

Protéjase de las estafas

La confianza y la seguridad son la máxima prioridad en CommBank. Hemos observado un creciente número de casos en los que los estafadores presionan o engañan a los clientes para que les envíen dinero. Estas estafas pueden ser sofisticadas y adoptan varias formas. Es importante estar alerta y avisarnos si hay algo que le parezca extraño. Para saber más acerca de cómo protegerse y denunciar una estafa, consulte commbank.com.au/safe.

Autenticación y verificación

- Complete el filtro de seguridad en la aplicación de CommBank.
- Active el sistema de autenticación múltiple, el cual permite añadir un nivel extra de seguridad y verificar su identidad.
- Utilice **CallerCheck** (verificación de llamadas) para verificar la identidad de las personas que llaman diciendo ser del banco.
- Utilice **CustomerCheck** (verificación de clientes) en la sucursal bancaria para verificar su identidad ante nuestro personal.
- **NameCheck** (verificación de nombre) le indicará si la información de la cuenta de un pago realizado por primera vez parece sospechosa.

Seguridad de dispositivo y de pago

- Tenga actualizado el software antivirus y proteja su computadora de las amenazas más frecuentes.
- Utilice métodos de pago seguros, como son el pago por contacto o la inserción de la tarjeta.
- No comparta dispositivos que tengan acceso a su monedero digital.

Contraseña e información personal

- Nunca comparta su contraseña ni su PIN, y tenga cuidado al compartir información personal.
- Nunca proporcione su NetCode a nadie; esto también incluye al personal de CommBank.
- Puede cambiar la contraseña a través de NetBank y de la aplicación de CommBank en cualquier momento.
- Cree contraseñas seguras y cámbielas periódicamente. Para acceder a más recomendaciones acerca de la creación de contraseñas, consulte commbank.com.au/password-security.

Correo electrónico, mensajes de texto y conexión en línea

- No haga clic en enlaces de correos electrónicos o mensajes de texto sospechosos.
- Si no está seguro/a de un mensaje, hable con alguien en quien confíe o contacte con la organización directamente a través de los datos de contacto oficiales.
- Cuelgue si recibe llamadas telefónicas automatizadas, sospechosas o amenazantes de terceros.
- Sea prudente con los contactos desconocidos en las redes sociales y en las plataformas en línea.

Deténgase. Compruebe. Rechace.

Deténgase. ¿Hay algo extraño? En caso de duda, lo mejor es no continuar. Tómese su tiempo.

Compruebe. Consulte con alguien de su confianza o llame directamente a la organización a través de sus datos oficiales.

Rechace. Cuelgue la llamada, borre el correo electrónico, bloquee el número de teléfono. Cambie las contraseñas.

Si cree que ha sido víctima de una estafa, contacte inmediatamente con CommBank en el **13 22 21**, o en el **+61 2 9999 3283** si se encuentra en el extranjero.

Si el inglés no es su lengua materna, el Servicio de Traducción e Interpretación del Gobierno le puede ayudar a comunicarse con nosotros. Este servicio está disponible en más de 150 idiomas. Podemos organizarlo cuando nos llame o visite en cualquier sucursal.

Cosas que debe saber: nunca le enviaremos un correo electrónico pidiéndole información, como su código de verificación de cliente NetBank (NetBank Client ID), contraseñas o NetCode, ni incluiremos un enlace para acceder directamente desde un correo electrónico o mensaje de texto. Escriba siempre commbank.com.au en el navegador o utilice la aplicación CommBank para acceder de forma segura a su banca electrónica. Si hay algo que resulta sospechoso, remítalo a hoax@cba.com.au y bórralo. Commonwealth Bank of Australia ABN 48 123 123 124 AFSL y licencia australiana de crédito 234945.

Información importante sobre estafas



Inversión (Incluye criptomoneda)

Los estafadores captan a las personas con la promesa de altas rentabilidades, a menudo en forma de criptomonedas u otras oportunidades de inversión. Es posible que los estafadores intenten contactar con usted por teléfono, correo electrónico o por medio de plataformas de redes sociales.

Consejos para protegerse:

- Si parece demasiado bueno para ser verdad, probablemente lo sea.
- Sea prudente con las ofertas no solicitadas y la presión para invertir o actuar rápidamente.
- Primero verifique la legitimidad de la compañía o del bróker en el sitio web de ASIC.



Acceso remoto

Se da cuando un estafador le llama e intenta acceder a sus cuentas o a su dispositivo haciéndose pasar por un representante de una compañía u organización de confianza.

Consejos para protegerse:

- Nunca descargue software de acceso remoto si se lo solicitan o bajo presión de un tercero que llame.
- Siempre puede contactar con una compañía utilizando sus datos legítimos de contacto, que podrá encontrar en su sitio web oficial.
- Si recibe una llamada diciendo pertenecer a CommBank, nos puede solicitar que verifiquemos la llamada a través de la función de CallerCheck (verificación de llamadas) en nuestra aplicación.

Vulneración de correo electrónico profesional



Los estafadores abordan a empresas con correos electrónicos desde una dirección vulnerada, o desde correos electrónicos que parecen proceder de un contacto de confianza, como por ejemplo su asistente, cliente, abogado/a, gerente o proveedor.

Consejos para protegerse:

- Antes de efectuar pagos por primera vez o cambiar la información de pago, contacte con la organización llamando al número de contacto oficial para confirmar los datos.
- Utilice la función NameCheck (verificación de nombre) cuando efectúe pagos para comprobar si el titular de la cuenta coincide con el número BSB y de cuenta que le han proporcionado.
- Eduque a sus empleados/as para que sepan reconocer y denunciar cualquier intento de «phishing».

«Phishing» y «smishing»



Los estafadores utilizan correos electrónicos engañosos que pueden contener enlaces directos a un sitio web fraudulento o pueden solicitarle información personal.

Consejos para protegerse:

- No pulse en enlaces contenidos en correos electrónicos o mensajes de texto sospechosos.
- Puede confirmar la autenticidad de un mensaje contactando directamente con la organización por medio de sus métodos de contacto oficiales disponibles.
- Informe de cualquier mensaje sospechoso que provenga de CommBank a hoax@cba.com.au

Información importante sobre estafas



Relación

Los estafadores crean perfiles falsos para formar relaciones y manipular a sus víctimas para que les envíen dinero o información personal.

Consejos para protegerse:

- No envíe nunca dinero ni comparta sus contraseñas ni información bancaria con nadie en quien no confíe.
- Investigue a su potencial pareja por Internet o a través de Google o de aplicaciones de redes sociales. Intente hacer una búsqueda inversa de imágenes para identificar si otra persona es el dueño/a de las fotos que le han enviado.
- Hable con su familia y amistades sobre su relación en Internet. Pueden ofrecerle otra perspectiva e identificar las señales de alarma que quizás usted no haya advertido.

Oportunidad de empleo



Son ocasiones en las que aparece una oferta que requiere poco o ningún esfuerzo para conseguir grandes ganancias económicas, o le prometen que ganará dinero rápidamente.

Consejos para protegerse:

- Verifique la compañía y la oferta a través de los canales oficiales e investigue a dicha compañía para asegurarse de que es legítima y se encuentra en funcionamiento actualmente.
- Desconfíe de ofertas laborales a través de redes sociales, chats encriptados, correos electrónicos o cartas de personas o de compañías que desconoce.
- Una compañía legítima nunca le solicitará que haga un pago por adelantado ni utilizará sus datos bancarios para facilitarle fondos de la compañía o para comerciar.



Compras en línea

Los estafadores crean negocios por Internet o anuncios para atraer a clientes y hacerles comprar productos falsos o inexistentes.

Consejos para protegerse:

- Haga sus compras únicamente en sitios web reputados y seguros, y desconfíe de cualquier oferta que parezca demasiado buena para ser verdad.
- Utilice métodos de pago seguros y evite hacer transferencias directas a los vendedores.
- Tómese su tiempo y evite ser presionado/a con «ofertas limitadas» o rebajas «a punto de terminar».

Amenazas y multa



Los estafadores se hacen pasar por autoridades u organizaciones legítimas para extorsionar dinero por medio de amenazas de multas o acciones judiciales.

Consejos para protegerse:

- Cuelgue las llamadas amenazantes y contacte directamente con la organización.
- Una organización legítima nunca le pedirá que efectúe pagos a través de métodos poco comunes, como tarjetas regalo o de tiendas, cupones de iTunes, transferencias bancarias o Bitcoins.
- Si está preocupado por su seguridad, póngase en contacto con la línea de asistencia policial.

