Campaña de correos fraudulentos contra Unidades de Contratación

Estimados compañeros,

Os informamos que se ha reportado una **campaña de correos electrónicos fraudulentos a nivel nacional contra las Unidades de Contratación de las administraciones públicas**, suplantando a proveedores **para solicitar el cambio del número de cuenta bancaria a efectos de facturación**, por lo que rogamos extreméis la precaución al respecto.

Un **ejemplo del tipo de mensaje** que se está recibiendo es el siguiente:

> **De: Patricia Lozano contabilidad@unidadfinanciera.com**
>
> **Para: XXXXXXXXXXXXXXXXXXXXXXXXXX**
>
> **Asunto: Cambio de cuenta bancaria a partir del 25/08/2025**
>
> ***Estimados señores,***
>
> ***Por la presente, les informamos que a partir del día de hoy, 25 de agosto de 2025, hemos procedido al cambio de nuestra cuenta bancaria.***
>
> ***Les rogamos que, a partir de ahora, utilicen exclusivamente la nueva cuenta para todas las transferencias futuras.***
>
> ***Agradeceríamos mucho que nos confirmaran la recepción de este aviso, para poder enviarles la confirmación por escrito junto con los nuevos datos bancarios.***
>
> ***En caso de que necesiten algún otro documento adicional, además del certificado bancario, para proceder con el cambio de cuenta, les rogamos que nos lo indiquen.***
>
> ***Quedamos a su entera disposición para cualquier consulta adicional.***
>
> ***Atentamente,***
>
> ***Patricia Lozano***
>
> ***Departamento Financiero***
>
> ***EMPRESA XXXXXXXXXXX***

Los **correos** son **bastante sofisticados,** ya que **incluso contienen PDFs de certificados de titularidad emitidos por bancos**. Asimismo, es importante destacar que **estos mensajes fraudulentos se están enviando desde** cuentas que contienen los siguientes dominios: **unidadfinanciera.com; plataforma-financiera.com y area-financiera.com**

Todas las direcciones de correo electrónico que contengan esos dominios (ejemplo, contratacion@unidadfinanciera.com) **son ilegítimas**, por lo que no debe tomarse en consideración absolutamente nada de lo que provenga de ellas.

Este tipo de campañas fraudulentas por correo electrónico **se conoce como "*Ataque BEC*"** (por las siglas en inglés de *Business Email Compromise)*) o "*Fraude del correo electrónico corporativo comprometido*". Es un **tipo de *phishing*** dirigido y **refinado** en el que los ciberdelincuentes suplantan por correo electrónico **la identidad de personas** o entidades de **confianza**, como proveedores habituales o directivos, para desviar fondos o información sensible.

Aprovechamos este suceso para remitiros a un vídeo explicativo sobre este tipo de ataques que publicamos hace pocos meses en ayudaDIGITAL: ver vídeo

Por último, hay que indicar que los **Centros de Operaciones de Seguridad (SOC) de la Junta de Andalucía están llevando a cabo las medidas oportunas para solucionar las incidencias de esta campaña**, por lo que **no es necesario que hagáis nada por vuestra parte**, **salvo que extreméis la precaución** si recibís un correo de las falsas direcciones arriba indicadas y que nos ayudéis a difundir esta información entre el resto de profesionales para evitar estas estafas.

Rogamos, hagáis llegar esta información a aquellos profesionales del Servicio Andaluz de Salud que pueda interesarles.

Gracias por vuestra colaboración.

Comunicación

Dirección General de Sistemas de Información y Comunicaciones

Servicio Andaluz de Salud