Medidas de seguridad con tarjetas de crédito y débito

Medidas de Seguridad con el PIN:

- Memorice el número secreto (PIN). Nunca anote su número de identificación personal.
- Nunca entregue su PIN a nadie.
- No escriba su número de PIN en la tarjeta.
- No guarde su número de PIN en el mismo lugar que guarda su tarjeta de crédito.
- Nunca proporcione su número de tarjeta de crédito u otra información personal por teléfono, a menos que su persona pueda verificar que está hablando con un funcionario de la institución financiera.

Medidas de Seguridad en los Cajeros:

- Si usted ha notado alguna vez algo sospechoso cerca de un cajero automático, o si el cajero retiene su tarjeta sin razón aparente, informe al banco inmediatamente.
- Si detecta cualquier anomalía en el cajero, como por ejemplo un dispositivo extraño, repórtelo de inmediato a la entidad bancaria, y como medida preventiva, no realice ninguna operación en ese cajero automático.
- Actúe con rapidez en caso de bloqueo de la tarjeta en el cajero automático.
- Solicite inmediatamente la presencia de un profesional de la entidad financiera donde se encuentre el cajero y no acepte la ayuda de personas ajenas a dicha entidad: pueden estar esperando la oportunidad de sustraer su tarjeta o conocer su número secreto.

Medidas de seguridad con los robos:

- No pierda de vista sus pertenencias.
- Nunca lleve todas sus tarjetas; sólo lleve una o dos como mucho.

- Lleve sus tarjetas de crédito fuera de su billetera, en un estuche para tarjetas de crédito o en otro compartimiento de su bolsa.
- Si le roban su cartera o la bolsa, llame a la entidad emisora inmediatamente.

Medidas de Seguridad para el fraude de suplantación de identidad:

- No preste su tarjeta a nadie, porque usted es responsable por todos los cargos.
- No le dé su número de cuenta a nadie que lo llame por teléfono o le envía un correo electrónico.
- Verifique siempre cuidadosamente los cobros detallados en su estado de cuenta y compárelos con las copias de los recibos de sus compras.
- Mantenga un registro de sus números de cuenta de las tarjetas de crédito y débito para que, en caso de extraviarse su tarjeta, pueda informarle rápidamente a la entidad financiera.
- Lleve siempre con usted todos los recibos de los cajeros automáticos, supermercados y gasolineras. Verifique que el importe en la copia del recibo que le entreguen en el establecimiento de comercio sea el mismo que aparece en el extracto de la entidad financiera.

Recomendaciones de seguridad

1. Cuide su clave:
   - Cubra el teclado cuando digite la clave.
   - Nunca revele su número de clave.
   - Cambie su clave periódicamente.
   - Siempre que le entreguen una tarjeta nueva, fírmela en el momento de recibirla, verifique frecuentemente que la tarjeta que porta corresponde a la suya.
   - Nunca asigne la misma clave para diferentes productos (Ahorros, Cuenta Corriente, Tarjeta de Crédito, entre otros) o medios (audio, Internet, cajeros automáticos, entre otros).

2. Nunca pierda de vista su tarjeta:
    - Jamás entregue por ningún motivo su tarjeta a personas extrañas.
    - No permita que deslicen su tarjeta por dispositivos diferentes a los definidos para tal fin. (Cajeros automáticos y datafonos).
    - Siempre que utilice su tarjeta verifique que sea deslizada en su presencia (no la pierda de vista, principalmente en restaurantes o bares) y que solamente lo hagan una vez.

3. Use una red segura para transacciones en Internet:
    - No use redes públicas (cafés Internet, por ejemplo).
    - Digite siempre la dirección de la página de su banco.
    - Siempre busque la salida segura en la página oficial de su entidad bancaria.

4. Cajeros automáticos seguros:
    - Use cajeros que conozca, de lo contrario busque los que estén bien iluminados y en una ubicación donde se sienta seguro.
    - Mire bien los alrededores del cajero automático antes de acercarse y no lo use si ve personas sospechosas alrededor.
    - No abra su cartera o monedero mientras está en la cola del cajero.
    - Lleve su tarjeta lista antes de acercarse al cajero.
    - Revise si hay algún objeto extraño en las aberturas del cajero o en el teclado.
    - Evite ayuda de extraños.
    - No siga instrucciones ni indicaciones en avisos adjuntos al cajero que le ordenen marcar la clave de su tarjeta varias veces.
    - Siga únicamente las instrucciones en la pantalla del cajero.
    - No marque su clave hasta que el cajero automático no se lo solicite.
    - Si cree que el cajero automático no está funcionando correctamente, oprima la tecla 'Cancel' o Cancelar, retire su tarjeta y diríjase a otro cajero.
    - No fuerce su tarjeta en la ranura donde se inserta la misma.
    - Siempre asegúrese de terminar su operación presionando la tecla CANCELAR, antes de retirarse del Cajero Automático.

- Siempre espere hasta que en la pantalla se indique que su operación ha finalizado.
- Verifique el saldo y estados de su cuenta regularmente y reporte cualquier discrepancia al banco de manera inmediata.

5. En las oficinas bancarias:
   - Identifique plenamente los funcionarios del banco.
   - Entregue su dinero solamente en la ventanilla.
   - Cualquier anormalidad que observe dentro de la entidad, comuníquela en forma inmediata a un funcionario de la entidad identificado con carné.
   - Si retira efectivo, evite contarlo en presencia de otras personas y guárdelo en un lugar seguro.

6. Después de salir del banco o cajero:
   - Evite desplazarse en tramos largos a pie, observar vitrinas durante largo tiempo o hablar en la calle.
   - Si ha realizado transacciones de grandes sumas de dinero, solicite a una persona de confianza que lo acompañe, o pida acompañamiento a la autoridad competente.

7. Internet:
   - Siempre haga sus transacciones bancarias en equipos de uso personal; no use café Internet, salas de sistemas u otros sitios públicos.
   - Siempre escriba la dirección de su banco www.nombre de la página del banco.com.co directamente en el navegador (browser).
   - Nunca ingrese usando un link que aparezca escrito en un correo, aunque el correo provenga de alguien conocido. No crea en aquellos mensajes de correo que le sugieren entrar a su cuenta o dar información. Esto se conoce como 'phishing', una práctica ilegal en la que los delincuentes montan páginas web similares a las de la entidad bancaria para allí robarle sus claves y luego desocuparle la cuenta.

- Siempre que ingrese a una página para realizar transacciones sobre su cuenta, verifique que la dirección electrónica presentada en la parte superior de la pantalla sea https:// -en lugar de la habitual http://- y que el navegador muestre el símbolo del candado cerrado en la parte inferior de la misma.
- Evite diligenciar formatos incluidos en mensajes de correo electrónico, las cuales preguntan por información financiera personal.

Cuidado con las Llamadas Telefónicas y Correos Electrónicos Fraudulentos

En Banco Cathay lo primordial es su seguridad, por lo que aprovechamos esta oportunidad para alertarle sobre una modalidad de fraude en telefónico y por correo electrónico que se está efectuando en nuestro país.

¿Cómo está operando?

Mediante llamadas telefónicas o correos electrónicos, personas desconocidas que se hacen pasar por personal de una Entidad Financiera, tratando de obtener información confidencial de clientes, como identificación, usuario y clave del sitio de Internet, número de tarjetas, números de cuenta, direcciones, teléfonos o direcciones de correo electrónico, aduciendo que es por un tema de actualización de información que la Entidad necesita o que es para formalizar algún crédito aprobado.

Algunos consejos para evitar este tipo de llamadas y correos:

- No responda a llamadas telefónicas ni a correos en los que le soliciten bajo algún pretexto ingresar al sitio de Internet de la Entidad Financiera. Estos correos pueden llegar a parecer legítimos al igual que las llamadas.
- El contacto entre Banco Cathay y sus clientes se realiza por medio de su Ejecutivo (a) asignado, por lo que si tiene dudas sobre la identidad de su ejecutivo asignado puede consultar en cualquiera de nuestras Sucursales.

- Banco Cathay NUNCA pedirá a través de llamadas telefónicas o correos electrónicos información confidencial como: usuario, claves, números de cuenta, números de tarjeta.
- Siempre que vaya a utilizar nuestros servicios de Internet escriba directamente las direcciones correspondientes en el navegador. Nunca ingrese a través de vínculos o "links" recibidos por cualquier medio.
- Procure no utilizar sitios públicos (como cafés Internet) para realizar transacciones financieras de cualquier tipo ya que su información confidencial podría ser capturada.

¿Cómo detectar una llamada o correo electrónico fraudulento?

Normalmente, un correo electrónico fraudulento contiene nombres de remitentes (“From” “De”) que parecen legítimos y tiene logotipos copiados de la página web de la Entidad Financiera.

Los elementos que lo identifican son:

- El correo tiene un tono de alarma, que exige actuar rápidamente.
- Incluye un link en el cual se le solicitará accesar con el fin de que valide o actualice su información personal.
- Frecuentemente presenta errores gramaticales, los cuales no son usuales en la comunicación habitual de la institución.
- El correo electrónico llega a su buzón en forma de SPAM.

Mientras tanto las llamadas telefónicas fraudulentas la hacen personas desconocidas que se hacen pasar por funcionarios de la Entidad Financiera, incluso pueden dar nombres reales de funcionarios.

Los elementos que las identifican son:

- La llamada se recibe de teléfonos privados que no se pueden identificar.

- Solicitan al cliente que responda algunas preguntas para confirmar su identificación.
- Normalmente la llamada es rápida y sin entrar en detalles, por lo que “apresuran” al cliente a responder.
- Las llamadas fraudulentas pueden hacerlas varias veces al día al mismo número hasta encontrar al cliente.

¿Cómo reportar una posible llamada o correo fraudulento?

Si en algún momento cree que ha recibido una llamada o correo electrónico fraudulento de parte de Banco Cathay, contáctatenos de inmediato llamando al teléfono 2527-7728/2527-7716 o bien al correo de atencionalcliente@bancocathay.cr