“SMISHING” BANCARIO POR SMS

El SMISHING (combinación de las palabras SMS y Pishing) es el intento de fraude para obtener información personal, financiera o de seguridad a través de un mensaje de texto.

¿Cómo lo hacen?

A tu teléfono celular llega un mensaje … El mensaje de texto te pedirá que hagas clic en un enlace o que llames a un teléfono para “verificar”, “actualizar” o reactivar tu cuenta. Pero, el enlace te lleva a una página web falsa, y el número de teléfono es el de un estafador que suplanta a una empresa.

¿Cómo evitar ser víctima del Smishing?

1. Ninguna institución financiera o empresa te enviará un SMS que te pida actualizar la información de tu cuenta o confirmar el código de tu tarjeta de cajero automático. En caso de recibir un mensaje de este estilo, llama a tu banco o a la empresa si tienes dudas.
2. Nunca hagas clic en un enlace o número de teléfono de un mensaje del que no estás seguro o conozcas su procedencia.
3. No guardes información bancaria en tu dispositivo móvil.
4. Ante la duda, no respondas a los SMS.
5. Desconfía de los SMS que te hablan de trabajos (que no existen), premios (sin haber jugado) o paquetes recibidos (sin haberlos pedido).
6. Vigila regularmente el consumo que realizas, en caso de notar incrementos notables en la factura, contacta con la operadora telefónica.