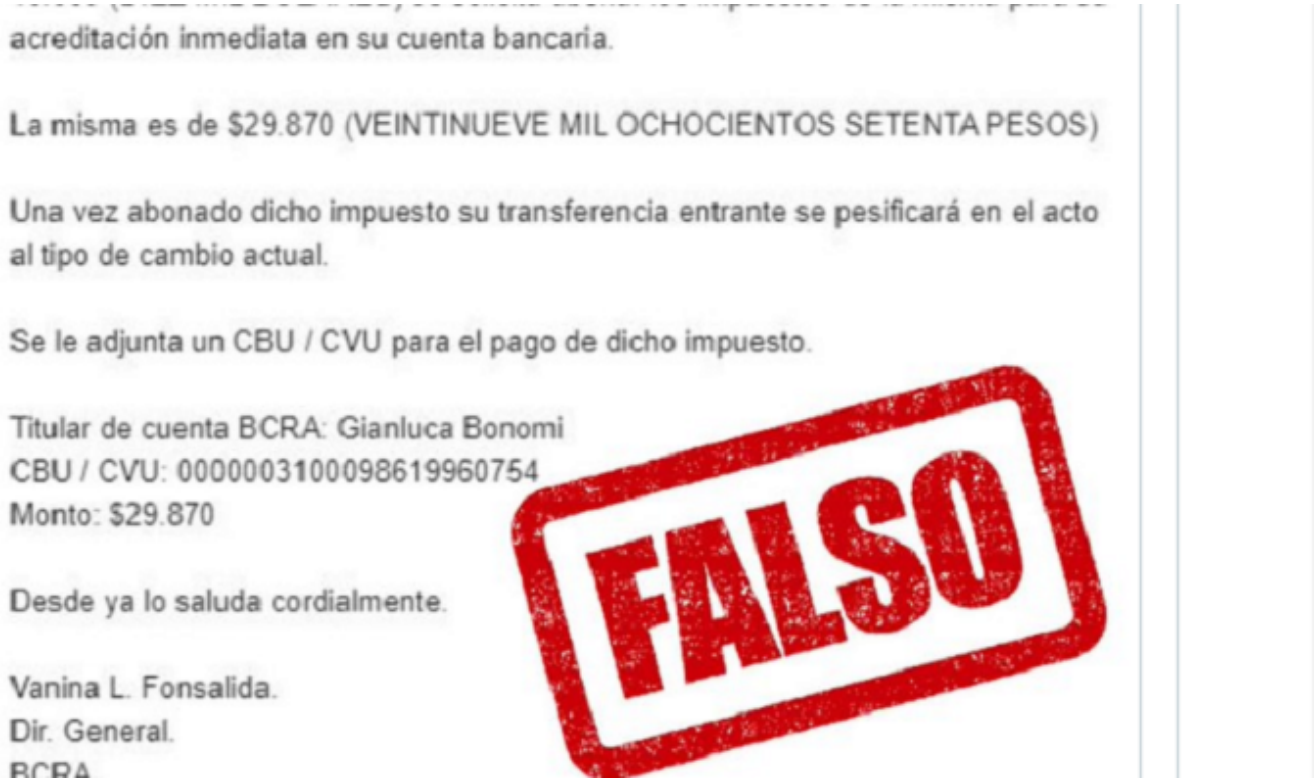
¡Atención! El Banco Central alerta sobre una nueva forma estafa virtual: cómo evitar ser engañado

27 abril, 2021



Aclararon que es importante no responder los mensajes.

Este lunes, el Banco Central de la República Argentina (BCRA) advirtió sobre una nueva modalidad de estafa bancaria difundida a través de correos electrónicos y mensajes de texto que simulan ser de la entidad con el objetivo de poder acceder a las cuentas bancarias de las víctimas.

El comunicado que se envía desde una casilla de mensajería falsa, llega a clientes del banco alertando sobre “una falla” en las transferencias e invita a que resuelvan la situación abonando una suma de dinero correspondiente a “impuestos”.

Frente a esta situación, el Banco Central aclaró que no se

comunican con clientes mediantes correos, ni mensajes e informaron que estos avisos son una nueva práctica ilegal.

"*Desde el BCRA no te contactaremos por correo electrónico ni ningún otro medio para hacer reclamos de impuestos o pagos pendientes. Los avisos sobre supuestos errores al realizar transferencia son una nueva práctica ilegal detectada. Los correos electrónicos que simulan ser legítimos (#phishing), llamados y mensajes de texto falsos (#smishing) son técnicas habituales para estafar. Es importante que no respondas estos mensajes y te comuniques con tu banco a través de los medios oficiales que te ofrece. Quienes realizan estafas informáticas usan métodos de ingeniería social para engañarte*", comunicaron desde la entidad.

> *Detectamos un nuevo correo electrónico con una nueva modalidad de estafa virtual.*
> *Tiene la firma del BCRA pero es falso*
> *pic.twitter.com/RpjxZdQ04z*
>
> *— BCRA (@BancoCentral_AR) April 26, 2021*

Por otro lado, compartieron **recomendaciones para evitar estafas**:

Cómo prevenir estafas virtuales

Los canales de comunicación a través de medios digitales cobraron protagonismo indiscutible a partir de la pandemia. En este contexto, se perfeccionan cada vez más rápido **las modalidades de estafas y fraudes: perfiles falsos en redes sociales que envían mensajes directos, llamadas telefónicas, mensajes de texto o de *WhatsApp* y otras aplicaciones de mensajería, además de correos electrónicos engañosos para obtener datos personales y bancarios**.

Ante esta situación, recordá que desde el Banco Central no te contactaremos de ninguna manera para pedir datos personales o

bancarios.

Recomendaciones para proteger tu información personal

El desafío en este escenario es proteger tu información personal y adoptar buenas prácticas para el uso de redes sociales, sitios y plataformas digitales.

1. **Activá la autenticidad de dos factores** en cuentas de redes sociales y *WhatsApp* o las plataformas digitales que utilices. Esta herramienta es una capa adicional de seguridad que ayuda a verificar que solo la persona usuaria de la cuenta pueda acceder a sus redes sociales y plataformas digitales. Se activa ingresando al menú de ajustes o configuración de la cuenta que se quiere proteger, opción "Autenticación en dos pasos".
2. **No brindes ningún dato personal** (usuarios, claves, contraseñas, pin, Clave de la Seguridad Social, Clave Token, DNI original o fotocopia, foto, ni ningún tipo de dato), **por teléfono, correo electrónico, red social, *WhatsApp* o mensaje de texto**.
3. **No ingreses datos personales en sitios por medio de enlaces que llegan por correo electrónico**, podrían ser fraudulentos.
4. **Usá contraseñas fuertes** mezclando mayúsculas, minúsculas y números. Tienen que ser fáciles de recordar pero difíciles de adivinar por otras personas. No uses la misma clave para distintas aplicaciones, cuentas, plataformas o sitios.
5. **Leé cada correo electrónico recibido con cuidado**. Verificá que los sitios remitentes sean legítimos.
6. **Tené cuidado con los enlaces sospechosos y asegurate siempre de estar en la página legítima** antes de ingresar información de inicio de sesión.
7. **No uses equipos públicos o de terceras personas para acceder a aplicaciones, redes sociales o cuentas personales**.
8. **No uses redes de *wi-fi* públicas para acceder a sitios**

que requieran contraseñas.

9. **Mantené actualizado el navegador, el sistema operativo de tus equipos y las aplicaciones** (borrá las que no uses).
10. Siempre hay que **tomarse un minuto antes de actuar**. Quienes realizan este tipo de estafas apelan a las emociones, descuidos y urgencias.
    #VosSosLaClave

¿Cómo diferenciar un perfil verdadero de uno falso en redes sociales?

-Los perfiles legítimos tienen una tilde azul de autenticidad.

-Los perfiles falsos generalmente solo tienen publicaciones muy recientes y poca cantidad de seguidores.

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.

Estos son los perfiles oficiales del Banco Central en plataformas digitales:

- Facebook: https://www.facebook.com/BancoCentralAR/
- Instagram: https://www.instagram.com/bancocentral_ar/
- LinkedIn: https://www.linkedin.com/company/bcra
- Twitter: https://twitter.com/bancocentral_ar y https://twitter.com/BCRAusuarios
- YouTube: https://www.youtube.com/channel/UCq1CEC9JxvblsszG71-CPKw
- Sitio web: https://www.bcra.gob.ar/

Otras modalidades de engaño o estafa frecuentes

¿Qué es el phishing?

Es un correo electrónico que aparenta ser legítimo que se utiliza para que la persona destinataria abra un enlace, complete formularios con información personal o descargue

archivos que contienen *malware* o programas maliciosos. En caso de recibirlo se recomienda eliminarlo inmediatamente.

¿Qué es el smishing?

Es una modalidad de estafa mediante mensajes de texto o cualquier aplicación de mensajería que tiene como objetivo obtener información privada. Al igual que los casos de *phishing* la recomendación es eliminar el mensaje.

¿Qué es el spoofing?

Es el uso de técnicas de suplantación de identidad. Hay diferentes tipos de spoofing, entre ellos el envío de correos electrónicos o páginas fraudulentas, falsificación de dispositivos o de direcciones IP. Independientemente del tipo, los ataques de *spoofing* son maliciosos. Es decir, quienes realizan este tipo de fraudes buscan hacerse pasar por otras personas, organizaciones o empresas para acceder a datos personales, distribuir *malware* o generar algún tipo de perjuicio.

¿Cómo denunciar? 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.gob.ar).