



## CAMPAÑA DE PHISHING SUPLANTANDO A CORREOS Y TELÉGRAFOS

- El Instituto Nacional de Ciberseguridad (INCIBE) alerta de una campaña de correos fraudulentos que tratan de suplantar al servicio de Correos.
- Asunto: **“RE: Envío número 1-ES196 \*\*\*\* 726 ! “**

El **INCIBE** informa sobre la reciente detección de una campaña de envío de correos electrónicos que, con la intención suplantar a Correos, tratan de obtener información bancaria de las víctimas.

El correo tiene como asunto **“RE: Envío número 1-ES196 \*\*\*\* 726 ! “**. En el cuerpo del mensaje nos informan de que no se nos ha podido entregar un paquete y se nos insta a que reprogramemos la entrega, previo pago clicando en el enlace **“COMPLETE MI DIRECCIÓN DE ENTREGA”** que figura en el correo. Al pinchar en el enlace, nos dirigirán a una página web falsa para hacerse con nuestra información bancaria.

Se reiteran las pautas generales para evitar ser víctima de este tipo de delitos:

- **No abrir correos de usuarios desconocidos** o que no haya solicitado: hay que eliminarlos directamente.
- Los correos de una **entidad bancaria legítima, nunca contendrá enlaces** a su página de inicio de sesión o documentos adjuntos.
- **No contestar en ningún caso** a estos correos.
- Tener **precaución al seguir enlaces o descargar ficheros adjuntos** en correos electrónicos, SMS, mensajes en WhatsApp o redes sociales, aunque sean de contactos conocidos.
- Tener siempre **actualizado el sistema operativo y el antivirus**. En el caso del antivirus, comprobar que está activo.
- Utilizar **contraseñas robustas**.

Para más información seguir el siguiente enlace:

<https://www.incibe.es/protege-tu-empresa/avisos-seguridad/detectada-campana-phishing-suplanta-correos>

