Mètodes de frau basats en el correu electrònic

PID_00269962

Thomas Holt

Temps mínim de dedicació recomanat: 3 hores

Universitat Oberta de Catalunya

Thomas Holt

L'encàrrec i la creació d'aquest recurs d'aprenentatge UOC han estat coordinats pel professor: Marc Balcells Magrans (2019)

Primera edició: setembre 2019

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

Índex

Introducció

En altres mòduls hem estudiat els delictes cibernètics que requereixen un cert grau d'interacció entre la víctima i el delinqüent, però això no és essencial perquè es dugui a terme qualsevol tipus de frau o dany econòmic. Un pirata informàtic pot accedir a dades confidencials o a un sistema informàtic sense necessitat que la víctima participi en una conversa o sense que hi hagi una interacció perllongada. No obstant això, hi ha diversos ciberdelictes econòmics que obliguen el delinqüent a buscar maneres de contactar amb les possibles víctimes i establir-hi una relació. Tots aquests delictes impliquen algun tipus de frau, com s'adverteix en el mòdul 1, per exemple, l'ús de l'engany o de la força per obtenir alguna cosa de valor. Algunes d'aquestes estafes requereixen que el delinqüent estableixi una relació amb la víctima, que ha de tenir un cert grau de confiança amb el delinqüent (Maurer, 1981). Com a resultat, la víctima tendirà a donar a l'estafador el que li demani, generalment diners o altres béns, que no seran retornats a la víctima ni li proporcionaran beneficis directes. Aquestes estafes se solen agrupar en el que s'anomena *abús de confiança* (en anglès, *confidence schemes*), i aquest tipus d'estafadors se solen denominar *scammers* (Maurer, 1981).

En espais virtuals, els delinqüents han adaptat a l'estafa en línia nombrosos mètodes de frau utilitzats en les trobades cara a cara. De fet, els mètodes de frau han evolucionat en funció de les diverses innovacions tecnològiques, des de diaris i telèfons fins a màquines de fax durant la dècada del 1980 (Departament d'Estat dels Estats Units, 1997). Als anys noranta, els estafadors van començar a cometre fraus per correu electrònic i mitjançant llocs web. Els estudiosos del cibercrim argumenten que aquests delictes es poden considerar ciberdelictes o delictes basats en l'ús de la informàtica (vegeu, per exemple, Furnell, 2002; Wall, 2004). Aquest terme és important perquè reconeix que cometre un delicte, encara que es pugui fer sense l'ajuda d'un ordinador, és més fàcil amb la tecnologia.

Com ja hem après al mòdul 1, les persones que participen en fraus cibernètics gaudeixen d'innombrables beneficis. Les xarxes socials i el correu electrònic permeten als estafadors distorsionar la seva identitat i ubicació reals, de manera que poden presentar-se amb el gènere, l'edat o l'ètnia que creguin adients per dur a terme el seu pla. A més, les plataformes de comunicacions en línia permeten als delinqüents accedir directament a milions de possibles víctimes a un preu generalment baix (Wall, 2004). Els sistemes de comunicacions en línia redueixen en gran part els costos que han d'invertir els delinqüents en les seves estafes, ja que el correu electrònic és gratuït per a tots els usuaris. Així mateix, el correu electrònic permet als remitents distribuir imatges, tex-

tos, enllaços HTML i diversos arxius adjunts. Els estafadors poden manipular correus electrònics perquè sembli que s'originen en qualsevol font i utilitzar imatges i textos per fer que els seus reclams siguin més versemblants.

Un altre benefici que els estafadors obtenen de la tecnologia és el fet de poder enviar correus electrònics, missatges de text o missatges directes no sol·licitats en massa a les seves possibles víctimes. Aquests missatges sovint es denominen *spam* i són una amenaça comuna que el públic en general ha d'afrontar diàriament (Wall, 2004). Per exemple, un proveïdor de seguretat va afirmar que el 2018 el 52% dels correus electrònics van ser correus *spam*, dels quals la majoria van enviar-se des de la Xina (Vergelis, Shcherbakova i Sidorina, 2018). Tenint en compte els centenars de milions de correus electrònics que s'envien cada dia, una gran part d'aquest contingut el constituirien nombrosos delictes de frau i intents de cometre altres ciberdelictes.

Aquest mòdul proporcionarà una descripció general de les diverses formes de frau en línia que es cometen per mitjà de missatges de correu electrònic no desitjat i de les xarxes socials. A més, s'abordaran la dinàmica dels mètodes de frau empleats i l'abast dels danys segons les víctimes. No en farem una llista exhaustiva, sinó que ens centrarem en les formes més investigades i impactants que afecten tant les persones com les empreses. El mòdul conclou amb una discussió sobre les característiques personals i demogràfiques associades a algunes formes de victimització per frau.

1. Els correus electrònics nigerians

Una de les formes més antigues i més comunes de frau en línia basat en *spam* és l'estafa de pagament per avançat (o *advance fee fraud scheme*). En aquests missatges un estafador sol·licita una petita quantitat de diners al destinatari, però realment espera poder rebre més endavant una quantitat de diners més elevada. A vegades aquests esquemes de frau es coneixen com a *estafes nigerianes*, ja que molts dels remitents d'aquests missatges afirmen viure en països estrangers, especialment a Nigèria i altres països africans o de l'Orient Mitjà (Smith, Holmes i Kaufmann, 1999). Col·loquialment, també es parla d'estafes 419, en referència al codi legal utilitzat per processar el frau a Nigèria (Edelson, 2003; Holt i Graves, 2007). Es desconeix quants dels remitents viuen realment a Nigèria, però les dades suggereixen que hi ha fraus i estafes que no es cometen en nacions africanes (Tade, 2016).

Com ja sabem, hi ha nombrosos tipus d'estafa de pagament per avançat; una de les més comunes es produeix quan el remitent afirma ser hereu de la reialesa o algú extremadament ric. El remitent necessita ajuda per moure els fons heretats dels seus comptes a una nació estrangera perquè s'enfronta a algun risc (Edelson, 2003; Holt i Graves, 2007; Nhan, Kinkade i Burns, 2009). En una variant d'aquest esquema el remitent afirma que ha estat greument ferit o que s'està morint i que busca ajuda per distribuir la seva fortuna en organitzacions benèfiques de tot el món (Holt i Graves, 2007; Nhan i altres, 2009). El destinatari rebrà aquests fons si proporciona informació al remitent i ajuda a distribuir-la, com s'indica en l'exemple següent:

Bon dia:

Aquest missatge és privat i molt important. El Senyor em demana que comparteixi la meva història amb tu. Si us plau, llegeix el correu per poder entendre la meva situació actual i ajudar-me. Em dic Isabella Carmel, i soc l'única supervivent d'una família de quatre. Vaig aconseguir sobreviure al desastre del tsunami que em va afectar la medul·la espinal i el timpà i que va causar la mort de tota la meva família, el meu marit (Denis Carmel) i els meus dos fills (Ugo i Tom), que eren de vacances a Sri Lanka.

Ara mateix visc a Kuala Lumpur, Malàisia. Vaig estar una setmana a l'hospital de la meva família, però la catàstrofe em va provocar una discapacitat i, tot i el tractament, he d'anar en cadira de rodes. Com que no puc rebre cap tipus de medicina, els metges diuen que em queden pocs mesos de vida. No he tingut una bona vida, ja que sempre m'he centrat en el negoci del meu pare, en pau descansi. El meu pare era una persona molt rica, però gens generosa. Ara em penedeixo de tot, perquè he après que guanyar diners o voler tenir-ne molts no ho és tot a la vida. La Bíblia diu: de què li serveix a un home guanyar-se el món sencer si hi perd l'ànima? Crec que si Déu em dona una segona oportunitat en aquest món, ara viuré la vida d'una manera diferent. He donat la majoria de les propietats del meu pare als menys privilegiats perquè vull que Déu sigui misericordiós amb mi i accepti la meva ànima. He decidit oferir la meva ajuda a les ONG per ajudar a socórrer i consolar els menys privilegiats de la societat. Vull que aquesta sigui una de les últimes bones obres que faci a la Terra. D'aquesta manera vull redimir el que el meu pare no va fer mai.

Per ara he anat repartint diners en organitzacions benèfiques, però la meva salut s'ha deteriorat tant que ja no tinc forces per fer-ho. Per això necessito la teva ajuda, per-

què faci aquesta donació en nom meu. Dels diners del meu difunt pare que estic disposada a donar als menys privilegiats en aquest moment en queda l'enorme suma de 10,6 milions de dòlars nord-americans, ocults en un enviament i dipositats a la (COMISSIÓ INTERNACIONAL DE CRÈDIT) que els custodia, amb la intenció d'invertir tots els diners en una profitosa indústria econòmica.

Necessito que m'ajudi a reclamar aquests fons i repartir-los per organitzacions benèfiques als menys privilegiats de la societat. Li agrairé que indiqui el seu interès pel desemborsament i que també inclogui els seus números de telèfon o fax, que enviaré a la (COMISSIÓ INTERNACIONAL DE CRÈDIT) perquè contactin amb vostè com a beneficiari designat. També li donaré el certificat de dipòsit i la carta d'autoritat perquè pugui reclamar l'enviament dels fons.

Si està disposat a ajudar-me amb aquest projecte, enviï'm un correu electrònic a [adreça eliminada] al més aviat possible. Resto a l'espera de la seva resposta. Gràcies un cop més per la seva amabilitat, que Déu el guiï i recompensi en totes les seves tasques mentre m'ajuda a fer realitat els meus últims somnis i desitjos.

Que Déu el beneeixi.

Sra. Isabel Carmel

En un altre esquema de frau relacionat amb aquest el remitent es fa passar per un banquer o advocat que vol tancar el compte d'un client mort fent servir el destinatari del correu electrònic com a parent més proper del difunt (Edelson, 2003). En aquest cas, el remitent afirma que donarà al destinatari part d'una gran suma de diners a canvi d'assistència financera i legal (Edelson, 2003; Holt i Graves, 2007). Heus aquí un excel·lent exemple:

Estimat amic:

Perdoni si abuso de la seva privacitat, ja que no ens coneixem, però no hi fa res. El més important és que l'acord al qual arribem sigui totalment transparent. Em dic Favor Adim Duke i soc comptable d'Inland Bank, SA. He trobat el seu correu tot buscant una persona fiable i de bona reputació que pogués dur a terme aquesta transacció comercial de manera confidencial. Un estranger, el difunt Engr Burke Sean, que va ser contractista del Govern Federal fins que va morir en el vol 801 de Korean Air que es va estavellar a Guam l'agost del 1997, tenia el seu compte bancari amb nosaltres a Inland Bank, SA i tenia un saldo de 20,5 milions de dòlars. Fa temps que el banc espera que algun familiar proper al difunt reclami aquests diners, ja que altrament seran lliurats a un fons fiduciari desacreditat per comprar armes i municions a un col·legi militar de Nigèria.

L'Inland Bank ha fet un enorme esforç per posar-se en contacte amb qualsevol dels familiars de Burke, però no ha servit de res. És possible que això es degui al fracàs percebut en no poder localitzar cap dels familiars propers del difunt. El familiar més proper de Burke Sean afirma que l'Administració, sota la influència del nostre president i els membres de les juntes directives, el senyor I. Yuguda, va fer un pacte perquè els fons fossin declarats com a no reclamables i que posteriorment fossin donats al fons fiduciari amb el qual es compren armes i municions i es promou la guerra a l'Àfrica i la fi del món en general, perquè ja sap vostè que aquesta guerra portarà en un futur la destrucció de la humanitat.

Amb l'objectiu d'evitar aquesta catàstrofe, li voldria demanar que es fes passar pel familiar més proper d'Engr Burke Sean amb l'objectiu que els fons de 20,5 milions de dòlars americans s'alliberin i s'ingressin al seu compte bancari, si vostè fos el seu familiar més proper. Aquest és un acord exclusiu entre vostè i jo, ja que tots els documents i proves que li permetrien obtenir aquest fons es gestionaran amb precaució. A més, li garanteixo que aquest acord és totalment segur i que no comporta cap risc. Només podrà rebre la seva part si accepta aquest acord. Si m'ajuda, després de ferli la transferència, també m'agradaria invertir els meus propis diners al seu país. Si considereu que aquesta proposta és vàlida, si us plau envieu-me un correu electrònic. Li ho agraeixo per endavant. Per a més informació, visiti aquest lloc web.

Atentament,

Sr. Favor Adim Duke.

Comptable a Inland Bank, SA, Sucursal de Lagos

En una variant similar i molt popular d'aquest tipus d'estafa el remitent es fa passar per un funcionari públic que ha sobrecarregat fons d'un contracte comercial o governamental (Edelson, 2003). Aquesta activitat il·legal pot cridar l'atenció del remitent, de manera que es busca una part externa que pugui ajudar-lo a moure els fons fora del país. Al seu torn, el remitent tindrà dret a una part d'aquests fons, com s'indica en aquest exemple:

De: Prince Joe Eboh

Data: dimecres 21 d'abril del 2004, 12:53

Assumpte: TRANSFERÈNCIA

Prince Joe Eboh

Estimat senyor/a:

Com està? Jo estic bé. Espero que quan llegeixi aquesta carta es trobi en molt bon estat de salut. Em dic Prince Joe Eboh i soc el president del Comitè d'adjudicació de contractes de la Comissió de Desenvolupament del Delta del Níger (CDDN), una subsidiària de la Corporació Nacional de Petroli de Nigèria (CNPN).

La Comissió de Desenvolupament del Delta del Níger (CDDN) va ser creada pel difunt cap d'Estat, el general Sani Abacha, que va morir el 18 de juny del 1998, per administrar l'excés d'ingressos provinents de les vendes de petroli i altres productes relacionats, com un augment del preu del petroli en el mercat nacional i ajudar el desenvolupament de les comunitats que viuen a les àrees productores de petroli del delta del Níger. L'ingrés anual estimat per al 1999 va ser de 45.000 milions de dòlars nord-americans, FMF A26 unitat 3Bp paràgraf *d* de l'auditor general de la República Federal de Nigèria, informe de novembre del 1999 sobre ingressos estimats.

El meu comitè és l'únic responsable de guardar i pagar els contractes en nom del Govern Federal de Nigèria. El meu comitè va atorgar contractes a contractistes estrangers per a la perforació i per qüestions mediambientals en les àrees productores de petroli del delta del Níger. Superem la suma del contracte en 25.000.000 dòlars nord-americans. Hem pagat als contractistes i retingut un saldo de 25.000.000 dòlars nord-americans. No obstant això, a causa de l'existència d'algunes lleis nacionals que prohibeixen als funcionaris públics a Nigèria obrir, operar i mantenir comptes a l'estranger, no tenim els coneixements necessaris per transferir aquest saldo de fons a un compte a l'estranger.

No obstant això, aquest saldo de 25.000.000 dòlars nord-americans ha estat assegurat en forma de crèdit/pagament a un contractista estranger, per tant, desitgem transferir-li al compte bancari aquests diners com a beneficiari del fons. També hem arribat a la conclusió que se li donarà el 20% de la suma total transferida com a soci estranger, mentre que el 5% es reservarà per a despeses incidentals en què incorreran ambdues parts en el curs d'aquesta transacció; el 75% restant es mantindrà per als membres del comitè.

Si es considera capaç d'ajudar-nos a fer aquesta transacció, ha de enviar-me immediatament els detalls de les seves dades bancàries o obrir un nou compte bancari on puguem transferir els diners de 25.000.000 dòlars nord-americans, que mantindrà en fideïcomís per a nosaltres fins que arribem al seu país per repartir la nostra part. La seva ocupació habitual no és important en aquesta transacció. Els detalls requerits inclouen el nom de la seva empresa, la direcció, els seus números de telèfon o fax personals, el seu nom complet i adreça i les seves dades bancàries íntegres perquè el fons transferit sigui enviat per Apex Bank.

Recordeu que s'espera que aquesta transacció s'actualitzi dins dels vint-i-un dies hàbils a partir del dia en què la informació que se li demana s'enviï al Ministeri Federal de Finances, moment en què s'aprovarà l'assignació de control de divises necessària per

enviar aquests diners al seu compte. Si us plau, tingui en comte que aquest assumpte és totalment secret. Posi's en contacte amb mi urgentment.

Gràcies per la seva cooperació.

Atentament,

Prince Joe Eboh

En totes aquestes variants d'estafes de pagament per avançat, hi ha unes sol·licituds recurrents que es fan a les possibles víctimes que reben el missatge. Primer, i fonamentalment, el destinatari es comunicarà amb el remitent per correu electrònic i hi entaularà una conversa (Holt i Graves, 2007). Després d'aquest intercanvi, l'estafador demanarà al destinatari que proporcioni un pagament que pugui servir com a dipòsit, donació o manera de pagar una tarifa o servei per facilitar la transferència de fons. Un cop fet aquest primer pagament, el remitent continuarà sol·licitant petits pagaments a la víctima sota el pretext de complicacions legals, tarifes addicionals o altres problemes que impedeixin traslladar els fons (Smith i altres, 1999). El remitent continuarà demanant diners fins que la víctima no pugui pagar més o s'adoni que es tracta d'una estafa i no estigui disposada a fer més pagaments.

Alguns estafadors que treballen per mitjà del correu electrònic també poden intentar cometre actes relativament immediats de frau i robatori d'identitat sense que les víctimes s'hi impliquin a llarg termini. Per exemple, alguns correus *spam* poden sol·licitar als destinataris informació personal que els permetrà dur a terme el robatori i el frau d'identitat, com el seu nom, adreça, patró i informació financera (Holt i Graves, 2007). Els remitents poden suggerir que aquesta informació és necessària per garantir les transaccions inicials o demostrar la fiabilitat al remitent (Edelson, 2003; King i Thomas, 2009). No està clar quantes víctimes hi ha d'aquesta manera indirecta de victimització, però aquests correus ofereixen l'oportunitat als delinqüents de victimitzar fàcilment els destinataris del correu electrònic.

Tot i que aquesta és una de les formes més antigues de frau per correu electrònic, es desconeix quantes persones reben aquests missatges cada dia, i molt menys quantes responen a la sol·licitud. Les dades existents sobre la victimització per frau suggereixen en general que només una petita part de la població que rep correus d'estafes de pagament per avançat respon a aquests correus (vegeu Internet Crime Complaint Center, 2019). Però hi ha gent que té enormes pèrdues econòmiques cada any per aquest motiu. L'Internet Crime Complaint Center (2019) va assenyalar que aquestes víctimes van perdre més de 92.000.000 de dòlars a causa de diverses estafes de pagament per avançat. A més, sembla que les víctimes van perdre una mitjana de més de 5.000 dòlars, que se solen donar de mica en mica en múltiples pagaments. Així doncs, si bé aquestes estafes són força antigues, també són eficaces, amb la qual cosa als estafadors els surt a compte enviar aquests correus amb l'esperança d'obtenir una resposta per part del destinatari.

2. Estafes d'extorsió

Una altra estafa comuna basada en *spam* consisteix en l'enviament de correus electrònics en què es fan reclams escandalosos en un intent de fer que el destinatari pagui una tarifa al remitent per evitar una experiència negativa. Aquest tipus d'estafa és similar a l'extorsió en el món real, ja que el remitent intenta fer creure al destinatari que hi ha una amenaça real per a la seva seguretat o la de la seva família. L'amenaça ha de ser prou legítima com perquè la víctima estigui disposada a pagar una tarifa al remitent i aquest retiri l'amenaça. En un dels correus més habituals el remitent afirma que és un assassí a sou que ha cobrat per assassinar el destinatari, com passa en el missatge següent:

> Hola:
>
> Em sap molt de greu, és una pena que la teva vida s'hagi d'acabar d'aquesta manera, si no fas el que el dic. Com pots veure, no necessito presentar-me perquè no tinc cap relació amb tu, el meu deure en enviar-te aquest correu és simplement matar-te i he de fer-ho perquè ja m'han pagat.
>
> Algú a qui anomenes amic et vol mort sigui com sigui i ha invertit molts diners per aconseguir-ho. Aquesta persona es va dirigir a la nostra organització i ens va dir que et volia mort, ens va donar el teu nom, una foto i tota la informació que necessitem saber de tu.
>
> Fa uns dies vaig ordenar als meus companys que t'investiguessin. Com que ja ho han fet, els he dit que no et matin encara, que m'agradaria parlar amb tu i veure si realment t'importa la teva vida. Vaig trucar al meu client i li vaig preguntar la teva adreça de correu electrònic, no li vaig dir què volia fer-ne, però me la va donar sense preguntar. Mentre t'escric aquest correu, els meus homes et vigilen i m'ho expliquen tot sobre tu.
>
> Així doncs, vols VIURE O MORIR? El pla per matar-te ja està preparat, però si pagues el que et dic et perdonaré la vida: només cal que paguis 15.000 $; primer pagaràs 8.000 $ i després t'enviaré una cinta en la qual vaig gravar les converses que vaig tenir amb la persona que et volia mort, i tan aviat com rebis la cinta pagaràs el saldo restant de 7.000 $. Si no estàs disposat a rebre la meva ajuda, continuaré amb la tasca que se m'ha demanat.
>
> ADVERTÈNCIA: NO CONTACTIS AMB LA POLICIA NI AVISIS NINGÚ, PERQUÈ HO SABRÉ. RECORDA, ALGÚ QUE ET CONEIX MOLT BÉ ET VOL MORT! TAMBÉ MATARÉ LA TEVA FAMÍLIA SI NOTO RES ESTRANY, COM, PER EXEMPLE, QUE HAS PARLAT AMB LA POLICIA. ET TINC MOLT BEN VIGILAT.
>
> NO SURTIS PASSADES LES 7 DE LA TARDA. SI NO TINC TEMPS PER VEURE'T I DONAR-TE LA CINTA AMB LA CONVERSA DEL TEU ASSASSÍ, POTS EMPRENDRE QUALSEVOL ACCIÓ LEGAL. BONA SORT MENTRE ESPERO LA TEVA RESPOSTA.

També s'han registrat esquemes d'extorsió similars que consisteixen a al·legar que el destinatari estava veient pornografia infantil o algun altre tipus de contingut il·lícit en línia. Independentment del tipus d'estafa, l'Internet Crime Complaint Center (2019) va observar un augment del 242% de denúncies

d'extorsió el 2018 en comparació amb el 2017. A més, les víctimes van assegurar haver patit pèrdues de més de 83.000.000 milions de dòlars a causa dels diversos mètodes d'extorsió.

3. Estafes de loteria

Una altra forma comuna de frau basat en *spam* consisteix a enviar missatges que afirmen que el destinatari ha guanyat algun tipus de sorteig o loteria internacional. Molts d'aquests missatges afirmen que el sorteig que han fet està associat amb grans empreses o amb loteries estatals legítimes. En general, el remitent assegura que l'individu no necessitava comprar un bitllet per guanyar, com es mostra en el missatge:

FELICITATS! EL SEU CORREU ELECTRÒNIC HA ESTAT PREMIAT

Benvolgut guanyador,

Amb molt de gust li anunciem que ha estat el guanyador del sorteig (# 103) de la LOTERIA INTERNACIONAL DE CORREU ELECTRÒNIC ACCULOTTO que va tenir lloc el 17 de febrer del 2007. És una de les cent persones seleccionades que s'endurà un total de 1.100.000 $. La seva adreça de correu electrònic correspon al número de sèrie: 56475600545188. Per tant, ha guanyat 1.100.000 $ en efectiu, acreditats per KT U/9023118308/03.

TINGUI EN COMPTE QUE NO ES TRACTA D'UNA LOTERIA DE CUPONS i que les adreces de correu electrònic de tots els participants de la versió en línia s'han seleccionat aleatòriament de llocs de World Wide Web, directoris de correu electrònic, llibres de visites en línia del servidor d'índex de clau de correu electrònic, directoris de membres i moltes altres fonts, on tant els correus electrònics registrats recentment com els antics entren en el sistema de sorteig informàtic i s'extreuen de més de 100.000 sindicats, associacions i entitats corporatives en línia. Aquesta promoció és anual. Recordi que el número guanyador es troba a la nostra oficina de representació de fullets africans a l'Àfrica. Així doncs, qualsevol de les nostres oficines de pagament a l'Àfrica li lliurarà 1.100 $.

El nostre agent començarà immediatament el procés per facilitar la transferència dels fons tan aviat com vostè s'hi posi en contacte. Per raons de seguretat, es recomana que no comenti a ningú que ha guanyat fins que es processi la sol·licitud i se li enviïn els diners de la manera que consideri adient. Prenem aquestes mesures de precaució per evitar dobles sol·licituds i l'abús injustificat d'aquest programa. Si us plau, vagi amb compte!

Per fer la sol·licitud, poseu-vos en contacte amb el nostre agent fiduciari a través del següent correu electrònic. Comuniqueu-nos aquesta informació:

Dr. Allan Smith

1. Nom
2. Ocupació
3. Edat
4. Sexe
5. Nacionalitat
6. Número de telèfon
7. Adreça de contacte o adreça postal

Dr. Allan Smith

ENHORABONA!

Roben Gween

En general, la víctima ha de proporcionar un pagament per avançat al remitent per completar el procés i garantir que es faci la transferència (Internet Crime Complaint Center, 2019). Tot i que per a molts pot resultar obvi que no es tracta d'una notificació de loteria real, moltes persones són víctimes d'aquestes estafes any rere any. De fet, només el 2018 les víctimes nord-americanes van comunicar pèrdues de més de seixanta milions de dòlars relacionades amb fraus de loteries i sortejos (Internet Crime Complaint Center, 2019).

4. Estafes per treballar des de casa

Atès que hi ha diversos serveis en línia que publiquen ofertes de feina, no sorprèn que els estafadors hagin començat a fer servir aquestes plataformes per oferir ofertes fraudulentes. Una de les estafes més comunes implica l'ús de l'*spam* per enviar ofertes de feina per treballar des de casa per un sou força elevat sense la necessitat d'anar a una oficina física (vegeu Turner, Copes, Kerley i Warner, 2013). Moltes d'aquestes feines constitueixen tasques senzilles que es poden fer en diferents contextos, des del processament de dades fins a comprovar la productivitat dels empleats en una botiga i reenviar productes per a les empreses (Turner i altres, 2013). A més, aquests treballs no requereixen cap formació específica, títols o certificacions.

Per aconseguir la feina, el destinatari del correu electrònic s'ha de posar en contacte amb el remitent i proporcionar-li una petita tarifa per accedir als seus materials, bases de dades o paquets i productes (Turner i altres, 2013). En aquest punt, les víctimes solen obtenir una d'aquestes dues respostes. En primer lloc, no reben cap material de l'estafador, que simplement s'embutxaca els diners. En segon lloc, l'estafador convenç la víctima perquè actuï com una mula monetària, cobrant xecs fraudulents escrits pel remitent o reenviant béns i serveis obtinguts de transaccions fraudulentes (Turner i altres, 2013). Vegem un exemple de mula monetària amb diners obtinguts de manera fraudulenta:

> Em dic Shirley Freeman i treballo per a una companyia anomenada EuroCash. Em poso en contacte amb vostè perquè estem buscant professionals de confiança als Estats Units que estiguin interessats a formar una associació potencialment lucrativa amb una empresa internacional. He trobat el seu currículum a carrerabuilder.com.
>
> EuroCash és una companyia d'inversió líder a Letònia i ara expandim les nostres operacions als Estats Units. A causa de diverses restriccions bancàries i legals, no podem obrir comptes bancaris comercials en qualsevol estat. EuroCash està reclutant socis per fer les transaccions bancàries més senzilles en nom nostre.
>
> El procés és ben senzill. Si està interessat a convertir-se en un soci nord-americà d'EuroCash, haurà de signar un acord que el convertirà en un representant financer oficial de la nostra empresa, capaç d'acceptar pagaments de factures en nom nostre. En lloc de demanar als nostres clients nord-americans que facin les complexes transaccions de pagaments internacionals (sobretot per a les empreses de Finlàndia), els demanem que treballin amb els nostres socis i els enviïn els pagaments. Un cop fet el pagament, se li tornaria l'import íntegrament, una transacció ben senzilla de dur a terme per qualsevol. EuroCash paga als seus socis una comissió del 10% en cada transacció. A més, ens fem responsables dels assumptes tributaris en què es pugui veure involucrat. Depenent de l'Estat en què es trobi i, per descomptat, de les característiques del negoci, les comissions mensuals podrien arribar als 14.000 $ al mes.
>
> Si està interessat a treballar amb nosaltres o desitja rebre més informació sobre aquesta oferta, escrigui'm: [direcció eliminada]. Necessitaré el seu nom complet i l'adreça de correu per poder enviar-li el contracte i la resta de documents necessaris.
>
> Resto a l'espera de la seva resposta.

Una altra estafa similar basada en *spam* consisteix a enviar missatges que busquen compradors encoberts. En aquests fraus es vol convèncer el destinatari perquè accepti una feina en què haurà d'anar de botiga en botiga a comprar productes i fer un control dels béns o serveis del minorista (Turner i altres, 2013). Els remitents solen tenir èxit a l'hora d'atreure empleats potencials, ja que es tracta d'un càrrec comú a les empreses. Els delinqüents poden jugar amb la legitimitat d'aquests rols i manipular els destinataris perquè creguin que l'empresa falsa busca un empleat real (Turner i altres, 2013). Això s'exemplifica en aquest correu electrònic:

Compres encobertes (CE)

Volem oferir-li una feina ben remunerada!

Si treballa per a nosaltres com a comprador encobert podrà guanyar entre 1.400 $ a la setmana o 5.000 $ al mes!

La seva feina consistirà a avaluar i comentar el servei al client en diferents punts de venda, com supermercats, restaurants, botigues de minoristes, casinos, centres comercials, bancs o hotels.

La majoria de les empreses ens demanen ajuda quan els clients es queixen dels seus serveis o quan consideren que necessiten millorar l'atenció al client, i les compres encobertes ens permeten recopilar informació sobre aquests aspectes.

La CE és una eina fiable per reduir la despesa anual de manteniment de les instal·lacions i el risc corporatiu; aquesta estratègia ajuda els executius d'una companyia a dur a terme les seves pròpies tasques per millorar els serveis que ofereixen.

Quan hem d'executar un contracte, fem que el nostre agent es dirigeixi a l'establiment amb tots els fons per dur a terme la feina.

El nostre empleat actua com un client habitual, de manera que el personal de servei no sap qui és, i avalua l'atenció al client i la capacitat de tractar amb clients difícils.

El nostre empleat, basant-se en la seva experiència en diferents botigues, escriu un informe detallat sobre els aspectes següents: el temps d'espera, la cortesia i la professionalitat de la persona que l'atén i la seva pròpia opinió.

Requisits:

1. Només adults
2. Ciutadà dels Estats Units
3. Bones habilitats de comunicació
4. Accés a internet
5. Usuari d'un ordinador

Si us plau, empleneu i reenvieu el formulari següent a: [correu electrònic eliminat]

- Nom complet
- Edat
- Ocupació
- Número de telèfon
- Estat
- Direcció
- Codi postal

Gràcies.

Quan la possible víctima respon, se li demana que cobri un xec o un gir postal per fer una compra en una botiga. La víctima també rep una part del valor total del xec com a pagament pels seus serveis. Després se li exigeix que faci

una compra específica del producte, que escrigui una avaluació de la botiga en què relati l'experiència de compra en general i que enviï els productes a un lloc diferent en el qual «opera» l'empresa (Turner i altres, 2013). En realitat, la víctima està ajudant a blanquejar diners i a cometre un frau en cobrar xecs sense fons i comprar béns amb fons il·legals adquirits mitjançant targetes (vegeu mòdul 3) o altres mitjans. Aquestes estafes suposen un gran risc per a les víctimes, ja que creuen que treballen per una empresa legal i corren el risc de ser arrestades per haver participat en un esquema il·legal (Internet Crime Complaint Center, 2019). De fet, als Estats Units el 2018 l'Internet Crimes Complaint Center va registrar gairebé 15.000 queixes per estafes relacionades amb l'ocupació, amb una pèrdua mitjana de 3.036 $ per víctima (Internet Crimes Complaint Center, 2019).

5. Estafes romàntiques

Les estafes descrites anteriorment atrauen els destinataris per obtenir, principalment, un benefici econòmic. No obstant això, en alguns casos els estafadors prometen a les víctimes que hi mantindran una relació romàntica, el que sovint s'anomena *estafa romàntica* (Buchanan i Whitty, 2013; Cross, 2015). Els estafadors han aprofitat el fet que s'hagin popularitzat els llocs de cites en línia i les xarxes socials com un mitjà per conèixer gent i mantenir-hi una relació romàntica. Els estafadors creen perfils falsos amb imatges i contingut extret de diversos espais virtuals, inclosos titulars de comptes reals, per atraure possibles víctimes (Buchanan i Whitty, 2013; Cross, 2015).

Un dels esquemes d'estafa romàntica més comuns comença quan un estafador envia missatges no sol·licitats a comptes reals en webs de cites i perfils de xarxes socials per obtenir una resposta. Els missatges solen ser cordials, en els quals es demana al destinatari que es presenti o se li pregunta per què li han agradat les fotos de perfil o la descripció (Buchanan i Whitty, 2013; Cross, 2015). Si algú respon l'estafador, aquest intenta començar una conversa profunda i crear vincles emocionals reals parlant sobre la família, els amics i la vida en general.

Durant les converses, l'estafador també indica que és un ciutadà nord-americà o europeu que treballa a l'estranger i que se sent sol. La seva necessitat de connexió social és deliberada i té la intenció d'enfortir un vincle potencial amb la víctima (Buchanan i Whitty, 2013; Cross, 2015). En el transcurs de les converses, l'estafador també fa a la víctima una sèrie de preguntes personals i li envia fotos amb la intenció d'apropar-s'hi i conèixer-se personalment. Tot i que pugui semblar que s'ha establert una connexió entre totes dues persones, en realitat l'estafador està recopilant tanta informació de la víctima com pot per manipular-la millor. Al cap d'un temps, l'estafador li comenta a la víctima que sent alguna cosa per ella i fins i tot pot arribar a dir-li que l'estima (Buchanan i Witty, 2013).

Quan l'estafador sent que la relació amb la víctima s'ha consolidat, busca altres maneres d'enganyar-la.

Exemple

A vegades l'estafador insinua que vol visitar la víctima en persona però que no té prou diners per fer el viatge (Whitty i Buchanan, 2012). També pot ser que l'estafador demani ajuda a la víctima per pagar alguna despesa inesperada per garantir que pugui sortir del país o cobrir les despeses dels hotels (Whitty i Buchanan, 2012). Així mateix, pot afirmar que està tenint problemes i que necessita ajuda; per exemple, que li han robat o que l'han assaltat i que necessita ajuda pagar-ho tot (Whitty i Buchanan, 2012). En alguns casos, també pot demanar a la víctima que cobri un xec en nom seu i li transfereixi els fons o que accepti un enviament i l'enviï a un altre lloc (Cross, 2015).

Independentment de quina sigui l'estafa, l'estafador mantindrà la víctima involucrada tant de temps com pugui.

Les estafes romàntiques constitueixen un mètode recurrent i cada vegada més comú de frau en línia en l'última dècada. Tot i això, les dades suggereixen que les taxes de victimització poden ser més altes del que s'observa en les fonts estadístiques però que les víctimes no ho comuniquen per vergonya (Cross, 2015). Això passa perquè aquests fraus porten les víctimes a experimentar tant danys financers greus com seqüeles emocionals derivades de la traïció (Cross, 2015). Algunes persones fins i tot afirmen tenir pensaments suïcides com a resultat de la seva victimització i mostren angoixa emocional després d'adonar-se del que ha succeït (Cross i altres, 2015).

La magnitud del dany causat pels fraus romàntics és dramàtica, sobre tot als Estats Units, ja que només el 2018 hi va haver 18.493 víctimes d'estafes romàntiques (Internet Crime Complaint Center, 2019). Aquestes víctimes van afirmar haver patit pèrdues massives de diners: més de 362.000.000 milions de dòlars, una xifra més elevada respecte a anys anteriors (Internet Crime Complaint Center, 2019). A Austràlia, per exemple, les estafes romàntiques van ser un dels tipus de fraus que va augmentar més ràpidament el 2018 (Comissió de Competència i Consumidors d'Austràlia), en què les víctimes van perdre un total de 60,5 milions de dòlars australians (Chau, 2019). S'han observat pèrdues similars al Regne Unit, on les víctimes van perdre més de 39 milions de lliures el 2016 (Cacciotto i Rees, 2017). Per tant, les estafes romàntiques constitueixen una forma particularment terrible de frau per internet (Buchanan i Whitty, 2013; Cross, 2015).

6. Fraus de compravenda d'accions

Fins ara hem vist exemples de fraus organitzats de diverses maneres per estafar un individu en concret. No obstant això, hi ha altres fraus de correu electrònic basats en *spam* que afecten principalment les empreses i que perjudiquen les persones en un segon pla. Una de les estafes principals la constitueix l'anomenat *pump and dump* (literalment, 'encolomar i rebutjar') de correu no desitjat que dirigeix especialment el comerç d'accions a través d'inversions de baix cost (Tillman i Indergaard, 2005). Gràcies a internet i a les plataformes d'intercanvi en temps real, ara la gent pot invertir directament en accions i gestionar la compra i venda de carteres. També pot recopilar informació sobre possibles inversions sense necessitat de comprometre's amb corredors de borsa i empreses d'inversió (Tillman i Indergaard, 2005).

Com a resultat, els estafadors han trobat diverses maneres d'explotar els nous sistemes de compra i venda d'accions per manipular-ne el valor en els mercats d'intercanvi obert. Concretament, identificaran petites empreses amb un preu molt baix en el mercat actual i que es poden comprar. Aquestes companyies no han de negociar-se en borses de valors gaire grans, com la Borsa de Nova York, sinó que estan disponibles en qualsevol tipus de borsa sempre que la companyia pugui identificar-se en el mercat obert. Després compren participacions d'aquestes accions al preu més baix possible per establir la seva pròpia inversió llavor (*seed investment*).

Llavors, els estafadors creen missatges de *spam* per anunciar el valor de les accions i indiquen que s'està produint un nou producte o forma de propietat intel·lectual que tindrà un impacte transformador en el mercat (Tillman i Indergaard, 2005). És possible que aquesta informació no sigui certa, però els estafadors, meticulosos, utilitzaran deliberadament companyies que no poden ser investigades o identificades de manera immediata a través de fonts públiques. Al seu torn, la seva esperança és empènyer els possibles inversors a comprar les accions sobre la base que qualsevol informació per correu electrònic és rigorosa (Tillman i Indergaard, 2005). A més, l'idioma dels missatges pot variar. Vegem un exemple d'aquest tipus d'estafa:

Notícies del mercat nord-americà.

T'has preguntat mai per què els altres obtenen grans beneficis en el mercat però tu tens la cartera estancada?

Això és perquè s'atreveixen a seguir la seva intuïció i compren accions en companyies com [nom eliminat].

Dimecres vam comunicar als nostres membres que les accions augmentarien considerablement i així ha estat. La setmana passada van augmentar més d'un 50% i està previst que durant les properes setmanes augmentin més de 2 dòlars.

Actua abans que sigui massa tard.

Els estafadors observaran atentament els patrons de compra al voltant de l'estoc i continuaran enviant missatges per incrementar-ne el valor artificialment en el mercat general. A mesura que el valor augmenti, o sigui «impulsat» per les compres derivades dels missatges de *spam*, la confiança individual en l'estoc augmentarà de manera independent. Això pot fer créixer encara més el valor de les accions. Quan els estafadors percebin que el valor de les accions ha arribat al seu màxim potencial, vendran o repel·liran la inversió. Aquest procés pot donar-se uns dies després que s'enviï el correu brossa per primera vegada per maximitzar la taxa de rendibilitat (Hanke i Hauser, 2006). Això beneficia els estafadors pels guanys obtinguts del preu de compra, inicialment baix en relació amb el valor de venda un cop inflat. La seva liquidació començarà a fer que el preu baixi, de manera que tothom qui hagi comprat les accions perdrà els seus fons d'inversió segons el moment en què les venguin (Tillman i Indergaard, 2005).

En general, aquestes estafes són úniques, ja que beneficien directament els estafadors i perjudiquen indirectament altres inversors i el negoci que és blanc de l'estafa. Per tant, aquests esquemes només beneficien els estafadors, que saben quan s'està inflant el preu i quan s'han de vendre les existències per obtenir-ne el màxim rendiment. Els esquemes d'accions de Penny també s'observen de manera inconsistent any rere any, la qual cosa dificulta saber quan s'està executant un esquema veritablement fraudulent (Divine, 2018; MarketWatch, 2014). Quan aquest s'executa, els estudis suggereixen que els *spammers* poden obtenir grans beneficis i una taxa de rendibilitat de fins a un 4% de la inversió inicial (Frieder i Zittrain, 2007). Aquestes estafes també presenten un risc potencial de detecció per part de les forces de l'ordre públic, ja que hi ha hagut diverses detencions d'estafadors de *pump and dump* arreu del món (US Attorney's Office, 2013).

7. Frau del CEO

Una altra forma de frau que ha sorgit en els últims anys combina múltiples aspectes dels altres esquemes de frau basats en correu electrònic i implica, en alguns casos, pirateria i programari maliciós. Aquesta estafa sovint s'anomena frau del CEO o BEC (en l'anglès *business e-mail compromise*), ja que es dirigeix a una gran varietat de negocis i intenta que aquests traslladin grans sumes de diners ràpidament sota el pretext de transaccions que, en aparença, són legítimes (Mansfield-Devine, 2016).

A diferència dels missatges que s'esmenten en aquest mòdul, els remitents no utilitzen missatges de *spam* per contactar amb les possibles víctimes. Per contra, han de prendre mesures per escollir amb cura una víctima i crear un escenari convincent que augmenti la probabilitat d'obtenir resposta (Mansfield-Devine, 2016). El remitent també pot utilitzar eines per falsificar o fer que un compte de correu electrònic no relacionat aparegui com una adreça de correu electrònic legítima. Això és essencial per garantir que la sol·licitud sembli legítima a primera vista i per semblar convincents.

Hi ha diferents tipus de BEC, des de relativament simples fins a més complexes, en funció de les eines utilitzades per cometre el frau. En alguns dels esquemes més directes un remitent es posa en contacte amb una empresa amb el pretext de ser un proveïdor de serveis legítim amb el qual vol fer negocis (Mansfield-Devine, 2016). El remitent indicarà que es deu un pagament, però que s'ha de fer mitjançant una transferència bancària a un compte diferent del que es fa servir normalment. També es poden fer passar per executius dins de l'organització que és el blanc de l'estafa per augmentar la legitimitat de la sol·licitud. Els remitents sovint intentaran atacar les adreces de correu electrònic del departament de comptes per cobrar/pagar amb l'objectiu de minimitzar el nombre de destinataris dins de l'organització i reduir la probabilitat de ser identificats com a estafadors (Mansfield-Devine, 2016).

Les formes més sofisticades de BEC comporten que un estafador posi en risc els comptes de correu electrònic existents dins de l'organització víctima. Si poden obtenir el nom d'usuari i la contrasenya d'un empleat per accedir al seu sistema de correu electrònic, utilitzaran el compte per enviar missatges al departament de Comptabilitat de l'empresa o al dels seus clients en un intent de rebre pagaments pels serveis prestats (Trend Micro, 2018). També s'han registrat casos d'estafadors que ataquen comptes de correu electrònic d'executius d'alt nivell i que després envien missatges a recursos humans i departaments de comptabilitat per sol·licitar informació personal d'altres empleats i clients, inclosos detalls fiscals i de l'assegurança de responsabilitat professional (Trend

Micro, 2019). Aquesta informació s'utilitza després per presentar declaracions d'impostos fraudulentes i participar en diferents tipus de frau i robatori (Trend Micro, 2019).

Les diverses formes de BEC causen enormes danys econòmics a les seves víctimes i s'estima que hi va haver més d'1.200.000 milions de dòlars en pèrdues relacionades amb aquest frau als Estats Units només el 2018 (Internet Crime Complaint Center, 2019). Així mateix, el nombre d'estafes ha augmentat de manera constant any rere any, segons múltiples fonts d'informes (Internet Crime Complaint Center, 2019; Trend Micro, 2019). Les estafes emprades pels remitents també estan evolucionant amb mètodes més sofisticats en els últims anys (Internet Crime Complaint Center, 2019). A més, el rang d'organitzacions específiques està canviant i hi ha més companyies immobiliàries i hipotecàries com a objectiu (Trend Micro, 2018). Com a resultat, hi ha la necessitat de comprendre millor aquestes estafes per reduir la probabilitat de victimització en general.

8. Comprendre les dinàmiques de l'atacant i la víctima en els fraus en línia

La varietat de possibles esquemes de frau basats en correus *spam* fa plantejar-nos quins factors estan associats amb la victimització. Atès que moltes de les víctimes no denuncien els fets, és difícil identificar els factors que influeixen constantment en el risc de respondre missatges de correu electrònic fraudulents (Cross, 2013). No està clar fins a quin punt la cobdícia podria ser un factor en els fraus de pagament per avançat i en les estafes de loteria, ja que els remitents destaquen les enormes sumes de diners que podrien guanyar en respondre els missatges (Holt i Graves, 2007; King i Thomas, 2009). A més, alguns autors afirmen que hi podria influir la nacionalitat del destinatari. L'escassetat d'estudis empírics que quantificarien aquest problema, amb tot, suposa un impediment per saber fins a quin punt podria influir en la susceptibilitat de la víctima aquest tipus de fraus.

La manera en què els estafadors estructuren el llenguatge dels seus missatges també pot tenir un paper important per augmentar la probabilitat de respostes. Les dades disponibles suggereixen que el llenguatge d'alguns fraus basats en *spam* pot incitar els destinataris a respondre.

Exemple

Molts missatges de frau de pagaments per avançat inclouen un llenguatge basat en la fe i apel·len al sentit d'amabilitat o solidaritat del destinatari, fet que ajudaria a estimular una resposta (Holt i Graves, 2007; Nhan i altres, 2009; Onyebadi i Park, 2012).

Alguns missatges també presenten un llenguatge optimista, el que fa que als destinataris els resulti versemblant. En alguns missatges s'afegeixen errors tipogràfics o gramaticals deliberadament per reforçar la noció que el remitent és estranger i no és un parlant nadiu (Holt i Graves, 2007; Nhan i altres, 2009).

Els remitents també poden fer servir un llenguatge que emfatitzi la seva fiabilitat, com el d'un empleat del Govern o un advocat, per aportar validesa a les seves afirmacions (Holt i Graves, 2007; Nhan i altres, 2009). En altres casos, fan servir aquest llenguatge per reforçar la impressió que el destinatari és de fiar, inflar el seu ego i augmentar la probabilitat que aquest respongui (Onyebadi i Park, 2012). En altres casos, els remitents també utilitzen enllaços a llocs web, que poden ser legítims o falsificats, per suggerir que la història relatada en el seu missatge és real (Nhan i altres, 2009; Turner i altres, 2013). Aquests factors poden ser suficients per persuadir una víctima potencial que pot ignorar la seva preocupació inicial sobre la falsedat del missatge (Cross, 2013).

Tampoc hi ha gaire dades disponibles sobre el patró demogràfic associat amb les víctimes d'estafes basades en *spam*. La majoria dels estudis empírics se centren en gran mesura en el contingut dels missatges, donada la dificultat inhe-

rent a la identificació de les víctimes dels esquemes de frau de pagar per avançat. No obstant això, cada vegada hi ha més anàlisis relatives a la victimització per estafa romàntica, fet que suggereix que les víctimes són de diverses edats, races i orientacions sexuals (Buchanan i Whitty, 2013; Cross i altres, 2015; Whitty i Buchanan, 2012). Alguns s'han centrat més en les víctimes d'edat avançada per l'impacte que suposa per a aquesta població, en cobrar els estalvis de jubilació amb la finalitat de proporcionar fons als estafadors (Cross, 2015). De totes maneres, les dades suggereixen que les víctimes d'estafes romàntiques s'involucren emocionalment en la seva relació amb l'estafador i adopten una visió idealitzada de l'individu que els porta a ignorar qualsevol atribut negatiu que l'estafador pugui mostrar (Buchanan i Whitty, 2013).

Resum

Hi ha innombrables tipus de fraus basats en *spam*, que produeixen grans pèrdues econòmiques cada any. El fet que aquestes estafes segueixin tenint èxit malgrat el pas dels anys i malgrat els milers de víctimes demostra per què els delinqüents escullen aquest ciberdelicte. A més, aquests fraus probablement evolucionaran amb el temps en funció dels patrons d'ús i de l'adopció de diverses tecnologies i plataformes de xarxes socials en la societat.

Bibliografia

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

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

Chau, D. (28 d'abril de 2019). «Australians lost nearly half a billion dollars to scammers in 2018, says ACCC» [en línia]. *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* (pàg. 188-198).

Cross, C. (2015). «No laughing matter: Blaming the victim of online fraud». *International Review of Victimology* (núm. 21, pàg. 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, pàg. 1-14).

Divine, J. (març de 2018). «Penny Stocks: 5 Ways to Spot a Pump-and-Dump Scam» [en línia]. *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, pàg. 392-401).

Frieder, L.; Zittrain, J. (2007). «Spam works: Evidence from stock touts and corresponding market activity» [en línia]. *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, pàg. 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, pàg. 137-154).

Internet Crime Complaint Center (2019). *2018 Internet Crime Report* [en línia]. <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* (pàg. 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, pàg. 5-10).

MarketWatch (2014). *Huge surge in spam emails pitching penny stocks* [en línia]. <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, pàg. 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, pàg. 181-199).

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

Tade, O. (28 de juliol de 2016). «Meet the "yahoo boys"- Nigeria's undergraduate conmen» [en línia]. *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 desembre de 2018). «Year-End Review: Business Email Compromise in 2018» [en línia]. <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/year-end-review-business-email-compromise-in-2018>

Trend Micro (16 d'abril de 2019). «New Business Email Compromise Scheme Reroutes Paycheck by Direct Deposit» [en línia]. *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., pàg. 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 línia]. Federal Bureau of Investigation. <https://bit.ly/2m4Itvh>

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, pàg. 309-335).

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