Cómo prevenir el fraude de acceso remoto

Los ciberdelincuentes utilizan técnicas cada día más evolucionadas para realizar fraudes y estafas.

Mediante el envío de SMS, correos electrónicos o llamadas inesperadas, suplantan la identidad de la entidad y te alertan de incidencias falsas que están ocurriendo en tus cuentas.



Con la excusa de realizar una acción como anular una operativa sospechosa, o revisar la supuesta incidencia, solicitan que les des acceso remoto o que compartas tu pantalla para ayudarte a resolverlas.

Consejos para protegerte antes estas estafas

Desconfía de los SMS que contengan enlaces; **no introduzcas tus datos ni descargues archivos adjuntos**, podría tratarse de un malware

No facilites tus contraseñas, claves y datos personales o financieros, ya sea a través de un enlace o en una llamada

Nunca te pediremos que **realices o firmes una operación** que no quisieras iniciar

No compartas pantalla a través del control remoto. No te pediremos que instales o utilices este tipo de aplicaciones

Si desconfías de la llamada, cuelga y ponte en contacto con tu gestor

Recuerda: no compartas tus datos, ni facilites tus claves de acceso a la Banca Online o los datos de pago de tus tarjetas

¿Quieres saber más?

Conoce los principales riesgos a los que puedes estar expuesto