Comunicado

Recomendaciones del BCRA para evitar estafas virtuales

Las estafas virtuales son cada vez más frecuentes y sus modalidades cambian de manera constante. Para evitar ser víctimas de una ciberestafa, el Banco Central de la República Argentina (BCRA) recuerda a las personas usuarias de servicios financieros que es clave proteger su información personal y adoptar buenas prácticas para prevenir fraudes y robos de identidad.

Importante: el Banco Central nunca se comunica directamente con clientes bancarios para solicitar datos personales o bancarios, ya sea por teléfono, correo electrónico, mensajes de texto o redes sociales. El BCRA no ofrece servicios bancarios ni financieros al público general. Tampoco pide información de cuentas, ni claves de acceso a redes sociales, ni datos personales para realizar trámites o gestiones ante alguna entidad bancaria.

Recomendaciones:

- No compartir información personal ni bancaria. Los bancos y organismos públicos nunca solicitan la modificación de datos personales o claves, ni la entrega de códigos de verificación recibidos por ningún medio.
- No abrir enlaces enviados por WhatsApp o Telegram, aunque el número tenga el nombre “Mesa de ayuda” o una imagen de perfil similar a la de una billetera digital, entidad bancaria o empresa conocida.
- Ante llamados telefónicos, mensajes de WhatsApp o Telegram, mensajes de texto o correos electrónicos ofreciendo algún servicio financiero como un préstamo, no responder de inmediato. Comunicarse directamente con esa entidad por sus canales oficiales para verificar su autenticidad.
- No responder mensajes que mencionen errores en transferencias. Si alguien se contacta por un supuesto error, no brindar información y consultar directamente al banco.
- No operar con el cajero automático, la app o el *home banking* si se está en comunicación con un presunto representante del banco. En esos casos, cortar la llamada y verificar por los canales oficiales.
- Activar el doble factor de autenticación en todas las aplicaciones.
- Elegir contraseñas seguras y cambiarlas con frecuencia.
- No aceptar la sugerencia de guardar las contraseñas en el navegador.
- Evitar el uso de redes públicas y desactivar bluetooth, wifi o NFC para que los dispositivos no se conecten automáticamente.
- Verificar los remitentes de los correos electrónicos recibidos porque suelen ser engañosamente muy parecidos a los de las entidades bancarias.

¿Cómo denunciar? ¿Qué hacer al detectar un fraude virtual o un engaño?

Contactar lo antes posible al banco o entidad financiera.

Realizar la denuncia ante la Unidad Fiscal Especialidad en Ciberdelincuencia (UFECI) escribiendo a: denunciasufeci@mpf.gob.ar.

Martes 5 de agosto de 2025