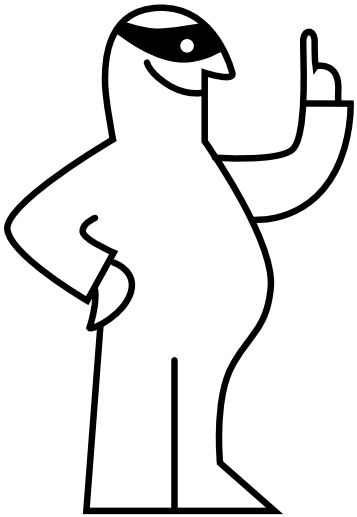
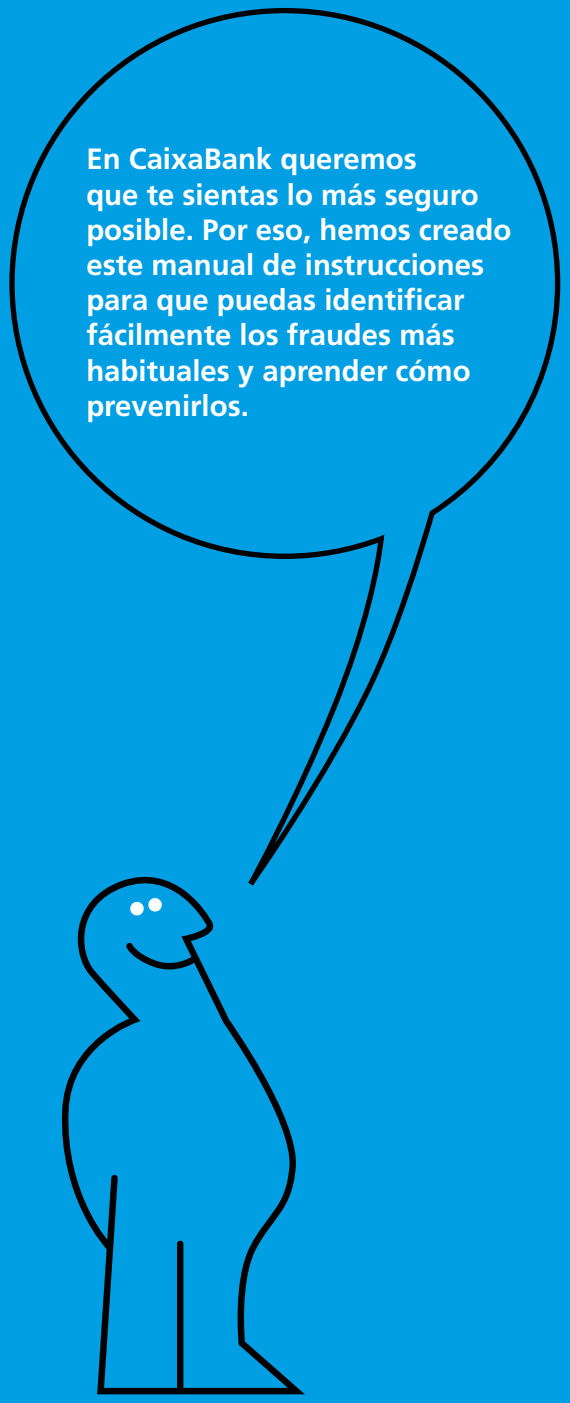
¿CÓMO PROTEGERSE DE LOS FRAUDES?

MANUAL DE INSTRUCCIONES



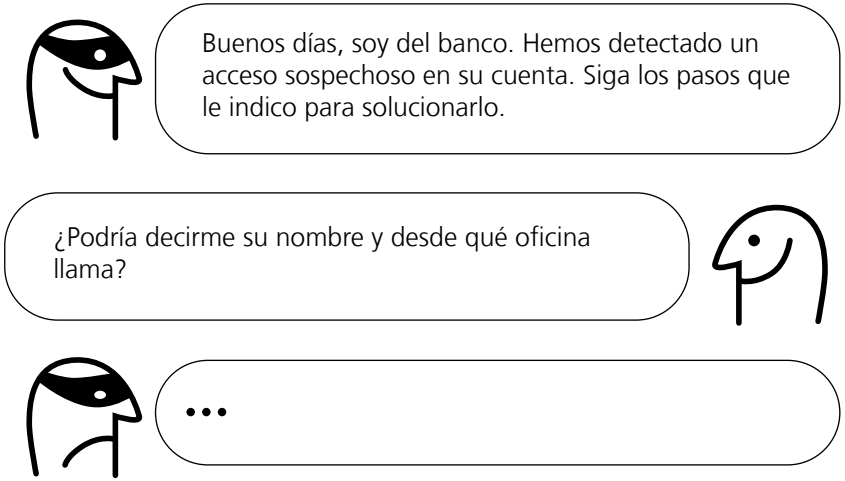
CaixaBank



1

Llamadas telefónicas inesperadas

Desconfía de aquellas llamadas en las que te pidan hacer transferencias, firmar operaciones o compartir datos personales o bancarios, o en las que te ofrezcan grandes rentabilidades, beneficios o descuentos. Sospecha si te dicen que tienes cualquier problema con tu cuenta, pero que te van a ayudar a solucionarlo si sigues los pasos que te indican.



Nunca facilites tus claves ni firmes operaciones por teléfono. Ante cualquier llamada sospechosa, cuelga y llama tú al número oficial.

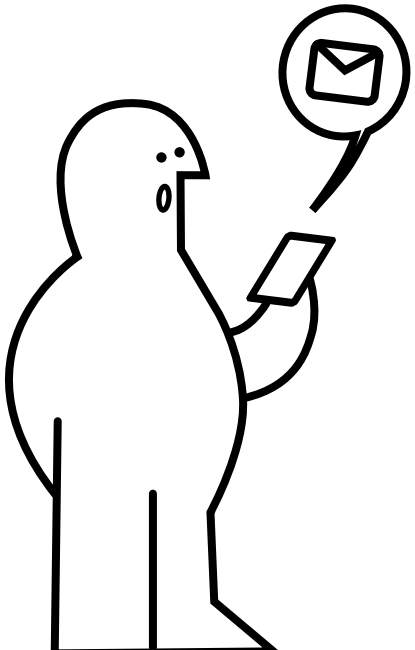
2

E-mails y mensajes sospechosos

Si te piden actuar con urgencia, hacer transferencias o facilitar datos personales o bancarios haciendo clic en un enlace o documento, no lo hagas. Desconfía siempre, aunque parezcan enviados por un familiar o alguien conocido.

CaixaBank: Su cuenta ha sido bloqueada. Active el acceso en *bit.ly/caixalogin*

Qué raro… el enlace no parece oficial.



No pulses enlaces sospechosos ni de remitentes dudosos. Accede siempre desde la *app* o la web oficiales.

3

Alguien te pide tus contraseñas

No las compartas nunca ni las anotes en ningún lugar accesible: son personales e intransferibles.

Su cuenta será bloqueada en 10 minutos. Envíenos su clave para evitarlo.

Si me presionan con urgencias…, mala señal.

Tu banco nunca te pedirá claves por mensaje, *e-mail* ni teléfono.

4

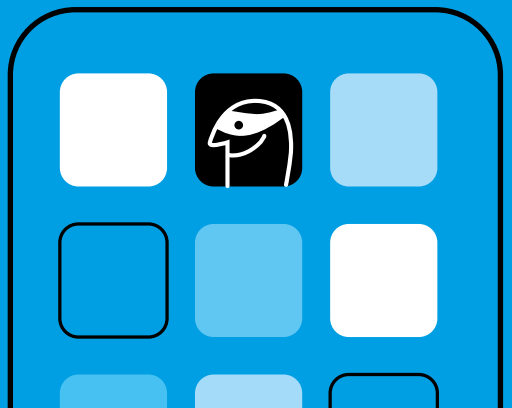
Te piden instalar un programa o una *app*

Por muy convincente que sea el motivo, no los descargues nunca en tus dispositivos a petición de desconocidos, ni permitas que nadie tome el control de ellos.

Le vamos a enviar un enlace para instalar una *app* de asistencia para ayudarle. Pulse "Permitir control remoto" cuando se lo pida.

¿Control remoto? No lo había solicitado.

No instales nada ni permitas acceso remoto a desconocidos, aunque digan ser tu gestor. Si lo piden, es fraude.



5

Alguien te pide dinero

Sé prudente si alguien desconocido (o conocido por internet) te pide dinero bajo cualquier pretexto.

Mamá, se me ha roto el móvil. ¿Podrías enviarme dinero rápidamente?

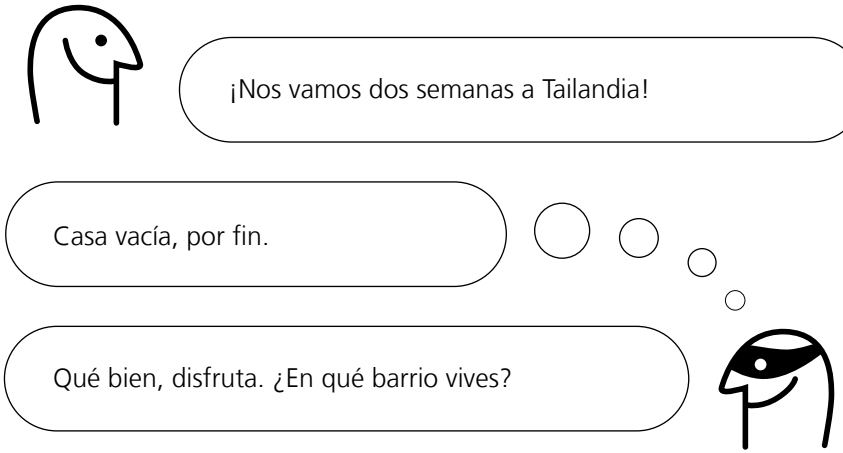
¿Eres tú? ¿Por qué escribes desde otro móvil?

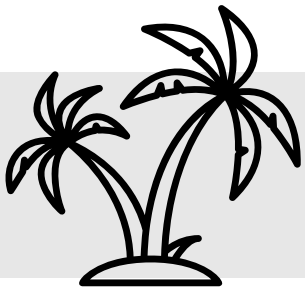
Si te piden dinero con urgencia, confirma la identidad por otro canal habitual.

6

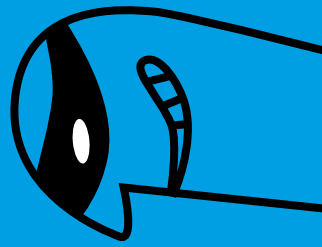
Ojo con lo que compartes en tus redes sociales

Protege tu información personal en las redes sociales: no compartas información personal o sensible y no aceptes a desconocidos.





Evita publicar información personal o de tus ausencias. Protege tu privacidad.

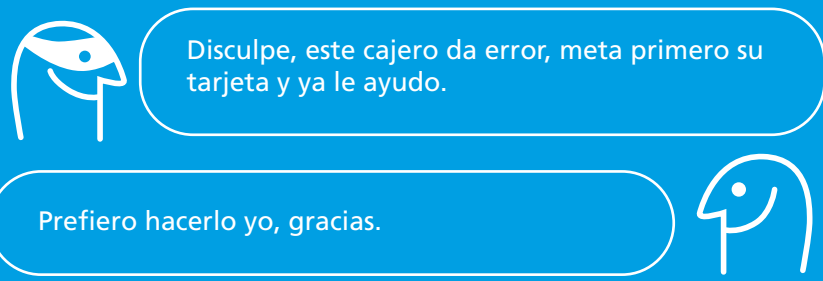


7

Cuando vayas a sacar efectivo del cajero

Procura que nadie se acerque ni te distraiga mientras retiras dinero. Si vas a sacar una cantidad importante, mejor que alguien de confianza te acompañe. Y guarda el dinero en un lugar discreto.

Si ves algún elemento extraño en el cajero o sospechas que está manipulado, no lo uses. Contacta con el teléfono de atención al cliente o con un empleado.

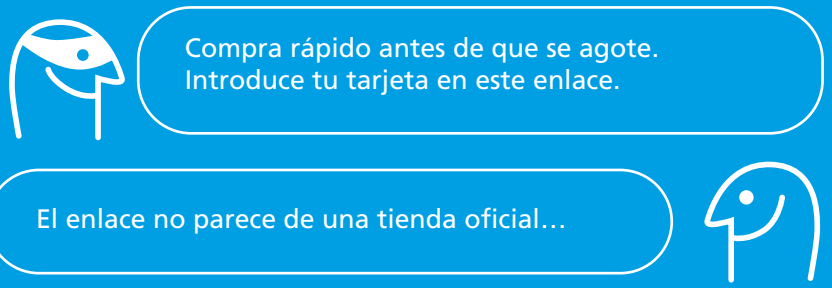


No aceptes ayuda en el cajero. Si notas algo raro, cancela la operación y usa otro.

8

Si vas a comprar *on-line*

Cuidado con los "chollos". En internet, los ciberdelicuentes intentan seducirnos con superofertas. Asegúrate de comprar únicamente en webs oficiales, revisa las opiniones de otros usuarios y evita realizar los pagos fuera de los métodos que ofrece la página web o aplicación.

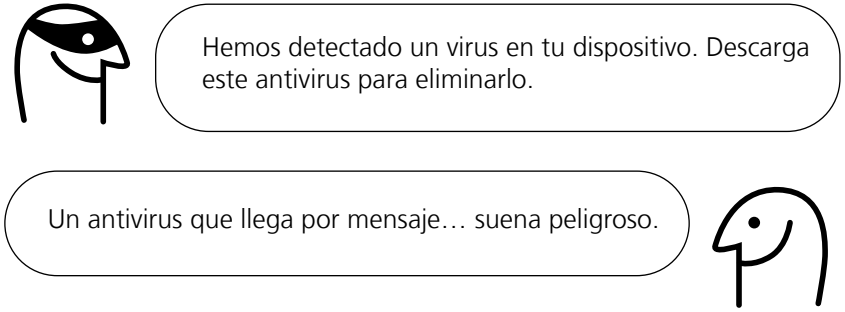


Si algo es demasiado bueno o excesivamente barato, lo más seguro es que sea un fraude.

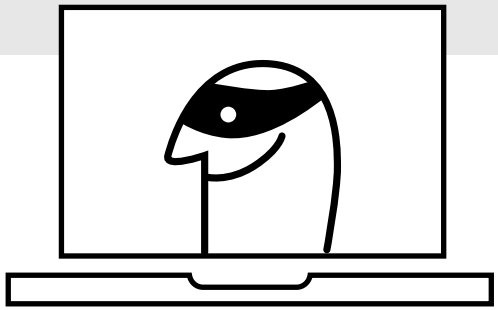
9

Protege tus dispositivos

Mantén tus dispositivos y aplicaciones actualizados e instala un antivirus. Configura el bloqueo de pantalla y utiliza siempre contraseñas seguras para tus aplicaciones. Descarga solo aplicaciones oficiales desde tiendas autorizadas.



Los ciberdelincuentes pueden usar *apps* falsas para controlar tu dispositivo y robar tus datos.



10

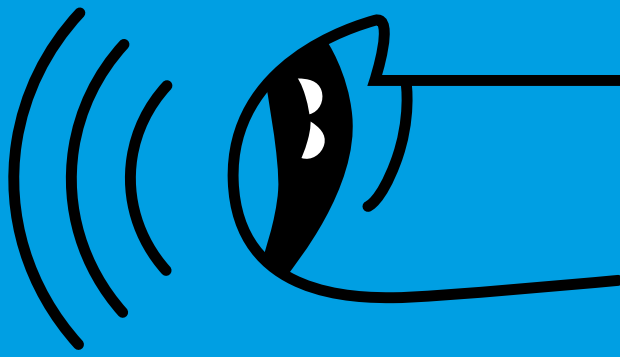
Cuidado con las redes wifi gratuitas y los QR

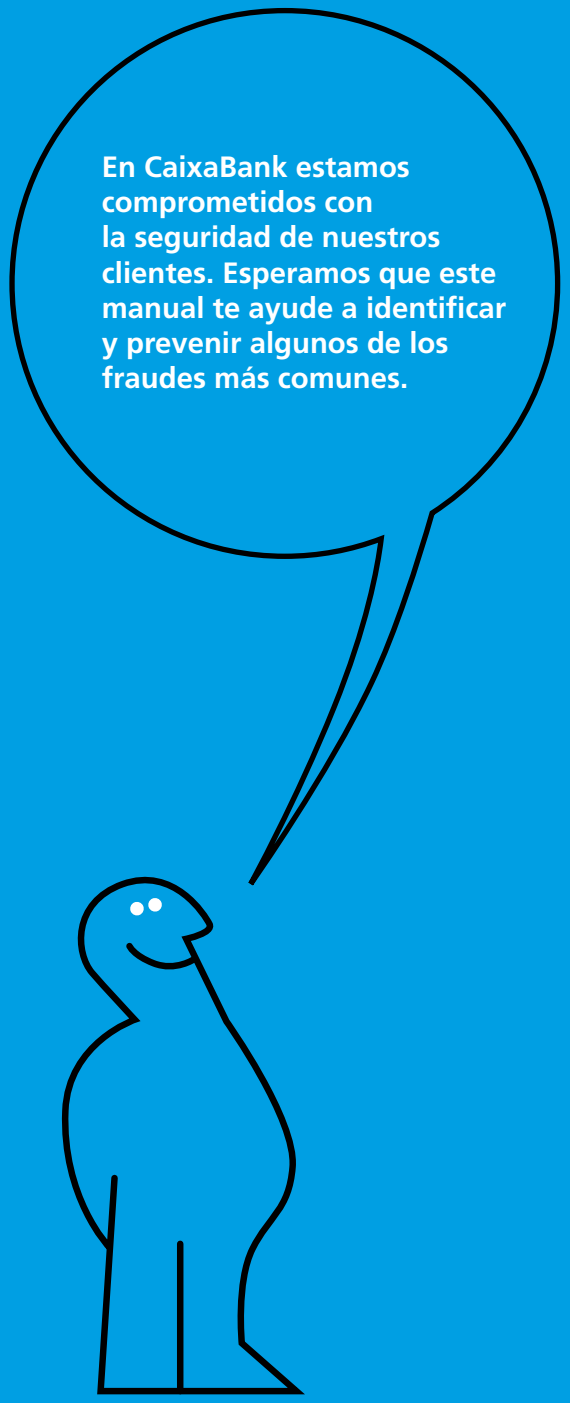
Desconfía de QR que te llevan a páginas web y te piden datos personales: no los facilites nunca. Evita también usar redes wifi públicas cuando necesites acceder a webs o aplicaciones que requieran datos personales o financieros.

Para seguir navegando, introduce tus datos bancarios. Es solo un control rutinario de seguridad.

¿Datos bancarios para usar el wifi? Esto no tiene sentido…

No introduzcas nunca tus claves ni accedas a la banca *on-line* desde redes wifi de lugares públicos. Los ciberdelincuentes pueden crear redes falsas para robar tus datos.





Recuerda:

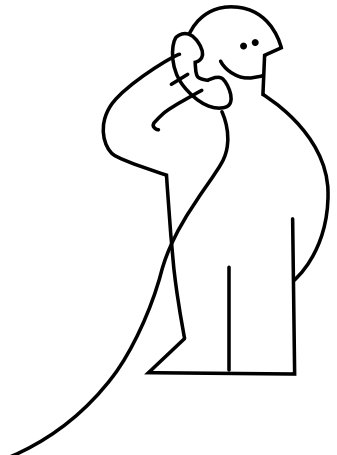
Utiliza siempre el **sentido común**.
Desconfía de **situaciones urgentes, inesperadas** o **"demasiado buenas"**.
Los estafadores buscan que actúes rápido y sin pensar.

Si ves algo raro, detente y piensa si tiene sentido lo que te piden. **Confírmalo con quien te hace la petición usando los canales oficiales para salir de dudas**.

Si sospechas que has podido ser víctima de un fraude, **ponte de inmediato en contacto con CaixaBank** o con tu gestor.

Atención al Cliente:
938 872 525
Las 24 horas del día, los 7 días de la semana

Atención al Cliente Sénior:
938 872 524
Las 24 horas del día, los 7 días de la semana




CaixaBank