Australian Banking Association

Manténgase a salvo:
esté atento a los engaños y fraudes

Es probable que las estafas y fraudes relacionados con la COVID-19 aumenten en los próximos meses.

Los estafadores utilizan correos electrónicos falsos, llamadas de teléfono o mensajes de texto para intentar obtener información personal. Simulan pertenecer a su banco, a la Organización Mundial de la Salud, al gobierno, a organizaciones benéficas u otros negocios legítimos como agencias de viaje, compañías proveedoras de servicios de electricidad, teléfono o Internet, o a su supermercado local.

Protéjase

Su banco NUNCA enviará correos electrónicos o mensajes de texto pidiéndole información de su cuenta o de datos financieros. Esto incluye la actualización de su dirección o sus datos de ingreso para los servicios bancarios por teléfono, móvil o Internet.

El gobierno u otras organizaciones legítimas NUNCA le pedirán que actualice su información pulsando en un enlace. En caso de duda, hable con un amigo o un familiar, o bien póngase en contacto con la organización directamente y pregunte.

Si usted recibe una llamada de teléfono de alguien que no conoce pidiéndole información personal, CUELGUE. Llame directamente a la compañía y compruebe si llamaron.

NUNCA abra archivos adjuntos de personas u organizaciones que no conozca. Desconfíe siempre de ofertas que parezcan demasiado buenas para ser ciertas o que pidan demasiada información.

Su banco puede ayudar, póngase en contacto con él inmediatamente.

- compartió su información bancaria en respuesta a una llamada de teléfono fraudulenta, correo electrónico o mensaje.
- abrió accidentalmente algunos enlaces o descargó archivos adjuntos.
- detectó transacciones extrañas en sus cuentas.

Cómo detectar una estafa

- Se le pide que actualice o confirme información personal que incluye la dirección, fecha de nacimiento, datos de la cuenta bancaria, número de identificación fiscal o cualquier número de identificación personal o contraseña.
- El correo electrónico o mensaje de texto contiene un enlace que parece sospechoso. Si no está seguro, pídale ayuda a un amigo o familiar.
- Se le pide un pago inmediato o un depósito por adelantado.
- Si la oferta suena demasiado buena para ser verdad, probablemente lo sea.
- El correo electrónico no coincide con la compañía.
- La persona que llama le pide acceso remoto a su ordenador.

Australian Banking Association

www.ausbanking.org.au

Consejos útiles para proteger su información financiera de estafas y fraudes.

- Cuelgue aquellas llamadas de teléfono que parezcan sospechosas y visite la página web de la compañía o busque su número de contacto y llámeles directamente.
- Nunca comparta contraseñas ni números de identificación personal. Proteja sus dispositivos con una contraseña. Si comparte el ordenador, nunca guarde las contraseñas y siempre cierre la sesión de su cuenta.
- Compruebe sus cuentas bancarias periódicamente para poder detectar rápidamente transacciones sospechosas.
- Evite deslizar la tarjeta al hacer compras. Hacer contacto o insertar la tarjeta son generalmente formas de pago más seguras.
- Bloquee anticipos en efectivo en las tarjetas de crédito.
- Hable con su banco acerca de la mejor manera de proteger su cuenta.
- Si cree que le han estafado, informe inmediatamente a su banco.

Los estafadores utilizarán muchas formas para robarle, aquí presentamos las principales.

Phishing – Se emplea un correo electrónico o mensaje de texto para obtener su información personal al hacerse pasar por una fuente fidedigna como por ejemplo un banco, una organización benéfica o el gobierno. El mensaje parece real y a menudo le pedirá que inserte información personal en una página web falsa o que pulse en un enlace, esto permitirá al estafador acceder a su ordenador y a su información personal.

Estafas en compras por Internet– los estafadores simulan ser tiendas por Internet auténticas, ya sea con una página web falsa o con un anuncio falso en una página auténtica de compras. Las páginas falsas de compras, a menudo le pedirán métodos de pago inusuales mediante pagos por adelantado con un giro postal, transferencia bancaria, transferencia internacional de fondos o con una tarjeta-regalo.

Estafas de inversión– los estafadores se hacen pasar por un corredor de bolsa o un jefe de cartera y ofrecen asesoramiento financiero o de inversión. Le pedirán que les facilite dinero para una oportunidad de inversión que puede o no ser real, para después quedarse con su dinero.

Estafas de acceso remoto – los estafadores le informarán de que hay algo extraño con su ordenador o conexión a Internet, o bien que su ordenador se ha infectado con un programa malicioso. Tratarán de convencerlo para que instale una aplicación o que les dé acceso a su ordenador. Utilizarán esto para acceder a su información personal o exigir una "tarifa" para solucionar el problema.

Estafas relacionadas con relaciones y citas en línea – los estafadores empiezan una relación con usted para obtener dinero o regalos. Establecen una relación a lo largo del tiempo y puede que le pidan que les transfiera bienes a nombre de ellos o que le pidan que sea un beneficiario en su testamento. A menudo, le pedirán dinero para solucionar problemas de salud, de viaje o familiares.

ENLACES ÚTILES:

www.ausbanking.org.au/safe-savvy-a-guide-to-help-older-people-avoid-abuse-scams-and-fraud

www.esafety.gov.au/seniors/staying-safer-online

www.scamwatch.gov.au/