Métodos de fraude basados en el correo electrónico

PID_00270255

Thomas Holt

Tiempo mínimo de dedicación recomendado: 3 horas

Universitat Oberta de Catalunya

Thomas Holt

El encargo y la creación de este recurso de aprendizaje UOC han sido coordinados por el profesor: Marc Balcells Magrans (2019)

Primera edición: septiembre 2019

Av. Tibidabo, 39-43, 08035 Barcelona
Realización editorial: FUOC

Índice

Introducción

Los módulos anteriores exploraron los delitos cibernéticos que requieren cierto grado de interacción entre la víctima y el delincuente, aunque esto no es esencial para facilitar cualquier tipo de fraude o daño económico. Un pirata informático puede obtener acceso a datos confidenciales o a un sistema informático sin la participación de una víctima en una conversación o una interacción prolongada. Sin embargo, hay una variedad de ciberdelitos económicos que obligan al delincuente a encontrar formas de contactar con las posibles víctimas y establecer una relación con ellas. Todos estos delitos implican algún tipo de fraude, como se advierte en el módulo 1, por ejemplo, el uso del engaño o de la fuerza para obtener algo de valor. Algunas de estas estafas necesitan que el delincuente establezca una relación con la víctima, que debe tener cierto grado de confianza con el delincuente (Maurer, 1981). Como resultado, la víctima tenderá a darle al estafador lo que le pida, generalmente dinero o bienes, que no le serán devueltos ni le proporcionarán a la víctima beneficios directos. Es por eso por lo que muchas de estas estafas a veces se denominan abuso de confianza (o en inglés, *confidence schemes*), y esta clase de estafadores, *scammers* (Maurer, 1981).

En espacios virtuales, los delincuentes han adaptado numerosos métodos de fraude utilizados en encuentros cara a cara en la estafa en línea. De hecho, los métodos de fraude han evolucionado en función de varias innovaciones tecnológicas, desde periódicos y teléfonos hasta máquinas de fax en la década de 1980 (United States Department of State, 1997). En los años noventa, los estafadores comenzaron a utilizar el correo electrónico y los sitios web como lugares para cometer fraudes, por lo que los estudiosos del cibercrimen argumentan que estos delitos pueden considerarse ciberdelitos o delitos basados en el uso de la informática (véase, por ejemplo, Furnell, 2002; Wall, 2004). Este término es importante porque reconoce que cualquier delito, aun pudiendo cometerse sin ayuda de un ordenador, se vuelve más fácil con la tecnología.

Como se señaló en el módulo 1, existen innumerables beneficios para las personas que participan en fraudes cibernéticos. Las redes sociales y el correo electrónico permiten a los estafadores hacer confusa su identidad y ubicación reales, y presentarse como de cualquier género, edad, raza o etnia que crean que pueda beneficiar su plan. Además, las plataformas de comunicaciones en línea permiten a los delincuentes el acceso directo a millones de posibles víctimas a un precio generalmente bajo (Wall, 2004). Los sistemas de comunicaciones en línea reducen en gran medida los costes que deben invertir los delincuentes para sus estafas, ya que el correo electrónico es gratuito para los usuarios en general. Asimismo, el correo electrónico permite a los remitentes distribuir imágenes, texto, enlaces html y varios archivos adjuntos. Los esta-

fadores pueden manipular correos electrónicos para que parezcan originarse en cualquier fuente y utilizar imágenes y texto para hacer sus reclamos más verosímiles.

Otro beneficio que los estafadores obtienen de la tecnología es que pueden utilizar herramientas para enviar correos electrónicos, mensajes de texto y mensajes directos no solicitados a posibles víctimas en grandes cantidades. Estos mensajes a menudo se denominan *spam* y son una amenaza común que el público en general debe afrontar a diario (Wall, 2004). Por ejemplo, un proveedor de seguridad señaló que el 52 % de todo el tráfico de correo electrónico observado en el 2018 se basó en correo *spam*, del cual la mayoría se originó en China (Vergelis, Shcherbakova y Sidorina, 2018). Teniendo en cuenta los cientos de millones de correos electrónicos que se envían cada día, una gran parte de ese contenido lo constituirían numerosos delitos de fraude e intentos de cometer otros ciberdelitos.

Este módulo proporcionará una descripción general de las diversas formas de fraude en línea que se cometen a través de mensajes de correo electrónico no deseado y de la manipulación de redes sociales. Se abordarán la dinámica de los métodos de fraude empleados y el alcance de los daños según las víctimas. Esta no es una lista exhaustiva, sino que se centra en las formas más investigadas e impactantes que afectan tanto a personas como a empresas. El módulo concluye con una discusión sobre las características personales y demográficas asociadas a algunas formas de victimización por fraude.

1. Los correos electrónicos nigerianos

Una de las formas más antiguas y más comunes de fraude en línea basado en *spam* se conoce comúnmente como estafas de pago por adelantado (o *advance fee fraud schemes*). Estos mensajes suponen que un estafador solicite una pequeña cantidad de dinero al destinatario para luego poder recibir una mayor cantidad de dinero. Estos esquemas de fraude se denominan a veces estafas nigerianas porque muchos de los remitentes en estos mensajes afirman vivir en países extranjeros, especialmente en Nigeria y otros países africanos y del Medio Oriente (véase Smith, Holmes y Kaufmann, 1999). Coloquialmente, también se les denomina timos 419, en referencia al código legal utilizado para procesar el fraude en Nigeria (Edelson, 2003; Holt y Graves, 2007). Se desconoce cuántos de los remitentes residen realmente en Nigeria, aunque los datos sugieren que existen fraudes y estafas que no se cometen en naciones africanas (Tade, 2016).

Como se señaló, existen numerosos tipos de estafa de pago por adelantado; una de las más comunes se produce cuando el remitente afirma ser heredero de la realeza o alguien extremadamente rico. El remitente necesita ayuda para mover los fondos heredados de sus cuentas a una nación extranjera porque se enfrenta algún tipo de riesgo (Edelson, 2003; Holt y Graves, 2007; Nhan, Kinkade y Burns, 2009). Una variante de este esquema consiste en que el remitente afirme que ha sido gravemente herido o se está muriendo y busca ayuda para distribuir su fortuna a organizaciones benéficas en todo el mundo (Holt y Graves, 2007; Nhan y otros, 2009). El destinatario recibirá dichos fondos si proporciona información al remitente y ayuda a distribuirlos, como se indica en el siguiente ejemplo:

Buenos días:

Mensaje privado para ti.

Este es un mensaje importante para ti. El Señor me indica que comparta esto contigo. Mientras lea el correo, debe simpatizar con mi situación actual y ayudarme. Mi nombre es Isabella Carmel, la única superviviente de una familia de cuatro. Me escapé por poco del desastre del tsunami que afectó a mi médula espinal y también a mi tímpano y que se cobró las vidas de toda mi familia, mi esposo (Denis Carmel) y mis dos hijos (Ugo y Tom), que se fueron de vacaciones a Sri Lanka.

Ahora mismo estoy en Kuala Lumpur, Malasia. Después de quedarme una semana en el hospital de mi familia, sufro una discapacidad a raíz de la catástrofe y tengo que ir en silla de ruedas después de todo el tratamiento. Esto dificulta cualquier forma de medicina y ahora solo tengo unos pocos meses de vida, según médicos expertos. No he tenido una buena vida, pues siempre estuvo enfocada al negocio de mi difunto padre. Mi padre es muy rico y nunca fue generoso. Y ahora me arrepiento de todo esto, ya que sé que hay más en la vida que solo querer tener o ganar todo el dinero del mundo. La Biblia dice: ¿de qué le servirá a un hombre ganarse el mundo entero y perder su alma? Creo que cuando Dios me dé una segunda oportunidad para venir a este mundo, viviré mi vida de una manera diferente a como lo había hecho antes. He querido y dado la mayoría de las propiedades de mi padre a los menos privilegiados porque quiero que Dios sea misericordioso conmigo y acepte mi alma. He decidido

ofrecer mi ayuda a ONG, y socorro y consuelo a los menos privilegiados en nuestras sociedades. Quiero que esta sea una de las últimas buenas obras que haga en la tierra, ya que mi padre nunca lo ha hecho.

Por ahora tengo que repartir todo el dinero a organizaciones benéficas, pero mi salud se ha deteriorado tanto que ya no puedo hacerlo más. Por eso estoy solicitando su ayuda para que se haga esta donación en mi nombre. Lo último que queda del dinero de mi difunto padre y que estoy dispuesta a donar a los menos privilegiados en este momento es la enorme suma de 10,6 millones de dólares estadounidenses, que está oculto en un envío y depositado en (COMISIÓN INTERNACIONAL DE CRÉDITO) para su custodia, con la intención de invertir todo el dinero en una provechosa industria económica.

Quiero que me ayude a reclamar estos fondos donde se encuentran y repartirlos a organizaciones benéficas y a los menos privilegiados de la sociedad. Le agradeceré que indique su interés por el desembolso y que también incluya sus números de teléfono/fax de contacto, que enviaré a la (COMISIÓN INTERNACIONAL DE CRÉDITO) para poder contactarlo como el beneficiario designado. Le proporcionaré el certificado de depósito y la carta de autoridad para permitirle reclamar el envío de los fondos.

Si está dispuesto a ayudarme con este proyecto, envíeme un correo electrónico a [dirección eliminada] sin demora. Quedo a la espera de su respuesta. Gracias una vez más por su amabilidad, que Dios lo guíe y recompense en todas sus tareas mientras me ayuda a realizar mis últimos sueños y deseos.

Bendiciones.

Sra. Isabel Carmel

Otro esquema de fraude relacionado consiste en que el remitente se haga pasar por un banquero o abogado que trata de cerrar la cuenta de un cliente muerto utilizando al destinatario del correo electrónico como pariente más cercano del fallecido (Edelson, 2003). En este caso, el remitente afirma que le dará al destinatario parte de una gran suma de dinero a cambio de asistencia financiera y legal (Edelson, 2003; Holt y Graves, 2007). He aquí un excelente ejemplo:

Querido amigo:

Perdóneme si me entrometo en su privacidad, no nos conocemos pero no importa. Lo que importa es la transparencia entre nosotros durante este acuerdo. Soy el señor Favor Adim Duke, contable de Inland Bank S. A. Lo he encontrado tras mi búsqueda de una persona fiable y de buena reputación para manejar la siguiente transacción comercial confidencial. Un extranjero, el difunto Engr Burke Sean, un contratista del Gobierno Federal hasta su muerte en el vuelo 801 de Korean Air, que se estrelló en Guam en agosto de 1997, tenía su cuenta con nosotros aquí, en Inland Bank S. A. y tenía un saldo final de 20,5 millones de dólares (veinte millones quinientos mil dólares) que el banco, sin duda, espera que sea reclamado por cualquier familiar cercano al difunto beneficiario, pues de lo contrario será entregado a un fondo fiduciario desacreditado por comprar armas y municiones a un colegio militar aquí en Nigeria.

El Inland bank ha hecho un enorme esfuerzo para ponerse en contacto con cualquiera de los familiares de Burke, pero no ha servido de nada. Probablemente se deba al fracaso percibido al no poder localizar a ninguno de los familiares cercanos del difunto. El familiar más cercano de Burke Sean afirma que la Administración, bajo la influencia de nuestro presidente y los miembros de las juntas directivas, el señor I. Yuguda, hizo un arreglo para que los fondos sean declarados no reclamables y que posteriormente puedan ser donados al fondo fiduciario para armas y municiones y así promover aún más el curso de la guerra en África y el fin del mundo en general, pues ya sabe usted que esta guerra traerá en un futuro la destrucción de la humanidad.

Con el objetivo de evitar esta catástrofe, pido su permiso para hacerse pasar por el familiar más cercano de Engr Burke Sean y que los fondos de 20,5 millones de dólares estadounidenses (veinte millones quinientos mil dólares) se liberen y paguen en su cuenta bancaria como Familiar Más Cercano. Este es un acuerdo exclusivo entre usted y yo, ya que todos los documentos y pruebas para permitirle obtener este fondo se manejarán con precaución. Además le garantizo una participación 100 % libre de

riesgos en este acuerdo. Su parte de los 20,5 millones de dólares depende de nuestro acuerdo según avancemos. También me gustaría invertir mi propia parte del dinero en su país con su ayuda después de la transferencia. Si esta propuesta es válida para usted, por favor contácteme enviándome un correo electrónico, lo que le agradezco de antemano. Me gustaría que visitara el siguiente sitio web para obtener más aclaraciones sobre este empeño.

Atentamente,

Sr. Favor Adim Duke.

Contable en Inland Bank S. A., Sucursal de Lagos

Una variante similar y popular de este tipo de estafa supone que el remitente se haga pasar por un funcionario público que ha sobregirado o cargado fondos de un contrato comercial o gubernamental (Edelson, 2003). Esta actividad ilegal puede llamar la atención del remitente, por lo que se busca una parte externa que pueda ayudarle a mover los fondos fuera del país. A su vez, el remitente tendrá derecho a una parte de esos fondos, como se indica en este ejemplo:

De: Prince Joe Eboh

Fecha: miércoles 21 de abril de 2004, 12:53 PM

Asunto: TRANSFERENCIA

Prince Joe Eboh

Querido señor, señora:

Hoy estoy bien, ¿cómo está usted? Espero que esta carta le encuentre en el mejor estado de salud. Soy Prince Joe Eboh, presidente del «Comité de adjudicación de contratos», de la «Comisión de Desarrollo del Delta del Níger (CDDN)», una subsidiaria de la Corporación Nacional de Petróleo de Nigeria (CNPN).

La Comisión de Desarrollo del Delta del Níger (CDDN) fue creada por el difunto jefe de Estado, el general Sani Abacha, que murió el 18 de junio de 1998, para administrar el exceso de ingresos provenientes de las ventas de petróleo y otros productos relacionados, como un aumento del precio del petróleo en el mercado nacional, y ayudar al desarrollo de las comunidades que viven en las áreas productoras de petróleo del Delta del Níger. El ingreso anual estimado para 1999 fue de 45.000 millones de dólares estadounidenses, FMF A26 Unidad 3B Párrafo "D" del Auditor General de la República Federal de Nigeria, informe de noviembre de 1999 sobre ingresos estimados.

Soy el presidente del Comité de Adjudicación de Contratos, y mi comité es el único responsable de guardar y pagar los contratos en nombre del Gobierno Federal de Nigeria. Mi comité otorgó contratos a contratistas extranjeros para la perforación y para cuestiones medioambientales en las áreas productoras de petróleo del Delta del Níger. Superamos la suma del contrato en 25.000.000 dólares estadounidenses. Hemos pagado a los contratistas y retenido un saldo de 25.000.000 dólares estadounidenses. No obstante, debido a la existencia de algunas leyes nacionales que prohíben a los funcionarios públicos en Nigeria abrir, operar y mantener cuentas en el extranjero, no tenemos los conocimientos necesarios para transferir este saldo de fondos a una cuenta en el extranjero.

Sin embargo, este saldo de 25.000.000 dólares estadounidenses ha sido asegurado en forma de crédito/pago a un contratista extranjero, por lo tanto, deseamos transferirlo a su cuenta bancaria como beneficiario del fondo. También hemos llegado a la conclusión de que se le dará el 20 % de la suma total transferida como nuestro socio extranjero, mientras que el 5 % se reservará para gastos incidentales en los que incurrirán ambas partes en el curso de esta transacción; el restante 75 % se mantendrá para los miembros del comité.

Si se considera capaz de ayudarnos a realizar esta transacción, debe enviarme de inmediato los detalles de sus datos bancarios o abrir una nueva cuenta bancaria donde podamos transferir el dinero de 25.000.000 dólares estadounidenses, que mantendrá

en fideicomiso para nosotros hasta que lleguemos a su país para repartir nuestra parte. Su ocupación habitual no es importante en esta transacción. Los detalles requeridos incluyen el nombre de su empresa, la dirección, sus números de teléfono/fax personales, su nombre completo y dirección, y sus datos bancarios íntegros para que el fondo transferido sea enviado por Apex Bank.

Tenga en cuenta que se espera que esta transacción se actualice dentro de los 21 días hábiles a partir del día en que los detalles requeridos se envíen al Ministerio Federal de Finanzas, que aprobará la asignación de control de divisas necesaria para enviar este dinero a su cuenta. Por favor, trate esto como alto secreto. Contáctame urgentemente.

Gracias por su cooperación.

Atentamente,

Prince Joe Eboh

En todas estas variantes de estafas de pago por adelantado, hay algunas solicitudes frecuentes que se hacen a las posibles víctimas que recibieron el mensaje. Primero, y fundamentalmente, el destinatario se comunicará con el remitente por correo electrónico y entablará una conversación (Holt y Graves, 2007). Después de este intercambio, el estafador pedirá al destinatario que proporcione un pago que pueda servir como depósito, donación o modo de pagar una tarifa o servicio para facilitar la transferencia de fondos. Una vez que se realiza este primer pago, el remitente continuará solicitando pequeños pagos a la víctima bajo el pretexto de complicaciones legales, tarifas adicionales u otros problemas que impidan trasladar los fondos (Smith y otros, 1999). El remitente continúa haciendo estas solicitudes hasta que la víctima no puede pagar más o se da cuenta de que puede tratarse de una estafa y no está dispuesta a realizar más pagos.

Algunos estafadores que trabajan por medio del correo electrónico también pueden intentar cometer actos relativamente inmediatos de fraude y robo de identidad sin que las víctimas se impliquen a largo plazo. Por ejemplo, algunos correos *spam* pueden solicitar a los destinatarios información personal que permitirá el robo y el fraude de identidad, como su nombre, dirección, patrón e información financiera (Holt y Graves, 2007). Los remitentes pueden sugerir que esta información es necesaria para garantizar las transacciones iniciales o demostrar su fiabilidad al remitente (Edelson, 2003; King y Thomas, 2009). No está claro cuántos son víctimas de esta manera algo indirecta de victimización, aunque estos correos ofrecen la oportunidad a los delincuentes de victimizar fácilmente a los destinatarios del correo electrónico.

Aunque esta es una de las formas más antiguas de fraude por correo electrónico, se desconoce cuántas personas reciben estos mensajes todos los días, y mucho menos cuántos responden en realidad a la solicitud. Los datos existentes sobre la victimización por fraude sugieren por lo general que solo una pequeña parte de la población que recibe correos de estafas de pago por adelantado responde a dichos correos (véase Internet Crime Complaint Center, 2019). Pero hay algunos que reportan enormes pérdidas económicas cada año. El Internet Crime Complaint Center (2019) señaló que estas víctimas perdieron más de 92.000.000 de dólares debido a diversas estafas de pago por adelantado. Ade-

más, parece que las víctimas perdieron un promedio de más de 5.000 dólares, lo que suele darse paulatinamente, a través de múltiples pagos a los estafadores. Por lo tanto, si bien estas estafas son bastante antiguas, de algún modo aún son eficaces y vale la pena enviarlas con la esperanza de obtener una respuesta por parte del destinatario de los correos electrónicos.

2. Estafas de extorsión

Otra estafa común basada en *spam* consiste en el envío de correos electrónicos en los que se hacen reclamos escandalosos en un intento de hacer que el destinatario pague una tarifa al remitente para evitar una experiencia negativa. Este tipo de estafa es similar a la extorsión en el mundo real, ya que el remitente intenta hacer creer al destinatario que existe una amenaza real para su seguridad o la de su familia. La amenaza debe ser lo suficientemente legítima como para que la víctima esté dispuesta a pagar una tarifa al remitente y este retire la amenaza. Una de las formas más comunes consiste en que el remitente dice ser un asesino a sueldo a quien se le ha pagado para asesinar al destinatario, como sucede con el siguiente mensaje:

> Hola:
>
> Lo siento mucho por ti, es una pena que sea de este modo como vaya a terminar tu vida si no cumples con lo que diré a continuación. Como puedes ver, no necesito presentarme porque no tengo ninguna relación contigo, mi deber al enviarte este correo es simplemente MATARTE y tengo que hacerlo porque ya me han pagado por ello.
>
> Alguien a quien llamas amigo te quiere muerto por todos los medios, y esta persona ha gastado mucho dinero para conseguirlo. Esta persona vino a nosotros y me dijo que te quería muerto y nos dio tu nombre, foto y otra información necesaria. La información que necesitamos saber de ti.
>
> Después envié a mis compañeros para que te encontraran e investigaran lo necesario y llevar así a cabo la operación, y lo hicieron, pero les dije que no te mataran, que me gustaría contactarte y ver si tu vida es importante para ti. Llamé a mi cliente y le pregunté tu dirección de correo electrónico, no le dije qué quería hacer con ella pero me la dio y ahora la estoy usando para contactarte. Mientras te escribo este correo, mis hombres te vigilan y me cuentan todo sobre ti.
>
> Así pues, ¿quieres VIVIR O MORIR? Todo el plan se ha tramado para matarte. Contáctame ahora si estás listo para pagar algunas tarifas y perdonarte la vida. 15.000 $ es todo lo que necesitas gastar en este proceso; primero pagarás 8.000 $ y luego te enviaré una cinta en la que grabé cada conversación que tuve con la persona que te quería muerto, y tan pronto como recibas la cinta pagarás el saldo restante de 7.000 $. Si no estás dispuesto a recibir mi ayuda, continuaré con mi trabajo directamente.
>
> ADVERTENCIA: NO PIENSES EN CONTACTAR CON LA POLICÍA O AVISAR A ALGUIEN PORQUE LO SABRÉ. RECUERDA, ALGUIEN QUE TE CONOCE MUY BIEN ¡TE QUIERE MUERTO! MATARÉ TAMBIÉN A TU FAMILIA EN CASO DE NOTAR ALGO RARO, COMO QUE HAS HABLADO CON LA POLICÍA, PUES TENGO UNA BUENA VIGILANCIA SOBRE TI EN ESTE MOMENTO.
>
> NO SALGAS UNA VEZ QUE SEAN LAS 7 DE LA TARDE. SI NO TENGO TIEMPO PARA VERTE Y DARTE LA CINTA CON LA CONVERSACIÓN DE TU ASESINO, PUEDES EMPRENDER CUALQUIER ACCIÓN LEGAL. BUENA SUERTE MIENTRAS ESPERO TU RESPUESTA.

También se han registrado esquemas de extorsión similares que consisten en alegar que el destinatario estaba viendo pornografía infantil o algún otro tipo de contenido ilícito en línea. Independientemente del tipo de estafa, el Internet Crime Complaint Center (2019) observó un aumento del 242 % de de-

nuncias de extorsión en 2018 en comparación con 2017. Además, las víctimas aseguraron haber sufrido pérdidas de más de 83.000.000 millones de dólares debido a los diversos métodos de extorsión que pueden darse.

3. Estafas de lotería

Otra forma común de fraude basado en *spam* consiste en enviar mensajes que afirman que el destinatario ha ganado algún tipo de sorteo o lotería internacional. Muchos de estos mensajes presentan afirmaciones de que su sorteo está asociado con grandes empresas o con loterías estatales legítimas. Por lo general, el remitente asegura que el individuo no necesitaba comprar un boleto para ganar, como se muestra en el siguiente mensaje:

¡FELICIDADES! SU CORREO ELECTRÓNICO GANÓ NUESTRA LOTERÍA

Estimado ganador,

Con mucho gusto le anunciamos el sorteo (# 103) de la LOTERÍA INTERNACIONAL DE CORREO ELECTRÓNICO ACCULOTTO realizada el 17 de febrero de 2007. Usted está entre las cien personas que fueron seleccionadas este año para reclamar la suma de 1.100.000 $ (un millón cien mil dólares). Su dirección de correo electrónico tiene el número de serie: 56475600545188. Por lo tanto, ha ganado una suma total de 1.100.000 $ (un millón cien mil dólares) en efectivo acreditado por KT U/9023118308/03.

TENGA EN CUENTA QUE ESTO NO ES UNA LOTERÍA DE CUPONES y que las direcciones de correo electrónico de todos los participantes para la versión en línea se seleccionaron aleatoriamente de sitios de World Wide Web, directorios de correo electrónico, libros de visitas en línea del servidor de índice de clave de correo electrónico, directorios de miembros y una gran cantidad de otras fuentes, donde ¡tanto los correos electrónicos registrados recientemente como los antiguos entran en el sistema de sorteo informático y se extraen de más de 100.000 sindicatos, asociaciones y entidades corporativas que están en línea! Esta promoción tiene lugar anualmente. Tenga en cuenta que su número ganador se encuentra en nuestra oficina de representación de folletos africanos en África. Por ello, cualquiera de nuestras oficinas de pago en África le entregará 1.100 $ (un millón cien mil dólares).

Nuestro agente comenzará inmediatamente el proceso para facilitar el envío de sus fondos tan pronto como se ponga en contacto con él. Por razones de seguridad, se recomienda que no comente a nadie que ha ganado hasta que se procese su solicitud y se le envíe su dinero de la manera que considere adecuada para cobrar su premio. Esto forma parte de nuestra medida de precaución para evitar dobles solicitudes y el abuso injustificado de este programa. Por favor, ¡tenga cuidado!

Para presentar su solicitud, comuníquese con nuestro agente fiduciario a través del siguiente correo electrónico con la siguiente información:

Dr. Allan Smith

1. Nombre

2. Ocupación

3. Edad

4. Sexo

5. Nacionalidad

6. Número de teléfono

7. Dirección de contacto o dirección postal

Dr. Allan Smith

¡ENHORABUENA!

Roben Gween (Sr.)

Por lo general, la víctima tiene que proporcionar un pago por adelantado al remitente para completar el proceso y garantizar que se realice la transferencia (Internet Crime Complaint Center, 2019). Aunque para muchos pueda resultar obvio que esta no es una notificación de lotería real, numerosas personas son víctimas de estas estafas año tras año. De hecho, las víctimas estadounidenses comunicaron pérdidas de más de sesenta millones de dólares relacionadas con fraudes de loterías y sorteos solo en 2018 (Internet Crime Complaint Center, 2019).

4. Estafas para trabajar en casa

Dado que varios servicios en línea están disponibles para facilitar el empleo, no sorprende que los estafadores hayan comenzado a usar estas plataformas para ofrecer ofertas de empleo fraudulentas. Una de las estafas más comunes implica el uso de *spam* para enviar anuncios de trabajos que permiten trabajar desde casa, y donde el candidato puede ganar bastante dinero por hora sin la necesidad de presentarse en una oficina física (véase Turner, Copes, Kerley y Warner, 2013). Muchos de estos trabajos constituyen tareas sencillas que pueden realizarse en distintos contextos, desde el procesamiento de datos hasta comprobar la productividad de los empleados en tienda y reenviar productos para las empresas (Turner y otros, 2013). Además, estos trabajos no requieren capacitación, títulos o certificaciones para que alguien consiga el puesto.

Para ser contratados, los destinatarios del correo electrónico deben comunicarse con el remitente y proporcionar una pequeña tarifa para acceder a sus materiales de capacitación, bases de datos o paquetes y productos (Turner y otros, 2013). En este punto, las víctimas suelen obtener una de estas dos respuestas. En primer lugar, puede que no reciban ningún material del estafador, que simplemente se embolsará su dinero. En segundo lugar, el estafador puede convencer a la víctima de que actúe como una mula de dinero, cobrando cheques fraudulentos escritos por el remitente o reenviando bienes y servicios que se obtuvieron a partir de transacciones fraudulentas (Turner y otros, 2013). A continuación se proporciona un ejemplo de trabajo como mula de dinero fraudulento:

> Mi nombre es Shirley Freeman y trabajo para una compañía llamada EuroCash. Encontré su currículum en carrerabuilder.com porque estamos buscando profesionales de confianza en todo Estados Unidos que estén interesados en una asociación potencialmente lucrativa con una empresa internacional.
>
> EuroCash es una compañía de inversión líder en Letonia y actualmente estamos expandiendo nuestras operaciones a Estados Unidos. Pero debido a varias restricciones bancarias y legales, no podemos abrir cuentas bancarias comerciales en todos los estados. Como tal, EuroCash está reclutando socios para realizar transacciones bancarias simples en nuestro nombre.
>
> El proceso es sencillo. En caso de estar interesado en convertirse en un socio estadounidense de EuroCash, firmaría un acuerdo que lo convertiría en un representante financiero oficial de nuestra empresa, capaz de aceptar pagos de facturas en nuestro nombre. En lugar de pedirles a nuestros clientes estadounidenses que realicen complejas transacciones de pagos internacionales (especialmente complejas para las empresas de Finlandia), les pedimos que trabajen con nuestros socios para enviar los pagos. Luego nos devolverían los pagos, una transacción simple para cualquiera. EuroCash paga a sus socios una comisión del 10 % en cada transacción. Además, nos encargaremos de cualquier responsabilidad tributaria incremental en la que incurra. Dependiendo del Estado en el que se encuentre y, por supuesto, de lo bueno que sea el negocio, sus comisiones mensuales podrían alcanzar los 14.000 $ al mes.
>
> Si está interesado en trabajar con nosotros, o si desea más información, puede contactarme directamente en mi dirección de correo electrónico personal: [dirección eli-

minada]. Necesitaré su nombre completo y dirección de correo para poder enviarle el contrato y otros documentos necesarios y así poder comenzar.

Espero saber pronto de usted.

Otra estafa similar basada en *spam* consiste en enviar mensajes que buscan empleados para puestos como compradores encubiertos. Estos fraudes se estructuran en torno a la noción de que se contratará a un individuo para ir a las tiendas, comprar productos y realizar revisiones de los bienes o servicios del minorista (Turner y otros, 2013). Los remitentes suelen tener éxito en atraer a empleados potenciales, pues se trata de un cargo común entre las empresas. Los delincuentes pueden jugar con la legitimidad de estos roles y manipular a los destinatarios para que crean que su empresa falsa está llevando a cabo un trabajo real (Turner y otros, 2013). Esto se ejemplifica en el siguiente correo electrónico:

«Compras encubiertas» («CE»)

¡Queremos ofrecerle un trabajo bien remunerado!

¡Trabaje como «Comprador encubierto» y gane 1.400 $ a la semana o 5.000 $ al mes!

Su trabajo será evaluar y comentar el servicio al cliente en puntos de venta como: supermercados, restaurantes, tiendas minoristas, casinos, centros comerciales, bancos, hoteles, etc.

La mayoría de las empresas solicitan nuestra ayuda cuando los clientes se quejan de sus servicios o cuando consideran que necesitan mejorar su servicio al cliente.

Las «compras encubiertas» permiten recopilar información sobre el servicio al cliente.

La «CE» es una herramienta fiable para reducir el gasto anual relativo al mantenimiento de las instalaciones y para reducir el riesgo corporativo; esta estrategia ayuda a los ejecutivos de una compañía a llevar a cabo sus propias tareas para mejorar sus servicios.

Cuando tenemos un contrato que ejecutar, dirigimos a nuestro agente a la empresa o al establecimiento con todos los fondos para realizar el trabajo.

Nuestro empleado actúa como un cliente habitual, por lo que el personal de servicio no sabe quién es, y evalúa así el servicio al cliente y la capacidad de tratar con clientes difíciles.

Nuestro empleado, basándose en su experiencia en tienda, escribe un informe detallado sobre: cuánto tiempo tarda en ser atendido, así como la cortesía y profesionalidad del servicio al cliente, e incluye, además, su propia opinión.

Requisitos:

1. Solo adultos

2. Ciudadano de Estados Unidos

3. Buenas habilidades de comunicación

4. Acceso completo a internet

5. Usuario de un ordenador

Por favor, cumplimente y reenvíe el siguiente formulario a: [correo electrónico eliminado]

- Nombre completo
- Edad

- Ocupación
- Número de teléfono
- Estado
- Dirección
- Código postal

Gracias.

Una vez que la posible víctima responde, se le pedirá que cobre un cheque o un giro postal para realizar una compra en una tienda. La víctima también recibe una parte del valor total del cheque como pago por sus servicios. Luego se les exige que realice una compra específica del producto, escriba una evaluación de la tienda y la experiencia de compra en general, para después enviar los productos a un lugar diferente en el que «opera» la empresa (Turner y otros, 2013). En realidad, la víctima está ayudando al blanqueo de dinero y al fraude al cobrar cheques sin fondos y comprar bienes con fondos ilegales adquiridos mediante tarjetas (véase módulo 3) u otros medios. Estas estafas suponen un gran riesgo para las víctimas, pues puede que crean estar realizando un trabajo legal, pero corren el riesgo de ser arrestadas debido a su participación en un esquema ilegal (Internet Crime Complaint Center, 2019). De hecho, hubo casi 15.000 quejas por estafas relacionadas con el empleo y comunicadas en el Internet Crimes Complaint Center en Estados Unidos durante 2018, con una pérdida promedio de 3.036 $ por víctima (Internet Crimes Complaint Center, 2019).

5. Estafas románticas

Las estafas descritas anteriormente atraen principalmente a sus destinatarios sobre la base de la ganancia económica. También hay varios tipos de estafa que se dirigen a víctimas prometiendo posibles relaciones románticas, lo que a menudo se denomina estafa romántica (Buchanan y Whitty, 2013; Cross, 2015). Estas estafas aprovechan el uso popular de los sitios de citas en línea y las redes sociales como un medio para conocer a otros, especialmente para las relaciones románticas. Los estafadores suelen crear perfiles falsos en estos sitios utilizando imágenes y contenido extraído de varios espacios virtuales, incluidos titulares de cuentas reales, para atraer a posibles víctimas (Buchanan y Whitty, 2013; Cross, 2015).

Uno de los esquemas de estafa romántica más comunes comienza cuando un estafador envía mensajes no solicitados a cuentas reales en webs de citas y perfiles de redes sociales para obtener respuesta. Los mensajes suelen ser cordiales, en los que se pide al destinatario que les cuente más sobre sí mismos porque están interesados en él por sus imágenes de perfil o descripción (Buchanan y Whitty, 2013; Cross, 2015). Si alguien responde al estafador, este tratará de iniciar una conversación profunda y crear vínculos emocionales reales al hablar sobre la familia, los amigos y la vida en general.

Durante las conversaciones, el estafador también indicará que es un ciudadano estadounidense o europeo que trabaja en el extranjero y que se siente solo. Su necesidad de conexión social es deliberada y tiene la intención de fortalecer un vínculo potencial con la víctima (Buchanan y Whitty, 2013; Cross, 2015). En el transcurso de las conversaciones, los estafadores también harán a la víctima una serie de preguntas personales y compartirán fotos en un intento de conocerlas personalmente. Si bien esto parece ser una manera de entenderse mejor, en realidad es un modo que tiene el estafador de mejorar su conocimiento sobre la víctima y poder manipularla mejor. Después de un período de tiempo, el estafador le dirá a la víctima que tiene sentimientos románticos por ella, incluso es probable que diga que la ama (Buchanan y Witty, 2013).

Una vez que el estafador siente que su relación con la víctima se ha consolidado, encontrará maneras de engañarla.

Ejemplo

Pueden insinuar que desean visitar a la víctima en persona pero que necesitan ayuda financiera para realizar el viaje (Whitty y Buchanan, 2012). Pueden pedir ayuda para pagar pequeñas tarifas inesperadas y garantizar que puedan salir del país o cubrir los costes de los hoteles (Whitty y Buchanan, 2012). Alternativamente, pueden afirmar que están teniendo problemas y necesitan ayuda, por ejemplo, que les han robado o asaltado y necesitan ayuda para cubrir sus gastos (Whitty y Buchanan, 2012). En algunos casos, también pueden pedirle a la víctima que cobre un cheque en su nombre y le transfiera fondos, o que acepte un envío y lo envíe a otro lugar (Cross, 2015).

Independientemente de cuál sea la estafa verdadera, el estafador mantendrá a la víctima involucrada durante el mayor tiempo posible.

Las estafas románticas constituyen un método recurrente y cada vez más común de fraude en línea en la última década, aunque los datos sugieren que las tasas de victimización pueden ser más altas de lo que se observa en las fuentes estadísticas debido a la vergüenza de las víctimas (Cross, 2015). Esto es particularmente cierto porque estos fraudes llevan a las víctimas a experimentar tanto daños financieros graves como secuelas emocionales derivadas de la traición en la estafa (Cross, 2015). Algunas personas incluso afirman tener pensamientos suicidas como resultado de su victimización y muestran angustia emocional después de darse cuenta de lo que ha sucedido (Cross y otros, 2015).

La magnitud del daño causado por los fraudes románticos es dramática, particularmente en Estados Unidos, ya que solo en 2018 se reportaron 18.493 víctimas de estafas románticas (Internet Crime Complaint Center, 2019). Estas víctimas afirmaron haber sufrido pérdidas masivas de dinero, por un total de más de 362.000.000 millones de dólares, una cifra mayor con respecto a años anteriores (Internet Crime Complaint Center, 2019). Las estafas románticas también son una de las estafas de más rápido crecimiento reportadas en 2018 por la Australian Competition and Consumer Commission (Comisión de Competencia y Consumidores de Australia), que halló que las víctimas perdieron un total de 60,5 millones de dólares australianos en 2018 (Chau, 2019). Se han observado pérdidas similares en el Reino Unido, donde las víctimas perdieron más de 39 millones de libras en 2016 (Cacciotto y Rees, 2017). Por lo tanto, las estafas románticas constituyen una forma particularmente terrible de fraude por internet (Buchanan y Whitty, 2013; Cross, 2015).

6. Fraudes de compraventa de acciones

Si bien los ejemplos anteriores se dirigen específicamente a las víctimas de fraude por diversos medios, existen otros fraudes de correo electrónico basados en *spam* que afectan principalmente a las empresas y perjudican a las personas en un segundo plano. Una de las estafas principales la constituye el llamado *pump and dump* (literalmente, 'endilgar y desechar') de correo no deseado que dirige especialmente al comercio de acciones a través de inversiones de bajo coste (Tillman e Indergaard, 2005). Gracias a internet y a las plataformas de intercambio en tiempo real, ahora la gente puede invertir directamente en acciones y gestionar la compra y venta de sus carteras. También puede recopilar información sobre posibles inversiones sin necesidad de comprometerse con corredores de bolsa y empresas de inversión (Tillman e Indergaard, 2005).

Como resultado, los estafadores han encontrado formas de explotar los nuevos sistemas de compra y venta de acciones para manipular directamente su valor en los mercados de intercambio abierto. Concretamente, identificarán pequeñas empresas con un precio muy bajo en el mercado actual y que están disponibles para su compra. Estas compañías no tienen por qué negociarse en bolsas de valores más grandes como la Bolsa de Nueva York (New York Stock Exchange, o NYSE), sino que están disponibles en cualquier tipo de bolsa siempre y cuando la compañía pueda identificarse en el mercado abierto. Luego compran participaciones de dichas acciones al precio más bajo posible para establecer su propia inversión semilla (*seed investment*).

Entonces, los estafadores crean mensajes de *spam* para anunciar el valor de las acciones e indican que se está produciendo un nuevo producto o forma de propiedad intelectual que tendrá un impacto transformador en el mercado (Tillman e Indergaard, 2005). Es posible que esta información no sea cierta, y aquellos estafadores meticulosos utilizarán deliberadamente compañías que pueden no ser investigadas o identificadas de manera inmediata a través de fuentes públicas. A su vez, su esperanza es empujar a los posibles inversores a comprar las acciones sobre la base de que cualquier información por correo electrónico es rigurosa (Tillman e Indergaard, 2005). El idioma de los mensajes varía, a continuación se muestra un ejemplo de estafa:

Noticias del mercado estadounidense.

¿Alguna vez te has sentado y preguntado cómo todos los demás consiguen ganancias significativas en el mercado mientras tu cartera está estancada?

Eso es porque se atreven a seguir su intuición y compran acciones en compañías como [nombre eliminado].

El miércoles les dijimos a nuestros miembros que las acciones aumentarían considerablemente y, en efecto, este incremento ha comenzado.

Solo la semana pasada hasta más del cincuenta por ciento; para las próximas semanas pronosticamos un aumento de más de 2 dólares.

Actúa ya, antes de que sea demasiado tarde.

Los estafadores observarán atentamente los patrones de compra en torno al *stock* y continuarán enviando mensajes para incrementar artificialmente su valor en el mercado general. A medida que el valor aumenta, o es «impulsado» por las compras derivadas de los mensajes de *spam*, la confianza individual en el *stock* puede aumentar de manera independiente. Esto puede acrecentar aún más el valor de las acciones. Una vez que los estafadores perciben que el valor de las acciones ha alcanzado su máximo potencial, venden o repelen la inversión. Este proceso puede darse unos días después de que se envíe el correo no deseado por primera vez para maximizar la tasa de rentabilidad (Hanke y Hauser, 2006). Esto beneficia a los estafadores por las ganancias obtenidas de su precio de compra, inicialmente bajo en relación con el valor de venta una vez inflado. Su liquidación comenzará a hacer que el precio baje, por lo que todos aquellos que compraron las acciones pierden sus fondos de inversión según el momento en que las vendan (Tillman e Indergaard, 2005).

En general, estas estafas son únicas, pues benefician directamente a los estafadores y perjudican indirectamente a otros inversores y al negocio que es blanco de la estafa. Por lo tanto, estos esquemas solo valen la pena para aquellos que están relacionados con la estafa y saben cuándo se está inflando el precio y cuándo ahuyentar o vender las existencias con el máximo rendimiento. Los esquemas de acciones de Penny también se observan de manera inconsistente año tras año, lo que dificulta saber cuándo se está ejecutando un esquema verdaderamente fraudulento (Divine, 2018; MarketWatch, 2014). Cuando este se ejecuta, los estudios sugieren que los *spammers* pueden obtener grandes ganancias, y una tasa de rentabilidad de hasta un 4 % de su inversión inicial (Frieder y Zittrain, 2007). Estas estafas también presentan un riesgo potencial de detección por parte de las fuerzas del orden público, ya que ha habido varios arrestos de estafadores de *pump and dump* en todo el mundo (US Attorney's Office, 2013).

7. Fraude del CEO

Otra forma de fraude que ha surgido en los últimos años combina múltiples aspectos de los otros esquemas de fraude basados en correo electrónico, e implica, además, piratería y *malware* en algunos casos. Esta estafa a menudo se denomina fraude del CEO o BEC (por el inglés *Business E-mail Compromise*), pues se dirige a una variedad de negocios e intenta que estos trasladen grandes sumas de dinero rápidamente bajo el pretexto de transacciones en apariencia legítimas (Mansfield-Devine, 2016).

A diferencia de los mensajes que se mencionan en este módulo, los remitentes no utilizan mensajes de *spam* para contactar con las posibles víctimas. Por el contrario, deben tomar medidas para elegir cuidadosamente a una víctima específica y crear un escenario convincente que aumente la probabilidad de obtener respuesta (Mansfield-Devine, 2016). El remitente también puede utilizar herramientas para falsificar, o hacer que una cuenta de correo electrónico no relacionada aparezca como una dirección de correo electrónico legítima. Esto es esencial para garantizar que la solicitud parezca legítima a primera vista y ser así más convincente.

Existen varias formas de BEC, desde relativamente simples hasta más complejas en función de las herramientas utilizadas para cometer el fraude. Algunos de los esquemas más directos consisten en que un remitente se ponga en contacto con una empresa con el pretexto de ser un proveedor de servicios legítimo con el que realiza negocios (Mansfield-Devine, 2016). El remitente indicará que se debe un pago, pero que ha de realizarse mediante una transferencia bancaria a una cuenta diferente a la que se usa normalmente. También pueden hacerse pasar por ejecutivos dentro de la organización que es blanco de la estafa para aumentar la legitimidad de la solicitud. Los remitentes, a menudo, intentarán atacar aquellas direcciones de correo electrónico del departamento de cuentas por cobrar/pagar para minimizar el número de destinatarios dentro de la organización y reducir la probabilidad de ser identificados como estafadores (Mansfield-Devine, 2016).

Las formas más sofisticadas de BEC suponen que un estafador ponga realmente en riesgo las cuentas de correo electrónico existentes dentro de la organización víctima. Si pueden obtener el nombre de usuario y la contraseña de un empleado para acceder a su sistema de correo electrónico, utilizarán la cuenta para enviar mensajes al departamento de contabilidad de la empresa o al de sus clientes en un intento de recibir pagos por los servicios prestados (Trend Micro, 2018). También se han registrado casos de estafadores que atacan cuentas de correo electrónico de ejecutivos de alto nivel y que luego envían mensajes a recursos humanos y departamentos de contabilidad para solicitar información personal de otros empleados y clientes, incluidos detalles fiscales y del

seguro de responsabilidad profesional (Trend Micro, 2019). Esta información se utiliza después para presentar declaraciones de impuestos fraudulentas y participar en diferentes formas de fraude y robo (Trend Micro, 2019).

Las diversas formas de BEC causan enormes daños económicos a sus víctimas, y las estimaciones sugieren que hubo más de 1.200.000 millones de dólares en pérdidas relacionadas con este fraude en Estados Unidos solo en 2018 (Internet Crime Complaint Center, 2019). Asimismo, el número de estafas reportadas ha aumentado de manera constante año tras año según múltiples fuentes de informes (Internet Crime Complaint Center, 2019; Trend Micro, 2019). Las estafas empleadas por los remitentes también están evolucionando con métodos más sofisticados en los últimos años (Internet Crime Complaint Center, 2019). Además, el rango de organizaciones específicas está cambiando, con más compañías inmobiliarias e hipotecarias como objetivo (Trend Micro, 2018). Como resultado, existe la necesidad de comprender mejor estas estafas para reducir la probabilidad de victimización en general.

8. Comprender las dinámicas del atacante y la víctima en los fraudes en línea

La variedad de posibles esquemas de fraude basados en correos *spam* hace plantearnos qué factores están asociados con la victimización. Dado que muchas víctimas no informan sobre sus experiencias, es difícil identificar los factores que influyen constantemente en el riesgo de responder a mensajes de correo electrónico fraudulentos (Cross, 2013). No está claro hasta qué punto la codicia podría ser un factor en los fraudes de pago por adelantado y en las estafas de lotería, ya que los remitentes destacan las enormes sumas de dinero que podrían ganar al responder a los mensajes (Holt y Graves, 2007; King y Thomas, 2009). Además, algunos autores afirman que podría influir la nacionalidad del destinatario en cierto grado. La escasez de estudios empíricos que cuantificarían este problema, con todo, supone un impedimento para saber hasta qué punto podría influir en la susceptibilidad de la víctima este tipo de fraudes.

La manera en que los estafadores estructuren el lenguaje de sus mensajes también puede desempeñar un papel importante para aumentar la probabilidad de respuestas. Los datos disponibles sugieren que el lenguaje en ciertas formas de fraudes basados en *spam* puede incitar a los destinatarios a responder.

Ejemplo

Muchos mensajes de fraude de pagos por adelantado pueden incluir un lenguaje basado en la fe y apelaciones al sentido de amabilidad o solidaridad del destinatario, lo que ayudaría a estimular una respuesta (Holt y Graves, 2007; Nhan y otros, 2009; Onyebadi y Park, 2012).

Algunos mensajes también presentan un lenguaje optimista que ayudarían a que la solicitud resulte verosímil a los destinatarios. Parte de los mensajes también usarían errores tipográficos o gramaticales deliberados para reforzar la noción de que el remitente es extranjero y no puede ser un hablante nativo de inglés (Holt y Graves, 2007; Nhan y otros, 2009).

Los remitentes también pueden usar un lenguaje que enfatice su fiabilidad, como el de un empleado del Gobierno o un abogado, para así validar sus afirmaciones (Holt y Graves, 2007; Nhan y otros, 2009). En algunos casos, los remitentes pueden usar este lenguaje para reforzar la impresión que tienen de que el destinatario es de fiar y así inflar su ego y aumentar la probabilidad de que este responda (Onyebadi y Park, 2012). En otros casos, los remitentes también utilizan enlaces a sitios web, que pueden ser legítimos o falsificados, para sugerir que la historia relatada en su mensaje es real (Nhan y otros, 2009; Turner y otros, 2013). Estos factores pueden ser suficientes para persuadir a una víctima potencial de que puede ignorar su preocupación inicial sobre la falsedad del mensaje (Cross, 2013).

Tampoco hay muchos datos disponibles sobre el patrón demográfico asociado con las víctimas de estafas basadas en *spam*. La mayoría de los estudios empíricos se centran en gran medida en el contenido de los mensajes, dada la dificultad inherente a la identificación de las víctimas de los esquemas de fraude de pagos por adelantado. Sin embargo, cada vez hay más análisis relativos a la victimización por estafa romántica, lo que sugiere que las víctimas son de varias edades, razas y orientaciones sexuales (Buchanan y Whitty, 2013; Cross y otros, 2015; Whitty y Buchanan, 2012). Algunos se han centrado más en las víctimas de edad avanzada por el impacto que supone para esta población, al cobrar los ahorros de jubilación con el fin de proporcionar fondos a los estafadores (Cross, 2015). De todos modos, los datos sugieren que las víctimas de estafas románticas se involucran emocionalmente en su relación con el estafador, y adoptan una visión idealizada del individuo que los lleva a ignorar cualquier atributo negativo que el estafador pueda mostrar (Buchanan y Whitty, 2013).

Resumen

Existen innumerables formas de fraudes basados en *spam*, que producen grandes pérdidas económicas cada año. El hecho de que estas estafas sigan siendo exitosas a pesar del paso de los años de uso y de sus miles de víctimas demuestra por qué este ciberdelito es preferible para algunos delincuentes. Además, estos fraudes probablemente evolucionarán con el tiempo en función de los patrones de uso y de la adopción de diversas tecnologías y plataformas de redes sociales en la sociedad.

Bibliografía

Buchanan, T.; Whitty, M. T. (2013). «The online dating romance scam: Causes and consequences of victimhood». *Psychology, Crime & Law* (núm. 20, págs. 261-283).

Cacciotto, M.; Rees, N. (23 de enero de 2017). «Online dating fraud victim numbers at record high» [en línea]. *BBC News*. <https://www.bbc.com/news/uk-38678089>

Chau, D. (28 de abril de 2019). «Australians lost nearly half a billion dollars to scammers in 2018, says ACCC» [en línea]. *ABC News*. <https://www.abc.net.au/news/2019-04-29/accc-report-scams-2018-surge489-million/11053946>

Cross, C. A. (2013). «Fraud and its PREY: Conceptualizing social engineering tactics and its impact on financial literacy outcomes». *Journal of Financial Services Marketing* (págs. 188-198).

Cross, C. (2015). «No laughing matter: Blaming the victim of online fraud». *International Review of Victimology* (núm. 21, págs. 187-204).

Cross, C.; Richards, K.; Smith, R. G. (2016). «The reporting experiences and support needs of victims of online fraud». *Trends & Issues in Crime and Criminal Justice* (núm. 518, págs. 1-14).

Divine, J. (marzo de 2018). «Penny Stocks: 5 Ways to Spot a Pump-and-Dump Scam» [en línea]. *US News and World Report*. <https://money.usnews.com/investing/stock-market-news/articles/2018-03-08/penny-stocks-5-ways-to-spot-a-pump-and-dump-scam>

Edelson, E. (2003). «The 419 scam: Information warfare on the spam front and a proposal for local filtering». *Computers and Security* (vol. 22, núm. 5, págs. 392-401).

Frieder, L.; Zittrain, J. (2007). «Spam works: Evidence from stock touts and corresponding market activity» [en línea]. *Berkman Center Research Publication* (año 2006, núm. 11) / *Harvard Public Law Working Paper* (núm. 135) / *Oxford Legal Studies Research Paper* (núm. 43). <http://ssrn.com/abstract=920553 or http://dx.doi.org/10.2139/ssrn.920553>

Furnell, S. (2002). *Cybercrime: Vandalizing the Information Society*. Boston: Addison-Wesley.

Hanke, M.; Hauser, F. (2006). «On the effects of stock spam emails». *Journal of Financial Markets* (núm. 11, págs. 57-83).

Holt, T. J.; Graves, D. C. (2007). «A qualitative analysis of advanced fee fraud schemes». *The International Journal of Cyber-Criminology* (núm. 1, págs. 137-154).

Internet Crime Complaint Center (2019). *2018 Internet Crime Report* [en línea]. <https://pdf.ic3.gov/2018_IC3Report.pdf>

King, A.; Thomas, J. (2009). «You Can't Cheat an Honest Man: Making ($$$s and) Sense of the Nigerian Email Scams». En: F. Schmalleger y M. Pittaro (eds.). *Crime of the Internet* (págs. 206-224). Saddle River, NJ: Prentice Hall.

Mansfield-Devine, S. (2016). «The imitation game: How business email compromise scams are robbing organizations». *Computer Fraud & Security* (núm. 11, págs. 5-10).

MarketWatch (2014). *Huge surge in spam emails pitching penny stocks* [en línea]. <http://www.marketwatch.com/story/penny-stock-schemes-not-just-for-the-wolf-of-wall-st-2014-05-27>

Maurer, D. W. (1981). *Language of the Underworld.* Louisville, KY: University of Kentucky Press.

Nhan, J.; Kinkade, P.; Burns, R. (2009). «Finding a pot of gold at the end of an Internet rainbow: Further examination of fraudulent email solicitation». *International Journal of Cyber Criminology* (vol. 3, núm. 1, pág. 452).

Onyebadi, U.; Park, J. (2012). «"I'm Sister Maria. Please help me": A lexical study of 4-1-9 international advance fee fraud email communications». *International Communication Gazette* (vol. 74, núm. 2, págs. 181-199).

Smith, R. G.; Holmes, M. N.; Kaufmann, P. (1999). «Trends and issues in crime and criminal justice» [en línea]. *Nigerian Advance Fee Fraud* (núm. 121). Australian Institute of Criminology. <http://bit.ly/2lRsLnk>

Tade, O. (28 de julio de 2016). «Meet the "yahoo boys"- Nigeria's undergraduate conmen» [en línea]. *US News and World report*. <https://www.usnews.com/news/best-countries/articles/2016-07-28/meet-the-yahoo-boys-nigerias-undergraduate-conmen>

Tillman, R. H.; Indergaard, M. L. (2005). *Pump and Dump: The Rancid Rules of the New Economy*. Newark: Rutgers University Press.

Trend Micro (19 de diciembre de 2018). «Year-End Review: Business Email Compromise in 2018» [en línea]. <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/year-end-review-business-email-compromise-in-2018>

Trend Micro (16 de abril de 2019). «New Business Email Compromise Scheme Reroutes Paycheck by Direct Deposit» [en línea]. *Trend Micro*. <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/new-business-email-compromise-scheme-reroutes-paycheck-by-direct-deposit>

Turner, S.; Copes, H.; Kerley, K. R.; Warner, G. (2013). «Understanding Online Work-At-Home Scams through an Analysis of Electronic Mail and Websites». En: T. J. Holt (ed.). *Crime On-line: Causes, Correlates, and Context* (2.ª ed., págs. 81-108). Raleigh, NC: Carolina Academic Press.

United States Attorney's Office (2013). *Nine individuals indicted in one of the largest international penny stock frauds and advance fee schemes in history* [en línea]. Federal Bureau of Investigation. <https://archives.fbi.gov/archives/newyork/press-releases/2013/nine-individuals-indicted-in-one-of-the-largest-international-penny-stock-frauds-and-advance-fee-schemes-in-history>

United States Department of State (1997). *Nigerian Advance Fee Fraud*. Bureau of International Narcotics and Law Enforcement Affairs.

Wall, D. (2004). «Digital realism and the governance of spam as cybercrime». *European Journal on Criminal Policy and Research* (núm. 10, págs. 309-335).

Whitty, M. T.; Buchanan, T. (2012). «The online romance scam: A serious cybercrime». *CyberPsychology, Behavior, and Social Networking* (vol. 15, núm. 3, págs. 181-183).