CajaIngenieros
BANCA COOPERATIVA

Humanizamos tus finanzas

¡EVITA LA TRAMPA!

10 consejos básicos de ciberseguridad

Con la colaboración de Selva Orejón



Los fraudes digitales son cada vez más sofisticados y cualquier persona puede ser víctima de los ciberdelincuentes en algún momento. Conocer cómo actúan y saber **identificar las señales de alerta** es el primer paso para proteger nuestros datos y nuestro dinero.

¿Cómo consiguen ganarse nuestra confianza? ¿Qué señales deberían hacernos sospechar?

Desde Caja Ingenieros, **con la colaboración de Selva Orejón**, consultora experta en ciberseguridad e identidad digital, queremos ayudarte a conocer las trampas digitales más habituales, aprender a identificarlas y, sobre todo, **saber cómo evitarlas.**

Porque, aunque tienen nombres tan curiosos como *phishing, smishing, vishing* o *quishing*, estas estafas son, desgraciadamente, mucho más habituales de lo que pensamos.

¡Ten siempre presentes estos 10 consejos y no bajes nunca la guardia!



1 Correos electrónicos y *phishing*: no te dejes engañar

El *phishing* consiste en **correos electrónicos que imitan la imagen de una entidad bancaria** para conseguir tus claves de acceso, datos de la tarjeta o códigos de verificación. A menudo utilizan **mensajes urgentes**, como «Tu cuenta será bloqueada», con enlaces a páginas web falsas que parecen auténticas.

No accedas a la banca a través de enlaces de correos sospechosos. Entra directamente en la web oficial o en la aplicación de Caja Ingenieros. Y recuerda que nunca te pediremos la contraseña completa, el PIN o los códigos de verificación por correo electrónico.

2 SMS y *smishing*: cuidado con los mensajes que parecen de tu banco

El *smishing* utiliza **SMS fraudulentos que suplantan a una entidad bancaria.** Pueden incluir datos personales reales para resultar más creíbles y pedirte que hagas clic en un enlace para resolver una incidencia urgente.

Desconfía de los mensajes que te pidan datos personales, claves o códigos. No hagas clic en los enlaces y comprueba cualquier aviso directamente a través de los canales oficiales de Caja Ingenieros.

3 Llamadas y *vishing*: no te fíes de quien te llama

El *vishing* es una estafa telefónica mediante la cual **alguien se hace pasar por un profesional del banco**, con un tono urgente y convincente, para conseguir datos confidenciales o hacer que autorices una operación.

Nunca facilites por teléfono contraseñas, PIN ni códigos de un solo uso. Si tienes dudas, cuelga inmediatamente y llama a Caja Ingenieros a través de nuestros canales oficiales.

4 Códigos QR y *quishing*: no todos te llevan adonde esperas

El *quishing* consiste en utilizar **códigos QR manipulados, a menudo pegados sobre códigos legítimos** en carteles, aparcamientos o establecimientos, que te dirigen a páginas fraudulentas.

Antes de abrir un enlace, comprueba la dirección web que aparece al escanear el código. Desconfía de los QR manipulados o que te pidan datos bancarios de forma inesperada.

5 Inteligencia artificial: no todo lo que ves u oyes es real

Con la inteligencia artificial se pueden **clonar voces, manipular vídeos** (*deepfakes*) y **crear perfiles o conversaciones que parecen auténticos.** Los estafadores pueden simular la voz de un familiar que necesita dinero urgentemente o utilizar a personas conocidas para promocionar inversiones falsas.

Si recibes una petición urgente, aunque reconozcas la voz o la imagen, no actúes inmediatamente. Contacta con la persona a través de un número que ya tengas guardado y confirma que la petición es real. O pregúntale por algo que solo vosotros conozcáis.

6 Inversiones fraudulentas: demasiado buenas para ser verdad

Los llamados ***chiringuitos financieros*** son **entidades que ofrecen servicios de inversión sin la autorización correspondiente**. A menudo contactan por WhatsApp, Telegram o redes sociales y prometen rentabilidades muy elevadas, rápidas y sin riesgo. Evidentemente, falsas.

Identifica estas **señales de alerta**: contactos inesperados con ofertas de inversión, rentabilidades muy altas y «garantizadas», presión para invertir o reinvertir rápidamente, plataformas con ganancias aparentemente crecientes, pero imposibles de verificar... Antes de invertir, comprueba si la entidad está autorizada a través de la CNMV (cnmv.es). Y, si tienes dudas, consulta con Caja Ingenieros.







7 **Banca digital y compras:** opera siempre con seguridad

Operar desde webs poco fiables, utilizar redes Wi-Fi públicas o comprar en tiendas en línea fraudulentas **puede poner en peligro tus datos bancarios y tu dinero**.



Cuando operes con tu dinero en Internet, toma algunas precauciones básicas.

- Accede a BancaONLINE solo desde la web oficial o desde la app de Caja Ingenieros.
- Evita las redes Wi-Fi públicas para realizar operaciones bancarias.
- Revisa periódicamente los movimientos de tus cuentas.
- Cierra la sesión cuando termines de operar.
- Compra solo en webs de confianza, consulta las opiniones sobre el vendedor y utiliza métodos de pago seguros.

8 **Identidades falsas e ingeniería social:** cuando la confianza es la trampa

La ingeniería social es una técnica que utilizan los ciberdelincuentes para **manipular tu confianza**. Pueden hacerse pasar por un vendedor, un asesor financiero o incluso un familiar para conseguir dinero o información personal.

Desconfía de las peticiones inesperadas de dinero o datos, **especialmente si van acompañadas de presión o urgencia**. Antes de hacer nada, verifica siempre la identidad de quien te lo pide llamando directamente a esa persona.

9 **Contraseñas y dispositivos:** pon barreras a los ciberdelincuentes

Las **contraseñas poco seguras**, los **dispositivos desprotegidos** o las **aplicaciones desactualizadas** pueden facilitar que los ciberdelincuentes accedan a tus datos personales y a tus cuentas.





Proteger tus cuentas y dispositivos es esencial para **evitar accesos no autorizados**.

- Utiliza contraseñas largas, robustas y diferentes para cada servicio.
- Activa la verificación en dos pasos, especialmente en el correo electrónico.
- Bloquea el móvil con PIN, patrón o identificación biométrica.
- Mantén los dispositivos y las aplicaciones actualizados.
- No descargues archivos de fuentes desconocidas.
- Activa Face ID en la app de Caja Ingenieros, si el dispositivo lo permite.
- No compartas las contraseñas con nadie.

10 **Y en todos los casos:** si sospechas de un fraude, actúa rápidamente

Cuando se produce un fraude digital, los ciberdelincuentes **pueden actuar en cuestión de minutos**. Por eso, detectar cualquier movimiento sospechoso y reaccionar rápidamente es fundamental para limitar sus consecuencias.

Ante una operación sospechosa, **el tiempo es clave**.

- Contacta inmediatamente con Caja Ingenieros si detectas una operación que no reconoces.
- Si sospechas que han utilizado tu tarjeta, desactívala desde BancaONLINE o BancaMOBILE.
- Si crees que alguien ha accedido a tus cuentas, comunícalo a la entidad para que pueda aplicar las medidas de protección adecuadas.
- Llama al 017 de INCIBE, el servicio gratuito de ayuda en ciberseguridad.
- Consulta periódicamente los avisos y las recomendaciones de seguridad de Caja Ingenieros.





GRUPO CajaIngenieros
BANCA COOPERATIVA

Humanizamos tus finanzas

¿Quieres conocer las últimas tendencias en fraude y estafas?

Visita nuestro espacio de seguridad en la web de Caja Ingenieros y descubre más consejos y recomendaciones para protegerte de los fraudes digitales.

Infórmate sobre nuestro Seguro Protección Digital.