Banco ProCredit

Parte del Grupo ProCredit

Seguridad

Información de seguridad en línea

Banco ProCredit se compromete a proteger la integridad de sus transacciones y los detalles de su cuenta bancaria. Por lo tanto, Banco ProCredit utiliza el software y los procedimientos de seguridad más recientes para proteger sus transacciones en línea. Sin embargo, siempre debe tener en cuenta que Internet y el correo electrónico se pueden utilizar como vehículos para actividades ilegales, por lo que le recomendamos que tome algunas precauciones simples para garantizar la seguridad.

Consejos para mantenerse seguro en línea

Sepa con quién está tratando
Acceda siempre a la banca por Internet escribiendo la dirección del banco en su navegador web [www.banco-procredit.com.ec]. Nunca vaya a un sitio web desde un enlace en un correo electrónico e ingrese sus datos personales. En caso de duda, comuníquese con el Banco al 1800 100 400.

Mantenga las contraseñas y los PIN seguros
Siempre tenga cuidado con los correos electrónicos no solicitados o las llamadas que le piden que revele cualquier información personal o número de tarjeta. Mantenga esta información en secreto. Tenga cuidado de divulgar información personal a alguien que no conoce. Su banco y la policía nunca lo contactarán y le pedirán que divulgue su PIN o información de contraseña.

¡Sostén tu dinero!
No se deje engañar por correos electrónicos de sonido sincero que le ofrecen la oportunidad de ganar dinero fácil. Si parece demasiado bueno para ser verdad, ¡probablemente lo sea! Sea especialmente cauteloso con los correos electrónicos no solicitados desde fuera del país: será mucho más difícil verificar si son quienes dicen ser.

Mantenga su PC segura
Utilice un software antivirus actualizado y un firewall personal y, si su computadora usa el sistema operativo Microsoft Windows, manténgalo actualizado a través del sitio web de Microsoft. Utilice siempre la versión más reciente de su navegador de Internet, que incluye todas las actualizaciones de seguridad. Tenga mucho cuidado si utiliza cibercafés, bibliotecas o cualquier PC que no sea de su propiedad y sobre la que no tenga control.

Medidas de protección adicionales
Siempre memorice su contraseña y otra información de seguridad y luego destruya el aviso que contiene esta información tan pronto como sea posible. Nunca escriba ni registre su contraseña u otra información de seguridad a menos que esté oculto. Asegúrese de seguir siempre los términos y condiciones de su banco. Siempre tome medidas razonables para mantener su contraseña y otra información de seguridad en secreto en todo momento, nunca la revele a familiares o amigos. No use la misma contraseña que usa para realizar operaciones bancarias en línea en sitios que no sean bancarios. Si cambia su contraseña, elija una que no pueda adivinarse fácilmente. Nunca le dé detalles de su cuenta o información de seguridad a nadie. Si llama al banco, tenga en cuenta qué información le preguntará: normalmente no se le pedirá su contraseña completa.

Asegúrese de usar siempre el servicio seguro de banca electrónica de Banco ProCredit. Siempre vaya directamente al sitio web escribiendo [www.bancoprocredit.com.ec]. Asegúrese de que haya un candado cerrado o una llave intacta en la parte inferior derecha de la ventana de su navegador antes de acceder al sitio web del banco. El comienzo de la dirección de Internet del banco cambiará de "http" a "https" cuando se realice una conexión segura. Verifique que el símbolo de conexión segura esté visible. Puede consultar el Certificado de seguridad del sitio web de Banco ProCredit haciendo clic en el candado que aparece en su navegador.

Cualquier excepción a la rutina normal con respecto a su banca por Internet se debe tratar como sospechosa. Si tiene alguna duda, comuníquese con Banco ProCredit visitando su sucursal más cercana, comunicándose con su asesor de clientes o llamando a nuestra línea de ayuda: 1800 100 400. Nunca deje su computadora desatendida cuando inicia sesión en la banca por Internet. Asegúrese de cerrar sesión correctamente cuando haya finalizado la banca en línea.

Más información sobre seguridad en línea

¿Qué es phishing?
Phishing es el nombre dado a la práctica de enviar correos electrónicos al azar que pretenden provenir de una empresa genuina que opera en Internet, en un intento de engañar a los clientes de esa empresa para que revelen información en un sitio web falso operado por estafadores. Estos correos electrónicos generalmente afirman que es necesario "actualizar" o "verificar" la información de su cuenta de cliente e instan a las personas a hacer clic en un enlace en el correo electrónico que los lleva al sitio web falso. Cualquier información ingresada en el sitio web falso será capturada por los delincuentes para sus propios fines fraudulentos.

¿Cómo puedo evitar ser víctima de phishing?
La clave es seguir siendo sospechoso de todos los correos electrónicos no solicitados o inesperados que reciba, incluso si parecen originarse en una fuente confiable. Los correos electrónicos se envían completamente al azar con la esperanza de llegar a una dirección de correo electrónico en vivo de un cliente con una cuenta en el banco al que se dirige.

Aunque Banco ProCredit puede contactarlo por correo electrónico, nunca lo contactará por correo electrónico para pedirle que ingrese su contraseña o cualquier otra información confidencial haciendo clic en un enlace y visitando un sitio web. Deje de pensar en cómo su banco normalmente se comunica con usted y nunca divulgue su contraseña completa ni ninguna información personal.

Cómo detectar un correo electrónico de phishing

1 - ¿De quién es el correo electrónico?
Suplantación de identidad

Los correos electrónicos de phishing pueden parecer que provienen de una dirección de correo electrónico real de Banco ProCredit. Desafortunadamente, debido a la configuración del correo electrónico de Internet, es relativamente fácil para los phishers crear una entrada falsa en el campo "De:".

La dirección de correo electrónico que aparece en el campo "De:" de un correo electrónico NO es una garantía de que proviene de la persona u organización indicada en la dirección de correo electrónico. Estos correos electrónicos no se enviaron usando los propios sistemas del banco.

2 - ¿Para quién es el correo electrónico?
Los correos electrónicos se envían al azar a listas de correo masivo y los defraudadores casi seguros no sabrán su nombre real o cualquier otra cosa sobre usted, y se dirigirán a usted en términos vagos como "Estimado Cliente Valioso".

3 - Eche un vistazo más de cerca al correo electrónico - ¿se ve "phishy"?
Lo primero que debe recordar es que los bancos nunca le escribirán y le pedirán su contraseña o cualquier otra información confidencial por correo electrónico. También es probable que el mensaje contenga "spe11ings" o cApitALs impares en el campo "Asunto:" (este es un intento de evitar el software de filtro de spam), así como errores gramaticales y de ortografía.

Nunca inicie sesión en su cuenta bancaria en línea haciendo clic en un enlace en un correo electrónico. Abra siempre su navegador web y escriba usted mismo la dirección del sitio web de Banca por Internet de Banco ProCredit.

Si tiene alguna duda sobre la validez de un correo electrónico que pretenda provenir de Banco ProCredit, informe inmediatamente visitando su sucursal más cercana, comunicándose con su asesor de clientes o llamando al siguiente número [1800 100 400].

4 - ¿A dónde va ese hipervínculo?
Desafortunadamente, es muy fácil ocultar el destino real de un enlace, por lo que el enlace que se muestra y todo lo que aparece en la barra de estado de su programa de correo electrónico puede ser fácilmente falsificado.

Cómo detectar un sitio web de Phishing.

¿Cuál es la dirección del sitio?
Si visita un sitio web después de hacer clic en un enlace en un correo electrónico, hay muchas maneras de ocultar la verdadera ubicación de un sitio web falso en la barra de direcciones. La dirección del sitio puede comenzar con el nombre de dominio del sitio original, pero eso no es garantía de que conduzca al sitio real. Otros trucos incluyen usar direcciones numéricas, registrar una dirección similar (como www.mybank-verify.com) o incluso insertar una barra de dirección falsa en la ventana del navegador. Muchos de los enlaces de estas páginas pueden ir al sitio web genuino, pero no se deje engañar.

Puede confirmar que se encuentra en el sitio web oficial seguro de Banco ProCredit comparando el símbolo de conexión segura.

Puede consultar el Certificado de seguridad del sitio web de Banco ProCredit haciendo clic en el candado que aparece en su navegador.

Tenga cuidado con las ventanas emergentes fraudulentas
En lugar de mostrar un sitio web completamente falso, los estafadores pueden cargar el sitio web genuino en la ventana principal del navegador y luego colocar su propia ventana emergente falsa sobre la mayor parte. Si se muestra de esta manera, podrá ver la barra de direcciones del sitio web real en segundo plano, aunque cualquier información que escriba en la ventana emergente será recopilada por los estafadores para su propio uso.

Para acceder a su cuenta bancaria en línea, escriba la dirección en una nueva ventana usted mismo. La dirección de su sitio web de banca en línea real comenzará con "https" e incluirá un pequeño candado en la parte inferior de la ventana del navegador.

Haga clic en este icono de candado y verá el Certificado de identificación de seguridad del sitio web.

Informar correos electrónicos sospechosos

Si recibe un correo electrónico sospechoso, informe inmediatamente a Banco ProCredit visitando su sucursal más cercana, comunicándose con su asesor de clientes o llamando al siguiente número [1800 100 400].

Recuerde: los bancos nunca le enviarán un correo electrónico para solicitar que "confirme" o "actualice" su contraseña o información personal haciendo clic en un enlace y visitando un sitio web. Trate todos los correos electrónicos no solicitados con cuidado y nunca haga clic en enlaces en tales correos electrónicos ni ingrese cualquier información personal. Para iniciar sesión en la banca por Internet, abra su navegador web y escriba la dirección en usted mismo. Si tiene dudas sobre la validez de un correo electrónico, o si cree que puede haber revelado información confidencial, informe inmediatamente a Banco ProCredit visitando su la sucursal más cercana, contactando a tu asesor de cliente o llamando al siguiente número [1800 100 400].

Recordatorio: trate con precaución todos los correos electrónicos no solicitados (especialmente los de remitentes desconocidos) y nunca haga clic en los enlaces de dichos correos electrónicos para visitar sitios web desconocidos. Instale el software antivirus, manténgalo actualizado y realice escaneos de seguridad regularmente. Instale y aprenda cómo use un firewall personal Instale las últimas actualizaciones de seguridad, también conocidas como parches.