El Consorcio Extremeño de Información al Consumidor, órgano dependiente del Instituto de Consumo de Extremadura, ha comenzado a recibir una serie de reclamaciones por parte de personas consumidoras desde diferentes localidades de Extremadura sobre fraudes utilizando la técnica del **'Vishing'**.

Por ejemplo:

"Una señora recibe llamada de alguien haciéndose pasar por Telefónica-Movistar y tras la conversación la señora recibe un paquete en casa que supuestamente es un router…"

La estafa sigue porque la llaman indicando que hay un error, que no abra el paquete y que enviarán un alguien para que lo recoja.

En realidad, con los datos de la señora, han contratado en Movistar dos dispositivos IPhone 15, por valor de casi 4000 euros (que pagará en plazos de 80 euros/mes durante 48 meses)."

Ese "alguien" que lo recoge se llevará el paquete con los teléfonos dentro y esa señora seguirá pagando mensualmente hasta el pago total del envío.

La palabra 'Vishing' es la unión de 'voz' y 'phishing'.

La suplantación de identidad consiste en utilizar el engaño para que una determinada persona caiga en el engaño orquestado por los ciberdelincuentes.

- En la mayor parte de los casos, en lugar de usar el correo electrónico, los cibercriminales utilizan un servicio telefónico para estafar a sus víctimas, mediante llamadas en las que se hacen pasar por empresas como por ejemplo Movistar.
- Suele ocurrir con personas de edad más avanzada
- En localidades pequeñas

Podemos intentar evitar estas situaciones:

1. **Comprobando en la empresa**: que la información que acabas de recibir en la llamada es verdaderamente información de dicha empresa. Si el remitente proporciona un número de devolución de llamada, puede ser parte de la estafa, así que no lo uses. Para eso, una vez se termina la llamada, llamaremos nosotros mismos, no al número del que hemos recibido la llamada, sino al **teléfono oficial de atención al cliente de la empresa**.
2. **No facilitando NUNCA información personal o confidencial**: ni tampoco respondas a requerimientos sobre tu tarjeta de débito o crédito, documento de identidad, dirección, fecha de nacimiento, etc. Ante cualquier duda, debes llamar al banco y notificar que te han solicitado información financiera en nombre de su entidad, ellos suelen estar informados de los modus operandi de Vishing, Phishing, etc.
3. **Colgando la llamada si sospechamos**: En el momento en que sospeches que se trata de una llamada telefónica fraudulenta, no sientas la obligación de tener que mantener una conversación cortés. Los cibercriminales suelen ser muy persuasivos mediante técnicas de manipulación e ingeniería social. Simplemente cuelga y bloquea el número.

Si no estás seguro

"POR TELÉFONO NUNCA ACEPTES NADA"