



¿CÓMO PROTEGERTE?

- ☛ **Desconfía de cualquier llamada que te pida datos sensibles.**
- ☛ **Cuelga y llama tú al número oficial del banco para verificar.**
- ☛ **El banco nunca te va a solicitar contraseñas ni códigos por teléfono.**
- ☛ **No instales software** a petición de una llamada telefónica.

¿QUÉ HACER SI YA HAS CAIDO?

- ☛ **Contacta inmediatamente** con el banco.
- ☛ **Cambia contraseñas** de banca online.
- ☛ **Denuncia la estafa** a la Policía Nacional.
- ☛ **Conserva cualquier prueba**, grabación o registro de llamadas.
- ☛ **Acude a tu Asociación de Consumidores.**

☎ **Si tienes dudas, consulta a tu Asociación de Consumidores ACTORA CONSUMO.**

¡Estamos para ayudarte!

Tlf: 976211321



11:00



Vishing

Llamada entrante...



Rechazar



Contestar

11:00



<  **Estafador**
Suplantando banco



Buenos días, le llamamos del Departamento de Seguridad de [Nombre del Banco]. Hemos detectado movimientos sospechosos en su cuenta. ¿Puede confirmarme si acaba de realizar un cargo de **850 euros** en [una plataforma extranjera por ejemplo]?

(El estafador genera alarma para que la víctima actúe rápido y no piense.)

No, yo no he hecho ningún pago de ese tipo.

Perfecto, entonces alguien ha intentado usar su tarjeta sin autorización. Para bloquear la operación necesito confirmar con usted unos datos de seguridad. ¿Tiene a mano su tarjeta?

(Aquí buscan que la víctima dé datos sensibles: número de tarjeta, CVV, fecha de caducidad, etc.)

Sí, la tengo.

Muy bien, por favor, dígame los 16 dígitos completos de su tarjeta y la fecha de caducidad. Con eso podemos proceder a la anulación.

(En realidad, lo están recopilando para operar en su nombre.)

(Da los datos.)



11:00



<  **Estafador**
Suplantando banco



Gracias. Ahora el sistema me pide un **código de confirmación** que usted va a recibir en unos segundos por SMS. Es para bloquear la transacción. Por favor, léamelo en cuanto lo reciba.

(Ese código en realidad es de la operación fraudulenta que el estafador está intentando confirmar en la banca online.)

Ya me ha llegado, es el xxxxxxxx

Perfecto, ya está todo solucionado. En unas horas verá reflejado el bloqueo en su cuenta. Muchas gracias por su colaboración.

(El estafador ya ha completado la transacción y el dinero ha salido de la cuenta.)

**¡AVISO!**

Es una estafa que se realiza por llamadas telefónicas. La persona que trata de estafar se hace pasar por empleado de banca o de algún organismo oficial y de manera muyyyy convincente intenta conseguir datos bancarios y confidenciales o que realices una transferencia.

Son capaces incluso de usar técnicas por las que suplantán el número real de la entidad bancaria.