DETECTADA NUEVA CAMPAÑA DE *SMISHING* QUE SUPLANTA EL SERVICIO DE SEUR

- **El objetivo es redirigir a la víctima a una página que simula ser la web legítima de la empresa.**
- **Se recuerda que ninguna empresa solicita datos personales o bancarios mediante correo electrónico.**

La estafa se basa en enviar un **SMS malicioso** avisando al usuario de que su paquete está pendiente de entrega y debe confirmar el pago de los gastos de envío. Para ello, **facilita un enlace que redirige a una página web que imita a la de la legítima empresa.** En ella se solicita el **ingreso de los datos personales y bancarios** de la víctima para pagar los supuestos gastos de envío (por un valor de 1,99€, el cual, sospechosamente, cambia automáticamente a 2,99€ conforme se van introduciendo los datos bancarios).

Tras pulsar en el **botón "Pagar", el usuario es redirigido a una página con un formulario donde se solicita un código que supuestamente le debería llegar por SMS.** Esta estrategia se utiliza para dotar de mayor credibilidad al proceso de pago y, aunque el SMS nunca lo recibirá, **los ciberdelincuentes ya han cumplido su objetivo, que es hacerse con sus datos de la tarjeta bancaria.**

RECOMENDACIONES:

- **Escribe directamente la URL de la empresa en el navegador**, en lugar de llegar a ella a través de enlaces disponibles desde páginas de terceros, en correos electrónicos o mensajes de texto.
- **No te fíes de los mensajes de usuarios desconocidos o que no hayas solicitado y no contestes a los mismos,** especialmente si detectas errores de ortografía en el mensaje.
- **Ninguna empresa envía por correo electrónico solicitudes de pago donde se soliciten datos personales de sus clientes.** En caso de duda, contacta directamente con el proveedor del servicio.