biblioteca-tirant-com.unileon.idm.oclc.org/cloudLibrary/ebook/show/9788490865576].

nocivos[114]. Su admisión dependerá de si se puede hacer compatible la actuación con dolo eventual y el especial elemento subjetivo que requiere el delito de estafa (y, por extensión también el delito de estafa informática), el ánimo de lucro.

9. El ánimo de lucro

Es el objetivo y pretensión del *Phisher* derivado del fraude, un beneficio patrimonial[115], que supone correlativamente el perjuicio patrimonial para el tercero derivado de la transferencia realizada tras la manipulación informática utilizada por aquel[116].

Correlativamente al perjuicio suele producirse un aprovechamiento para el autor o para un tercero, este aprovechamiento deberá ser la finalidad del autor al cometer el delito. El ánimo de lucro se perfila a través de todo un montaje, por ejemplo, plantear de manera urgente mediante un reclamo de aportación de datos.

El ánimo de lucro es la persecución de un beneficio patrimonial, una ventaja patrimonial, con la finalidad de obtener cualquier utilidad o provecho, sin necesidad de que estos últimos sean de carácter económico[117].

10. Otros aspectos del delito de estafa informática

La pena base del delito de estafa informática comprende prisión de 6 meses a 3 años (art. 249 CP). Para su graduación el legislador tomará en consideración los siguientes aspectos:

- Importe de lo defraudado
- El quebrantamiento económico causado al perjudicado
- Las relaciones entre este y el defraudador

---

[114] BREL PEDREÑO, en: SANCHIS CESPO (dir), *Fraude Electrónico su gestión penal y civil,* 2015, 25 [en línea].
[06/07/2022].[https://biblioteca-tirant-com.unileon.idm.oclc.org/cloudLibrary/ebook/show/9788490865576].
[115] MATA Y MARTÍN, *Delincuencia Informática y Derecho Penal,* 2001, 39.
[116] VELASCO NÚÑEZ, *Delitos Tecnológicos,* 2021, 49, 50.
[117]RAGUÉS i VALLÉS en: AYALA GÓMEZ/ORTIZ DE URBINA GIMENO (coords.), *Memento penal económico y de la empresa*, 2016, *424.*

- Los medios empleados por el defraudador
- Otras circunstancias que sirvan para valorar la gravedad de la infracción.

Si el valor de lo defraudado no excede de los 400 euros la pena es de multa, que puede ir desde uno hasta tres meses[118]; si supera esta cuantía la pena es de prisión de seis meses a tres años.

En cuanto a la aplicación o no del art. 250 CP, el legislador, al referirse delito de estafa, debe entenderse que la agravación de la pena se extiende solamente a aquellas conductas previstas en el art 248.1 CP y compatibles, pero no al delito considerado en el art. 248.2 b), pues estas, al ser técnicamente actos preparatorios, no permiten la aplicación del tipo agravado del art. 250[119].

Entendiendo la estafa informática de una manera amplia, comprenderemos las siguientes posibles agravantes contenidas en el art. 250 CP; su aplicación supone la elevación de la pena a prisión de uno a seis años y multa de seis a doce meses, cuando:

- Bien patrimonial específico. Recaiga sobre bienes que integren el patrimonio artístico, histórico, cultural o científico.

Abriendo la ventana a víctimas que mediante phishing pierdan un bien artístico electrónico valuable, como sería un NFT[120], las cuales son consideradas obras digitales que pueden ser compradas y vendidas como cualquier otra propiedad, pero no tienen tangibilidad (al ser Tokens No Fungibles) consideradas obras digitales que no están en el mundo físico.

- Cuantía. El valor de la defraudación supere los 50.000 euros, o afecte a un elevado número de personas. Si el valor de la defraudación supera los 250.000 euros la pena puede llegar hasta cuatro a ocho años y multa de doce a veinticuatro meses[121].

---

[118] *Memento Experto Ciberseguridad,* 2021, 278.
[119] ROCA AGAPITO, en: SANZ DELGADO/FERNÁNDEZ BERMEJO (coords.), *Tratado de Delincuencia Cibernético,* 2021, 419.
[120] Los NFT surgen como un tipo especial de token criptográfico que representa algo único. La diferencia con otros activos digitales, como pueden ser las criptomonedas, reside en que dichos NFTs no son fungibles. Estos tokens, por tanto, se caracterizan porque tienen propiedades únicas, por lo que no se pueden intercambiar. En la práctica, son activos individuales, indivisibles e insustituibles, que se generan digitalmente e identifican inequívocamente su propiedad. *OBSERVATORIO DE LA DIGITALIZACIÓN FINANCIERA, Llegan los tokens no fungibles (NFT)* 13 de abril de 2021, 29/2021, 1-3. [29/06/2022][https://www.funcas.es/wp-content/uploads/2021/04/NL_ODF_29_2021.pdf].
[121] *Memento Experto Ciberseguridad,* 2021, 278.

- Vínculo preexistente. Se cometa con abuso de las relaciones personales existentes entre víctima y defraudador, o aproveche este su credibilidad empresarial o profesional[122].

Sería el caso donde aquel empleado o exempleado disconforme, abusando de su conocimiento interno organizacional, envía *Phishing* a una base de datos de empleados dentro de una organización o aquella expareja que realiza un *Phishing* por motivo de venganza al intentar apropiarse de una cuenta, servicio o bien y posteriormente transferirlo.

- Agravante por reincidencia específica o la multirreincidencia: cuando el culpable haya sido condenado ejecutoriamente por al menos 3 delitos de defraudación[123].

- Afectación de bienes de primera necesidad. Entendiendo por estos: cosas de primera necesidad, entrando alimentos, vestido, calzado, documentos necesarios para la licita residencia o trabajo, cosas de las que no se puede prescindir[124].

El art. 251 bis CP establece la responsabilidad penal de las personas jurídicas por la comisión de los delitos incluidos en la sección dedicada a los delitos de estafa, por tanto, abarcando también la estafa informática.

Para que la persona jurídica responda penalmente de este delito ha de estarse a lo dispuesto en el art. 31 bis.1 CP, precepto en el que se regulan los criterios de imputación de la responsabilidad penal de las personas jurídicas por la comisión de determinados delitos tipificados en el CP. En concreto, los criterios de imputación son:

- De los delitos cometidos en nombre o por cuenta de estas, y en su beneficio directo o indirecto, *por sus representantes legales o por aquellos* que, actuando individualmente o como *integrantes* de un *órgano de la persona jurídica*, están autorizados para tomar decisiones en nombre de la persona jurídica u ostentan facultades de organización y control dentro de la misma[125].

---

[122] ROCA DE AGAPITO, en: SANZ DELGADO/FERNÁNDEZ BERMEJO (coords.), *Tratado de Delincuencia Cibernética,* 2021, 452-459.
[123]RAGUÉS i VALLÉS en: AYALA GÓMEZ/ORTIZ DE URBINA GIMENO (coords.), *Memento penal económico y de la empresa*, 2016, 431, 432.
[124] ROCA DE AGAPITO, en: SANZ DELGADO/FERNÁNDEZ BERMEJO (coords.), *Tratado de Delincuencia Cibernética*, 2021, 427-429.
[125] ORTIZ DE URBINA GIMENO, en: AYALA GÓMEZ/ORTIZ DE URBINA GIMENO (coords.), *Memento penal económico y de la empresa*, 2016, 175.

- De los delitos cometidos, en el ejercicio de actividades sociales y por cuenta y en beneficio directo o indirecto de las mismas, *por quienes, estando sometidos a la autoridad de las personas físicas mencionadas* en el párrafo anterior, han podido realizar los hechos por haberse incumplido gravemente por aquéllos los *deberes de supervisión, vigilancia y control* de su actividad atendidas las concretas circunstancias del caso.

A la persona jurídica se le impondrá la siguiente pena por la comisión del delito de estafa informática:

- multa del triple al quíntuple de la cantidad defraudada, si el delito cometido por la persona física tiene prevista una pena de prisión de más de cinco años.
- multa del doble al cuádruple de la cantidad defraudada, en el resto de los casos.

De manera facultativa, se autoriza al juez a imponer además alguna de las penas previstas en el art. 33.7 CP, atendiendo a las reglas para la determinación de la pena previstas en el art. 66 bis CP.

La pena básica y obligatoria es la multa (optando por el sistema de multa proporcional); el resto de penas previstas no son de obligada imposición; su aplicación se va a basar en los siguientes criterios: la necesidad para prevenir la continuidad delictiva o sus efectos; las consecuencias económicas y sociales, y, en especial, los efectos para los trabajadores; el puesto que en la estructura de la persona jurídica ocupa la persona física u órgano que incumplió el deber de control[126].

Las penas que, adicionalmente, puede acordar el juez son las siguientes:

- Disolución de la persona jurídica
- Suspensión de sus actividades por un plazo máximo de cinco años).
- Clausura de locales y establecimientos por un plazo que no puede exceder de cinco años.
- Prohibición, temporal o definitiva, de realizar en el futuro las actividades en cuyo ejercicio se haya cometido, favorecido o encubierto el delito.

[126] ORTIZ DE URBINA GIMENO, en: AYALA GÓMEZ/ORTIZ DE URBINA GIMENO (coords.), *Memento penal económico y de la empresa*, 2016, 165.

- Inhabilitación para obtener subvenciones y ayudas públicas, para contratar con el sector privado y para gozar de beneficios e incentivos fiscales o de la Seguridad Social (el plazo no puede exceder de 15 años).

- intervención judicial, total o parcial, para salvaguardar los derechos de los trabajadores o de los acreedores (el plazo no puede exceder de cinco años)[127].

Atenuantes en la responsabilidad penal de las personas jurídicas.

Son atenuantes post delictivas; tras la realización del delito, los representantes legales o por aquellos que, actuando individualmente o como integrantes de un órgano de la persona jurídica, han de realizar alguna de las siguientes conductas:

1. Confesión de la infracción ante las autoridades antes de conocer que el proceso se dirige contra ella.

2. Colaboración en la investigación en cualquier momento del proceso mediante la aportación de pruebas nuevas y decisivas.

3. Reparación o disminución del daño del delito antes del juicio oral.

4. Establecimiento antes del inicio del juicio oral de medidas eficaces para prevenir y descubrir delitos[128].

La exención de la responsabilidad penal para las personas jurídicas tiene una regulación especial, a través de los programas de cumplimiento, regulados en el art. 31 bis CP[129].

El compliance es el conjunto normativo que le señala a la corporación obligaciones con sanciones de esa naturaleza, algunas preventivas y otras reactivas, mientras esté desarrollando su actividad. Es un estándar legal que alcanza, si no a prevenir, al menos a eludir incurrir, mientras despliegan su actividad, en la comisión de determinados delitos. El CP no lo exige de manera obligatoria, porque la corporación puede ahorrarse lo que valen no delinquiendo nunca, pero al tenerlos reduce, minora, prevé y evita delitos, en general, optando por premiar a la corporación que los instale, siempre que sean eficaces y están confeccionados con medidas de vigilancia y control idóneas; además de ayudar a introducir cultura de cumplimiento normativo y la ética corporativa, le permitirá optar a ventajas legales como:

---

[127] *Memento Experto Ciberseguridad,* 2021, 279.
[128] ORTIZ DE URBINA GIMENO, en: AYALA GÓMEZ/ORTIZ DE URBINA GIMENO (coords.), *Memento penal económico y de la empresa*, 2016, 189.
[129] VELASCO NÚÑEZ, en: RODRÍGUEZ GARCÍA/RODRÍGUEZ LÓPEZ (eds.), *Compliance y responsabilidad de las personas jurídicas,* 2020, 223 ss.

- Conseguir la exención de la responsabilidad penal, pese haber ocurrido el delito, si los modelos implantados antes de producirse el mismo tenían la capacidad de haberlo evitado.
- Conseguir la atenuación de la responsabilidad penal, si los modelos se instalan después de cometido el delito y antes del juicio oral, siempre que sean eficaces para previsiones de futuro.
- Conseguir otras atenuaciones, como puede ser la colaboración, al ofrecer procesos que permitan al juez la identificación del autor de la acción penal.
- Conseguir la imposición por el juez de concretas sanciones penales en su grado mínimo.
- Facilitar la conformidad en el juicio, obtener la reducción penológica asociada.
- Aminorar la afectación de su reputación, dado que tener modelos de cumplimiento normativo supone querer evitar o aminorar los efectos del delito.

V. CONCLUSIONES

En los delitos Patrimoniales se ha producido una evolución significativa en la concepción del bien jurídico, consecuencia también de la evolución continua de las TIC y la informática obligando a interpretar de forma amplia el concepto, solo así podrá ser encuadrada de forma correcta las diversas conductas de fraude informático.

El Phishing es un delito tan soluble que puede ser transformado y adecuado a cualquier evento, al ser de fácil elaboración cualquiera puede realizarlo y, por lo tanto, la sociedad está expuesta a ser tentada a cometerlo y, sobre todo, a caer en él. La manera más efectiva de combatir el Phishing es la educación anti Phishing, y los programas de cumplimiento en el caso de personas jurídicas, pero otra medida de disminuir el Phishing será elevar el nivel informático medio de la sociedad porque, en general, vivimos en un mundo altamente informatizado y pocos comprenden el funcionamiento de las herramientas tecnológicas, estas herramientas como pueden ser la identificación de dos factores deben de ser más rigurosas e incluso buscar nuevas maneras de identificación y de autenticación siempre en beneficio del consumidor.

La utilización de malware y de ingeniería social elevan el nivel de complejidad de los fraudes informáticos, al tiempo que cada vez que surge algún evento relevante este se "utiliza" para aprovechar el contexto y la urgencia, facilitando así la consumación. Un claro ejemplo de esto lo ofrece la pandemia: las medidas de distancia social incrementaron significativamente el uso de QR en la contratación de servicios varios, así que el Phishing rápidamente se adaptó a esta nueva realidad, aprovechando este nuevo "campo de actuación" defraudatorio.

Existe una necesidad extrema de educar a la población que se encuentra dentro del rango de brecha digital, así como de educar con programas especializados a los jóvenes, niños y adolescentes sobre el uso correcto y ético de las TIC, para así evitar que el número de ciber delincuentes disminuya.

El recurso al Derecho penal para tratar de evitar el fraude informático está justificado; la regulación del art. 248.2 a) CP, dando una definición amplia de este delito, debe valorarse de manera positiva, pues esto permite que se vaya adaptando a los avances y cambios "tan frenéticos" como es el cibernético; los elementos manipulación informática o artificio semejante tienen la suficiente amplitud como para englobar cualquier cambio y avance que se produzca en esta materia.

La estafa informática no pertenece a la categoría de delito informático puro si este término se utiliza para identificar a delitos que tratan de proteger nuevos bienes jurídicos surgidos como consecuencia del uso y desarrollo de las TIC. Porque a través del art. 248.2 CP se pretender proteger el patrimonio, un bien jurídico individual que ha de ser entendido en sentido mixto, jurídico y económico.

En materia de sujeto activo, la explicación criminológica sobre el autor del delito de estafa informática resulta muy útil, pues permitirá adoptar mejores medidas (no penales) para luchar contra este tipo de comportamiento delictivo. Mayor relevancia práctica tiene la figura del llamado mulero, una persona que, en muchas ocasiones, su intervención resulta vital, pues es el intermediario entre la víctima y el sujeto que se va a beneficiar del fraude informático-el autor. El estudio jurisprudencial de esta figura se considera aún insuficiente, a lo que sin duda contribuye la falta de claridad sobre el momento en el que se ha de considerar consumado el delito de estafa informática, si con el momento en el que se hace la transferencia no consentida del activo patrimonial por parte del sujeto pasivo, como es mi opinión, o es en otro momento posterior. Esto dejando a parte otro problema que también ha de ser destacado, la propia teoría que se mantenga en la explicación de la autoría y la participación. En todo caso, la no aplicación del delito de fraude informático al mulero (bien a título de coautor, bien a título de partícipe) deja abierta la posibilidad de recurrir a otras figuras delictivas, en concreto, al delito de blanqueo de capitales, donde se ha tipificado tanto la modalidad dolosa como la imprudente.

La estafa informática tiene unos elementos típicos específicos, propios, porque se utilizan las TIC para generar el engaño e inducir a error al sujeto engañado, pero otros elementos típicos son los mismos que la estafa tradicional (así que la teoría general elaborada para el delito de estafa es aplicable aquí): en ambos casos se protege el mismo bien jurídico, patrimonio, en mi opinión, entendido desde una concepción mixta, y, en ambos casos se ha de actuar dolosamente y con ánimo de lucro. Como se ha comentado anteriormente, el delito de estafa informática se consuma en el momento en el que el sujeto pasivo realiza la transferencia no consentida de un activo patrimonial, por tanto no se requiere que se produzca efectivamente el perjuicio en su patrimonio (el efectivo perjuicio sería, en todo caso, el agotamiento del delito).

Siguiendo el sistema de numerus clausus, el legislador ha previsto la responsabilidad penal de la persona jurídica por la comisión de una estafa informática. Para ello ha de cumplirse alguno de los criterios de imputación que se mencionan en el art. 31 bis CP. Los programas de cumplimiento, al contener dentro de sus pilares la ética, la gestión de riesgos y la sanción

interna, debe prestar especial atención a la realización de fraudes no solo tradicionales, sino también a los informáticos.

BIBLIOGRAFÍA Y WEBGRAFÍA

ABADÍAS SELMA, Alfredo/FERNÁNDEZ ALBESA, Nuria/LEAL RUIZ Rocío. *Ciberdelincuencia*, Madrid, Colex, 2021.

ACURIO DEL PINO, Santiago *Delitos Informáticos: Generalidades.20.* [10/07/2022]. [en linea]. [https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf].

ALONSO, Jaime/LASCUARAÍN SÁNCHEZ, Juan A./RODRÍGUEZ MOURULLO, Gonzalo. *El Fraude Informático,* en: CREMADES/FERNÁNDEZ ORDÓÑEZ/ILLESCAS (coords.), *Régimen Jurídico de Internet,* Madrid, La Ley, 2002, 290-297.

ÁLVAREZ LEÓN, José A. *Tópicos de Política Criminal 2. Ciencia y Tecnología,* México, UNAM POSGRADO Derecho, 2021.

ANDRÉ MORALES José. *Ingeniería Social.* [en línea] [https://cybercamp.es/cybercamp2014/attachments/multimedia/CyberCamp_IngenieriaSocial.pdf].

ANTI-PHISHING WORKING GROUP. *Phishing Landscape 2020: A Study of the Scope and Distribution of Phishing*. [25/052022]. [https://apwg.org/phishing-landscape-2020-a-study-of-the-scope-and-distribution-of-phishin/] .

ANTOKOLETZ HUERTA, Daniel. *Ingeniería social* [en línea].[03/06/2022] [https://www.researchgate.net/publication/327285308_Ingenieria_Social].

BLOG:INTERDOMINIOS. *Sniffer, la nueva amenaza aumenta cada día su importancia.* [en línea]- [05/07/2022]. [https://blog.interdominios.com/sniffer-la-amenaza-que-va-cobrando-mas-importancia/].

BORGHELLO, Cristian. *El Arma Infalible: La Ingeniria Social.*[en línea] [03/06/2022] [https://p303.zlibcdn.com/dtoken/dfdbdbc908ca3791794e6fd56ed0d675].

BREL PEDREÑO, América. *La intervención del mulero informático,* en: SANCHIS CRESPO (dir.), *Fraude Electrónico, su gestión penal y civil*, Valencia, Tirant lo Blanch, 2015, 18-36. [en línea] .[06/07/2022]. [https://biblioteca-tirant-com.unileon.idm.oclc.org/cloudLibrary/ebook/show/9788490865576].

CANO TERUEL,Quim. *Ciberdelincuencia en el Código Penal. [10/07/2022].[en linea].[https://cibercrim.com/ciberdelincuencia-en-el-codigo-penal/].*

CÁMARA ARROYO/CANO CARRILLO/GARCÍA RUIZ/GIL GIL (coord.)/HERNÁNDEZ BERLINCHES (coord.)/MARTÍN FERNÁNDEZ/PASTOR VARGAS/ROBLES GÓMEZ/TOBARRA ABAD, *Cibercriminalidad,* Madrid, Dykinson, 2019.

CARPENTIER, Jean-François. *La seguridad informática en la PYME.* [10/05/2022]. [https://www.ediciones-eni.com/open/mediabook.aspx?idR=cbc5b457b60ff38bb7e4e6f90df31bec].

CAVADA HERRERA, Juan P. *Cibercrimen y delito informático: Definiciones en legislación internacional, nacional y extranjera.* 6. [10/07/2022]. [en linea]. [https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/29012/2/Definicion_y_regulacion_de_cibercrimen_y_delito_informatico_JPC_edit.pdf].

CRESPO SANCHÍS, Carolina. *Fraude electrónico su gestión penal y civil,* Valencia, Tirant lo Blanch, 2015 [https://biblioteca-tirant-com.unileon.idm.oclc.org/cloudLibrary/ebook/show/9788490865576].

CUEVAS RUÍZ, José L. *El papel de la Ciberseguridad en el proceso de la transformación digital en México.* [20/05/2022]. [https://centrodeestudios.ift.org.mx/documentos/publicaciones/2021/1er_Sem_JLCR_El_papel_de_la_Ciberseguridad_en_el_proceso_de_la_transformaci%c3%b3n_digital_en_M%c3%a9xico.pdf].

DEVIA GONZALEZ. Edmundo A. *Delito Informatico: Estafa informática del articulo 248.2 del Codigo Penal.* 247-269 [10/07/2022]. [en linea]. [https://idus.us.es/bitstream/handle/11441/75625/Tesis%20Edmundo%20Devia%20Completa%20Final%2031%20Mayo%202017.pdf?sequence=1&isAllowed=y]·

DE LA CUESTA ARZAMENDI, José Luis/PEREZ MACHÍO Ana Isabel. *Ciberdelincuentes y cibervíctimas,* en: DE LA CUESTA ARZAMENDI (dir.)/DE LA MATA BARRANCO (coord.), *Derecho Penal Informático,* Navarra, Aranzadi, 2010, 100-135.

ENCICLOPEDIA JURÍDICA. *Delito instantáneo.* [04/07/2022]. [en línea]. [http://www.enciclopedia-juridica.com/d/delito-instant%C3%A1neo/delito-instant%C3%A1neo.htm].

ESPINOSA, Óscar. *Mejora la seguridad de tus cuentas con la autenticación en dos pasos* [10/05/2022]. [https://www.redeszone.net/tutoriales/seguridad/autenticacion-dos-pasos/].

FANJUL FERNÁNDEZ, en: APARICIO ORDAZ (coord.), *Conceptualización, evolución y clasificación del ciberdelito empresarial*, Madrid, 2018 [en línea]. [05/07/2022]. [https://es.eserp.com/wp-content/uploads/2019/09/conceptualizacion-evolucion-y-clasificacion-del-ciberdelito-empresarial.pdf]

FARALDO CABANA, Patricia. *Los conceptos de Manipulación Informática y artificio semejante en el delito de estafa informática*, en: Eguzkilore 21 (2007), 33-57.

FIDALGO VEGA, Manuel. *NTP 390: La conducta humana ante situaciones de emergencia: análisis de proceso en la conducta individual.* [en línea]. [03/07/2022].[https://www.insst.es/documents/94886/326853/ntp_390.pdf/967860c0-87f3-4cb8-8421-6e3a8583a941?version=1.0&t=1614698481311].

FLORES PRADA, Ignacio. *Criminalidad Informática aspectos sustantivos y procesales,* Valencia, Tirant lo Blanch, 2012 [https://biblioteca-tirant-com.unileon.idm.oclc.org/cloudLibrary/ebook/show/978849033570].

FUNDACIÓN BBVA. *Uso de internet en España y la Unión Europea*. [en línea] [05/07/2022] [https://www.fbbva.es/wp-content/uploads/2018/10/FBBVA_Esenciales_29.pdf].

GRIS Manuel. *Hackers, Crakers, e Ingeniería Social.* [en línea] [03/06/2022] [https://pdflife.one/download/4660813-hackers-crackers-e-ingenieria-social].

GUÉREZ TRICARICO, Pablo. *Delitos patrimoniales y contra el orden socioeconómico,* en: MOLINA FERNÁNDEZ (coord.), *Memento práctico penal*, Madrid, Francis Lefebvre, 2021, 1350-1407

HADNAGY, Christopher. *Ingeniería Social el Arte del Hacking personal*, Anaya Multimedia. 2011.

INCIBE CERT. *Artefactos - Implementación. Diciembre de 2021 Ciberejercicios – Ataque dirigido.Exp. 017/19 - Lote 3.* [https://www.incibe-cert.es/cyberex-espana].

INCIBE. *Temáticas Phishing.* [10/05/2022]. [https://www.incibe.es/protege-tu-empresa/tematicas/phishing].

- *Ayuda ransomware* [en línea]. [05/07/2022]. [https://www.incibe.es/protege-tu-empresa/herramientas/servicio-antiransomware].

- *OSI. Aprendiendo a identificar* [en línea]. [10/05/2022].[https://www.osi.es/sites/default/files/docs/guia_fraudes/guia-fraudes-online.pdf].

KASPERSKY. *¿Qué es el pharming y cómo evitarlo?* [en línea]. [05/07/2022]. [https://latam.kaspersky.com/resource-center/definitions/pharming].

- *¿Qué es el scareware? Definición y explicación* [en línea]. [05/07/2022]. [https://latam.kaspersky.com/resource-center/definitions/scareware].

- *¿Qué es el spear phishing?* [en línea]. [05/07/2022]. https://latam.kaspersky.com/resource-center/definitions/spear-phishing].

- *¿Qué es una amenaza avanzada persistente (APT)?* [en línea]. [05/07/2022].[https://latam.kaspersky.com/resource-center/definitions/advanced-persistent-threats].

LA LEY. *Guías jurídicas: Delito en masa* [04/07/2022]. [en línea]. [https://guiasjuridicas.wolterskluwer.es/Content/Documento.aspx?params=H4sIAAAAAAAEAMtMSbF1jTAAAUMjI3NDtbLUouLM_DxbIwMDCwNzAwuQQGZapUt-ckhlQaptWmJOcSoAenxOMTUAAAA=WKE#I58].

MATA Y MARTÍN, Ricardo M. *Delincuencia Informática y Derecho Penal,* Madrid, Edisofer, 2001.

Memento Experto Ciberseguridad, Madrid, Francis Lefebvre, 2021.

MESTRE DELGADO, Esteban. *Las ciber estafas,* en: SANZ DELGADO/FERNÁNDEZ BERMEJO (coords.), *Tratado de Delincuencia Cibernético*, Navarra, Aranzadi, 2021, 327-338.

MOSQUERA, Andrea. *Anonimizadores*. [en línea]. [03/06/2022]. [https://es.scribd.com/doc/230334053/Anonimizadores].

MUÑOZ CONDE, Francisco. *Derecho penal Parte Especial*, 23ª, Valencia, Tirant lo Blanch, 2021 [https://biblioteca-tirant-com.unileon.idm.oclc.org/cloudLibrary/ebook/show/978841397907].

MUÑOZ CONDE, Francisco/GARCÍA ARÁN, Mercedes. *Derecho penal Parte General*, 10ª, Valencia, Tirant lo Blanch, 2019 [https://biblioteca-tirant-com.unileon.idm.oclc.org/cloudLibrary/ebook/show/978841313940].

OBSERVATORIO DE LA DIGITALIZACIÓN FINANCIERA. *Llegan los tokens no fungibles (NFT)13 de abril de 2021, 29/2021, 1-3* [29/06/2022] [https://www.funcas.es/wp-content/uploads/2021/04/NL_ODF_29_2021.pdf].

OBSERVATORIO DE LA DIGITALIZACIÓN FINANCIERA . Llegan los tokens no fungibles (NFT)13 de abril de 2021, 29 / 2021, 1-3. [29/06/2022][https://www.funcas.es/wp-content/uploads/2021/04/NL_ODF_29_2021.pdf] .

PAGNOTTA SANABRIA. *Noti_infosegura: ¿Cuáles son las preguntas de seguridad de la información más adecuadas según Google?* [en línea]. [03/07/2022]. [https://www.uv.mx/infosegura/general/noti_google-4/].

PARIS BALLEZA, Juan C. *QRshing: conoce los riesgos de la nueva estafa* [10/05/2022]. [https://es.linkedin.com/pulse/qrshing-conoce-los-riesgos-de-la-nueva-estafa-paris-balleza?trk=articles_directory].

PEREZ-MATEO SUBIRÁ, María. *La Dimensión Social en el Proceso de Aprendizaje Colaborativo Virtual: El caso de la OUC*, tesis doctoral, Universitat Oberta de Catalunya, 2010 [en línea]. [03/07/2022]. [https://www.tdx.cat/bitstream/handle/10803/37113/tesi_mperezmateo-1.pdf].

PEREZ-MATEO SUBIRÁ, María. (2010). La Dimensión Social en el Proceso de Aprendizaje Colaborativo Virtual:EL caso de la OUC [Tesis de doctorado publicada]. Universitat Oberta de Catalunya [en linea] [03/07/2022].

POSADA MAYA, Ricardo. *El cibercrimen y sus efectos en la teoría de la tipicidad: de una realidad física a una realidad virtual. 93. [10/07/2022]. [en linea]. [file:///home/chronos/u-ab4b79542e3553828d070ffa3039bf9e8e20557b/MyFiles/Downloads/Dialnet-ElCibercrimenYSusEfectosEnLaTeoriaDeLaTipicidad-6074006.pdf].*

PRIETO ÁLVAREZ, Víctor M/PAN CONCHEIRO, Ramón A. *Virus Informáticos,* Trabajo de Máster en informática, Universidade da Coruña, [10/05/2022]. [http://sabia.tic.udc.es/docencia/ssi/old/2006-2007/docs/trabajos/08%20-%20Virus%20Informaticos.pdf].

RAGUÉS i VALLÉS; Ramón-, *Responsabilidad penal de las personas jurídicas*, en; AYALA GÓMEZ/ ORTIZ DE URBINA GIMENO (coord), Memento penal económico y de la empresa, 2016, Madrid, Francis Lefebvre, 2016, 165-220.

REBOLLO VARGAS, Rafael. *Limitaciones de Derecho Penal en la Prevención del Blanqueo de Capitales*, en: GARCÍA ARÁN (dir.), *La delincuencia económica Prevenir y Sancionar*, Valencia, Tirant lo Blanch, 2014, 125-166. [https://biblioteca-tirant-com.unileon.idm.oclc.org/cloudLibrary/ebook/show/978849053667].

ROCA DE AGAPITO, Luis. *Modalidades agravadas de estafa mediante la utilización de las tecnologías de la información y la comunicación*, en: SANZ DELGADO/FERNÁNDEZ BERMEJO (coords.), *Tratado de Delincuencia Cibernético,* Navarra, Aranzadi, 2021, 415-461.

SANCHÍS CRESPO, Carolina. *Fraude electrónico su gestión penal y civil,* 2015, 95. [10/05/2022].

[https://biblioteca-tirant-com.unileon.idm.oclc.org/cloudLibrary/ebook/show/9788490865576]

SERRANO FERRER, María P. *Derecho Penal y Nuevas Tecnologías*, Navarra, Aranzadi, 2021.

STACY, Shelley. *Advancement in Phishing Redictor Script* [25/052022]. [https://www.phishlabs.com/blog/advancements-in-phishing-redirector-scripts/].

THEASTROLOGYPAGE. *Definición - ¿Qué significa Script Kiddie?* [en línea]. [05/07/2022]. [https://es.theastrologypage.com/script-kiddie].

UNIVERSITY CREDIT UNION. *Phishing/Vishing/Smishing* [en línea]. [05/07/2022]. [https://ucumiami.org/es/education-3/phishing-vishing-smishing#:~:text=Es%20una%20pr%C3%A1ctica%20criminal%20fraudulenta,%22%20(voz)%20y%20phishing.].

VELASCO NÚÑEZ, Eloy. *Efectividad de los programas de cumplimiento*, en: RODRÍGUEZ GARCÍA/RODRÍGUEZ LÓPEZ (eds.), *Compliance y responsabilidad de las personas jurídicas*, Valencia, Tirant lo Blanch, 2020, 223-251.

- *Delitos Tecnológicos,* Madrid, La Ley, 2021.

VELASCO NÚÑEZ, Eloy/SANCHÍS CRESPO, Carolina. *Delincuencia Informática Tipos Delictivos e Investigación Con jurisprudencia tras la reforma procesal y penal de 2015,* Valencia, Tirant lo Blanch, 2019.

VELASCO NÚÑEZ; Eloy,Efectividad de los programas de cumplimiento, en RODRÍGUEZ GARCÍA, RODRÍGUEZ LOPEZ (Ed) . Compliance y responsabilidad de las personas jurídicas, Tirant lo blanch, Valencia, 2020. 223-251.