

## Decálogo de buenas pautas para prevenir el fraude en el acceso a la banca digital

El acceso a los servicios bancarios que proporciona la banca electrónica requiere que los usuarios observen una serie de recomendaciones para prevenir ser víctimas de fraudes. Autoridades públicas como el Instituto Nacional de Ciberseguridad (Incibe), así como las propias entidades financieras, están siendo las primeras en promover un conjunto de buenas pautas para protegerse frente a los ciberdelincuentes.



En primer lugar, debe advertirse que los intentos de fraude de los que pueden ser objeto los clientes bancarios no son exclusivos de este sector. En este sentido, las pautas aplicables al buen uso de la banca digital pueden extrapolarse a cualquiera de las actividades que los usuarios realicen *online*

(como compras en comercios electrónicos, interacciones en redes sociales o contratación de cualquier otro servicio digital). Aunque las prácticas maliciosas que pueden llevar a cabo los ciberdelincuentes son variadas (robos de contraseñas, suplantaciones de identidad, incitación de acceso a falsas webs bancarias) existen una serie de procedimientos de actuación muy útiles para estar protegido frente a todas ellas.



Puede establecerse un decálogo de buenas conductas para los usuarios:

1. Mantenga actualizada la aplicación móvil de su banco y el sistema operativo de su ordenador o *smartphone*.

2. Instale en su ordenador y/o móvil un antivirus, que debe estar actualizado, y compruebe que está siempre activo.
3. Preferiblemente, conéctese desde una red segura, siendo las mejores opciones el ordenador de casa o del trabajo. Es recomendable evitar conectarse a la banca electrónica usando ordenadores o redes *wifi* públicas.
4. No abra correos de usuarios sospechosos, aunque estos parezcan proceder de su entidad bancaria.
5. En el caso de que reciba un correo electrónico que procede de una entidad bancaria legítima, debe tener presente que nunca contendrá enlaces a su página de inicio de sesión o documentos adjuntos.
6. Nunca revele las contraseñas a través de email, SMS o WhatsApp. Las entidades bancarias nunca le pedirán las claves por estos medios.



7. Preferiblemente, no acceda nunca a la banca electrónica desde enlaces o anuncios en buscadores. Es recomendable escribir la dirección web del banco directamente en la barra del navegador.
8. En caso de que tenga dudas acerca de la autenticidad del acceso, consulte antes de iniciar sesión con su banco.
9. Antes de acceder a la banca electrónica, compruebe que el sitio web es seguro. Para ello es fundamental buscar el "candado" junto a la URL y examinar que las credenciales son válidas haciendo clic en él. Además, compruebe siempre que la dirección comienza con "https://."
10. Después de haber realizado las gestiones en su banca electrónica asegúrese de haber cerrado adecuadamente la sesión.

Asimismo, para una mayor seguridad, los usuarios de



la banca digital pueden acceder al servicio de notificaciones y alertas de seguridad que Incibe ha puesto en marcha.<sup>1</sup> Este servicio permite que cualquier usuario digital esté alerta de todas las posibles amenazas.

---

<sup>1</sup> Avisos de seguridad. Incibe.  
<https://www.incibe.es/protege-tu-empresa/avisos-seguridad>