proofpoint.

LIBRO ELECTRÓNICO

Análisis de las estafas BEC

Marco del CISO moderno para identificar, clasificar y detener las estafas por correo electrónico

Introducción al marco taxonómico de Proofpoint para las estafas por correo electrónico

Las estafas Business Email Compromise (BEC), también conocidas como estafas o fraude por correo electrónico, son una de las amenazas de ciberseguridad más costosas y menos conocidas. Se trata sin duda de un método que ha evolucionado rápidamente y que no siempre capta tanta atención como otros ciberdelitos más notorios. Sin embargo, en costes económicos directos, las estafas BEC eclipsan fácilmente a otros tipos de fraude.

Solo en 2020, los ataques BEC costaron a organizaciones y particulares más de 1800 millones de dólares[1], cifra que supera en más de 100 millones la de 2019 y que representa el 44 % de las pérdidas totales por ciberdelincuencia.

Con la evolución de los ataques BEC, la nomenclatura del sector ha quedado obsoleta. Los términos utilizados para explicar las tácticas y técnicas BEC se han vuelto ambiguos, se confunden con otros conceptos y se utilizan de forma errónea. Sin un marco para describir los ataques BEC —y mucho menos para conceptualizarlos—, investigar y gestionar la amenaza es difícil, si no imposible.

Por eso hemos creado la taxonomía de Proofpoint para las estafas por correo electrónico. Este marco está diseñado para ayudar a los profesionales de la seguridad a identificar, clasificar y, en última instancia, bloquear mejor esta costosa amenaza.

Por qué es importante la terminología

El término "BEC" suele utilizarse de manera generalizada para describir toda una subclasificación de amenazas por correo electrónico. Se utiliza como término genérico para hacer referencia a un número indefinido de tácticas y técnicas vinculadas a los engaños por correo electrónico que utilizan **ingeniería social**, que tienen una motivación económica y que dependen de la respuesta.

Esto no es solo una larga descripción. Es un claro indicio de que el término "BEC" se ha convertido en una designación demasiado inclusiva. La amenaza ha superado a las palabras que la describen, lo que ha complicado los esfuerzos de los investigadores para estudiar los ataques BEC y los planes de las organizaciones para gestionarlos.

1 FBI. "Internet Crime Report 2020" (Informe sobre delitos en Internet de 2020), marzo de 2021.

Una nueva manera de considerar los ataques BEC y las estafas por correo electrónico

Para simplificar y destacar los aspectos principales de las estafas BEC (y del fraude por correo electrónico en general), hemos creado esta taxonomía. Nuestro objetivo es ayudar a las organizaciones a identificar, conocer y gestionar mejor las numerosas formas de estafas por correo electrónico a las que probablemente se enfrentarán.

Identidad

Nuestro enfoque de las estafas por correo electrónico está centrado en las personas, de ahí que nuestra taxonomía empiece por la *Identidad*. En este nivel, "Identidad" se refiere a la persona o la entidad que el ciberdelincuente (o sea, el atacante) finge ser. Hemos dividido Identidad en "empleado", "proveedor" y "desconocido", pero, si prefiere una clasificación aún más detallada, "empleado" puede subdividirse en "directivos" y "empleados generales".

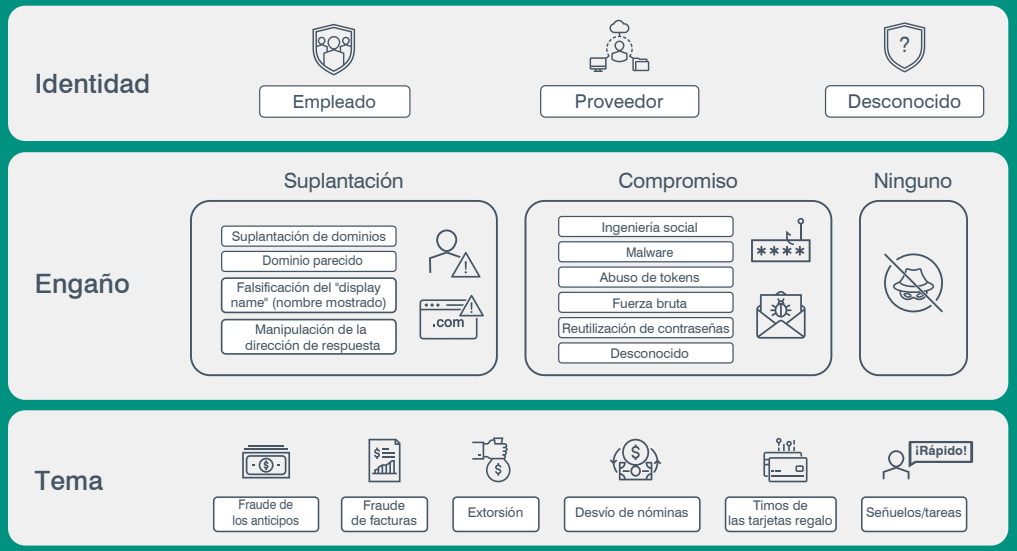


Figura 1: Taxonomía de Proofpoint para las estafas por correo electrónico

Engaño

El siguiente nivel es *Engaño*, que cubre las técnicas que los estafadores utilizan por correo electrónico. Este nivel incluye "suplantación", "compromiso" y "ninguno".

"Suplantación" se refiere a las técnicas en las que el ciberdelincuente manipula uno o varios encabezados del mensaje para enmascarar su origen. Aquí podemos encontrar los encabezados falsos, los "lookalike domains" (dominios parecidos) y otras técnicas empleadas para suplantar a otra persona.

"Compromiso" es cuando el ciberdelincuente consigue acceder a un buzón de correo electrónico legítimo para enviar mensajes. La cuenta puede pertenecer a un proveedor de confianza, un compañero de trabajo o una figura de autoridad. El destinatario no tiene motivos para cuestionar la legitimidad del mensaje y carece de las típicas pistas para detectar el ataque.

Cuando la técnica de engaño es "ninguno", el ciberdelincuente utiliza una táctica BEC que no se basa en la suplantación. El ciberdelincuente puede enviar mensajes desde proveedores gratuitos sin necesidad de falsificación.

Tema

El último nivel, *Tema*, contiene la información más útil y con la que el destinatario se puede identificar mejor. Es con diferencia la parte más importante de esta taxonomía. Los temas incluyen:

- Fraude de facturas
- Desvío de nóminas
- Extorsión
- Señuelos y tareas
- Timos de las tarjetas regalo
- Fraude de los anticipos

Estos temas cubren las categorías que nos han parecido más relevantes en el panorama de las amenazas BEC y más útiles para la mayor variedad de organizaciones. Si bien son lo suficientemente amplios para dar cabida a los matices —porque cada ataque es único—, los temas también son lo suficientemente específicos para ayudarle a identificar, clasificar y gestionar con rapidez toda la gama de amenazas BEC.

Tema 1: Fraude de facturas

En esencia, el fraude de facturas es un intento de engañar a alguien para que pague productos o servicios que no ha comprado o redirigir un pago legítimo a la cuenta del ciberdelincuente. Entre los temas de estafa por correo electrónico de nuestra taxonomía, el fraude de facturas puede ser indudablemente el más costoso. Las transacciones entre empresas tienden a ser numerosas y cuantiosas, lo que ofrece a los estafadores amplias oportunidades e incentivos para enriquecerse.

Las líneas de asunto de los mensajes de facturas fraudulentas suelen hacer alusión al pago. Las facturas falsas pueden también parecer genuinas al llevar el logotipo de la empresa, tener un formato profesional, etc. Además, el mensaje puede detallar cargos específicos y expresar urgencia, por ejemplo: "Esta factura venció hace 90 días y debe abonarse inmediatamente". A menudo, el ciberdelincuente utiliza un lenguaje amenazador por si el destinatario no actúa con rapidez.

En el nivel *Identidad*, una factura fraudulenta puede parecer enviada por cualquiera, ya sea un compañero de trabajo o alguien externo a la organización. Pero los fraudes que tienen más éxito aprovechan las relaciones con proveedores existentes. Los fraudes de proveedores, buenos ejemplos de fraudes de facturas, pueden terminar costando desde decenas de miles a varios millones de dólares.

Cómo funciona

En el nivel *Engaño*, los ataques de fraude de facturas de proveedores pueden perpetrarse a través de la suplantación o el compromiso.

Suplantación

La suplantación de proveedores consiste en que el ciberdelincuente utiliza técnicas ordinarias de suplantación de identidad para hacerse pasar por el proveedor. A menudo, estos mensajes fraudulentos se envían desde dominios de correo web gratuitos o cuentas comprometidas ajenas que controla el agresor.

Como muestra la Figura 2, la suplantación no siempre es simple. En algunos casos, primero el ciberdelincuente puede suplantar a la empresa elegida para obtener una factura real del proveedor y después utilizar esa factura para cambiar de papel y suplantar al proveedor. (Al tratarse de una factura auténtica de un proveedor real, al principio este ataque bidireccional puede parecer un caso de compromiso de cuentas).

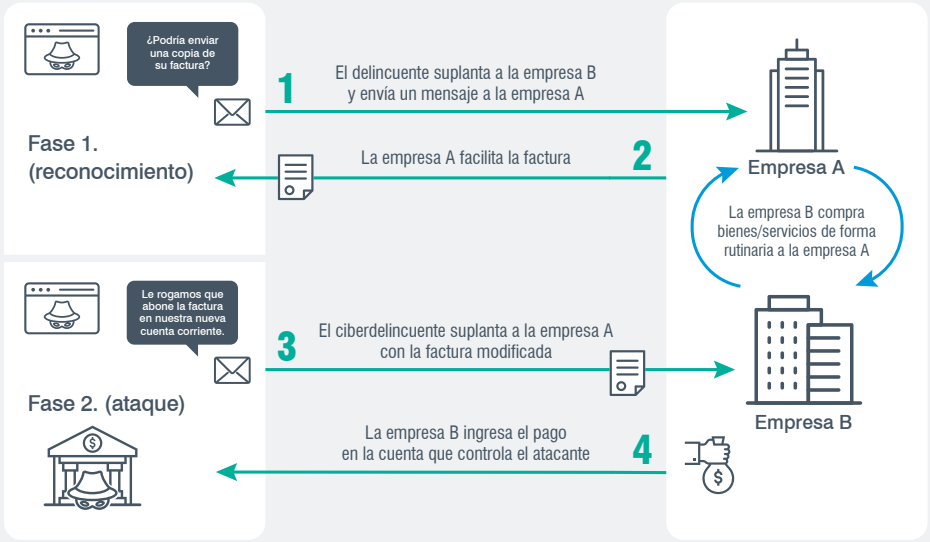


Figura 2: Anatomía de un ataque de fraude de facturas de proveedores en el que los agresores utilizan varias capas de suplantación

Compromiso

El compromiso de proveedores consiste en que un ciberdelincuente obtiene acceso no autorizado a la cuenta de correo electrónico de un proveedor de confianza y después utiliza esa cuenta para lanzar ataques BEC contra los clientes del proveedor. Normalmente, el ciberdelincuente obtiene acceso a la cuenta a través de una campaña anterior de phishing o de credenciales compradas.

En algunos casos, puede incluso "colarse" en un hilo de correo existente de una cuenta comprometida. (Esta técnica se denomina "secuestro de hilos"). Observando, imitando y respondiendo a conversaciones reales en el hilo de correo electrónico, pueden redactar mensajes verosímiles acompañados de documentación complementaria.

Es la táctica de suplantación de identidad por excelencia. Los mensajes de correo electrónico BEC se convierten en parte de una conversación activa. El destinatario no tiene motivos para sospechar que la persona con la que se está comunicando ha sido súbitamente sustituida por un impostor. No es de extrañar que estos mensajes figuren entre los ataques BEC más convincentes a los que los usuarios llegarán a enfrentarse jamás.

¿Por qué no ambas tácticas?

A menudo, como tácticas de engaño, los ciberdelincuentes utilizan tanto la suplantación como el compromiso. Algunos de estos ataques son ataques dirigidos, pero muchos son oportunistas, surgen a partir de la información que los agresores averiguan al atacar cadenas de suministro. (Nuestra taxonomía da cuenta de este matiz clasificando estos ataques como compromiso y también como suplantación en el nivel *Engaño*, como muestra la Figura 3).

Figura 3: Ejemplo de fraude de facturas de proveedores con tácticas de suplantación y de compromiso

Ejemplo del mundo real

En un ataque de fraude de facturas de proveedores que observamos recientemente, un ciberdelincuente intentó robar más de 100 000 dólares a una empresa haciéndose pasar por su proveedor de vino habitual.

El atacante respondió a un hilo de correo electrónico existente entre el cliente y el proveedor y le pidió al cliente que le enviara el pago directamente a una cuenta bancaria especificada. (Como muestra la Figura 4, el mensaje también especificaba que toda comunicación debía tener lugar por correo electrónico). Aunque el ciberdelincuente había secuestrado un hilo de correo electrónico real y parecía tener conocimiento interno del proveedor, el ataque utilizaba mensajes falsificados en lugar de una cuenta de correo comprometida.

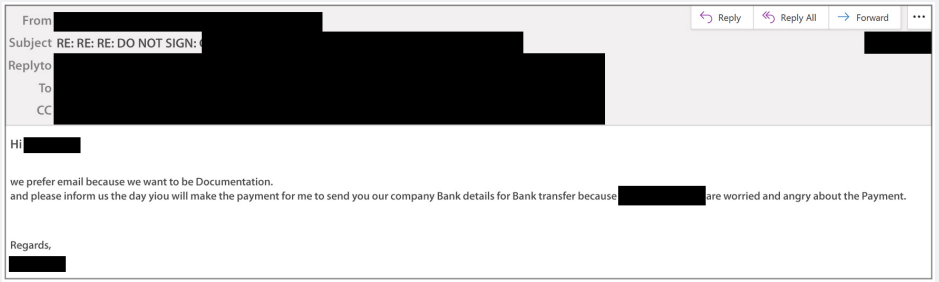


Figura 4: Intento inicial de fraude de facturas

Al no obtener la respuesta esperada, el ciberdelincuente envió un mensaje de seguimiento más urgente, como muestra la Figura 5. El mensaje incluía una factura detallada con el logotipo y el sello reales del proveedor para hacerla más convincente (véase la Figura 6 en la página siguiente).

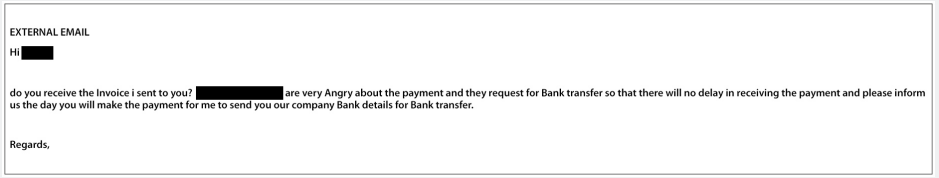
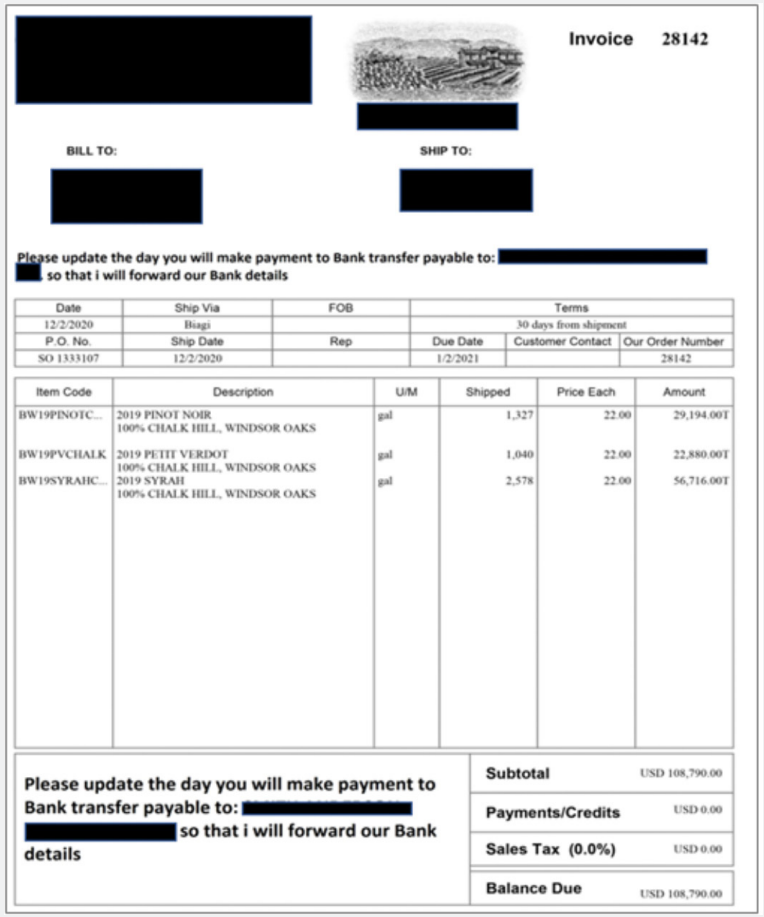


Figura 5: Segundo intento del mismo atacante



Invoice 28142

[redacted]

BILL TO: [redacted]

SHIP TO: [redacted]

Please update the day you will make payment to Bank transfer payable to: [redacted] so that i will forward our Bank details

Date	Ship Via	FOB	Terms		
12/2/2020	Biagi		30 days from shipment		
P.O. No.	Ship Date	Rep	Due Date	Customer Contact	Our Order Number
SO 1333107	12/2/2020		1/2/2021		28142

Item Code	Description	U/M	Shipped	Price Each	Amount
BW19PINOTC...	2019 PINOT NOIR 100% CHALK HILL, WINDSOR OAKS	gal	1,327	22.00	29,194.00T
BW19PVCHALK	2019 PETIT VERDOT 100% CHALK HILL, WINDSOR OAKS	gal	1,040	22.00	22,880.00T
BW19SYRAHC...	2019 SYRAH 100% CHALK HILL, WINDSOR OAKS	gal	2,578	22.00	56,716.00T

Please update the day you will make payment to Bank transfer payable to: [redacted] so that i will forward our Bank details

Subtotal	USD 108,790.00
Payments/Credits	USD 0.00
Sales Tax (0.0%)	USD 0.00
Balance Due	USD 108,790.00

Figura 6: Factura en PDF

Como los mensajes revelaban información que solo podía conocer el proveedor de vino real, sospechamos que este había sido comprometido antes del intento de estafa BEC. Es probable que el atacante utilizara detalles recopilados durante al ataque, además de falsificar el nombre mostrado ("display name") y manipular la dirección de respuesta para suplantar al proveedor. (La Figura 7 muestra cómo relacionamos el ataque con nuestro marco).

Figura 7: Ejemplo real de fraude de facturas de proveedores

Tema 2: Desvío de nóminas

El desvío de nóminas, también llamado redirección de pagos, es el ataque BEC más simple que hemos observado. Tanto si se dirige contra el departamento de servicios financieros y fiscales, de nóminas o recursos humanos (RR. HH.), el objetivo es sencillo: engañar al destinatario para desviar al ciberdelincuente la nómina que los empleados se han ganado con tanto esfuerzo o incluso una devolución de impuestos.

Detectamos una media de 2000 intentos de desvío de nóminas al día (véase la Figura 8) y consideramos estos ataques un riesgo medio para los empleados.

Según el FBI, la pérdida media debida a este tipo de ataques asciende a 7904 dólares por incidente denunciado[2]. El IRS incluía el desvío de nóminas en su lista de "doce malditos" entre los fraudes fiscales de 2020[3]. La agencia afirma que, en sus ataques de desvío de nóminas, los ciberdelincuentes utilizan documentos del IRS para convencer a los destinatarios de que las solicitudes de cambio de banco son legítimas.

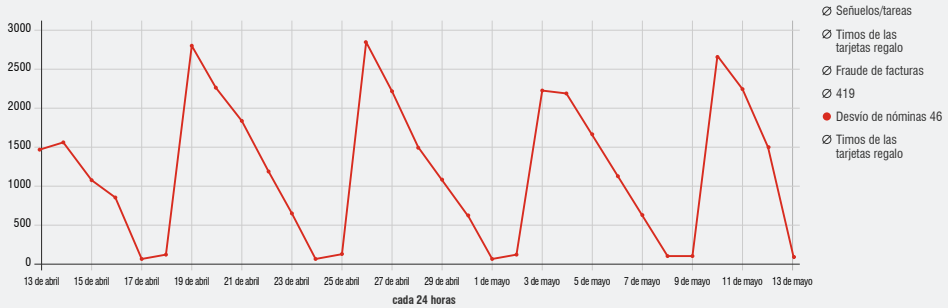


Figura 8: Intentos de desvío de nóminas (intentos totales en periodos de 24 horas, entre el 13 de abril y el 13 de mayo de 2021)

1. FBI. "2020 Internet Crime Report" (Informe sobre delitos en Internet de 2020), marzo de 2021.
2. IRS. "Dirty Dozen" (Los doce malditos), septiembre de 2021.

Cómo funciona

Los ataques de desvío de nóminas pueden utilizar el compromiso como técnica de *Engaño*, pero normalmente se basan en la suplantación. (Los ciberdelincuentes con acceso a una cuenta comprometida centran sus esfuerzos en formas más lucrativas de ataques BEC, como el fraude de facturas).

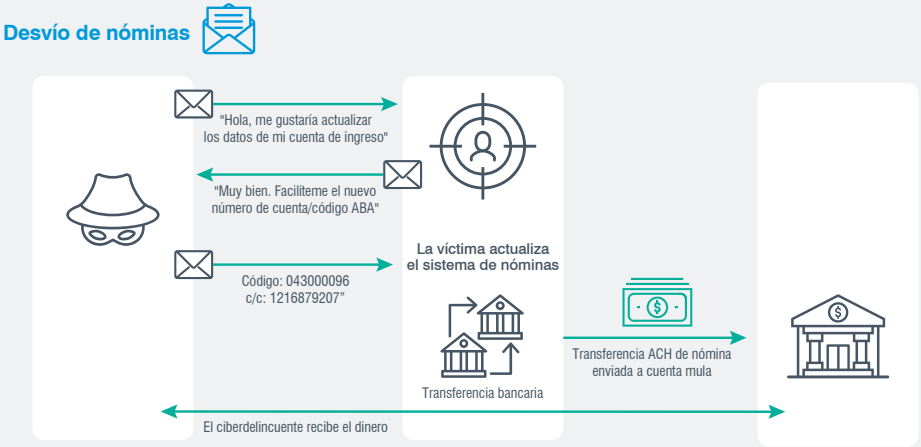


Figura 9: Anatomía de un ataque de desvío de nóminas con suplantación

La mayoría de los ataques de nóminas basados en la suplantación utilizan servicios de correo electrónico gratuitos, como Gmail. Normalmente, el ciberdelincuente falsifica el "display name" para que el mensaje parezca provenir de un empleado (véase la Figura 9 anterior).

Algunos ataques se dirigen contra la dirección de la empresa para poder hacerse con pagas de mayor envergadura. En estos intentos, los ciberdelincuentes pueden utilizar direcciones de correo electrónico con temas ejecutivos para conseguir más credibilidad e introducir cierta sensación de urgencia para los empleados deseosos de complacer al jefe. (Véase la Figura 10 en la página siguiente. Otros ejemplos recientes incluyen "ceo@companywebaxccs.com" y "ceo_task2@icloud.com").

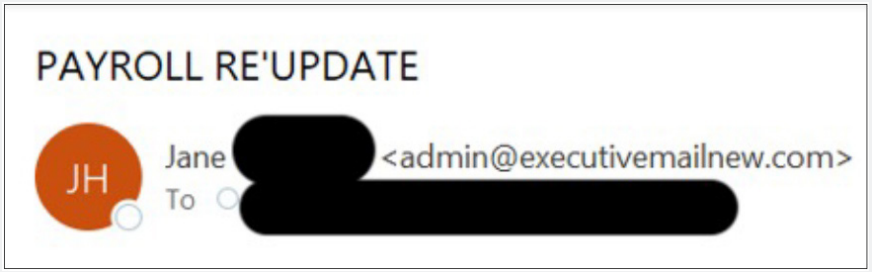


Figura 10: Dominio de correo electrónico diseñado para transmitir autoridad ejecutiva

La Figura 11 muestra cómo clasificaría nuestra taxonomía los dos ataques descritos.

Figura 11: Ataque de desvío de nóminas con "display name" falsificado en el mensaje de correo electrónico

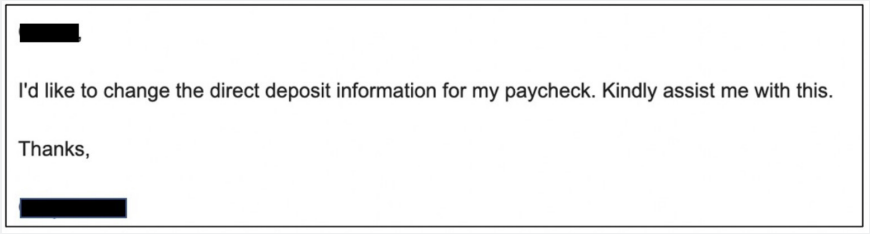
Ejemplos reales

Una seña de identidad de los ataques de desvío de nóminas es su simplicidad. En un ataque observado recientemente, el ciberdelincuente se hacía pasar por varios empleados que enviaban mensajes al departamento de nóminas de una gran empresa. Como muestra la Figura 12, todos estos mensajes utilizaban la misma estrategia y se diferenciaban únicamente en:

- A quién estaban dirigidos
- A quién suplantaban
- El idioma utilizado (inglés, alemán o español)

Figura 12: Muestra de mensajes suplantando a empleados en intentos de desvío de nóminas

Algunos intentos eran todavía más simples y descarados. En la Figura 13, el ciberdelincuente intenta suplantar al CEO de una empresa.


[redacted]

I'd like to change the direct deposit information for my paycheck. Kindly assist me with this.

Thanks,

[redacted]

Figura 13: Mensaje de desvío de nóminas suplantando a un CEO

A pesar de la poca tecnología que se emplea en estos ataques, pueden ser sorprendentemente eficaces. Esto se debe a que se aprovechan de un proceso empresarial normal. Los empleados de los departamentos de nóminas, servicios financieros, servicios fiscales y RR. HH. reciben a diario este tipo de solicitudes por correo electrónico, la mayoría de ellas legítimas.

Tema 3: Extorsión

La estafa por correo electrónico basada en el tema de la extorsión funciona igual que otras formas de extorsión. El atacante amenaza con destruir bienes, cometer actos de violencia o divulgar información confidencial, embarazosa o comprometedora a menos que el destinatario pague una suma (normalmente en criptomoneda) o entregue alguna otra cosa de valor. La extorsión tiene varios subtipos, concretamente:

- **Divulgación de datos.** El ciberdelincuente amenaza con divulgar información sensible, vergonzosa o comprometedora, datos o secretos comerciales del cliente, o bien pruebas de actividad delictiva (ya sean reales o no).
- **Denegación de servicio distribuido (DDoS).** El ciberdelincuente amenaza con desbordar las operaciones online del destinatario con tráfico falso para hacerlas inaccesibles a los usuarios legítimos.
- **Daño físico.** Este atacante amenaza con causar daño físico al destinatario o la organización. Las tácticas habituales incluyen amenazas de bomba, asesinatos por encargo y otras advertencias intimidatorias de violencia.
- **Extorsión sexual.** El ciberdelincuente amenaza con divulgar fotografías o vídeos sexuales de la víctima. La extorsión sexual o sextorsión es probablemente el más frecuente de estos subtipos de extorsión.

Cómo funciona

A diferencia de otros temas descritos en este libro electrónico, la estafa por correo electrónico con extorsión utiliza una sola táctica de engaño, si es que utiliza alguna: la suplantación. Cuando la estrategia es la suplantación, en general el agresor redacta el mensaje de forma que parezca que se ha enviado desde la cuenta de correo electrónico de la víctima.

El ciberdelincuente suele enviar a la víctima un mensaje asegurando haber accedido a su ordenador y haberle grabado viendo contenido para adultos. El mensaje incluye contenido sensible que aparenta proceder de la propia cuenta de correo electrónico del destinatario. El atacante advierte que, a menos que el destinatario pague, el contenido embarazoso se enviará a compañeros de trabajo y familiares.

La Figura 14 muestra cómo encaja este tipo de ataque en nuestro marco BEC.

Figura 14

A menos que los ciberdelincuentes intenten suplantar a alguien, normalmente utilizan proveedores de correo electrónico gratuitos y no se molestan en falsificar la dirección. Este tipo de escenario encajaría en el marco del modo siguiente (Figura 15).

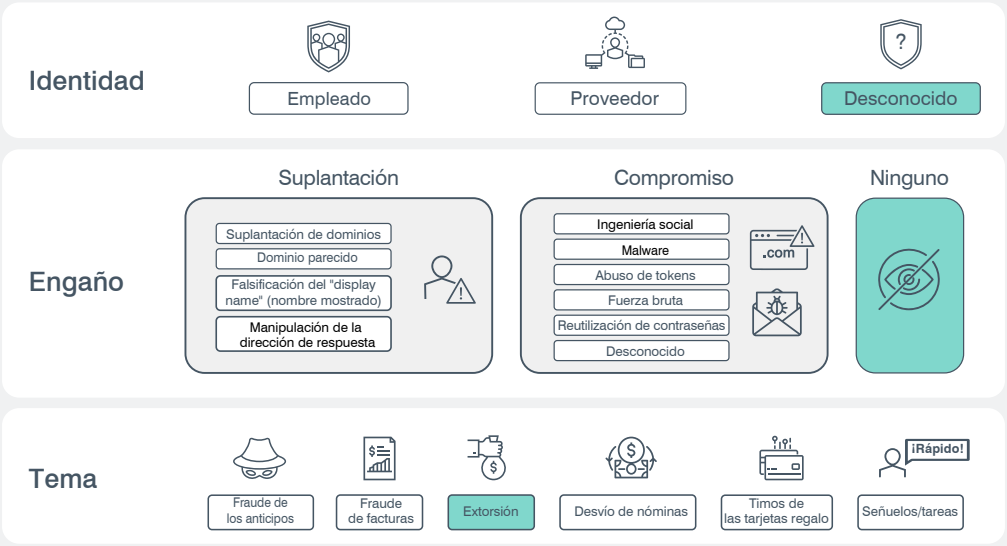
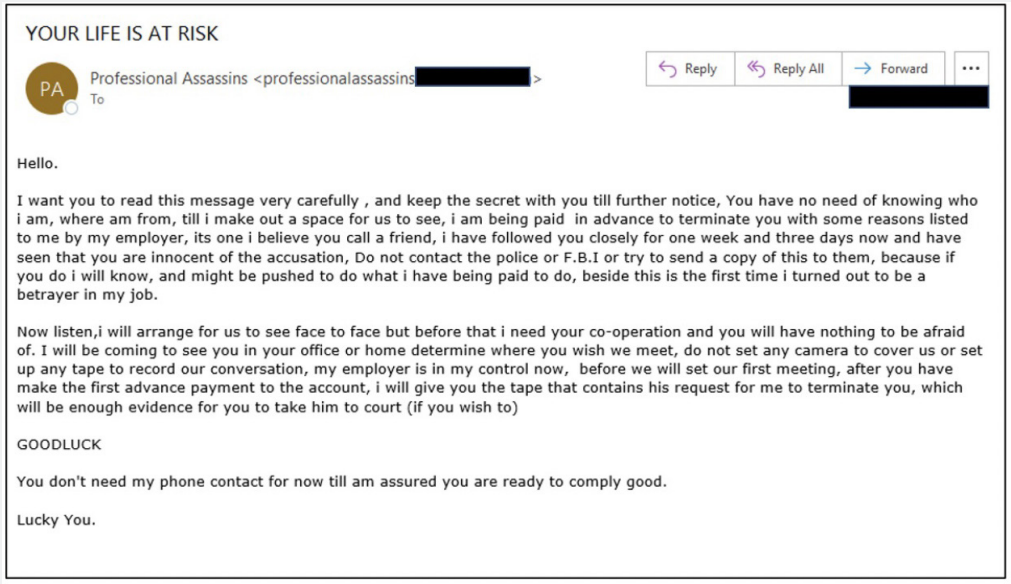


Figura 15: Algunos ataques de extorsión no utilizan tácticas de usurpación de identidad


YOUR LIFE IS AT RISK

PA Professional Assassins <professionalassassins[redacted]>
To

Reply | Reply All | Forward | ...

Hello.

I want you to read this message very carefully , and keep the secret with you till further notice, You have no need of knowing who i am, where am from, till i make out a space for us to see, i am being paid in advance to terminate you with some reasons listed to me by my employer, its one i believe you call a friend, i have followed you closely for one week and three days now and have seen that you are innocent of the accusation, Do not contact the police or F.B.I or try to send a copy of this to them, because if you do i will know, and might be pushed to do what i have being paid to do, beside this is the first time i turned out to be a betrayer in my job.

Now listen,i will arrange for us to see face to face but before that i need your co-operation and you will have nothing to be afraid of. I will be coming to see you in your office or home determine where you wish we meet, do not set any camera to cover us or set up any tape to record our conversation, my employer is in my control now, before we will set our first meeting, after you have make the first advance payment to the account, i will give you the tape that contains his request for me to terminate you, which will be enough evidence for you to take him to court (if you wish to)

GOODLUCK

You don't need my phone contact for now till am assured you are ready to comply good.

Lucky You.

Figura 16: Intento de extorsión prometiendo cancelar un asesinato por encargo si el destinatario paga al remitente

Ejemplos reales

La extorsión sexual es con diferencia la forma de extorsión observada más a menudo. Los mensajes tienden a ser largos y detallados, pero el objetivo es simple y pragmático: convencer a las víctimas de que tienen las de perder y deben satisfacer las exigencias del ciberdelincuente.

Las amenazas de daño físico son menos habituales, aunque lógicamente alarmantes para las personas que las reciben. Como hemos visto en la Figura 16, estas tácticas de mano dura intentan atemorizar a las víctimas para que piensen que su vida corre grave peligro a menos que paguen.

Sus principales atributos incluyen sensación de urgencia, plazos breves para pagar y serias advertencias de no avisar a la policía.

Tema 4: Señuelos y tareas

Dada su naturaleza básica, los mensajes de señuelos y tareas pasan fácilmente desapercibidos. Empiezan por solicitar un favor sencillo y casi rutinario. Aunque algunos ataques comienzan por una petición concreta, muchos solo contienen vaguedades y enredan a la víctima a lo largo de múltiples mensajes. En estos casos, los mensajes iniciales pueden hacer una petición general del tipo:

- "¿Estás disponible?"
- "Necesito un pequeño favor"
- "¿Tendrías un momento?"
- "Estás ahí? Necesito que me compres tarjetas regalo"

Con frecuencia, los mensajes de señuelos y tareas son una puerta, el primer paso de un ataque de varias etapas que contiene otros temas de estafa por correo electrónico. Un mensaje de señuelos/tareas capta la atención del destinatario para, con el tiempo, ir revelando el objetivo último del ciberdelincuente, como el desvío de pagos o el fraude de facturas.

Estos ataques de varias categorías pueden dificultar su clasificación. A menudo, la diferencia entre los mensajes de señuelos/tareas y otros de nuestra taxonomía es si vemos lo que hará el atacante a continuación. Si solo vemos un único mensaje de tipo señuelos/tareas, lo clasificamos como tal. Pero si los siguientes mensajes revelan un objetivo subyacente al mensaje inicial, lo clasificamos como señuelos y tareas y también bajo otro tema.

Cómo funciona

Los mensajes de señuelos y tareas solo utilizan una forma de *Engaño* de nuestra taxonomía: la suplantación. Los ciberdelincuentes tienden a hacerse pasar por alguien que la víctima elegida conoce o en quien confía:

- Figuras de autoridad, tanto personales como profesionales
- Amigos íntimos
- Familiares

La usurpación de la identidad de alguien conocido desarma todas las sospechas que el destinatario pueda tener sobre una solicitud inesperada o inusual y casi le obliga a responder.

Con una mera respuesta, el ciberdelincuente logra su objetivo primordial: identificar una cuenta de correo electrónico activa y una audiencia potencialmente receptiva.

La mayoría de los mensajes de señuelos/tareas utilizan la falsificación del "display name" para engañar al destinatario, como muestra la Figura 17. Algunos recurren a otras tácticas de suplantación, como la suplantación de dominios o la falsificación de las direcciones de respuesta. Tras recibir una respuesta, el ciberdelincuente puede cambiar las tácticas de engaño si con ello puede dar mayor credibilidad al ataque.

Figura 17

Ejemplos reales

Muchos de los mensajes fraudulentos de señuelos/tareas que vemos empiezan por un breve mensaje que calibra en qué medida es receptivo el destinatario. Como muestra la Figura 18, quizá estos primeros mensajes no intenten crear sensación de urgencia.

Figura 18: Mensaje de correo electrónico inicial con tema de señuelos/tareas

La estafa por correo electrónico con señuelos/tareas es prolífica y suma más de la mitad de las amenazas de estafa por correo electrónico que observamos en 2021. (Impedimos a diario la entrega de unos 30 000 mensajes de este tipo).

A primera vista, estos mensajes parecen benignos. Pero si el destinatario se deja engañar una vez, puede dar lugar a formas más graves de estafa por correo electrónico con resultados potencialmente costosos: tarjetas regalo, fraude de facturas, fraude de desvío de nóminas y similares.

Tema 5: Timos de las tarjetas regalo

En los ataques de las tarjetas regalo, los ciberdelincuentes se lucran con las tarjetas regalo de un minorista. El mensaje induce al destinatario a comprar tarjetas y a enviar el número de las tarjetas y los números PIN al atacante, que después las canjea o revende.

Estos ataques funcionan porque las tarjetas regalo son una práctica habitual en las empresas para recompensar a empleados y socios. Para el destinatario, la solicitud parece rutinaria. Si el mensaje suena urgente y ofrece una explicación aparentemente razonable, el destinatario puede actuar sin darle más vueltas.

Cómo funciona

En el nivel *Engaño*, los ciberdelincuentes normalmente suplantan a un directivo o a una persona con un cargo de autoridad para dar a la solicitud visos de legitimidad. Como ocurre con otras formas de estafa por correo electrónico, las probabilidades de que el destinatario caiga en la trampa aumentan si el remitente se hace pasar por alguien conocido, incluso amigos íntimos y familiares.

La mayoría de las estafas con tarjetas regalo falsifican el "display name" para engañar al destinatario (véase la Figura 19). A veces, los ciberdelincuentes utilizan otras tácticas de suplantación, como la suplantación de dominios o la alteración de la dirección de respuesta.

Figura 19: Taxonomía de los timos con tarjetas regalo

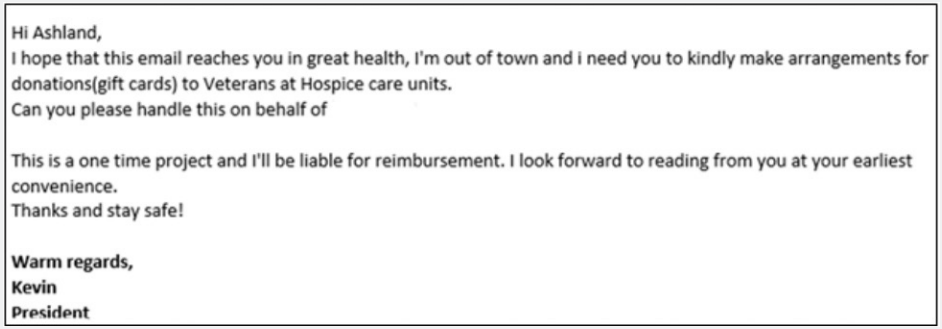
Ejemplos reales

La mayoría de los mensajes de correo electrónico con tarjetas regalo utilizan todo tipo de señuelos para que el destinatario considere válida la solicitud (véanse las figuras 20, 21 y 22 en la página siguiente). Los ciberdelincuentes pueden utilizar cualquier cosa, desde sucesos de actualidad, como la pandemia, hasta festivos nacionales. Sea cual sea el cebo, el objetivo es proporcionar una razón verosímil para la solicitud y suscitar solidaridad para aumentar las probabilidades de éxito.

Solidaridad con el timador

La Figura 20 y la Figura 21 son claros ejemplos de ciberdelincuentes que intentan tocar la fibra sensible del destinatario.

En la Figura 20, el remitente explica que la solicitud se debe a un problema de un centro de veteranos del ejército, ni más ni menos. En la Figura 21, el remitente asegura estar fuera de la ciudad y aislado, probablemente en alusión a la pandemia, y por lo tanto no puede comprar un regalo para el inminente cumpleaños de una sobrina

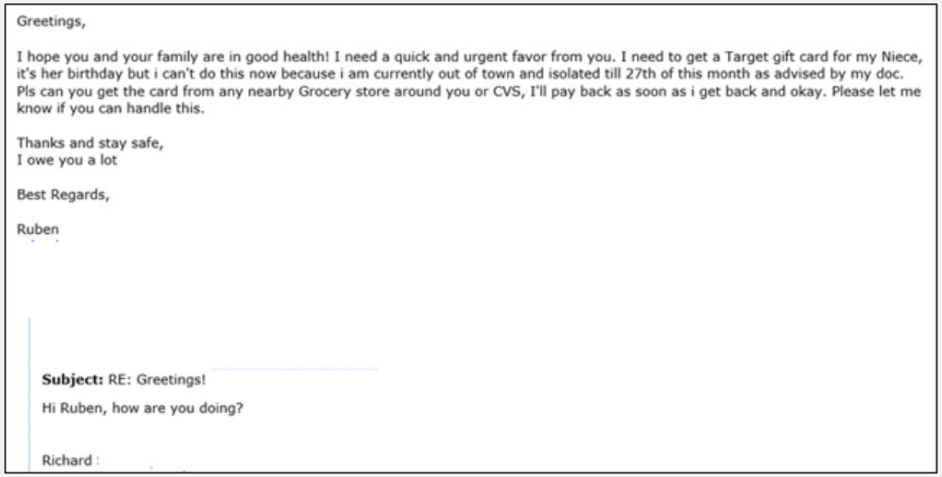


Hi Ashland,
I hope that this email reaches you in great health, I'm out of town and i need you to kindly make arrangements for donations(gift cards) to Veterans at Hospice care units.
Can you please handle this on behalf of

This is a one time project and I'll be liable for reimbursement. I look forward to reading from you at your earliest convenience.
Thanks and stay safe!

Warm regards,
Kevin
President

Figura 20: Mensaje solicitando al destinatario que compre tarjetas regalo para una presunta donación a un centro de veteranos



Greetings,

I hope you and your family are in good health! I need a quick and urgent favor from you. I need to get a Target gift card for my Niece, it's her birthday but i can't do this now because i am currently out of town and isolated till 27th of this month as advised by my doc. Pls can you get the card from any nearby Grocery store around you or CVS, I'll pay back as soon as i get back and okay. Please let me know if you can handle this.

Thanks and stay safe,
I owe you a lot

Best Regards,

Ruben

Subject: RE: Greetings!

Hi Ruben, how are you doing?

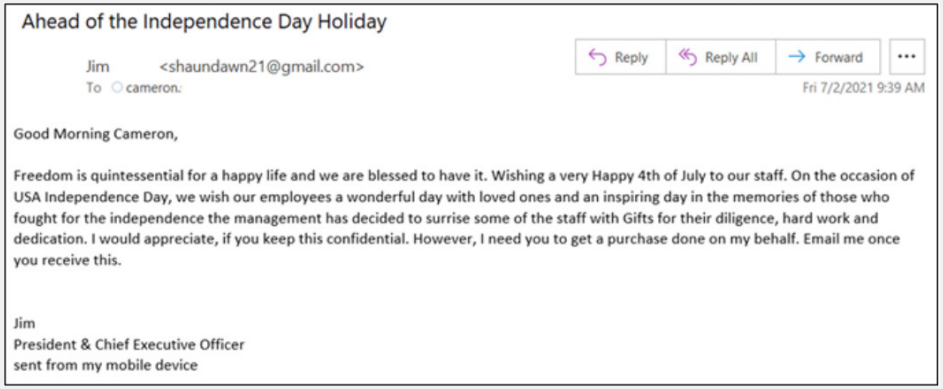
Richard :

Figura 21: Mensaje solicitando al destinatario que compre tarjetas regalo por estar el remitente confinado

La Figura 22 también demuestra que algunos timos de tarjetas regalo empiezan con un breve mensaje de señuelos y tareas para tantear la receptividad de la posible víctima (si desea obtener más información sobre este timo, consulte la sección anterior "**Tema 4: Señuelos y tareas**"). En este caso, el ciberdelincuente primero intentó averiguar la disponibilidad de la víctima elegida. Solo solicitó las tarjetas regalo cuando la persona respondió.

Timo de tarjetas regalo corporativas

En nuestro último ejemplo (Figura 22), el ciberdelincuente cuenta que necesita distribuir tarjetas regalo de agradecimiento entre sus empleados, una práctica corporativa habitual. En este caso, la solicitud está relacionada con el Día de la Independencia de Estados Unidos.



Ahead of the Independence Day Holiday

Reply | Reply All | Forward | ...

Jim <shaundawn21@gmail.com>
To cameron.
Fri 7/2/2021 9:39 AM

Good Morning Cameron,

Freedom is quintessential for a happy life and we are blessed to have it. Wishing a very Happy 4th of July to our staff. On the occasion of USA Independence Day, we wish our employees a wonderful day with loved ones and an inspiring day in the memories of those who fought for the independence the management has decided to surrise some of the staff with Gifts for their diligence, hard work and dedication. I would appreciate, if you keep this confidential. However, I need you to get a purchase done on my behalf. Email me once you receive this.

Jim
President & Chief Executive Officer
sent from my mobile device

Figura 22: Mensaje de alguien que se hace pasar por el CEO de la empresa y que pide al destinatario que compre tarjetas regalo como gratificación para los empleados; el atacante solicita al destinatario que mantenga la solicitud en secreto, supuestamente para no estropear la sorpresa

El regalo que sigue funcionando

Las tarjetas regalo son una forma habitual de estafa por correo electrónico. Con una media de 840 dólares por incidente, este delito ha defraudado casi 245 millones de dólares desde 2018. Nosotros detenemos al día entre 7000 y 10 000 de estos mensajes.

Tema 6: Fraude de los anticipos

El fraude de los anticipos es una antigua estafa que a veces, y de forma un poco engañosa, se denomina timo "419", "419 nigeriano" o "príncipe nigeriano". Tiene lugar cuando un ciberdelincuente pide a la posible víctima una pequeña cantidad de dinero como anticipo de un mayor pago posterior. Los fondos solicitados se suelen describir como el capital inicial para desbloquear o transferir la recompensa prometida.

Los ciberdelincuentes han ideado innumerables variaciones del fraude de los anticipos. A menudo elaboran intrincadas historias para explicar por qué hay una gran suma de dinero disponible y por qué, para hacérsela llegar al destinatario del mensaje, necesitan un pequeño adelanto. En general, los estafadores intentan que las víctimas piquen con líneas de asunto como:

- Herencia
- Premios de la lotería
- Galardones
- Desembolsos de la Administración
- Negocio internacional

Cuando la víctima facilita el anticipo, el estafador puede darle largas para sacarle más dinero (alegando complicaciones imprevistas) o simplemente romper el contacto y desaparecer.

Cómo funciona

En el nivel *Engaño* de nuestra taxonomía, el fraude de los anticipos utiliza técnicas de suplantación. Normalmente, los ciberdelincuentes se hacen pasar por un funcionario del gobierno, un representante legal o una persona en una situación extrema. La mayoría de los mensajes de fraude de los anticipos falsifican el "display name" (véase la Figura 23), aunque algunos utilizan otras tácticas de usurpación, como la suplantación de dominios o los "lookalike domains".

Figura 23: Taxonomía del fraude de los anticipos

Ejemplos reales

Los mensajes de correo electrónico del fraude de los anticipos utilizan varios señuelos para atraer a las víctimas, conservar su confianza y persuadirles a actuar. Como muestran los ejemplos siguientes, los ciberdelincuentes pueden aprovechar cualquier cosa que funcione, incluidos sucesos actuales, como la pandemia, acuerdos comerciales y herencias.

En la Figura 24 (véase la página siguiente), el remitente intenta capitalizar la COVID-19. En la Figura 25 (también en la página siguiente), el remitente urge al destinatario a actuar con rapidez, lo que le deja poco tiempo para considerar si el mensaje es fraudulento.

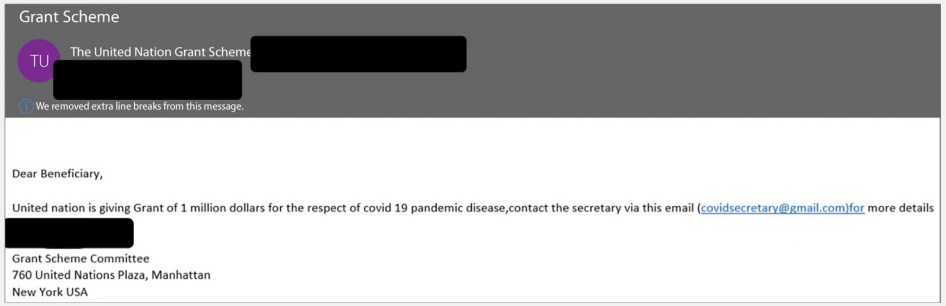


Figura 24: Mensaje de fraude de los anticipos prometiendo una subvención de 1 millón de dólares

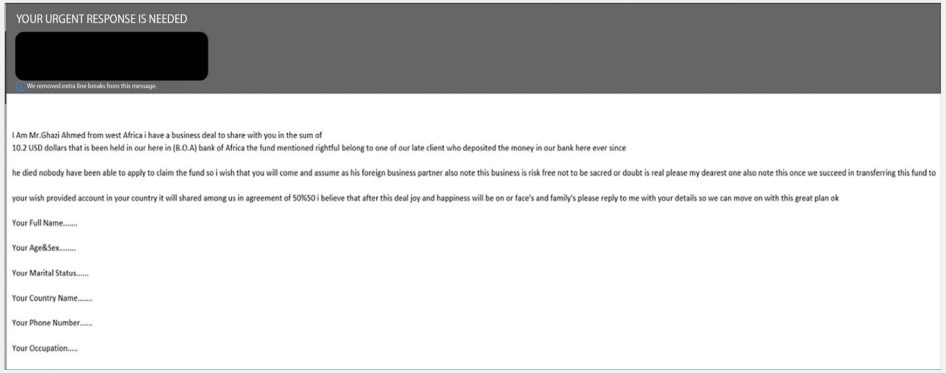


Figura 25: Este mensaje ofrece dividir una herencia no reclamada con el destinatario

En la Figura 26, el ciberdelincuente intenta tentar a la víctima con el pago de una sustanciosa herencia, una estrategia común en el fraude de los anticipos que aprovecha la codicia humana. Además de sacarle al destinatario una "fianza" de 95 dólares, el mensaje intenta obtener información de identificación personal.

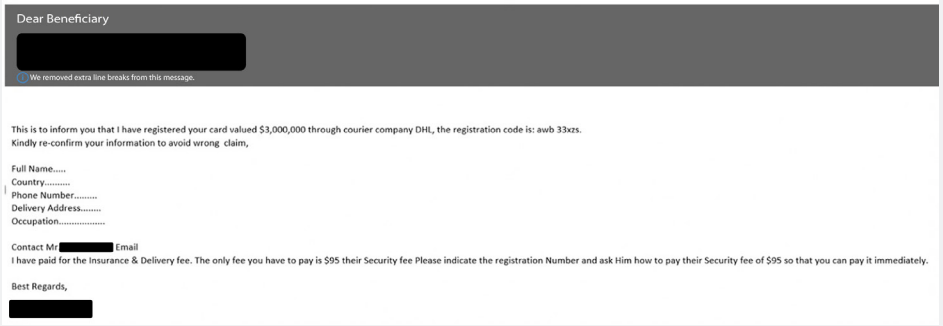


Figura 26: Mensaje que promete el pago de 3 millones de dólares en cuanto el destinatario abone una "fianza" de 95 dólares

La mayoría de los mensajes de fraude de los anticipos son sencillos y fáciles de identificar; pocos están bien diseñados o son más complejos que los ejemplos proporcionados aquí.

Los mensajes de fraude de los anticipos suman una pequeña parte de las estafas por correo electrónico que registramos. Aun así, hay gente que pica el anzuelo y las pérdidas medias alcanzan los 5100 dólares por incidente. Aunque la tasa de éxito es probablemente muy inferior a la de otros tipos de estafas, como las tarjetas regalo, el fraude de los anticipos puede resultar lucrativo para los perpetradores.

Conclusiones y recomendaciones

Los tipos de estafa por correo electrónico descritos en nuestra taxonomía son taimados, incesantes y difíciles de gestionar con las herramientas y los gateways tradicionales centrados en el perímetro. Al igual que la mayoría de los ciberataques modernos, su objetivo son las personas, no la tecnología. De ahí que detener este tipo de ataques exija una estrategia centrada en las personas.

Los controles financieros, como exigir que dos personas aprueben cambios en las cuentas de pago o los datos de la nómina, son un buen comienzo. Pero a la hora de detener las estafas BEC, también se precisa una protección avanzada del correo electrónico. Para obtener más visibilidad de esta superficie de ataque humana y detener los ataques BEC en todas sus distintas formas, hace falta una plataforma exhaustiva con controles integrados para correo electrónico, cuentas cloud, usuarios y proveedores.

Busque una solución que ofrezca:

- Visibilidad de su superficie de ataque humana. Debe saber quiénes son sus usuarios más atacados, los ciberdelincuentes que atacan a su organización y los proveedores que pueden haber sido comprometidos o suplantados.
- Funciones avanzadas de detección para detener las estafas BEC, de correo electrónico y otras amenazas que no utilizan malware. Las estafas por correo electrónico utilizan ingeniería social y tácticas en constante evolución que se aprovechan de la naturaleza humana. Esto significa que los conjuntos de reglas estáticas no son suficientes para identificarlas y detenerlas aunque se actualicen regularmente. Las mejores soluciones también emplean el aprendizaje automático para analizar factores tales como los encabezados de los mensajes de correo electrónico, la relación entre remitente y destinatario y la reputación del remitente. Pero la calidad del aprendizaje automático depende de los datos de los que se nutre y de los modelos de entrenamiento que lo conforman. Por lo tanto, busque proveedores con conjuntos de datos grandes y diversos y experiencia en amenazas humanas.
- Capacidad para impedir a los agresores que se apropien de las cuentas de los usuarios y las utilicen para ataques de estafa por correo electrónico. A medida que aumenta el número de empresas que migran a la nube, protegerse de las estafas por correo electrónico también significa proteger las cuentas cloud. Busque herramientas que impidan la apropiación de las cuentas de sus usuarios para utilizarlas en ataques de estafa por correo electrónico.
- Formación para concienciar en materia de seguridad y aumentar los controles técnicos. Con la formación adecuada —especialmente si está basada en amenazas del mundo real—, puede convertir a los usuarios en su última y sólida línea de defensa. Facilite que los usuarios denuncien los mensajes sospechosos y que su departamento de seguridad los verifique con análisis y corrección automatizados.

MÁS INFORMACIÓN

Para obtener más información sobre cómo puede ayudarle Proofpoint a gestionar las estafas BEC y por correo electrónico, visite **www.proofpoint.com/us/solutions/bec-and-eac-protection**.

ACERCA DE PROOFPOINT

Proofpoint, Inc. es una compañía líder en ciberseguridad y cumplimiento de normativas que protege el activo más importante y de mayor riesgo para las organizaciones: las personas. Gracias a una suite integrada de soluciones basadas en cloud, Proofpoint ayuda a empresas de todo el mundo a detener las amenazas dirigidas, a salvaguardar sus datos y a hacer a los usuarios más resilientes frente a ciberataques. Compañías líderes de todos los tamaños, entre las que se encuentran más de la mitad del Fortune 1000, confían en las soluciones de Proofpoint para su seguridad centrada en personas y su cumplimiento regulatorio, mitigando los riesgos más críticos en sus sistemas de correo electrónico, cloud, redes sociales y web. Encontrará más información en **www.proofpoint.com/es**.

proofpoint.

0500-000-01-01 01/22