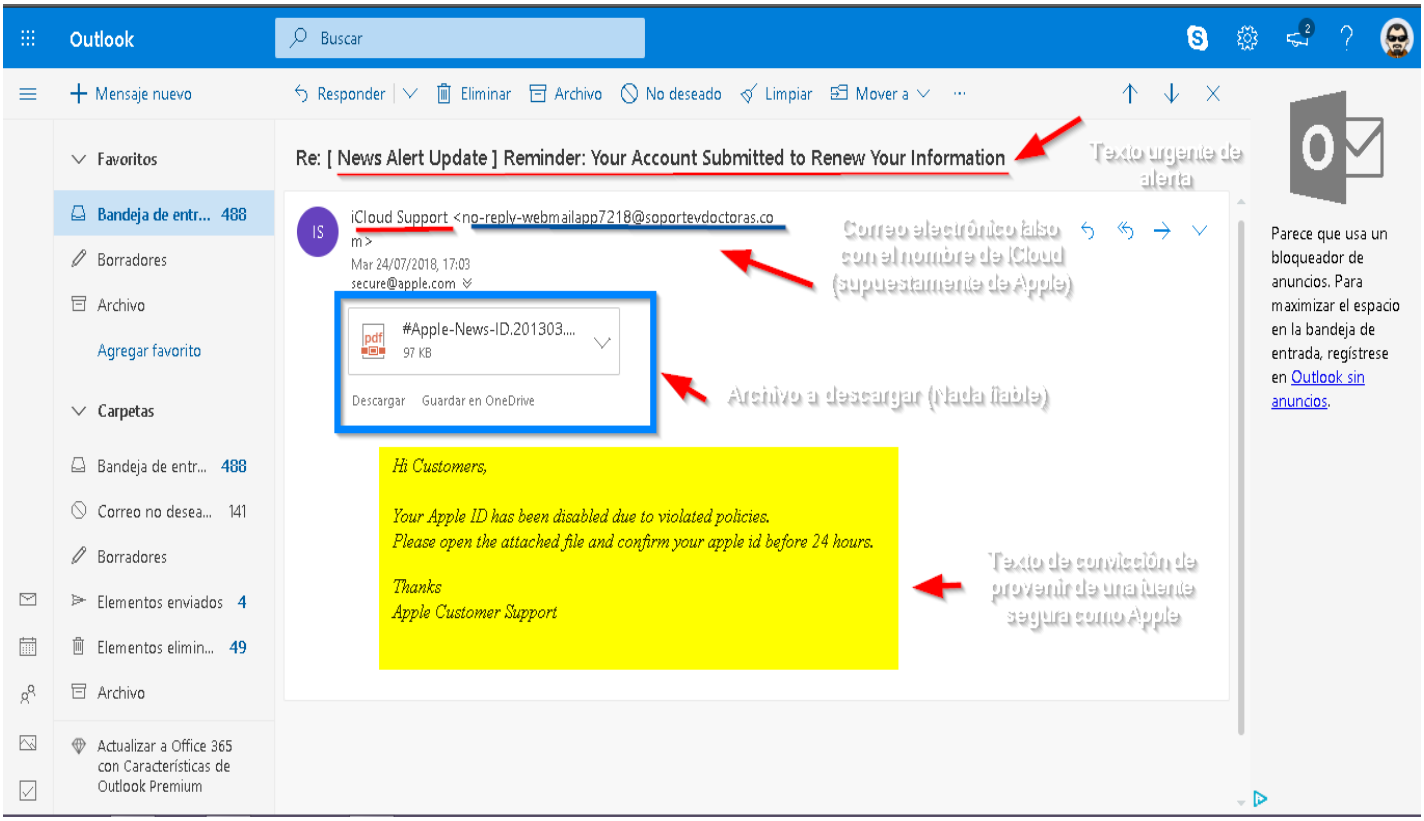
Anexo 4: Trabajando sobre un correo de “Phishing” real.

La siguiente captura que muestro es de un correo real recibido en mi bandeja de entrada el día 24/07/2018. Como veis el Phishing está a la orden del día. **¡QUÉ ME HACE SOSPECHAR DE QUE ESTE CORREO RECIBIDO NO ES LEGÍTIMO!**

Lo primero que tengo que decir es que no tengo ningún producto o cuenta de Apple y esto va va dirigido a todas aquellas personas que se dedican a leer y ver todos los correos que les llegan sin pensar si “conocen” o “tienen algún producto contratado” con la persona o empresa que les envía ese correo.

Si yo hubiera tenido algún producto de Apple, este correo podría haber pasado el primer filtro como correo auténtico. **¿Qué más cosas podemos comprobar?**



Segundo nos encontramos en un texto completamente en Inglés y en un formato que para nada utiliza una compañía para con sus clientes como “Thanks” que vendría a equivaler a Thank you very much, escrito desde el aspecto formal de una empresa. Por otro lado, recibir un texto en inglés si nuestro registro y producto de Apple se hizo en idioma español, hace aún más sospechoso el correo.

Hi Customers,

Your Apple ID has been disabled due to violated policies.
Please open the attached file and confirm your apple id before 24 hours.

Thanks
Apple Customer Support

Tercero, en el apartado asunto del correo, podemos observar:

Re: [News Alert Update] Reminder: Your Account Submitted to Renew Your Information

Un “Re:” que significa que el correo ha sido reenviado ¿Realmente una compañía necesita hacer reenvíos cuando teniendo el ,listado completos de todos sus clientes puede hacer los envíos de forma masiva?

Se nos avisa de una alerta o actualización importante y que debemos renovar nuestra información… Si es posible que una empresa quiera recordarnos algo, pero no suele hacerlo de forma tan intencional, que parece que te están obligando a hacerlo, sobre todo si seguimos leyendo en el cuerpo del mensaje que sólo **nos dan 24 horas para hacer la acción.**

Cuarto: **Debemos fijarnos bien en quien es el remitente del correo.** Muchas personas por prisas o por falta de hábito, sólo se suelen quedar en la primera parte “Icloud Support” y muchos pensarán , “pero si eso es de Apple”, SÍ, pero NO. Si seguimos leyendo, podemos ver el remitente desde dónde se ha enviado el correo “no-reply-webmailapp7218@soportevdoctoras.co” **¿A qué ya no parece tanto que este correo se haya enviado desde Apple?**

iCloud Support <no-reply-webmailapp7218@soportevdoctoras.co

Y Quinto y **lo que más distorsiona del correo es que se mande un fichero adjunto con el simbolito de PDF (Lo cual no significa nada: Os dejaré un ejemplo aparte de este documento para que veais a lo que me refiero)** el cual no me asegura que tipo de fichero es, aparte que en un principio la empresa hubiera colocado todo su contenido en formato de texto plano y a lo sumo un enlace donde ampliase la información en su página web para legitimar su contenido, no ampliaría la información en un fichero adjunto, el cual no sirve de nada para sus propósitos comerciales (*Bueno eso es una parte del marketing que no trataremos aquí*)

Hay infinidad más de circunstancias en las que nos podríamos fijar para saber si un correo electrónico es de procedencia legítima y segura, pero las que hemos visto hasta aquí son más que suficientes para defendernos en el entorno de nuestro hogar...