



El Banco Central advierte que no solicita datos personales o bancarios por ningún medio. Si detectás un perfil falso del Banco Central o de otra entidad podés reportar la cuenta como spam directamente en la aplicación para alertar sobre posibles estafas. También podés comunicarte con la Unidad Fiscal Especializada en Ciberdelincuencia (UFECI) para denunciar este tipo de fraudes.



“



Qué hacer si detectás un fraude virtual o un engaño:

Podés comunicarte con la Unidad Fiscal Especializada en Ciberdelincuencia (UFECI).
Dirección: Sarmiento 663, 6° Piso, CABA

Teléfono: (+54 11) 5071-0040 / 0041

Correo electrónico: denunciasufeci@mpf.gov.ar
Si recibís información o mensajes que simulan ser del Banco Central podés reenviarlos a Ayuda en Línea (ayudaenlinea@bcra.gov.ar).



SU
BANCO

ALERTA!!
Evite estafas por medios electrónicos





COMO PROTEGER TU INFORMACION

-Activa la autenticación de dos factores en tus cuentas de redes sociales, WhatsApp u otras plataformas digitales que utilices.

- No proporciones ningún dato personal (nombre de usuario, contraseñas, PIN, Clave de la Seguridad Social, Clave Token, número de identificación personal, foto, u otros datos) por teléfono, correo electrónico, redes sociales, WhatsApp o mensajes de texto.

- No ingreses datos personales en sitios web a través de enlaces recibidos por correo electrónico, ya que podrían ser fraudulentos.

- Utiliza contraseñas seguras que combinen mayúsculas, minúsculas y números. Deben ser fáciles de recordar pero difíciles de adivinar para otras personas.

- No utilices la misma contraseña para diferentes aplicaciones, cuentas, plataformas o sitios web.

No utilices la misma contraseña para diferentes aplicaciones, cuentas, plataformas o sitios web.

- Lee cuidadosamente cada correo electrónico que recibas. Asegúrate de que los remitentes sean legítimos.

- Ten precaución con los enlaces sospechosos y siempre asegúrate de estar en la página legítima antes de proporcionar información de inicio de sesión.

- Evita utilizar equipos públicos o de terceros para acceder a aplicaciones, redes sociales o cuentas personales.

- No utilices redes Wi-Fi públicas para acceder a sitios web que requieran contraseñas.

- Mantén actualizado tu navegador, el sistema operativo de tus dispositivos y las aplicaciones (elimina aquellas que no utilices).

