Universitat de les Illes Balears

TRABAJO DE FIN DE GRADO

BUSSINES EMAIL COMPROMISE: LA ÚLTIMA TENDENCIA EN PHISHING EMPRESARIAL

Lucia Abril Salar Serra

Grado de Derecho

Facultad de Jovellanos

Año Académico 2022-23

BUSSINESS EMAIL COMPROMISE, LA ÚLTIMA TENDENCIA EN PHISHING EMPRESARIAL

Lucia Abril Salar Serra

Trabajo de Fin de Grado

Facultad de Derecho

Universidad de las Illes Balears

Año Académico 2022-23

Palabras clave del trabajo:

Ciberdelitos, estafas informáticas, empresas, phishing, jurisprudencia, modus operandi, código penal, suplantación de identidad, blanqueo de capitales…

María Isabel Monserrat Sánchez Escribano

	Autor		Tutor	
Se autoriza la Universidad a incluir este trabajo en el Repositorio Institucional para su consulta en acceso abierto y difusión en línea, con fines exclusivamente académicos y de investigación	Sí	No	Sí	No
	☒	☐	☒	☐

Índice:

Resumen

Los delitos BEC han experimentado un aumento en los ultimos años, cada vez se utiliza más internet y el correo electrónico es una herramienta cotidiana en todos los negocios, las empresas hacen cada vez más uso de las plataformas digitales y los criminales están a la orden del día encontrando nuevos modos y más eficaces para estafarlas, atacando ahora no solo a las maquinas sino también al error humano. En este trabajo académico explicaremos estos delitos y su relación con otros además de su tipificación casuística penal.

Abstract

The incidence of BEC (Business Email Compromise) crimes has increased in recent years. With the growing use of the internet and email as a daily tool in business operations, companies are increasingly relying on digital platforms. However, criminals are constantly devising new and more effective ways to defraud them, targeting not only machines but also human error. In this academic paper, we will explain these crimes and their relationship with other types of offenses, as well as their legal classification and penal causation.

LA ESTAFA INFORMÁTICA, EL BEC

I.INTRODUCCIÓN

Durante los primeros meses del año 2022 se reportó un aumento significativo en la cantidad de conductas Business Email Compromise (en adelante, BEC) en todo el mundo. Según un informe de la compañía de seguridad informática Check Point, estos ataques han aumentado en un 15% en comparación con el mismo período del año anterior. Los delincuentes suelen utilizar técnicas de ingeniería social para engañar a los empleados de empresas y organizaciones, y luego obtener acceso a cuentas de correo electrónico y sistemas informáticos[1].

En la presente investigación, tenemos por objeto llevar a cabo un análisis de la tendencia del delito de estafa informática conocido BEC, empleando la doctrina y la jurisprudencia como herramientas fundamentales. En primer lugar, se llevará a cabo un sumario examen del fenómeno del phishing, para posteriormente abordar el BEC, su modus operandi y su casuística penal, como una variante de dicho delito. Se pondrá especial énfasis en el aspecto de la estafa informática al momento de analizar la tipicidad del BEC, con el propósito de aportar claridad a un tema novedoso y aún ambiguo para muchos en la materia.

En marzo de 2023, el Departamento de Justicia de los Estados Unidos anunció la detención de un grupo de hackers que se dedicaba a realizar ataques BEC a nivel global. Según el comunicado oficial, este grupo estaba integrado por ciudadanos de varios países y habían obtenido ganancias por más de 50 millones de dólares en los últimos tres años. Las autoridades señalaron que los delincuentes utilizaban correos electrónicos falsificados y la creación de sitios web fraudulentos. Esta detención es considerada una de las más importantes en la lucha contra el delito BEC en la historia reciente. Las autoridades destacaron la importancia de la cooperación internacional en la lucha contra este tipo de delitos[2].

El BEC es la última tendencia en materia empresarial en lo que concierne a delincuencia informática, concretamente phishing. En los últimos años, el avance tecnológico ha traído consigo importantes transformaciones en la forma en que se llevan a cabo los delitos tradicionales. La delincuencia informática ha surgido como un nuevo fenómeno que involucra la utilización de tecnología y medios electrónicos para cometer delitos. Se trata de un problema global que afecta a individuos, empresas e incluso

[1] CHECK POINT RESEARCH. (2022). Business Email Compromise: A Global Threat.
[2]DEPARTAMENTO DE JUSTICIA DE LOS ESTADOS UNIDOS. (2023). Global BEC Hackers Group Dismantled. Consultado 16 de marzo de 2023

gobiernos, y representa un gran desafío para la justicia penal. La tecnología ha creado nuevas oportunidades para la delincuencia, al tiempo que ha aumentado la complejidad y la escala de los delitos. La globalización y la conectividad han facilitado la propagación de la delincuencia informática a nivel mundial, lo que hace que sea difícil para los organismos de aplicación de la ley trabajar juntos y coordinar sus esfuerzos.

Un delito informático definido por DEVIA, *como aquel que tipifica cualquier acto del ser humano como ilícito cuando el mismo tiene por fin perturbar o afectar datos, información o sistemas de información teniendo como consecuencia el daño directo o indirecto en ellos asi como también el mal uso de los mismos*[3]. El autor ROMEO CASABONA refiere que con la expresión delitos informáticos, suele aludirse a conductas que atentan contra determinados bienes del individuo, pero también de la persona jurídica siendo un concepto demasiado amplio para que podamos usarlo indiscriminadamente[4], no es lo mismo una estafa informática que un robo de datos[5].

Al igual que se hace uso de la denominación delitos informáticos en la doctrina española máxime desde 2017 se considera más común y menos conflictivo el uso de la palabra cibercriminalidad, que desde nuestro punto de vista es una definición algo vacía de contenido[6]. ROMEO CASABONA, la define como *conducta relativa al acceso, apropiación, intercambio y puesta a disposición de información en red telemática, las cuales constituyen su entorno comisivo, perpetradas sin el consentimiento autorización exigibles o utilizando información de contenido ilícito, pudiendo afectar al bien jurídico diversa naturaleza individual o supraindividual*[7].

Para hacerlo más sencillo, nuestro legislador opta por añadir otra categoría más a algunos de los tipos de delito especialmente para cuando se cometen haciendo uso de tecnología. No existe en nuestro CP penal un Título dedicado a los delitos informáticos o a los cibercrímenes, sino que se encuentran recogidos tipos específicos en el marco de otros delitos más clásicos como el de estafa o el de daños. Pero estas características tan conocidas por todos nosotros no son siempre aplicables al delito de estafa informática, como veremos en los próximos apartados.

---

[3] DEVIA GONZÁLEZ, E.A. (2017). El delito informático: Estafa informática del artículo 249.1 del código penal. (Tesis Doctoral Inédita). Universidad de Sevilla, Sevilla. (153-159)

[4] ROMEO CASABONA, Carlos Mª, De los delitos informáticos al cibercrimen, en El Cibercrimen, nuevos retos jurídicos-penales, nuevas respuestas Político-Criminales, Editorial Comares S. L., Granada, 2006, p. 9.

[5] Tambien han sido definidos los delitos informáticos por otros autores siguiendo distintas corrientes, como, PARKER, Donn B.; PARKER, D. B. *Crime by computer*. New York: Scribner, 1976, MOLINA ARRUBLA, Carlos. Introducción a la Criminología. *Bogotá, Diké*, 1988, TIEDEMANN, Klaus; AMELIA TR MANTILLA VILLEGAS. *Poder económico y delito:(Introducción al derecho penal económico y de la empresa)*. 1985.

[6] Cierto sector doctrinal propone diferenciar de estos a los delitos telemáticos, en los que se busca perturbar las telecomunicaciones o las tecnologías de la información, los delitos computacionales que tipifican cualquier acto humano e ilegal que tenga como fin atacar, perturbar o afectar a cualquier ordenador. DEVIA, E. (2017). Tesis… op. cit. (3) p. 5

[7] ROMEO CASABONA, Carlos Mª, De los delitos… op. cit. 4 p. 5

II.A DEFINICIÓN Y CARACTERÍSTICAS DEL BEC

EL BUSINESS EMAIL COMPROMISE (BEC) COMO UNA MODALIDAD DE PHISHING

El Business Email Compromise, en adelante BEC, es un tipo de phishing que se comete en el ámbito empresarial, nuevo en el ámbito de las TIC[8]. Por este motivo, antes de referirnos a esta conducta como tal, definiremos qué debe entenderse como phishing.

1. PHISHING

El phishing no es algo nuevo o desconocido, sino que fue uno de los primeros fenómenos en aparecer con la informática. Aunque aparece como concepto en 1995, no fue sino hasta hace una década cuando se formuló una concepción uniforme del mismo. Concretamente, fue LASTDRAGER quien se propuso encontrar una noción consensuada de este. Para ello, consultó 2458 publicaciones, llegando a la siguiente definición: *el phishing es un acto escalable de engaño mediante el cual se utiliza la suplantación de identidad para obtener información de un objetivo*[9].

Como se observa, el phishing es un tipo de fraude que consiste en el envío de un email simulando ser una entidad legítima con el objetivo de robar información, realizar un cargo económico o infectar un dispositivo. Los "phishers" se valen, para cometer estas conductas, de la ingeniería social, término popularizado por Kevin Mitnick, un hacker estadounidense, en la década del 1970[10]. La ingeniería social es el método utilizado en estas conductas, no es nueva, se ha utilizado siempre para engañar a la víctima, hacerla confiar en ti y finalmente estafarla. La podemos encontrar en la mayoría de las estafas que necesitan de contacto o habilidad social para cometerse. Lo que podemos considerar nuevo es su aplicación al ámbito informático[11].

Esta conforma el conjunto de técnicas psicológicas y habilidades sociales (influencia, persuasión, sugestión) que busca de forma directa o indirecta que un usuario

[8] VALENTÍN FLORES, D. M. Análisis del caso: compromiso de correo electrónico empresarial (business email compromise). Revista Digital de Derecho Administrativo, n. º 20, p. 1-15, 2018. ISSN 1576-9810.
[9] LASTDRAGER, E. E. Achieving a consensual definition of phishing based on a systematic review of the literature. Crime Science, vol. 3, no. 1, p. 9, 2014.
[10] En el contexto de los delitos informáticos, el término "phisher" se refiere a un individuo que emplea técnicas de ingeniería social para obtener información confidencial de los usuarios, a través de la suplantación de identidad de una entidad de confianza. Por otro lado, el mulero actúa como intermediario para los delincuentes informáticos, realizando la transferencia de bienes o dinero obtenidos de forma ilícita.. Según autores como García J.A (2018) o Gómez J.A (2017) en la bibliografía referenciados.
[11] La ingeniería social es un tipo de ataque que manipula a las personas para obtener información comprometida. Los cuatro tipos de ataques son: técnico (simulando ser una entidad conocida), ego (apelando a la vanidad), simpatía (creando una situación de ayuda) e intimidación (aparentando ser alguien importante). Este último requiere más preparación e investigación. DOMINGUEZ CHAVEZ J. Aspectos interesantes de la ingeniería social. Revista Digital: Tecnología, Ciencia y Educación, vol. 2, no. 2, 2017, p. 36-47.

revele información sensible[12]. No se actúa contra un ordenador sino contra la persona que maneja el mismo, aprovechándose de la inocencia de los usuarios que desconocen de la misma para conseguir acceso a sus dispositivos[13].

Para ello, se suplanta la identidad de una persona o entidad con el objetivo de robar datos de la víctima y luego extorsionarla o conseguir un beneficio económico en su patrimonio mediante cargos en su tarjeta. Además, suele venir acompañado de otras conductas maliciosas, especialmente un "malware" o virus malicioso, para corromper un ordenador y robar toda la información que en el mismo se encuentra[14].

2. BUSINESS EMAIL COMPROMISE: UNA MODALIDAD PERSONALIZADA DE PHISHING EMPRESARIAL

Dentro de las tipologías de phishing empresarial encontramos el BEC, una conducta en la que, tal y como hemos adelantado, estas técnicas de ingeniería social se dirigen hacia una víctima muy concreta, las empresas, especialmente aquellas que realizan transferencias bancarias internacionales, ya que generalmente tienen públicos las direcciones de correo electrónico de los ejecutivos o altos cargos relacionados con las finanzas o que tienen acceso a las cuentas para realizar dichas transferencias[15].

Se sabe que no afecta solo a grandes compañías, pero la realidad es que se desconocen datos reales sobre esta conducta[16]. Se estima que la cifra negra de criminalidad es muy elevada, y que un alto número de casos no son denunciados ni comunicados al público porque las empresas no quieren perder la confianza de los usuarios, ya que ello conlleva una pérdida de clientes y, por tanto, pérdidas económicas.

El EGMONT GROUP**,** en julio de 2019, realizo un estudio nos define los delitos BEC como un tipo de fraude en el cual los criminales ponen en riesgo las cuentas email de las víctimas, para mandar instrucciones que den lugar una transferencia fraudulenta o

[12] OWASP Latam Tour. Ingeniería social: Hacking psicológico. 2016.
[13] AYERBE, A. La ciberseguridad de la industria 4.0: Un medio para la continuidad del negocio. Economía Industrial, n. 410, p. 37-46, 2018.
[14] El malware es un software malicioso que daña sistemas informáticos sin consentimiento. Puede adoptar diferentes formas y su objetivo es causar daño o robar información. Los "keyloggers" son una forma invasiva de malware que registra pulsaciones de teclas, incluyendo contraseñas.. Como afirman AYCOCK, John; AYCOCK, John. Keylogging. *Spyware and Adware*, 2011, p. 45-58., MEJÍA CHACÓN, Carlos. Delincuencia Informática. 2007 o MITNICK, Kevin. *The art of invisibility: The world's most famous hacker teaches you how to be safe in the age of big brother and big data*. Little, Brown, 2017
[15] En 2016 Steve Mansfield-Devine llevo a cabo un estudio en el que analizo como afectaba el Business Email Compromise a las empresas Este equipo tras un año de recolección de datos encontró que los BEC perpetrados a través de técnicas de phishing eran los más comunes y estos son generalmente combinados con la ingeniería social. REMORIN, L.; FLORES, R.; MATSUKAWA, B. Tracking trends in business email compromise (BEC) schemes. Trend Micro, v. 18, n. 1, 2018.
[16] ZWEIGHAFT, D. Business email compromise and executive impersonation: are financial institutions exposed? Journal of Investment Compliance, v. 18, n. 1, p. 1-7, 2017.

para causar que datos sean transmitidos de forma fraudulenta y asi cometer delitos económicos[17].

El BEC busca obtener información confidencial y comprometer a la empresa, interceptando comunicaciones, para después sacar un rendimiento económico. Concretamente, se pretende obtener la información sobre sistemas de pago corporativos y engañar a los empleados para que realicen las transferencias a sus cuentas bancarias[18].

Lo característico, pues, en este caso son dos notas: la personalización de este cibercrimen y la utilización de un empleado de la empresa para lograr la finalidad perseguida[19].

En cuanto a la primera, cuanto más conoce el atacante de la compañía que va a ser víctima del delito más probabilidades de lograrlo. Como nos explica el Real Instituto Elcano, estos ataques están específicamente diseñados para cada empresa perjudicada[20]. Es un traje de diseñador extremadamente caro que se ha hecho específicamente para cada organización en cuanto a color, tela y talla. En esta fase de personalización del ataque, hay cuatro puntos clave, que ahora enunciaremos y desarrollaremos más adelante.

- La investigación de la víctima
- El phishing que les permite penetrar en la empresa
- La información lograda
- La ganancia patrimonial

La segunda de las características es hacia quien se dirige como víctima. Así, mientras quien se ve perjudicada es la empresa, las técnicas de ingeniería social o el engaño concreto se enfocan hacia un empleado concreto. Generalmente consiste en un correo electrónico diseñado para un empleado del equipo financiero con acceso a las cuentas bancarias de la empresa[21].

Los atacantes que utilizan este tipo de phishing usualmente suplantan al CEO de la empresa o algún proveedor. Basado en los informes del FBI hay cinco tipos de estafas BEC:

[17] EGMONT GROUP. Business e-mail compromise fraud. 30 de julio de 2019
[18] INTERPOL. Estafas a empresas por e-mail mediante suplantación de identidad (BEC) (Business Email Compromise). Disponible en: Acceso el: 3 abr. 2023.
[19] ATLAM, H. F. y OLUWATIMILEHIN, O. Business Email Compromise Phishing Detection Based on Machine Learning: A Systematic Literature Review. Electronics, vol. 12, no. 1, p. 42, 2022.
[20] AYERBE, A. Hablemos de la ciberseguridad industrial. Análisis del Real Instituto Elcano (ARI), n. 33, 2019, p. 1.
[21] Europol. (2021). Internet Organised Crime Threat Assessment (IOCTA) 2021.

1. La factura falsa o el caballo de troya: compañías con proveedores extranjeros son las víctimas de este ataque, el criminal suplanta al proveedor y pide transferencias económicas en pago por los servicios o bienes provistos a la compañía. Falsifican una factura cambiando únicamente el número de cuenta.

2. El fraude del CEO: el atacante se hace pasar por el CEO de la compañía o algún ejecutivo de alto cargo y manda un correo electrónico a algún empleado de menor rango en el equipo de finanzas diciéndoles que transfieran dinero a una cuenta que el atacante controla.

3. Cuenta comprometida: Haciendo uso de un malware el atacante se hace con el control del correo electrónico de un ejecutivo o empleado y solicita a los clientes que se encuentran en la lista de contactos de ese email un pago mediante transferencia.

4. Suplantación de un bufete de abogados: el atacante se hace pasar por el abogado a cargo de algún tema o caso crucial que afecta a la empresa y es confidencial, procediendo a pedir el correspondiente pago por sus servicios.

5. Robo de datos: Este tipo de BEC es más un método para lograr información que facilite la comisión de alguno de los otros tipos de esta estafa, los objetivos son generalmente empleados de recursos humanos o departamento financiero que controla las declaraciones tributarias de la empresa lo que se busca es conseguir los datos necesarios para suplantar a la entidad deseada.

3. DISTINCIÓN DE FIGURAS AFINES

Definido qué debe entenderse por Business Email Compromise (BEC), para comprender completamente este fenómeno, debemos distinguirlo de otras figuras afines. Ataques informáticos que se combinan con este para crear otros más sofisticados, lo que los hace cada día más difíciles de reconocer. Pero, a pesar de las diferencias entre estos tipos de ataques informáticos, todos comparten una característica común: son estafas.

Cabe señalar que, aunque cada uno tiene su propia forma de comisión, todos reciben el mismo tratamiento jurídico como delito de estafa y, en el caso de los BEC, también como delito de suplantación de identidad[22].

a. Spoofing:

[22] MONSERRAT SANCHEZ-ESCRIBANO M.ª. I. TENDENCIAS ACTUALES EN MATERIA DE CIBERCRIMEN: La respuesta penal al phishing, ransomware y DoS, Las tres principales amenazas cibernéticas a plataformas digitales desde la pandemia (Pp. 165-199) en Aportaciones jurídicas a la economía de las plataformas, MARTINEZ NADAL A. (Dir.) 2022

Según la Profesora ROBLES CARRILLO, el spoofing debe distinguirse de otras figuras afines como el Business Email Compromise (BEC). El spoofing es una modalidad de ciberataque de naturaleza instrumental, porque no suele ser un fin por sí mismo sino un medio para conseguir otras finalidades que pueden, a su vez, ser diversas. En los otros casos, el principal elemento definitorio es su finalidad[23]. El spoofing es la suplantación del dominio no el ataque final en sí mismo se podría utilizar como instrumento para llevar a cabo un delito de tipo BEC.

b. La estafa del príncipe nigeriano

La estafa del príncipe nigeriano es uno de los tipos de phishing más famosos en el mundo del cibercrimen. En esta estafa, los delincuentes se hacen pasar por un príncipe nigeriano que necesita ayuda para mover grandes cantidades de dinero. Este tipo de engaño suele incluir una solicitud de información personal o bancaria, a cambio de una promesa de recompensa económica. Aunque parezca increíble, esta técnica sigue siendo efectiva hoy en día.

Afecta, esencialmente a particulares. En muchas ocasiones, las víctimas son personas mayores o con poca experiencia en el uso de internet, que creen que están ayudando a alguien en necesidad. Sin embargo, el objetivo de los delincuentes es robar información personal o bancaria, o incluso el propio dinero de las víctimas[24].

El autor y experto en ciberseguridad BRIAN KREBS señala que esta estafa es un ejemplo de "ingeniería social", que se basa en la manipulación psicológica de las personas para obtener información o dinero. Por su parte, la Comisión Federal de Comercio de los Estados Unidos considera que la estafa del príncipe nigeriano es un tipo de "phishing", que consiste en la suplantación de identidad para obtener información sensible[25].

c. El hijacking

El hijacking, un tipo de ataque informático más técnico que los BEC en el que los delincuentes modifican un servidor para que cuando quieras entrar en un dominio determinado como por ejemplo tu cuenta de ICloud se te redirigirá a una página falsa que suplanta a la legítima en la que al poner tus datos o descargar un archivo se instala un malware o spyware en tu ordenador con el cual los atacantes se harán con el control de tus archivos y contraseñas.[26]

[23] CARRILLO, M. R., & ROS, M. A. Email Spoofing: un enfoque técnico-jurídico. Revista de la Facultad de Derecho de México, vol. 67, no. 267, 2017, pp. 109-142.
[24] Wire Wire: A West African Cyber Threat, (2016).
[25] KREPS, Brian. 2000 Hamilton-Wentworth Health Survey Second-hand Smoke and Municipal Tobacco By-law Descriptive Report. 2001.
[26] MARTINI, A. BRADLEY, J. (2012). After the Arab Spring: How Islamists Hijacked the Middle East Revolts. Revista de Estudios Internacionales Mediterráneos, (17), pp. 29-44.

Según GARCÍA FERRER, se trata de una forma de phishing en la que los ciberdelincuentes utilizan una técnica de redirección para suplantar un sitio web legítimo por uno falso. Una vez en la página falsa, los atacantes pueden pedir a los usuarios que ingresen su información personal, incluyendo nombres de usuario, contraseñas y otra información confidencial.[27]

El objetivo de un ataque de hijacking es obtener acceso a la información personal y confidencial de los usuarios. Según ROCHA, los atacantes utilizan esta información para obtener acceso a las cuentas bancarias de las víctimas o para realizar otros tipos de delitos financieros. Además, los atacantes también pueden utilizar malware o spyware para infectar los dispositivos de las víctimas y obtener acceso a su información.[28]

[27]GARCIA FERRER, A. (2018). Ciberseguridad y Ciberdefensa.
[28] ROCHA, J. (2017). Análisis de la incidencia de técnicas de ingeniería social en el marco de la ciberseguridad en España. Tesis doctoral. Universidad de Zaragoza

II. B. MODUS OPERANDI

Vista la noción del BEC así como su distinción de figuras afines, es ahora fundamental analizar el *modus operandi* de este delito y las medidas de seguridad adoptadas por las víctimas. Los delitos informáticos, como los BEC, representan un reto importante para las autoridades y los profesionales del derecho, ya que exigen un conocimiento profundo de las nuevas tecnologías y de las leyes que rigen en el mundo digital. El método utilizado y las circunstancias del caso, así como si se logró el objetivo, o no, son muy importantes a la hora de juzgar este delito.

1. DESCRIPCIÓN DEL MODUS OPERANDI

Para el modus operandi, podemos referirnos a diversos estudios, uno muy completo es el ofrecido por el EGMONT GROUP en julio de 2019 y, en segundo lugar, el de Bournemouth University[29]. El BEC se compone del siguiente conjunto de etapas:

SELECCIÓN DEL OBJETIVO Y RECOLECCION DE INFORMACION

1. Identificación del objetivo: los delincuentes buscan empresas o personas que realicen transacciones financieras importantes, normalmente internacionales.

2. Obtención de información: se recopila información sobre la empresa y sus empleados, tales como nombres, correos electrónicos, cargos, proveedores y patrones de pago.

ENGAÑO

1. A continuación, se logra el robo de información a la víctima para luego introducirse en la compañía haciendo uso de un email falso con datos reales y robados o directamente robando el email completo. Para ello, se explotan dos tipos de vulnerabilidades: suplantación de identidad y ciberataques de hacking.

    i. Suplantación de identidad: se hacen pasar por empleados de la empresa o proveedores legítimos mediante el uso de correos electrónicos falsificados o hackeados, y se envía un mensaje engañoso solicitando una transferencia de dinero.

    ii. Se hackea el email de la víctima A y su información. Después de entrar en ese email para obtener información de la víctima A lo

[29] En el estudio realizado por Alessandro Ecclesie Aggazi profesor de Bournmouth University que analizo la criminología de los delitos, ATLAM, H. F. y OLUWATIMILEHIN, O. Business Email… op. cit. 20 p. 8

investigan haciéndose con el poder de datos importantes como los contactos, detalles de transacciones, etc.

EJECUCIÓN DEL FRAUDE (REALIZACIÓN DE UNA TRANSFERENCIA PATRIMONIAL NO CONSENTIDA)

1. Acto seguido, se envía un email en el que se solicita la realización de una transacción financiera o un intercambio de datos haciendo uso de la información robada la víctima. Para ello, suele crearse una falsa sensación de urgencia: el mensaje engañoso solicita la transferencia inmediata de dinero y se crea la sensación de que hay consecuencias negativas si no se realiza la transferencia.

2. Redireccionamiento de pagos: se proporcionan instrucciones para transferir el dinero a una cuenta bancaria controlada por los delincuentes, que suele estar ubicada en otro país y puede estar a nombre de una persona o empresa falsa.

3. Cobro y desaparición: los delincuentes reciben el dinero transferido y desaparecen, dificultando su identificación y detención.

2. EL MODUS OPERANDI DESCRITO A TRAVÉS DEL ANÁLISIS DE UN EJEMPLO REAL: EL CASO UBIQUITY

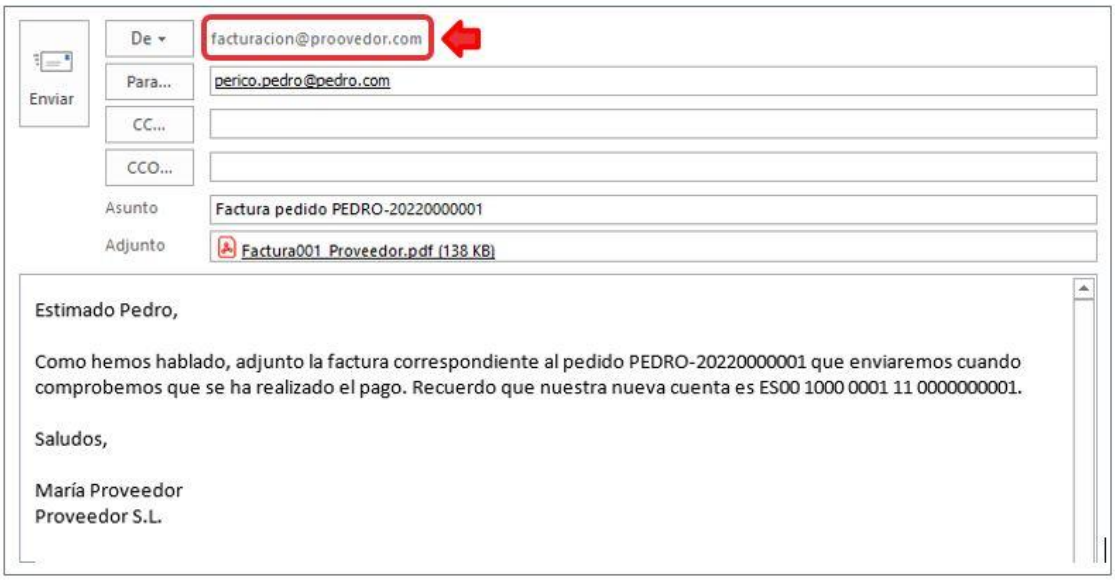
El estudio *Business Email Compromise: The $5.3 Billion Scam* (Bournemouth), se centra en dos casos paradigmáticos para explicar la teoría de estos ataques para explicar la teoría de los ataques BEC. Aunque estos casos no ocurrieron en Europa o España, son mencionados en este estudio debido a su relevancia en el análisis del modus operandi de este tipo de delitos. Por razones de practicidad nos centraremos en el caso Ubiquity, paradigmático de este tipo delictivo.

A) HECHOS:

Ubiquity es una compañía que vende productos de seguridad informática “online” y “offline”. En 2015 un miembro del departamento de finanzas recibió un email supuestamente de un ejecutivo de la empresa solicitando una transferencia de dinero por una adquisición. El email incluía instrucciones de un abogado externo. La víctima realizó 14 transferencias por un total de aproximadamente 47 millones de dólares a cuentas en el extranjero, siguiendo las instrucciones del phisher que suplantaba la identidad del ejecutivo y del abogado, durante un período de 17 días.

B) MEDIOS

Los investigadores llegaron a la conclusión de que los emails parecían muy reales e incluían una firma electrónica del despacho de abogados suplantado, pero se habían mandado desde una cuenta de email que terminaba en el dominio “consultant.com”



Creador: María Elisa Vivancos Cerezo para INCIBE

Estos errores no son tanto debidos a un sistema de seguridad débil sino a la ciega seguridad que sienten los humanos en lo relacionado con sus superiores que los lleva a no hacer preguntas si el email es medianamente creíble.

Los correos que utilizan los atacantes son la forma más común de ataque cibernético, se diseñan los correos para engañar a los usuarios y obtener información como ya hemos explicado. Estos correos parecen legítimos e incluso tienen detalles personales o corporativos, que el atacante ha obtenido antes en la fase de investigación y selección de la víctima.

Estos correos suelen incluir:

1. Una petición urgente para realizar una acción

2. Enlaces o archivos adjuntos maliciosos

3. Lenguaje persuasivo e insistente

Para pasar por un remitente legítimo se utilizan direcciones de correo electrónico lo más parecidas posibles a las reales, de esta forma se hace uso de errores ortográficos, como en el ejemplo mostrado o gramaticales que si te fijas sugieren que estamos contactando con alguien ilegítimo. Pero estos son cada vez más sofisticados, compran dominios como:

- @consultant.com
- @economics.com
- @admin.com

También pueden llegar a incluir logos y marcas de agua de empresas legítimas para parecer más auténticos. Como podemos ver en este ejemplo *(vid. supra)*, sería muy fácil creer que es un email real del proveedor, si estamos trabajando y tenemos prisa, tampoco nos lo esperamos. ¿Dónde está el error? Como podemos observar en el nombre del correo electrónico del estafador hay un error y es que pone "*proovedor*". Por muy concienciados que estemos con los delitos cibernéticos, no solemos esperar que un email dirigido especialmente a nosotros sea una estafa.

III. RESPUESTA JURÍDICA AL BEC

A.CARACTERIZACIÓN DEL BEC COMO DELITO DE ESTAFA INFORMÁTICA EN TRIÁNGULO

Definido qué es y expuesto el modus operandi utilizado en el BEC, debemos adentrarnos en la esfera jurídico-penal[30]. En la actualidad, las conductas BEC, en tanto modalidad de phishing, son castigadas como estafa informática, dado que se basan en las relaciones interpersonales, en el engaño y en el error humano. El Código Penal (CP, en adelante) regula la estafa genérica en el art. 248 y ss. y, concretamente, desde 2010, incluyó los fraudes informáticos como una nueva tipología de este delito en el art. 249.1 del CP, que hasta la reforma operada por la Ley 14/2022 era el art. 248.2 del CP.[31] El art. 249.1 del CP, castiga a "*Los que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro*."

El fraude informático en el que consiste el BEC se diferencia del tipo básico de estafa en los medios de comisión –el componente informático– y en el sujeto pasivo del delito. En relación con el primer aspecto enunciado, DEVIA GONZÁLEZ indica que esta conducta persigue la obtención de una ganancia patrimonial, propia de la estafa, pero que en este caso esta se logra a través de la apropiación, la falsificación, la interferencia y el uso de instrucciones o programas informáticos en dispositivos tanto de sobremesa como portable[32]. Se trata, según explican ÁLVAREZ VIZCAYA, CORCOY y JOSHI de manipulaciones del proceso de elaboración electrónica de carácter virtual[33]. Así pues, estos delitos se realizan a través de correos electrónicos, mensajes de texto, páginas web fraudulentas, y otros medios digitales para engañar a las víctimas y obtener un beneficio económico indebido.

---

[30] En fecha 22 de diciembre 2022 se publicó en el Boletín Oficial del Estado la reforma operada por la Ley Orgánica 14/2022 del Código Penal Español, la cual introduce cambios significativos en diversos aspectos del derecho penal.

[31] GALÁN MUÑOZ, Alfonso, El fraude y la estafa mediante sistemas informáticos, análisis del artículo 249.1 del Código Penal Español, Editorial Iirant lo Blanch, Valencia, 2005, p. 183. JAKOBS, Günther, Derecho penal parte general, fundamentos y teoría de la imputación, 2a edición corregida, Editorial Marcial Pons, Madrid, 1997. p. 14. En resumen, la estafa informática implica la transferencia no consentida de activos en sistemas informáticos. No siempre requiere la alteración del sistema, pero sí resultar en una transferencia patrimonial real y no consentida. Es necesario que la conducta realizada en el sistema informático sea adecuada para determinar una transferencia patrimonial efectiva.

[32] DEVIA GONZÁLEZ, E.A. (2017). El delito informático .. op. cit 3 p. 5; El TS indica "También hemos dicho que cuando la conducta que desapodera a otro de forma no consentida de su patrimonio se realiza mediante manipulaciones del sistema informático, bien del equipo, bien del programa, se incurre en la tipicidad del art. 248.2 del Código penal". STS, 2a de lo Penal, N° 368, de 09. V. 2007, (Ponente: Sr. Juan Ramón BERDUGO GOMEZ DE LA TORRE)

[33] VIZCAYA, Maite Álvarez. Consideraciones político-criminales sobre la delincuencia informática: el papel del derecho penal en la red. Cuadernos de derecho judicial, 2001, no 10, p. 255-280 y española, Mirentxu CORCOY y Ujala JOSHI , Delitos contra el patrimonio cometidos por medios informáticos, en "Revista Jurídica de Catalunya", 133 y ss. (1988)

En lo que respecta al sujeto pasivo del delito, lo primero que debe reseñarse es que, a día de hoy, se ha abandonado la idea de que en las estafas informáticas no hay relación interpersonal, tal y como manifestaban inicialmente autores como GALÁN MUÑOZ o JAKOBS GÜNTER[34]. En la actualidad, es ampliamente admitido, que no sólo puede darse esta posibilidad (que el error lo sufra una máquina), sino también una persona. Esto es lo que precisamente sucede en el BEC, donde el engaño y el error lo sufre un trabajador de la empresa, mientras que el perjudicado es la propia organización: El autor envía un correo electrónico falso a un empleado, engañándole y logrando con ello que este realice un desplazamiento patrimonial del patrimonio de esta al patrimonio del atacante. Por consiguiente, el sujeto pasivo o víctima del delito será el empleado, porque es quien sufre en engaño/error y el perjudicado será la empresa, pues es aquella la que ve afectado su patrimonio como consecuencia de la comisión del delito. Se trata, en este sentido, de una estafa en triángulo.

En esta modalidad de estafa, la víctima del delito es el empleado de la empresa, quien cae en el engaño y ejecuta la transferencia de activos. Sin embargo, el perjudicado es la empresa misma, ya que sufre la pérdida económica como consecuencia de la transferencia no consentida de sus activos patrimoniales.

Además, el BEC puede entrar en concurso con otros delitos. En este caso, es de reseñar el que se produce con el delito de blanqueo de capitales. Así pues, después de obtener ganancias ilícitas a través del fraude informático, los autores formas de ocultar o disfrazar el origen ilícito de los fondos obtenidos. Esto puede implicar la transferencia de los fondos a través de múltiples cuentas localizadas en jurisdicciones distintas, la creación de estructuras empresariales ficticias o la realización de transacciones complejas para dificultar la identificación del origen del dinero. Igualmente, puede entrar en concurso con delitos de acceso ilícito a sistemas informáticos, daños informáticos, falsificación de documentos, entre otros.

B. CASUÍSTICA DE LOS BEC

Existe muy poca casuística en la jurisprudencia sobre BEC. A continuación vamos a presentar los aspectos más relevantes de las sentencias donde se ha castigado esta estafa.

1. SAN 1461/2022 de 5 de abril[35]

En este caso la organización criminal llevaba a cabo facturas falsas de proveedores o hacia uso de la técnica del fraude del CEO con el objetivo de recibir dinero en las cuentas que los acusados habían abierto. Es interesante el análisis que la sentencia realiza de la propia distribución de roles en la organización:

[34] GALÁN MUÑOZ, Alfonso, El fraude y … op. cit. 32

[35] SAN Madrid 1462/2022 de 5 de abril de 2022 (Sala Penal) Pte. Rubio Encinas (ECLI:ES:AN:2022:1461)

Miembro relevante de la organización: Actúa directa o indirectamente en la comisión del delito, coordinando actividades y contactando con víctimas, proveedores y otros miembros de la organización para asegurar la eficacia del hecho delictivo.

Creadores de documentación: Son indispensables para dificultar la labor policial y engañar a las víctimas, ya que crean documentación falsa utilizada en la apertura de cuentas bancarias o en la relación con organismos públicos, usurpando identidades.

Captador: Contacta con personas cercanas a la cúpula de la organización ofreciéndoles la oportunidad de ganar dinero a cambio de abrir una cuenta bancaria con documentación falsa. También distribuyen a estas personas por todo el territorio nacional y facilitan su alojamiento y documentación para abrir cuentas en distintas localidades, complicando la investigación policial.

Mula: Contrata una cuenta bancaria con documentación falsa proporcionada por la organización y recibe el dinero obtenido ilícitamente en su cuenta. Son asesorados y ayudados por el captador para trasladarse, encontrar alojamiento y son redistribuidos periódicamente para dificultar la identificación del autor del delito. Los recurrentes del caso eran este tipo de miembro.

Testaferro: Figura como administrador de sociedades mercantiles y contrata una cuenta bancaria con su documentación legítima. Es titular de la cuenta donde se ingresa el dinero obtenido con engaños o se utiliza como intermediario en el proceso de introducción y reconducción de las cantidades defraudadas a cuentas en el extranjero.

Colaborador: Ayuda en la creación de una estructura societaria para introducir el dinero obtenido por la organización en el mercado lícito. Actúa como intermediario entre el responsable de la estructura y los testaferros, así como con entidades bancarias para gestionar y controlar las cuentas de la organización.

2. STSJ 83/2022 de 2 de marzo[36]

Esta sentencia trata sobre un correo electrónico fraudulento con una factura falsa adjunta que recibió una empresa de quien aparentaba ser de un proveedor y a consecuencia del que se realizó una transferencia de 10.261,99 euros a la cuenta indicada en el correo. En este caso, el phisher actuó a través de una segunda persona, un mulero, que recibió el dinero, lo retiró y cedió sus claves bancarias para que se realizaran más

[36] STSJM 83/2022 de 2 de marzo de 2022, (Sala Civil y Penal) Pte. Suarez Robledano (ECLI:ES:TSJ:MAD:2022:83)

operaciones fraudulentas. Sin embargo, no se pudo probar que este participara en la creación de la factura falsa ni que supiera que se iba a enviar con su correo.

Destaca en esta la interpretación que hace el Tribunal Superior sobre la cooperación necesaria del recurrente, en concreto, en el fundamento jurídico cuarto, exponiendo, la importancia de considerar los elementos de prueba que demuestran la cooperación necesaria en la comisión del delito, como la apertura de una cuenta bancaria específica para recibir fondos ilícitos y su posterior transferencia a otro destino de forma inmediata. Además, se menciona que la relación laboral en estos casos puede presentar características atípicas o indefinidas, lo cual puede indicar que el acusado tenía conocimiento de la naturaleza ilícita de los fondos y estaba colaborando con una organización criminal. Se subraya que la cooperación necesaria en el contexto de las estafas informáticas no requiere una participación material directa en la fase inicial del engaño, sino que puede implicar una actividad adyacente pero estrechamente relacionada con la del autor material del delito.

3. STS 845/2014 del 2 de diciembre[37]

En este caso, los phishers enviaron un correo electrónico falso desde una supuesta dirección de correo electrónico de la entidad bancaria Caja de Ahorros la Inmaculada a la empleada de una empresa, solicitando una actualización de la cuenta bancaria de la empresa. La empleada proporcionó el nombre de usuario y la contraseña de la cuenta, creyendo que estaba cumpliendo con una solicitud legítima de la entidad bancaria. Con los datos obtenidos, los acusados pudieron acceder a la cuenta bancaria y transferir más de 50.000 €, así como realizar varias disposiciones en efectivo. La entidad bancaria detectó la maniobra fraudulenta y realizó un retroceso por el importe no dispuesto.

En este caso es interesante la argumentación aducida por el recurrente, que cuestiona la idoneidad del engaño, que no considera bastante, así como la falta de adopción de las medidas recomendatorias sugeridas por la entidad bancaria por parte de la empresa víctima. El Tribunal Supremo considera que sí que se trata de un engaño idóneo[38], dado que estos hechos sucedieron en 2011, cuando las prácticas de "phishing" eran menos conocidas que en la actualidad y también porque el engaño funcionó en relación con dos personas y esto permitió obtener los datos necesarios para llevar a cabo la transferencia de dinero sin consentimiento, en perjuicio de un tercero y en beneficio de los acusados.

[37] STS 845/2014 (2a) de 2 de diciembre de 2014, Pte. Ferrer García (ECLI:ES:TS:2014:845)

[38] Sobre el engaño bastante, entre otras: STS 482/2008 de 28 de junio y STS 162/2012 de 15 de marzo "dejando al margen supuestos de insuficiencia o inidoneidad del engaño, en términos objetivos y subjetivos, o de adecuación social de la conducta imputada, la aplicación del delito de estafa no puede quedar excluida mediante la culpabilización de la víctima con específicas exigencias de autoprotección, cuando la intencionalidad del autor para aprovecharse patrimonialmente de un error deliberadamente inducido mediante engaño pueda estimarse suficientemente acreditada.

4. STS 291/2021, de 7 de abril[39]

Muy destacable resulta esta sentencia, en la que la organización utilizaba correos electrónicos fraudulentos en el proceso de obtener dinero de entidades públicas y particulares de manera fraudulenta. Los acusados enviaban correos electrónicos falsificados haciéndose pasar por empresas proveedoras que tenían contratos con entidades públicas. En estos correos, informaban a las entidades públicas que iban a cambiar su número de cuenta corriente y proporcionaban una nueva cuenta, que en realidad era controlada por la organización. Además, adjuntaban documentos falsificados, tanto de la empresa proveedora como bancarios, para respaldar el cambio de cuenta. Una vez que las entidades públicas recibían estos correos fraudulentos y los documentos falsificados, procedían a realizar los pagos en la nueva cuenta proporcionada por los acusados, creyendo que estaban pagando a la empresa proveedora legítima.

De la sentencia de origen, el análisis del delito en masa cometido por los acusados llegando estos a estafar más de 5.000.000 de euros a una cantidad ingente de perjudicados, entre ellos administraciones públicas y entidades financieras[40]. Tambien, la relación que establece el Juzgado de Instrucción entre la falsificación de documentos mercantiles y los delitos BEC y la estrategia fiscal y mercantil para encubrir los hechos cometiendo un ejemplar delito de blanqueo de capitales.

Gracias a esta sentencia, el Alto Tribunal ha establecido los criterios y los elementos que configuran la tipicidad penal de las conductas delictivas que enmarcan las prácticas fraudulentas de los diversos modelos de phishing BEC:

a. La falsedad cibernética no exige la realización material por el autor del delito, admite la coautoría mediata y la inducción
b. Sobre la competencia territorial, la teoría de la eficacia desplaza a la teoría de la ubicuidad
c. Todos los miembros de la organización responden de la totalidad defraudada, aunque solo hayan participado en una parte de ella.

En cuanto al concurso de delitos, establece que nos encontramos generalmente ante un concurso ideal entre los distintos delitos que se cometen en cada una de las estafas BEC, es decir la suplantación de identidad, la estafa informática y el blanqueo de capitales.

Por último, nos gustaría destacar que en su gran mayoría el BEC no se da contra una sola empresa, se da contra muchísimas, esto genera un delito continuado para los acusados e incluso un delito en masa.

[39] STS 291/2021 (2a) de 7 de abril de 2021, Pte. Gómez de la Torre ((ECLI: ES:TS: 2021:291)
[40] SAN 8/2020 de 15 de septiembre de 2020, Pte. Fernández Prado (ECLI: ES:AN:2020:4293)

C.COMMON LAW VS CIVIL LAW

A diferencia del legislador español, otros legisladores, como el italiano o el estadounidense, no optan por una regulación generalista del delito de estafa informática, sino que establecen una amplia lista de métodos comisivos, largas agravantes, tipos específicos si no que la incluye dentro del tipo básico de estafa. La legislación sobre delitos informáticos varía de un país a otro, pero existen similitudes en los criterios de tipificación de las conductas delictivas[41].

En el Reino Unido (GB), las estafas informáticas están tipificadas y castigadas bajo la Computer Misuse de 1991, en concreto en la sección 6 y 7 del Fraud Act 2006, Así como también bajo leyes específicas de delitos informáticos y de protección de datos[42].

En Estados Unidos se castiga la utilización ilegal de sistemas informáticos con el Acta Federal de Abuso Computacional (18 U.S.C. Sec.1030) que modificó al Acta de Fraude y Abuso Computacional de 1986, para aquellos que incurran en conductas delictivas como el acceso no autorizado a sistemas informáticos o la obtención de información confidencial mediante medios electrónicos[43].

En Italia, las estafas informáticas están tipificadas y castigadas bajo el Código Penal italiano en el 640-ter del Código Penal italiano[44].

En Francia, lo encontramos regulado en la *Lamy Droit de L'lnformatique, Paris, 1989, 1505 y ss.*[45].

D.NORMATIVA SUPRANACIONAL

La Unión Europea ha adoptado diversas medidas para prevenir y combatir los delitos informáticos, incluyendo los delitos BEC.

En primer lugar, el Convenio de Budapest–Convenio sobre el Cibercrimen 21 de noviembre de 2001– fija la directriz general para el delito de estafa informática en el artículo 8 [46]. Tras años de trabajo los 45 países que formaron parte del convenio

---

[42] Recuperado de: (25 de abril de 2023) https://www.legislation.gov.uk/ukpga/2006/35/section/6/2006-11-

[43] *Recuperado de: (25 de abril de 2023) https://uk.practicallaw.thomsonreuters.com/2-508-3428?transitionType=Default&contextData=(sc.Default)*

[44] Recuperado de: (25 de abril de 2023) https://www.brocardi.it/codice-penale/libro-secondo/titolo-xiii/capo-ii/art640ter.html

[45] NEDELEC, Bruno, "La criminalità informatica nel diritto penale francese", en Diritto Penale e Proceso, (febbraio, 2002), 241-245.

[46] Fraude informático. La norma establece que se deben tipificar como delito los actos ilegítimos que causen perjuicio patrimonial mediante la introducción, alteración o interferencia en datos informáticos con intención dolosa de obtener un beneficio económico, según el Convenio 185 del Consejo de Europa sobre la Ciberdelincuencia. Convenio 185, Del Consejo de Europa, sobre la Ciberdelincuencia, Budapest, 23. XI. 2001.

lograron la ratificación de este, pero, España no lo ratifico hasta 9 años más tarde, el 20 de mayo de 2010, siendo finalmente publicado en el BOE el 17 de septiembre de ese año[47]. Es igualmente destacable la falta de referencia directa al mismo, simplemente se mencionan las obligaciones internacionales suscritas por España, en la reforma del CP de 2010. Lo que si que se menciona de forma directa es la normativa europea:

La UE ha establecido un marco jurídico común transponiendo el Convenio sobre Cibercrimen de 2001, 23 de noviembre, a través de la Directiva (UE) 2013/40 relativa a los ataques contra los sistemas de información y por la que se sustituye la Decisión marco 2005/222/JAI del Consejo[48]. Esta directiva establece medidas para mejorar la prevención, detección e investigación de los delitos informáticos, incluyendo los delitos BEC, y para garantizar que los Estados miembros tengan sanciones efectivas, proporcionales y disuasorias contra dichos delitos[49].

La estafa informática se incorporó al Código Penal durante la reforma de 1995 y asi se puso fin a la discusión doctrinal sobre si se podía engañar a una maquina o no, que de nuevo ha sido probado en nuestro trabajo que curiosamente viene centrado en engañar al humano a través de la máquina. Asi pues no significo la aparición de un nuevo delito la adhesión de España al Convenio de Budapest de 2001 ni la normativa europea sino más bien un paso agigantado hacia la unificación de criterio, nomenclatura, definiciones, entre otro. Fue el primer paso hacia la colaboración entre Estados, para lograr una mayor seguridad contra estos delitos y seguridad jurídica en los mismos.

[47] Como dato curioso, esta modificación coincidió con el periodo de vacatio legis de la vigésimo cuarta reforma del CP

[48] Suscrito en Budapest el 23 de noviembre de 2001 y auspiciado por el Consejo de Europa y tiene como objetivos fundamentales armonizar las leyes penales aplicables a los delitos informáticos, establecer reglas de procedimiento penal para la investigación y persecución de estos delitos, y promover la cooperación internacional en este ámbito.

[49] Destaca de la reforma del Código Penal de 2010 LO 5/2010 de 22 de junio: la mención directa *en el marco de los denominados delitos informáticos para cumplimentar la Decisión Marco 2005/222/SAI de 24-2-2005, relativo a ataques contra Sistemas de Información se ha resuelto incardinar las conductas punibles en los apartados diferentes al tratarse de bienes jurídicos diversos […]*

IV. CONCLUSIONES: UN DELITO DE ANTES CON LOS MEDIOS DE AHORA.

En esta tesis se nos ha permitido llegar a cinco conclusiones:

En primer lugar, el BEC no es la estafa convencional ni tampoco tiene la naturaleza originaria del *phishing*. Aunque podemos unirlo a la estafa tradicional por su estructura triangular y por la tendencia que persigue el autor: se engaña para conseguir un beneficio económico, lo cierto es que en este caso los medios comisivos de esta estafa son altamente inteligentes y personalizados para cada víctima, para cada trabajador atacado. Se trata de una modalidad mucho más avanzada y sofisticada de estafa tradicional.

En segundo lugar, lo anterior nos demuestra que la importancia que está adquiriendo la tecnología en la comisión de las figuras tradicionales, lo que nos lleva a plantearnos si los delitos informáticos deberían tener un propio título en el CP, separado del resto de delitos.

En tercer lugar, analizada la jurisprudencia sobre las estafas informáticas BEC, cabe decir que nuestros tribunales se han adaptado a esta nueva realidad y aplican de forma uniforme el delito de estafa informática a los casos de BEC. No obstante, podemos apreciar que aún hay cierta confusión en cuanto a los términos tecnológicos en estas sentencias refiriéndose al BEC de formas distintas, y si bien consideramos que se necesita cierta uniformidad en esto.

Por último, este trabajo ha evidenciado la necesidad de medidas de seguridad, medidas de cooperación, capacitación de los trabajadores, entre otros. Hay brechas en los sistemas que ya no solo son tecnológicas si no humanas, debe ser considerado esencial la formación de los empleados y entidades en cuanto a este tipo de delitos. Y ser prioridad en la enseñanza de las nuevas generaciones. La cifra negra de estos delitos no para de aumentar, y se ha de fomentar la denuncia de los casos BEC por encima de la asunción del daño para no perder clientes, sin estos casos públicos no se puede concienciar a la sociedad sobre el problema, como se dio en el pasado con la violencia de genero.

V. REFERENCIAS BIBLIOGRÁFICAS:

1. ÁLVAREZ GARCÍA, Francisco Javier; y GONZÁLEZ CUSSAC, Jose Luís (Directores). Comentarios a la Reforma Penal de 2010. Valencia:Tirant lo Blanch Reformas, Trust CM, 2010. P.277-285.
2. ÁLVAREZ GARCÍA, Francisco Javier; y GONZÁLEZ CUSSAC, Jose Luís (Directores). Comentarios a la Reforma Penal de 2010. Valencia:Tirant lo Blanch Reformas, Trust CM, 2010. P.277-285.
3. AYERBE, A. Hablemos de la ciberseguridad industrial. Análisis del Real Instituto Elcano (ARI), n. 33, 2019, p. 1.
4. AYERBE, A. Hablemos de la ciberseguridad industrial. Análisis del Real Instituto Elcano (ARI), n. 33, 2019, p. 1.
5. *Business e-mail compromise fraud*. 30 de julio de 2019 ID: EG-Bulletin-01/2019.Disponible en: https://www.nbc.gov.kh/cafiu/download/The-Egmonts-Group
6. *Business Email Compromise: A Global Threat.* Recuperado de https://research.checkpoint.com/2022/business-email-compromise-a-global-threat/
7. (Business Email Compromise). Disponible en: https://www.interpol.int/es/Delitos/Delincuencia-financiera/Estafas-a-empresas-por-e-mail-mediante-suplantacion-de-identidad-BEC-Business-Email-Compromise. Acceso el: 3 abr. 2023.
8. CARRILLO, M. R., & ROS, M. A. Email Spoofing: un enfoque técnico-jurídico. Revista de la Facultad de Derecho de México, vol. 67, no. 267, 2017, pp. 109-142.
9. CHECK POINT RESEARCH. (2022). Business Email Compromise: A Global Threat. Recuperado de https://research.checkpoint.com/2022/business-email-compromise-a-global-threat/
10. DEPARTAMENTO DE JUSTICIA DE LOS ESTADOS UNIDOS. (2023). Global BEC Hackers Group Dismantled. Consultado 16 de marzo de 2023 de https://www.justice.gov/opa/pr/global-bec-hackers-group-dismantled
11. DEVIA, E. (2017). Tesis Completa. Consultado el 3 de abril de 2023, de https://idus.us.es/bitstream/handle/11441/75625/Tesis%20Edmundo%20Devia%20Completa%20Final%2031%20Mayo%202017.pdf?sequence=1&isAllowed=
12. DEVIA GONZÁLEZ, E. (2017). El delito informático: Estafa informática del artículo 249.1 del CP. (Tesis Doctoral Inédita). Universidad de Sevilla, Sevilla. (153-159)
13. DOMINGUEZ CHAVEZ J. Aspectos interesantes de la ingeniería social. Revista Digital: Tecnología, Ciencia y Educación, vol. 2, no. 2, 2017, pp. 36-47.
14. EGMONT GROUP. Business e-mail compromise fraud. 30 de julio de 2019 ID: EG-Bulletin-01/2019.Disponibleen: https://www.nbc.gov.kh/cafiu/download/The-Egmonts-Group Report/9.Business_Email_Compromise_July_2019.pdf

15. *Estafas a empresas por e-mail mediante suplantación de identidad* (BEC) (Business Email Compromise). Disponible en: https://www.interpol.int/es/Delitos/Delincuencia-financiera/Estafas-a-empresas-por-e-mail-mediante-suplantacion-de-identidad-BEC-Business-Email-Compromise. Acceso el: 3 abr. 2023. INTERPOL.
16. EUROPOL. (2021). Internet Organised Crime Threat Assessment (IOCTA) 2021. https://www.europol.europa.eu/iocta/2021
17. EUROPOL. (2019). Internet Organised Crime Threat Assessment (IOCTA) 2019. https://www.europol.europa.eu/iocta/2019
18. EUROJUST. (2018). Business Email Compromise fraudsters sentenced in multiple jurisdictions. Recuperado de https://www.eurojust.europa.eu/press/PressReleases/Pages/2018/2018-07-26.aspx
19. FERNÁNDEZ TERUELO, JavierGustavo. Cibercrimen. Los delitos cometidos a través de internet. Constitutio criminalis, carolina, 2010. P. 27-53.
20. FLORES, J. J. Ciberseguridad y protección de datos en el ámbito empresarial. Diálogo con la Jurisprudencia, vol. 1, no. 4, p. 263-273, 2020.
21. FLORES, V. Estrategias de ciberseguridad para la protección de la información en las organizaciones. AUS Artículos de Investigación y Desarrollo, vol. 4, no. 3, 2019.
22. FLORES-ALVAREZ, L. A. et al. Data breaches: un enfoque desde la ingeniería en sistemas. Revista Investigación en Educación en Ciencia y Tecnología, vol. 21, no. 1, 2020, pp. 75-96.
23. GARCÍA, J. A. (2018). Delitos informáticos: impunidad organizacional y su impacto en la sociedad. Revista de Derecho, 47, 7-28. https://doi.org/10.18682/pdc.v47i0.1047
24. GÓMEZ, J. A. (2017). Acerca de la imputación penal del "phishing" y el "pharming". Revista de Derecho Penal y Criminología, 17(49), 267-290. https://doi.org/10.5354/0719-2584.2017.46867
25. GÓMEZ TOMILLO, Manuel (dir.). Comentarios al Código Penal. Lex nova. P. 969-971.
26. DICCIONARIO de informática y telecomunicaciones, Inglés-Español, Editorial Ariel S.A., Barcelona, España 2001.
27. INTERPOL. Estafas a empresas por email mediante la suplantación de identidad (BEC) (Business Email Compromise). Disponible en: https://www.interpol.int/es/Delitos/Delincuencia-financiera/Estafas-a-empresas-por-e-mail-mediante-suplantacion-de-identidad-BEC-Business-Email-Compromise. Acceso el: 3 abr. 2023.
28. INCIBE. (2021). Alerta Fraude CEO. Recuperado de https://www.incibe.es/protege-tu-empresa/avisos-seguridad/alerta-fraude-ceo
29. INCIBE. (2022). Cibercrimen. Recuperado de https://www.incibe.es/protege-tu-empresa/desafios/cibercrimen
30. *Ingeniería social: Hacking psicológico*. 2016. OWASP Latam Tour.
31. Journal of Investment Compliance, v. 18, n. 1, p. 1-7, 2017.

32. LASTDRAGER, E. E. Achieving a consensual definition of phishing based on a systematic review of the literature. Crime Science, vol. 3, no. 1, p. 9, 2014.
33. JAKOBS, Günther, Derecho penal parte general, fundamentos y teoría de la imputación, 2a edición corregida, Editorial Marcial Pons, Madrid, 1997. p. 14.
34. Journal of Investment Compliance, v. 18, n. 1, p. 1-7, 2017.
35. KREPS, Brian. 2000 Hamilton-Wentworth Health Survey Second-hand Smoke and Municipal Tobacco By-law Descriptive Report. 2001.
36. Kleiman, E. M. (2018). Business email compromise: Emerging global threats and trends. Information Security Journal: A Global Perspective, 27(4), 228-235. https://doi.org/10.1080/19393555.2018.1444999
37. Cybersecurity, vol. 1, no. 1, 2018, pp. 1-7.
38. LÉON ALONSO, J. A., & GONZÁLEZ CARRILLO, D. La ciberseguridad en el ciberespacio. Revista de Investigación en Derecho y Tecnología, vol. 3, no. 2, 2018, pp. 33-58.
39. MARTÍNEZ GÓMEZ, A. Estudio sobre ciberseguridad industrial en España. Revista de Derecho Industrial, n. 340, p. 297-348, 2018.
40. MARTINI, A. BRADLEY, J. (2012). After the Arab Spring: How Islamists Hijacked the Middle East Revolts. Revista de Estudios Internacionales Mediterráneos, (17), pp. 29-44.
41. MOLINA ARRUBLA, Carlos. Introducción a la Criminología. Bogotá, Diké, 1988,
42. MONSERRAT SANCHEZ-ESCRIBANO Mª. I. TENDENCIAS ACTUALES EN MATERIA DE CIBERCRIMEN: La respuesta penal al phishing, ransomware y DoS, Las tres principales amenazas cibernéticas a plataformas digitales desde la pandemia (P.p 165-199) en Aportaciones jurídicas a la economía de las plataformas, MARTINEZ NADAL A. (Dir.) 2022
43. SÁNCHEZ BERNAL, J.: «El bien jurídico protegido en el delito de estafa informática», en: *Cuadernos del Tomás, Revista de estudio electrónica del C. M. Tomás Luis de Victoria*, N° 1, 2009.
44. OWASP Latam Tour. Ingeniería social: Hacking psicológico. 2016.
45. ANTÓN ONECA J. Voz «Estafa», en Nueva Enciclopedia Jurídica, Francisco Seix, Barcelona, 1958, pp. 56 y ss
46. PARKER, Donn B.; PARKER, D. B. Crime by computer. New York: Scribner, 1976,
47. REMORIN, L.; FLORES, R.; MATSUKAWA, B. Tracking trends in business email compromise (BEC) schemes. Trend Micro, v. 18, n. 1, 2018. ISSN 1386-3018.
48. ROCHA, J. (2017). Análisis de la incidencia de técnicas de ingeniería social en el marco de la ciberseguridad en España. Tesis doctoral. Universidad de Zaragoza
49. ROMEO CASABONA, Carlos M, De los delitos informáticos al cibercrimen, El Cibercrimen, nuevos retos jurídicos-penales, nuevas respuestas Político-Criminales, Editorial Comares S. L., Granada, 2006, p. 9.

50. Serrano Rodríguez, J. L. (2019). Delitos informáticos: un análisis comparativo de las normativas de la Unión Europea, España y Chile. Revista de Derecho, 51, 137-155.
51. TIEDEMANN, Klaus; AMELIA TR MANTILLA VILLEGAS. Poder económico y delito:(Introducción al derecho penal económico y de la empresa). 1985.
52. VALENTÍN FLORES, D. M. Análisis del caso: compromiso de correo electrónico empresarial (business email compromise). Revista Digital de Derecho Administrativo, n.º 20, p. 1-15, 2018.
53. Wire Wire: A West African Cyber Threat, (2016).
54. Zweighaft, D. (2017). Business email compromise and executive impersonation: are financial institutions exposed? Journal of Investment Compliance, 18(1), 1-7.