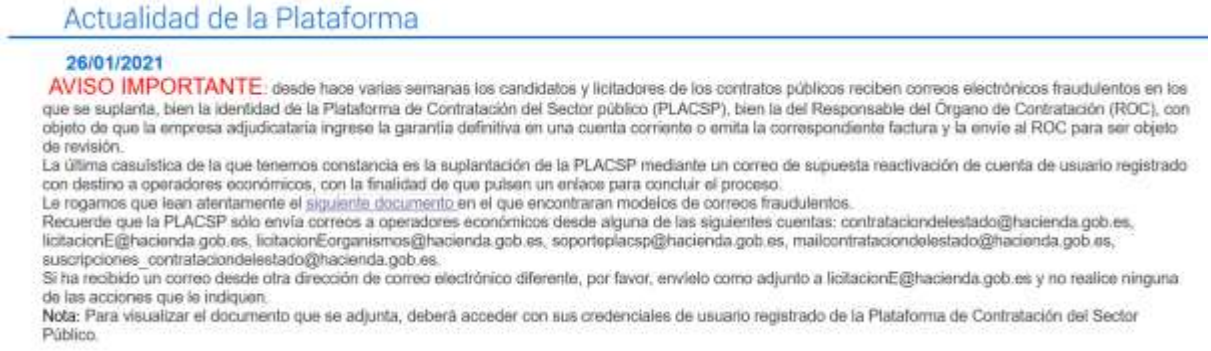
Autoridad Portuaria de Valencia
DIR3: EA0001321

NOTA INFORMATIVA

Asunto | Suplantación de identidad de la Plataforma de Contratación del Sector Público

A petición de la Plataforma de Contratación del Sector Público (PLACSP: https://contrataciondelestado.es/wps/portal/plataforma), comunicamos que el pasado 26-ene, este servicio fue objeto de una campaña de suplantación de identidad dirigida a empresas licitadoras de contratos públicos, según se recoge en el aviso incluido en su página web:



Actualidad de la Plataforma

26/01/2021

AVISO IMPORTANTE: desde hace varias semanas los candidatos y licitadores de los contratos públicos reciben correos electrónicos fraudulentos en los que se suplanta, bien la identidad de la Plataforma de Contratación del Sector público (PLACSP), bien la del Responsable del Órgano de Contratación (ROC), con objeto de que la empresa adjudicataria ingrese la garantía definitiva en una cuenta corriente o emita la correspondiente factura y la envíe al ROC para ser objeto de revisión.
La última casuística de la que tenemos constancia es la suplantación de la PLACSP mediante un correo de supuesta reactivación de cuenta de usuario registrado con destino a operadores económicos, con la finalidad de que pulsen un enlace para concluir el proceso.
Le rogamos que lean atentamente el siguiente documento en el que encontraran modelos de correos fraudulentos.
Recuerde que la PLACSP sólo envía correos a operadores económicos desde alguna de las siguientes cuentas: contrataciondelestado@hacienda.gob.es, licitacionE@hacienda.gob.es, licitacionEorganismos@hacienda.gob.es, soporteplacsp@hacienda.gob.es, mailcontrataciondelestado@hacienda.gob.es, suscripciones_contrataciondelestado@hacienda.gob.es.
Si ha recibido un correo desde otra dirección de correo electrónico diferente, por favor, envíelo como adjunto a licitacionE@hacienda.gob.es y no realice ninguna de las acciones que le indiquen.
Nota: Para visualizar el documento que se adjunta, deberá acceder con sus credenciales de usuario registrado de la Plataforma de Contratación del Sector Público.

Al margen del aviso anterior, la PLACSP ha procedido a una comunicación con las empresas licitadoras, aunque también nos ha pedido que colaboremos para divulgar esta información al haberse constatado que algunas de las campañas de ciberataque no suplantan a la propia PLACSP, sino a los organismos públicos que han lanzado los procesos de contratación, teniendo siempre como objetivo a las empresas licitadoras.

Por este motivo les rogamos que extremen la precaución en las comunicaciones por correo electrónico recibidas de la PLACSP o de cualquier organismo público a cuyos procesos de contratación se haya podido presentar su empresa.

Deben verificar que la dirección de correo del remitente del mensaje coincide con el dominio real del organismo al que pertenece dicho remitente, teniendo cuidado de no pasar por alto ningún pequeño "gazapo", ya que esta es una técnica frecuente para que las víctimas no se den cuenta de la suplantación (xxx@microsotf.com en lugar de xxx@microsoft.com, por ejemplo).

Tengan en cuenta, además, las recomendaciones de seguridad habituales frente a intentos de suplantación de identidad por correo electrónico, como, por ejemplo, las de la Oficina de Seguridad del Internauta (OSI):

> https://www.osi.es/es/actualidad/blog/2020/11/11/email-spoofing-comprueba-quien-te-envia-un-correo-sospechoso

Confiamos en que encuentren esta información de utilidad y aprovechamos para enviarles un cordial saludo.