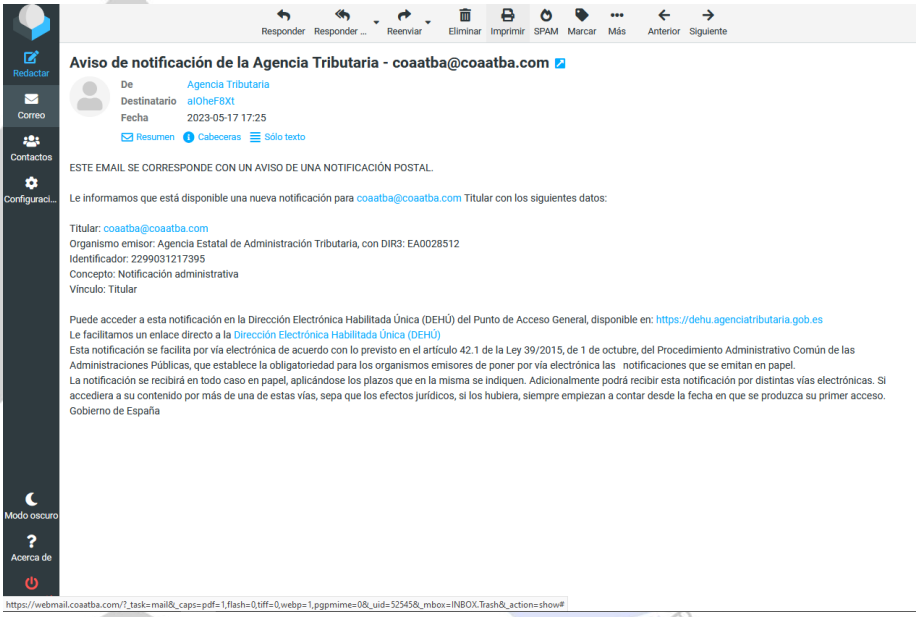
COLEGIO OFICIAL DE APAREJADORES Y ARQUITECTOS TÉCNICOS DE BADAJOZ
Plaza España, 16. 06002. Badajoz Tlf.: 924 25 48 11 / Fax.: 924 24 73 77 www.coaatba.com / coaatba@coaatba.com

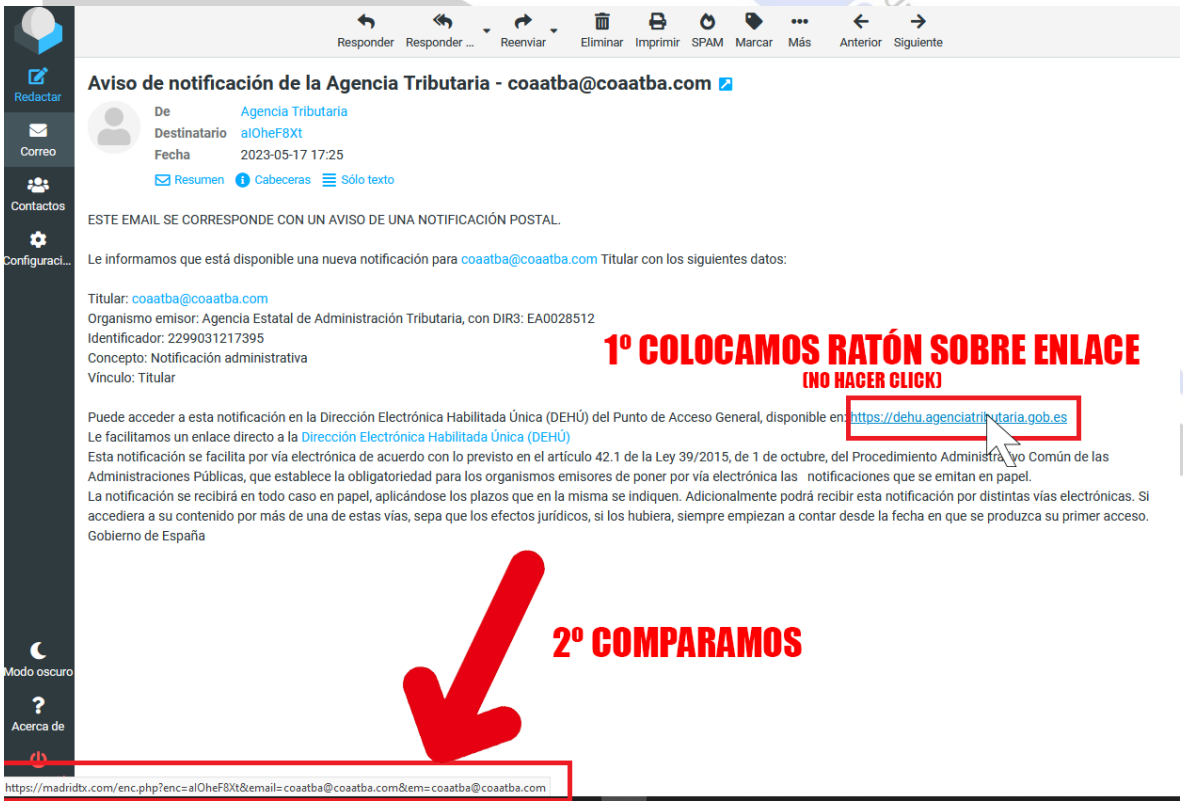
Estimados/as colegiados

Estamos recibiendo gran cantidad de correos electrónicos que dicen proceder de la "*Agencia Tributaria*" y seguramente que el 100% de los correos recibidos en nuestras cuentas colegiales es **phishing** o fraude, por eso, se recomienda que los marques como spam y elimines este/os correos inmediatamente. No obstante, os indico cómo distinguir de manera rápida un correo que pretende este intento de estafa:

1. A primera vista el correo recibido parece correcto:



2. Pero si colocamos el ratón (**SIN CLICKAR**) sobre cualquiera de los enlaces que aparece



COLEGIO OFICIAL DE APAREJADORES Y ARQUITECTOS TÉCNICOS DE BADAJOZ
Plaza España, 16. 06002. Badajoz Tlf.: 924 25 48 11 / Fax.: 924 24 73 77 www.coaatba.com / coaatba@coaatba.com

Como podemos observar, al comparar el texto escrito (https://dehu.agenciatributaria.gob.es) no tiene nada que ver con el sitio al que nos lleva (https://madridtx.com/enc.php?enc.....) por lo que nos indica que este correo es un intento de estafa que ha de ser eliminado.

Como recomendación y para evitar futuros problemas informáticos, ante un correo de una Administración Pública, al recibir cualquier correo de estos, es aconsejable que **escribáis** en la barra de dirección de vuestro navegador https://dehu.redsara.es y accediendo con vuestro certificado podréis ver si tenéis alguna notificación de alguna administración, ya que **dehú notificaciones es la herramienta que facilita el acceso a los ciudadanos y empresas a las notificaciones y comunicaciones emitidas por las Administraciones Públicas.**

COLEGIO OFICIAL DE APAREJADORES Y ARQUITECTOS TÉCNICOS DE BADAJOZ
Plaza España, 16. 06002. Badajoz Tlf.: 924 25 48 11 / Fax.: 924 24 73 77 www.coaatba.com / coaatba@coaatba.com

Para terminar, facilito una pequeña guía de cómo detectar en general correos electrónicos fraudulentos.

Siempre se ha dicho que el punto más débil de un sistema informático se encuentra detrás del teclado. Por ejemplo, somos los propios usuarios los que al final decidimos si confiamos o no en un mensaje, en una página web o en una tienda online. Y de eso se aprovechan los ciberdelincuentes para lograr sus propósitos. Vamos a ver cómo detectar un mensaje fraudulento.

¿Cómo podemos identificar si un correo electrónico es malicioso?

- **Analiza el remitente:** Lo primero que debemos hacer es comprobar que el remitente es conocido. Presta atención a su dirección de correo y comprueba si efectivamente es real y no una suplantación. Los piratas informáticos suelen utilizar direcciones similares a las reales cambiando algún número o letra para confundir y conseguir así su objetivo.
- **Observa el asunto del email:** La mayoría de los correos fraudulentos utilizan asuntos llamativos y altamente impactantes, como, por ejemplo, que tu cuenta personal ha sido robada, que has ganado un premio, etc. Desconfía de correos que tengan un cebo para captar tu atención y cuyo objetivo es que abras el e-mail.
- **Objetivo del mensaje:** Ten en cuenta que ninguno de las entidades que te prestan algún servicio, como **bancos**, suministros de **luz**, **agua**, **organismos oficiales**, **nunca te van a pedir datos personales**. Si es así, es muy probable que sea un fraude.
- **¿Cómo está redactado el texto?:** Si detectas errores ortográficos, malas traducciones y contenidos extraños es otro indicador de alerta.
- **Cuidado con los archivos adjuntos:** Revisa bien. Si no es un remitente conocido, analiza bien los adjuntos ya que puede ser un malware. Archivos **aparentemente inofensivos, un Word o un Excel** pueden resultar una amenaza importante. Un buen antivirus puede resultarte de gran utilidad ayudándote a identificar si dichos archivos están infectados.

Como puedes ver, detectar correos electrónicos falsos es relativamente fácil, pero nadie está a salvo de caer en una estafa o ser víctima de un ataque de phishing, por lo que la implantación de medidas de seguridad (antivirus, backup online, auditorías de seguridad, etc) puede contribuir a prevenir ciberataques indeseados.

Esto es sólo una pequeña guía de cómo identificar un correo malicioso en el día a día, pero si necesitas más información o simplemente te interesa el tema y queréis aprender un poco más, os dejo unos enlaces:

- INCIBE: Instituto Nacional de Ciberseguridad: Nos ofrece todo tipo de información informática, qué hacer en caso de haber sido víctima de un ciberataque, herramientas, etc.
- Cómo detectar un mensaje fraudulento y por qué la ingeniería social es el punto de entrada de los chicos malos - XATAKA
- Phishing: qué es y diferentes tipos que existen - GENBETA