Casbeep

Ciberseguridad para autónomos y micropymes

Cómo identifica Spiderman los fraudes online

FERNANDO CASTILLO

Hola,

En este pequeño ebook no me voy a entretener mucho.

Mi intención es que sea una guía clara y sencilla sobre **primeros pasos para detectar fraude online**.

En cualquier caso, espero que lo disfrutes y puedas implementar y aprender algo y que digas: “pues mira, mereció la pena”.

Lógicamente, no es un servicio a medida, ni un curso, ambas cosas tendrían un precio y una intensidad de trabajo muy diferentes.

Aquí como ves te estoy regalando algo que podría ser perfectamente una sección de una de mis formaciones.

Pero puedes tener la total tranquilidad de que todo lo que te digo aquí son buenos consejos que conozco desde la experiencia y después de **ver muchos fraudes online**.

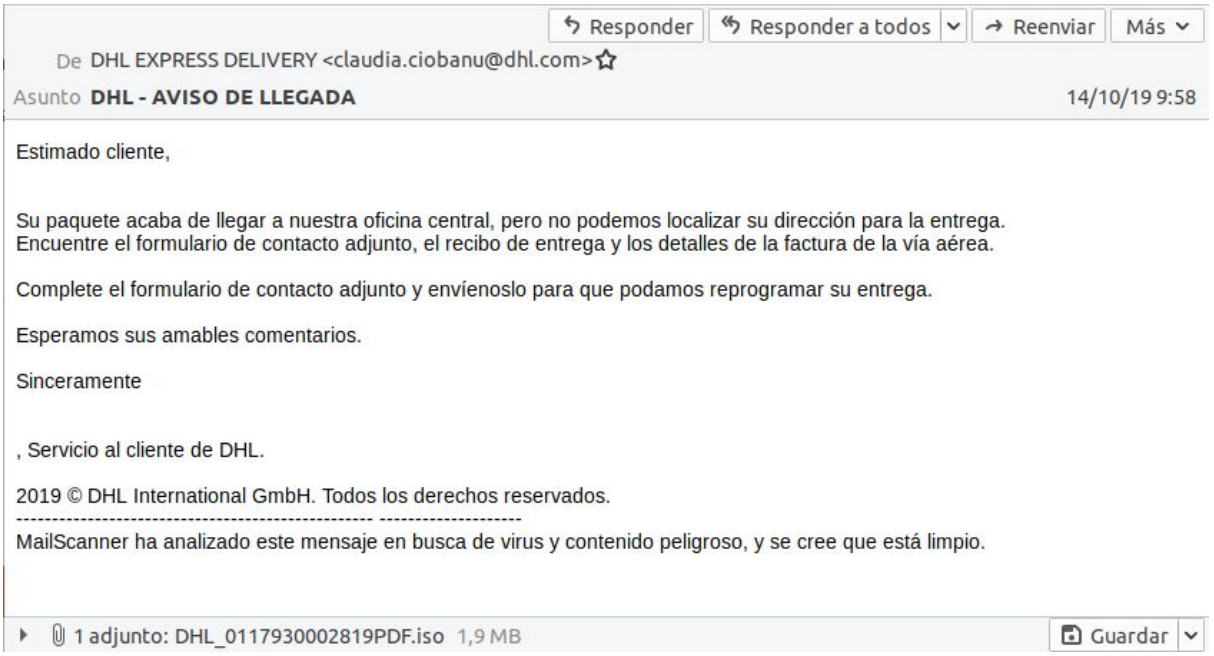
Es posible que algunas cosas las sepas y otras que no.

En todo caso, esta es una manera muy efectiva de empezar a entrenar nuestro sentido común de la ciberseguridad.

Email servicio de correos

Ponte en el caso que recibes este email, intenta olvidar que estamos hablando sobre fraude online y piensa que estás en una situación del dia a dia, frente a tu ordenador como de costumbre trabajando en tu negocio online.

¿Qué es lo primero que se te viene a la mente al leerlo?



Vale, aquí primero te voy a contar las distintas partes de un correo, esto lo sabrás ya pero como recordatorio nunca viene mal.

Una vez que sepamos identificar esas diferentes secciones dentro de cualquier correo podremos identificar los distintos vectores de entrada de fraude.

- Remitente
  Quién te manda el correo

- Asunto
  Breve descripción del motivo del correo

- Cuerpo
  El correo en sí

Estimado cliente,

Su paquete acaba de llegar a nuestra oficina central, pero no podemos localizar su dirección para la entrega. Encuentre el formulario de contacto adjunto, el recibo de entrega y los detalles de la factura de la vía aérea.

Complete el formulario de contacto adjunto y envíenoslo para que podamos reprogramar su entrega.

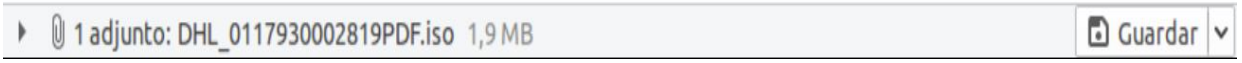
Esperamos sus amables comentarios.

Sinceramente

, Servicio al cliente de DHL.

MailScanner ha analizado este mensaje en busca de virus y contenido peligroso, y se cree que está limpio.

- Adjuntos
  Ficheros incluidos en el correo



Bueno, empecemos a analizar.

1. Hemos recibido un email del servicio de correos DHL.
2. Tenemos un paquete perdido y debemos hacer algo con el fichero adjunto para recuperarlo.
3. El email ha sido escaneado con un antivirus.
4. Un fichero adjunto con extensión ISO.

Aquí lo sospechoso es el fichero adjunto, se trata evidentemente de un tipo de archivo que no es común, por lo que podemos marcar como **FRAUDE** directamente este email.

No nos están adjuntando una imagen o un documento de Word que sí son comunes por ejemplo.

La frase de que el email ha sido escaneado por un antivirus es solo un engaño para tratar de dar más confianza.

El email aunque parezca mandado desde **dhl.com**, la realidad es que no es así y han suplantado su identidad. (Analizar esto es para un nivel más avanzado, si estás interesado en alcanzar este nivel puedes escribirme y te informo)

Email netflix

Esta vez hemos recibido un email de Netflix, con su logo y plantilla corporativa en vez de un correo con texto simple.

Volvamos a hacer un ejercicio de poner nuestra mente en blanco y leer el email sin más.

¿Qué es lo primero que se te viene a la mente al leerlo?

Vale, ahora toca analizarlo.

1. Hemos recibido un email de netflix.
2. Hay un problema de facturación y debemos hacer algo con el enlace para solucionarlo.

Aquí vemos claramente como el email no viene de Netflix, viene de **oncouranav.com** que aunque no tengamos ni idea de lo que es, desde luego no es Netflix.

Podemos marcar como **FRAUDE** directamente este email.

Además si pasamos por encima del enlace “actualizar cuenta”, vemos como el enlace apunta a “https://yescrm.**yes.my**/metadata/netflix.html”.

Yes.my otro sitio que no pertenece a netflix.

NUNCA HACEMOS CLICK EN LOS ENLACES DESCONOCIDOS

Simplemente pasamos el ratón por encima y ya nos muestra el destino del enlace sin necesidad de hacer click.

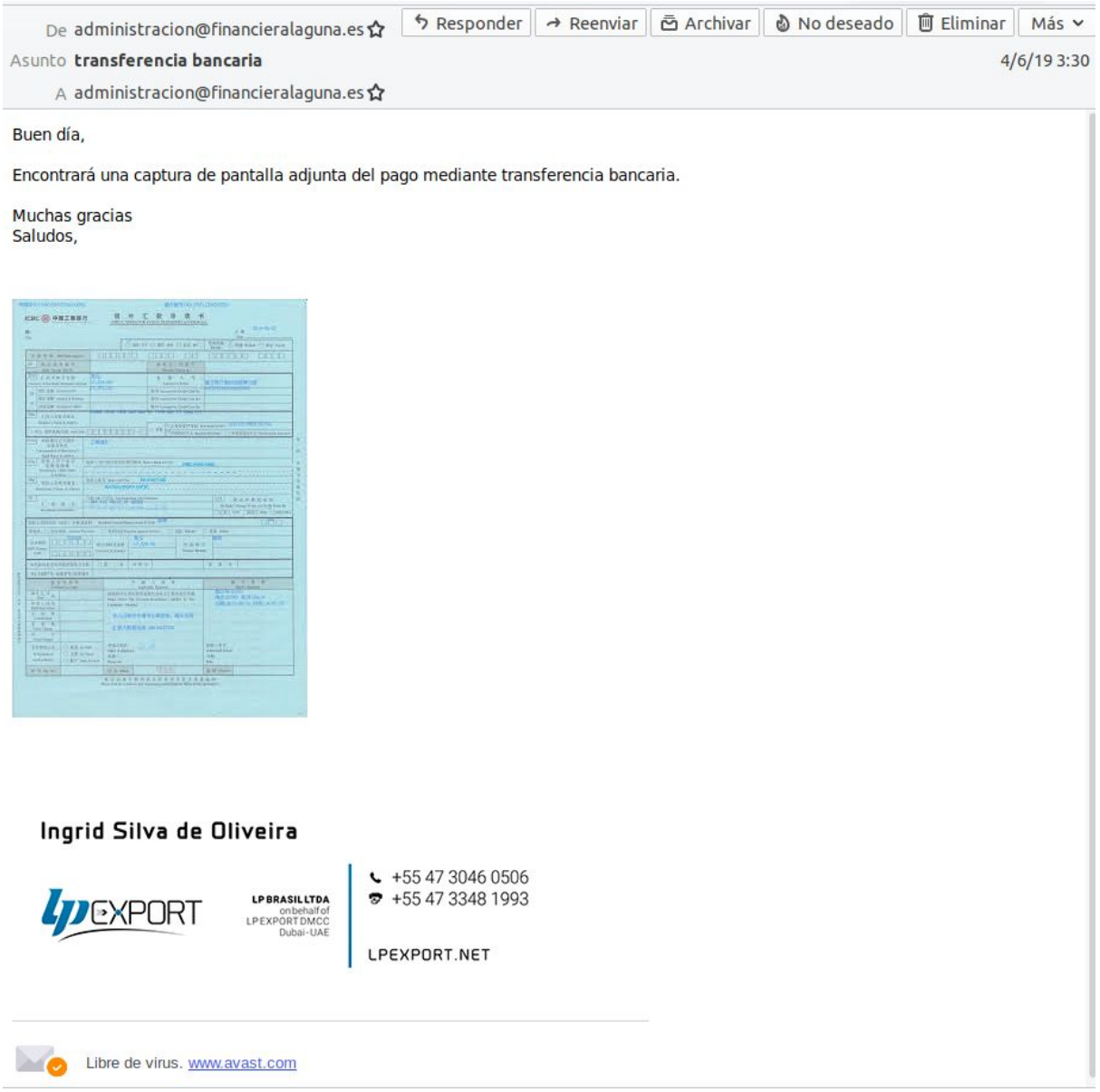
Email factura

Bien, ya llevamos la mitad de los ejercicios resueltos, espero que a estas alturas tengáis como mínimo un aprobado en este examen.

En esta ocasión parece que un proveedor nos quiere mandar la factura de un pago.

Volvamos a hacer un ejercicio de poner nuestra mente en blanco y leer el email sin más.

¿Qué es lo primero que se te viene a la mente al leerlo?



Bueno ya te he dejado bastante tiempo, empecemos a analizar.

1. Hemos recibido un email de financieralaguna.
2. Nos incluyen una imagen ilegible que supuestamente es una factura.

Obviamos primeramente si conocemos o no al proveedor, esto lo veremos después. Aunque si no conoces el proveedor, podría ser un motivo de rechazo del email.

Si pasamos por encima de la imagen vemos como en realidad es un enlace a "http://**realjobspa.it**/Swift_Caixabank_factura_June.jar". Además de no provenir de financieralaguna, la extensión de archivo JAR nos alerta.

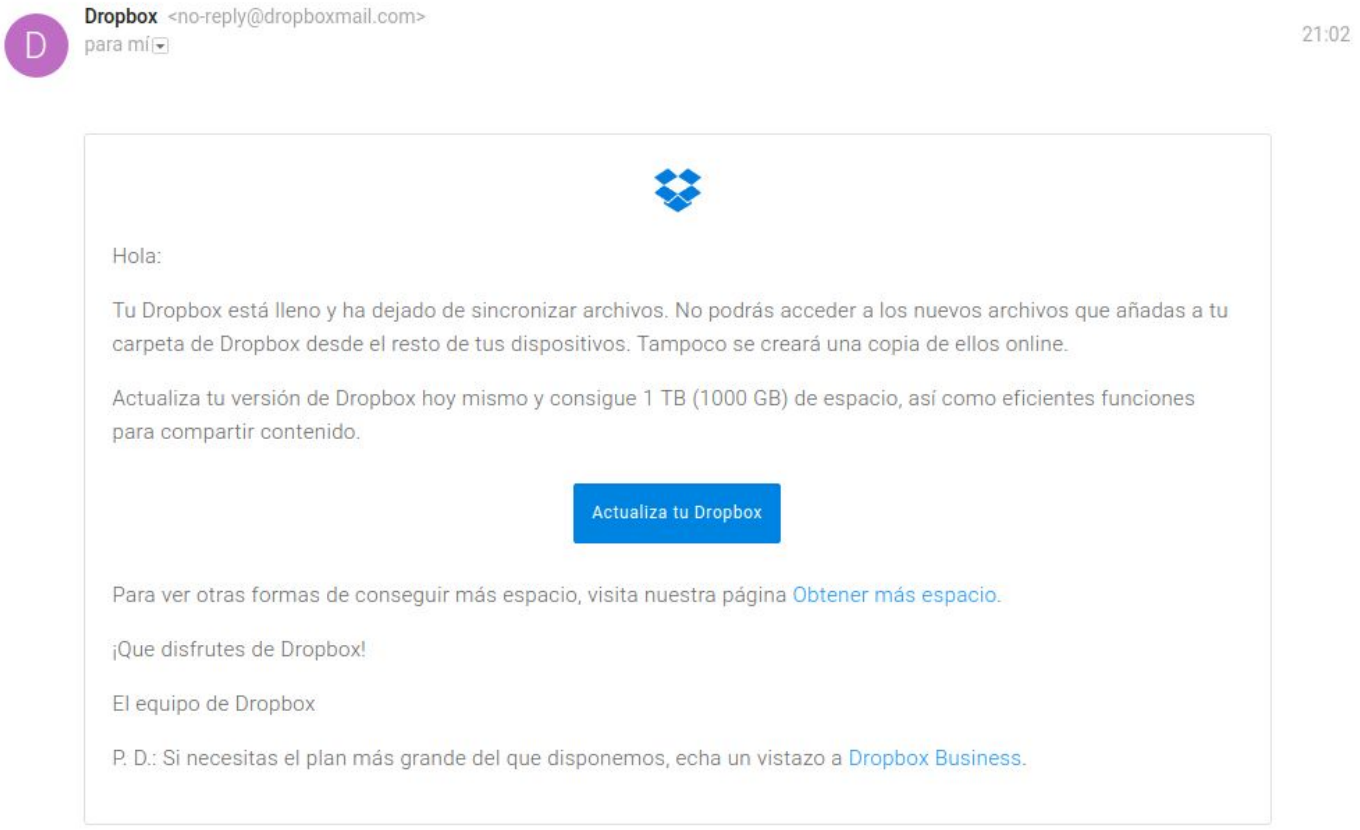
Podemos marcar como **FRAUDE** directamente este email.

La firma del email viene como Ipexport, un tercer proveedor distinto en vez de financieralaguna. Si ya de por si no conocíamos a financieralaguna, con esto terminamos de confirmar el fraude.

Email dropbox

Ya casi hemos terminado, nos falta solo analizar un email para sacar el sobresaliente.

¡Ánimo!



Y ahora, a analizar.

1. Hemos recibido un email de dropboxmail.
2. Hemos llegado al límite de almacenamiento y debemos hacer algo con el enlace para solucionarlo.

Quizás empezamos a sospechar porque el remitente es dropboxmail en vez de dropbox.

Si pasamos por encima del enlace vemos cómo apunta a “http://**dropbox.com**/buy”. Sitio oficial de dropbox, no hay ningún peligro en este enlace.

Podemos marcar por fin como **LEGÍTIMO** este email.

Te tengo que contar que Dropboxmail es un dominio oficial de dropbox, para saberlo hay que mirar el propietario del dominio. (Analizar esto es para un nivel más avanzado, si estás interesado en alcanzar este nivel puedes escribirme y te informo)

¡Bien!

Ya hemos acabado nuestro examen, espero que hayas sacado buena nota. Y en caso de que no, siempre puedes tomar notas y volverlo a repetir.

Recuerda:

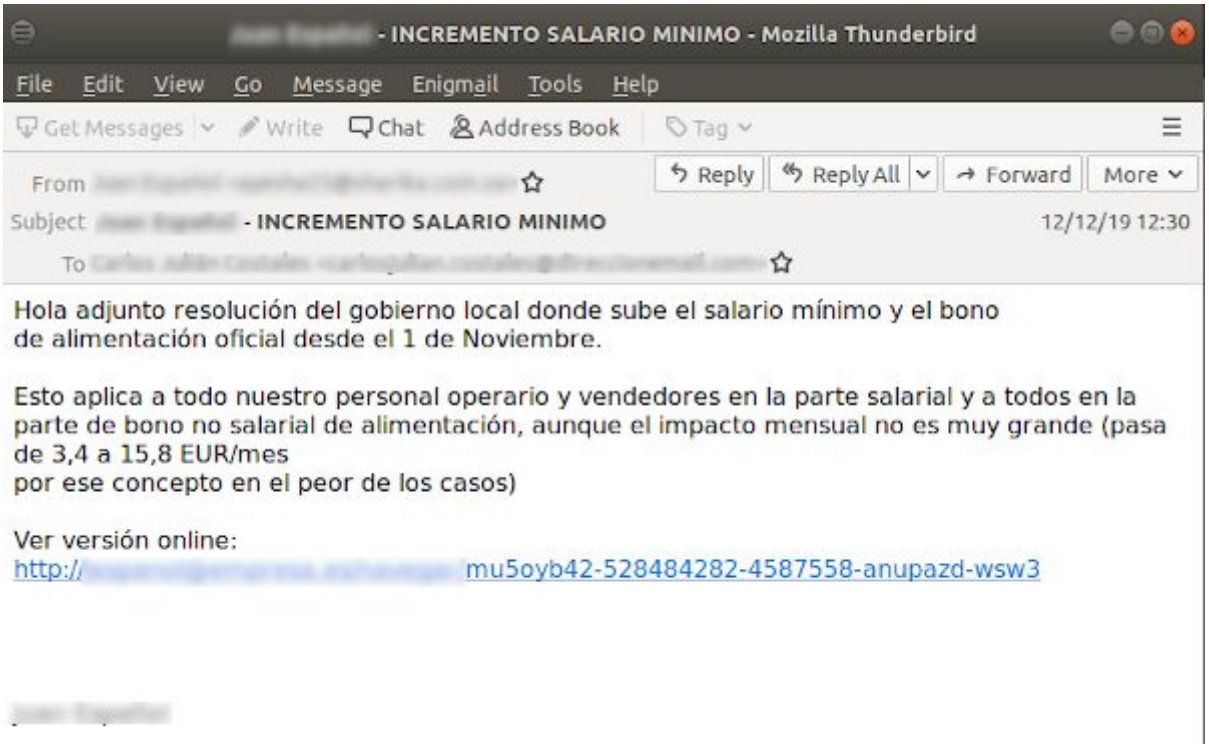
1. Fíjate bien en el remitente
2. Cuidado con los enlaces
3. Cuidado con los adjuntos
4. Confía en tu primera intención

Si parece sospechoso, trátalo primero como culpable hasta que demuestre lo contrario.

Y si tienes tantas dudas, siempre puedes preguntar al remitente para confirmar.

El email que más quebraderos de cabeza dió a los antivirus en 2019

Por último quiero enseñarte un email que aunque en un principio no debería tener mucha relevancia, el problema fue lo que originó después a los antivirus.



Como siempre, desglosamos el email:

El gancho que nos ofrece es un **Incremento de salario.**

Para generar confianza nos habla de que este incremento lo ha formalizado el gobierno y nos ofrece un enlace para ver los detalles.

El enlace como siempre apunta a un sitio sospechoso y descarga un documento de Word con macros.

Si abrimos el documento de Word malicioso, descargamos el troyano bancario **Emotet**

Y YA ESTAMOS INFECTADOS.

¿Por qué te cuento esto?

Porque quiero que entiendas que documentos comunes como un archivo de Word, también pueden tener regalito y debemos estar alertas.

¿Por qué complicó este troyano a los antivirus?

Emotet tiene cierta inteligencia y por cada vez que se descarga, puede cambiar su código. Esto hace que los antivirus tengan problemas para cazarlo.

Además se propaga rápidamente, roba tu lista de contactos y se envía a tus amigos, familiares, compañeros de trabajo y clientes.

Estos creerán que el correo viene de tí y como confían en tí es probable también que caigan.

Bueno, ya hemos llegado al final.

Espero que le saques mucho partido a este ebook que he querido regalarte.

Y sobre todo, veas los emails con otros ojos y tengas tu sentido común alerta.

Que pases un buen día.

Fernando Castillo.

PD: No olvides leer los emails que mando. Siempre puede caer algún regalito más.