Conozca cómo proteger su información y prevenir ser víctima de un fraude, le compartimos los tipos de fraudes más frecuentes:

Phishing:

Consiste en robarle información confidencial, haciéndole creer que está en un sitio de confianza, a través de correos electrónicos o mensajes que incluyen un enlace que lo dirigen al sitio web falso, el cual es creado por los defraudadores como una copia del original del Banco.

Los defraudadores le solicitan que amablemente "actualice, valide o confirme" información personal como:
Contraseñas o PIN
Usuario de banca en línea
Datos su tarjeta de crédito o cuenta bancaria.

¡Si usted los proporciona, está exponiendo su información y puede ser víctima de fraude!

Robo:

El delincuente puede haberse hecho de sus tarjetas de crédito o débito, así como de sus chequeras en un robo o asalto, con el objeto de utilizarlas sin su consentimiento. Por lo que es importante verificar que tengas en tu poder tus tarjetas de crédito o débito, así como tus chequeras.

Si fuiste víctima de un robo o no conoces la ubicación exacta de tus tarjetas de crédito o débito, así como de tus chequeras comunícate inmediatamente por medio de WhatsApp al número 4436-1724 o a nuestro centro de contacto 1724, para reportarlo y solicitar el bloqueo y evitar que se realicen consumos que no sean autorizados por tu persona.

¡Notifica inmediatamente la pérdida, robo o extravío de tus tarjetas o chequeras!

Conferencia bancaria o llamada de tres partes:

El defraudador, organiza una supuesta llamada entre un falso ejecutivo del Centro de Contacto, para realizar una transacción bancaria. Por ejemplo, el pago de un producto que el cliente tiene a la venta y simula tener problemas con su banca en línea para realizar la trasferencia de fondos.

El falso ejecutivo del banco le consulta sobre datos de contraseña, PIN o token, para validar la transacción, de esta forma son sustraídos sus datos y el defraudador procede a realizar transacciones como: desvío de fondos mediante la banca en línea del cliente o reseteo de contraseñas.

¡Si usted los proporciona, está exponiendo su información y puede ser víctima de fraude!

Llamada telefónica haciéndose pasar por un ejecutivo del Banco:

El defraudador haciéndose pasar por un ejecutivo del banco, solicita amablemente que usted le proporcione información que es de conocimiento "confidencial" como contraseñas, PIN o token, datos que el banco, en ningún momento le solicitará para realizar ningún tipo de gestión.

Los datos que son objeto de actualización son: direcciones, teléfonos, lugar de trabajo y correo electrónico.

¡Si usted los proporciona, está exponiendo su información y puede ser víctima de fraude!

Robo de contraseña de correo electrónico:

El objeto del defraudador es acceder a su cuenta de correo electrónico personal, para poder realizar transacciones desde su banca en línea.

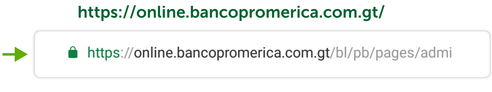
El defraudador puede contactarlo telefónicamente y pedirle que por seguridad y para actualizar datos o tener beneficios en sus productos, le comparta un código que le ha llegado a su celular por medio de SMS (mensaje de texto), que corresponde al código de validación cuando se resetea o cambia la contraseña de su cuenta de correo.

¡Si usted los proporciona, está exponiendo su información y puede ser víctima de fraude!

Toma estos consejos de seguridad para protegerte:

1. Asegúrate siempre de verificar que la dirección de tu Banca en Línea sea la correcta y esté antecedida por:

https://online.bancopromerica.com.gt/



2. Mantenga sus datos actualizados, para poder contactarlo y recibir información del Banco, con el objeto de identificar oportunamente casos de transacciones fraudulentas no autorizadas por su persona.
3. No proporciones información confidencial como contraseña, PIN o token, por ningún medio y por ningún motivo.
4. Consulta frecuentemente tus estados de cuenta para verificar que todas tus transacciones son legítimas y reporta inmediatamente cualquier anomalía por medio de WhatsApp al número 4436-1724 o a nuestro centro de contacto 1724.
5. Asegúrate de estar protegido ante posibles fraudes con el seguro ConPromerica.
6. Instala y mantén actualizado un software de antivirus y antimalware, en los equipos que utilices para ingresar a tu banca en línea.
7. Si tienes cualquier duda comunícate por medio de WhatsApp al número 4436-1724 o a nuestro centro de contacto 1724.