Nota informativa

Los Centros Europeos del Consumidor de la red ECC-Net nunca piden a los consumidores claves personales

Consumidores de Bélgica reciben llamadas telefónicas fraudulentas (vishing) solicitándoles el número de tarjeta bancaria y la clave de seguridad para poder cobrar el dinero de su reclamación

Madrid, 27 de julio de 2021. El Centro Europeo del Consumidor en España (CEC-España) advierte a todos los usuarios y usuarias de la red de Centros Europeos del Consumidor (ECC-Net) que, en ningún caso, se solicita a las personas consumidoras que faciliten claves personales o códigos PIN para gestionar sus reclamaciones o conseguir, cuando proceda, los correspondientes reembolsos reclamados.

Esta advertencia se produce como consecuencia de la alerta que el Centro de Bélgica (CEC-Bélgica) ha comunicado recientemente a la red ECC-Net ya que algunos de sus consumidores están recibiendo llamadas telefónicas de delincuentes en las que -haciéndose pasar de forma fraudulenta por trabajadores del Centro- se les solicita el número de la tarjeta bancaria y el código de seguridad como requisito para pagarles los reembolsos y/o indemnizaciones relacionadas con sus reclamaciones.

Por este motivo, CEC-España advierte a los consumidores que desconfíen de cualquier llamada telefónica o SMS que, en nombre del Centro, solicite datos personales del consumidor y, en especial, si se requieren claves personales. CEC-España NUNCA pedirá un código de seguridad (ya sea el de su cuenta bancaria o cualquier otro) para tramitar las reclamaciones.

La red ECC-Net, integrada por los Centros de los 27 países de la Unión Europea, además de los Centros de Islandia y Noruega, utiliza la plataforma online IT-Toll para la gestión las reclamaciones a través de la cual ,el consumidor recibirá en su correo electrónico todas las notificaciones y la información necesaria para el seguimiento de su caso. Las comunicaciones que recibe el consumidor durante todo el proceso de gestión del caso, se realizan principalmente a través de dicha plataforma y en ningún caso, se le solicitará sus datos personales por otra vía. Los datos personales necesarios para la correcta tramitación de reclamaciones (como su nombre y apellidos o el número de cuenta bancaria) son facilitados por la persona consumidora y, antes de proporcionarlos, deberá leer y aceptar de forma expresa la política de privacidad de la red ECC-Net. Los datos personales facilitados se gestionan y custodian conforme a la normativa nacional y europea en materia de protección de datos. Asimismo, los formularios de reclamaciones online que utiliza la red ECC-Net están integrados en dicha plataforma y están disponibles en las páginas web de cada uno de los Centros Europeos.

Algunos fraudes más habituales

Vishing

Es un tipo de estafa de ingeniería social por teléfono en la que, a través de una llamada, se suplanta la identidad de una empresa, organización o persona de confianza, con el fin de obtener información personal y sensible de la víctima.

Phising

Técnica que consiste en el envío de un correo electrónico por parte de un ciberdelincuente a un usuario simulando ser una entidad legítima (red social, banco, institución pública, etc.) con el objetivo de robarle información privada, realizarle un cargo económico o infectar el dispositivo. Para ello, adjuntan archivos infectados o enlaces a páginas fraudulentas en el correo electrónico.

Smishing

Técnica que consiste en el envío de un SMS por parte de un ciberdelincuente a un usuario simulando ser una entidad legítima -red social, banco, institución pública, etc. -con el objetivo de robarle información privada o realizarle un cargo económico. Generalmente el mensaje invita a llamar a un número de tarificación especial o acceder a un enlace de una web falsa bajo un pretexto.

Algunos consejos prácticos para evitar caer en engaños:

• Desconfiar de mensajes y llamadas que ofrecen trabajos (que no existen), premios (sin haber jugado) o paquetes recibidos (sin haberlos solicitado).

• No acceder a ninguna dirección web que llegue a través de SMS, más aún si desconoces el número telefónico.

• No proporcionar datos bancarios ni similares a través de SMS ni telefónicamente. En caso de recibir algún SMS de estas características y se tienen dudas sobre su veracidad, contactar directamente con tu banco utilizando los canales habituales y alertar a la Oficina de seguridad del internauta.

• Vigilar regularmente el consumo y, en caso de notar incrementos bruscos en la factura, contactar con la compañía telefónica. Es posible que la persona consumidora esté siendo víctima de un fraude.

• Informarse sobre las técnicas y modalidades de estafas que se utilizan para engañar a los usuarios.

• Comprobar los archivos adjuntos del e-mail antes de abrirlos. Desconfiar de nombres genéricos tipo “factura”, “recibo” o similares. Revisar tanto el aspecto como la extensión del fichero. Sospechar si se solicita habilitar las macros. Mucho cuidado con los archivos ejecutables y con los archivos javascript, aquellos con extensión “.js”, ya que se pueden saltar las protecciones del antivirus ocultándose en ficheros comprimidos.