SEATTLE
CREDIT UNION

EDUCACIÓN A SOCIOS

CONCIENTIZACIÓN SOBRE SEGURIDAD Y PREVENCIÓN DE FRAUDE

Seattle Metropolitan Credit Union DBA Seattle Credit Union (a continuación "Seattle Credit Union") está dedicado a proteger su información privada y en asegurarse que usted conozca las mejores maneras de mantener su dinero y datos tan seguros como sea posible. El estar consciente sobre riesgos potenciales puede ser un primer paso poderoso en reducir su exposición a fraude y robo de identidad. Para más información sobre estas y otras estafas actuales, visite **https://www.consumer.ftc.gov/scam-alerts** y **https://www.identitytheft.gov**.

CONCIENTIZACIÓN SOBRE SEGURIDAD

1. INFORMACIÓN SOBRE ACCESO AL SISTEMA

- Seattle Credit Union jamás lo llamará, le enviará un correo electrónico (email) ni se comunicará con usted para solicitarle su ID de acceso, contraseña ni ninguna otra credencial de ingreso a los servicios que ofrecemos en-línea. Si recibe tal solicitud, no proporcione la información. Comuníquese con Seattle Credit Union para reportar el incidente.

2. CONSEJOS DE SEGURIDAD PARA CONTRASEÑA

- No comparta su usuario ni contraseña con nadie. Manténgalos en un lugar seguro. Solo usted debería tener acceso.
- Cree un usuario y contraseña exclusivos para cada sitio web y no utilice la misma información de identificación en sitios múltiples.
- Cree un usuario y contraseña fuertes que incluyan letra(s) en mayúscula, en minúscula, número(s) y caracteres especiales como ser !@#$%^&*.
- Cambie su contraseña regularmente.

3. REPORTANDO ACTIVIDADES SOSPECHOSAS

- Si ve actividades sospechosas en sus cuentas o si ha recibido una llamada, email, carta u otra actividad sospechosa relativa a sus cuentas, repórtelo inmediatamente a Seattle Credit Union.
- Protección a Consumidores y Regulación E: Esta regulación proporciona reglas para resolución de errores y transacciones no-autorizadas sobre transferencias electrónica de fondos, que incluyen la mayoría de las transacciones procesadas en-línea. Además, establece límites sobre su responsabilidad financiera por transferencias electrónicas de fondos no-autorizadas. Sin embargo, estos límites están directamente relacionados a la puntualidad en su detección y reporte de los problemas a Seattle Credit Union. Lo alentamos a revisar inmediatamente los estados de cuenta periódicos y a monitorear la actividad de su cuenta en-línea regularmente. Esta declaración proporcionada a usted al abrir la cuenta provee información detallada. Le proporcionaremos, si lo solicitara, una copia impresa sin costo de esta declaración.

4. RIESGO DE ACCESO EN-LÍNEA

- Los consejos de seguridad y enlaces a sitios web en este documento, proporcionan información importante para ayudarlo a entender los riesgos de transacciones en-línea y opciones para ayudarlo a controlar estos riesgos. Es importante estar informado. Cuando se trata de fraude por Internet, toma de cuenta y robo de identidad, estos pasos lo ayudarán a prevenir exposición a riesgos adicionales.

5. CONSEJOS DE SEGURIDAD DEL SITIO WEB

- Monitoree la actividad de su cuenta. Vea en-línea la actividad de su cuenta en forma regular. Revise los estados de cuenta periódicos y reconcílielos con sus registros personales. Reporte cualquier actividad sospechosa inmediatamente a Seattle Credit Union.
- Cuando se desconecte de un sitio web, no cierre simplemente la página con la "X". Necesita "Log Out" o "Log Off" (Desconectarse/ Cerrar Sesión).
- Los sitios seguros de web tienen una dirección web que comienza con "https" en vez de "http". Si esto no está presente, ese sitio no es seguro. No ingrese ni conduzca negocios en ese sitio.

- Si un sitio web despliega un monitoreo de seguridad, verifique que tenga la fecha al día. Si no la tiene, no use el sitio: puede ser falsificado o pirateado.
- Al completar transacciones financieras, verifique que el cifrado y otros métodos de seguridad se hallen presentes, protegiendo su cuenta e información personal.

6. CONSEJOS DE SEGURIDAD PARA COMPUTADORAS Y REDES

- Use software de monitoreo de seguridad de buena calidad en su computadora que incluya antivirus, antimalware y funciones de firewall.
- Use las características de seguridad de su computadora, como inicio de sesión para cuentas individuales.
- Mantenga la seguridad del sistema operativo de su computadora al día, aplicando mejoras y actualizaciones.
- Proteja la red de su computadora (física o inalámbrica) con una contraseña.
- Use los recursos de la red web para aprender más y haga más para protegerse en-línea.

7. ENLACES DE AYUDA

- Dos sitios fáciles de usar para todas las edades e intereses:

  http://onguardonline.gov

  http://www.staysafeonline.com

- Sitio del FTC con alertas al consumidor y consejos de seguridad en-línea: **http://www.ftc.gov/bcp/menus/consumer/data/privacy.shtm**

8. ESTAFAS RECIENTES Y CÓMO REPORTAR ESTAFAS

- Visite el sitio web de IC3, un aliado del FBI, del Centro Nacional de Crimen de Cuello Blanco y de la Agencia de Justicia: **http://www.ic3.gov**.

9. ESTAFAS, FRAUDES Y CONSEJOS PARA EVITAR CAER VÍCTIMA

- Visite el sitio web del FBI: **http://www.fbi.gov/scams-safety**.
- Aprenda más sobre estafas y prevención: **http://www.fakechecks.org/index.html**.

10. INFORMACIÓN PARA USUARIOS COMERCIALES DE SERVICIOS EN-LÍNEA

Los reguladores financieros han notado que las transacciones comerciales, debido a su frecuencia y valor en dólares, son inherentemente más riesgosas que las transacciones de consumidores. El riesgo de fraude está incrementando, por ejemplo, un incremento en pirateo de cuentas y transferencias de fondos en-línea no-autorizadas relativas a cuentas comerciales. Los negocios pequeños y medianos han sido la meta principal ya que criminales cibernéticos han reconocido que los controles de seguridad que tienen establecidos no son tan robustos como aquellos de los negocios grandes.

Aquí están algunas de las sugerencias de los reguladores para mejorar los controles de parte de los negocios:

- Los socios con cuentas de negocios deben realizar una evaluación periódica de los riesgos y de la efectividad de los controles que tienen establecidos para minimizar los riesgos en el procesamiento de transacciones en-línea.
- Los consejos de contraseña, sitio web, computadora y red mencionados arriba son un punto de partida para este proceso y los enlaces de web proporcionados como recursos proveen información adicional detallada.
- El Centro para Negocios FTC tiene una gran cantidad de información para negocios en **http://business.ftc.gov/privacy-and-security/data-security**.
- Los socios con cuentas de negocios deberían comprender las características de seguridad del software y de los sitios web que utilizan y tomar ventaja de estas características. La separación de tareas- el proceso de separar deberes-para que no solo una persona pueda llevar a cabo todos los pasos de una transacción-es un ejemplo de una característica de seguridad muy importante.
- Las opciones de seguridad en capas que puede estar disponible para los socios con cuentas de negocios llevando a cabo transacciones incluyen umbrales, verificación fuera de banda (como

ser verificaciones por teléfono o email), detección de fraude y sistemas de monitoreo y servicios basados en reputación de IP.

CONSEJOS IMPORTANTES PARA PREVENCIÓN DE FRAUDE

1. **RECUERDE SIEMPRE:**
   - Si suena muy bueno para ser verdad, probablemente lo es.
   - No proporcione nunca sus credenciales bancarias en-línea a nadie.
   - Confíe en sus instintos- especialmente cuando tiene un mal presentimiento sobre una oferta o una compañía.
   - Si alguna vez le piden que deposite un cheque u orden de dinero y después que gire fondos – es una estafa.

2. **CONSEJOS DE SEGURIDAD PARA LA ATM:**
   Las ATMs pueden estar sujetas a fraude, vandalismo y robo. También pueden ser la escena de robos. Considere los consejos siguientes cuando utilice una ATM:

   - Use una ATM familiar cuando sea posible. Si no está cerca de una, elija una ATM bien iluminada y bien ubicada donde se sienta cómodo. De ser posible, utilice una ATM con carril de vehículos si está solo en la noche. Mantenga las puertas de su auto llaveadas y sus ventanillas alzadas, excepto por la ventanilla del conductor cuando utilice la máquina.
   - Monitoree toda el área de la ATM antes de usar la máquina. Evite usar una ATM si alguien está merodeando o si se ve muy aislada o insegura. Confíe en sus instintos.
   - Al usar una ATM donde deba caminar, evite abrir su cartera, bolsa o billetera. Tenga su tarjeta lista en mano antes de acercarse a la máquina.
   - Observe si algo se ve inusual o sospechoso sobre la ATM indicando que pudiera haber sido alterada. Si la ATM aparece tener el lector de tarjeta o el teclado alterados, no la use. Chequee instrucciones inusuales en la pantalla o si la pantalla está sospechosamente en blanco. Si sospecha que han alterado la ATM, proceda a otra ATM e informe a Seattle Credit Union o al dueño de la ATM.
   - Evite una ATM con un mensaje o un letrero adjunto a ella indicando que las direcciones en la pantalla han cambiado, especialmente si el mensaje está posicionado sobre el lector de tarjeta. Ni Seattle Credit Union ni otras instituciones financieras jamás publicarán mensajes dirigiéndolo a usar una ATM que ha sido alterada.

3. **CONSEJOS DE SEGURIDAD SOBRE COLACIÓN DE ATMS:**
   La colación (skimming) es un método de obtener datos personales de una tarjeta de ATM, de débito o de crédito mientras están siendo utilizadas en una máquina de ATM o en un local comercial. La gente puede alterar los equipos de ATM legítimas en un esfuerzo para robar tanto la cinta magnética de datos de las tarjetas siendo utilizadas, como los PINs asignados a esas tarjetas.
   Se instala un aparato al frente del lector de tarjeta original de la ATM. Los lectores falsos contienen un lector de tarjeta adicional llamado “colador” (skimmer en inglés). El skimmer capta y copia la información de la tarjeta.
   Luego, una cámara que lee el PIN de la tarjeta es alojado en un porta-panfletos que se ve inocente. La cámara dentro del porta-panfletos está angulada para ver el monitor y el teclado.
   La tecnología más reciente permite que el culpable se mantenga cerca, recibiendo la información en forma inalámbrica de un equipo que ha instalado en la ATM. Los ladrones pueden luego copiar las tarjetas y usar los números de PIN para retirar dinero de muchas cuentas en un corto período de tiempo directamente de la ATM.

   Por favor notar: Los ejemplos se refieren a ATMs pero se pueden colocar aparatos similares en lectores de tarjetas en estaciones de carga de combustible.

   ¿Qué puede hacer para protegerse?
   Manténgase alerta e inspeccione la ATM antes de usarla. Los aparatos de skimming que están colocados en o cerca del lector actual de una ATM son generalmente difíciles de detectar, pero si algo se ve diferente, inusual o flojo al tocarse en el lector de tarjeta o en el teclado del PIN, no la use. De ser posible, reporte esto a Seattle Credit Union o al dueño de la ATM lo antes posible.

   ¿Qué pasa si el aparato de skimming se encuentra en una ATM de Seattle Credit Union?
   Si sospecha que el aparato de skimming ha sido colocado en una ATM de Seattle Credit Union, no la use ni trate de remover el aparato. Hable con personal de una sucursal lo antes posible o llame a nuestro Centro de Contacto al 206.398.5500.

4. CONSEJOS DE SEGURIDAD SOBRE "PHISHING" SECURITY TIPS:

El Phishing (fraude electrónico) es una técnica que usa emails falsos o sitios web fraudulentos para obtener información personal con el propósito de robar identidad. Los emails fraudulentos o sitios web están diseñados para engañar a los destinatarios a divulgar información financiera personal tal como números de tarjeta de crédito, credenciales de acceso a banca en-línea, números de seguro social, etc.

A veces, los phisers (pescadores) crean sitios web falsos que parecen legítimos y adjuntan un enlace al sitio web falso en un email. Los destinatarios que inocentemente presionan este enlace encontrarán que el sitio web que abren se parece al sitio web correcto. Sin embargo, el usuario de la computadora no se da cuenta que ha sido redireccionado a un sitio web falso diseñado para recaudar información personal.

- Sospeche cualquier email que le solicite una respuesta urgente y que se vea alarmante o entusiasta. Los phisers enviarán un email solicitando su atención inmediata o para "verificar sus registros". Usualmente pedirán información como ser usuarios, contraseñas, números de cuenta, números de seguro social, etc. Los emails de phisers generalmente no son personalizados y pueden parecer como de distribución masiva.
- No presione enlaces enviados por email que soliciten información. Los emails sugiriendo "presione aquí" a fin de ingresar información personal pueden terminar redireccionándolo a un sitio falso que podría estar recaudando sus datos para usos maliciosos. Si no está seguro de la legitimidad de un email de Seattle Credit Union, comuníquese con nosotros al 206-398-5500.
- Evite completar formularios que soliciten información confidencial o financiera a no ser que esté trabajando con un sitio de buena reputación que pueda verificar que es auténtico. Si ingresa información alguna, asegúrese que sea hecho a través de un enlace seguro (SSL). Esto se puede verificar chequeando el ícono del candado en la venta del servidor o si se muestra https:// en la barra de dirección web (https:// - la "s" representa seguro).

5. ESTAFAS DE FRAUDE

No caiga en estas estafas, explicadas en detalle en: **http://www.smcu.com/fraud-protection**.

- Fraude de Lotería/ Rifas
- Fraude de Tarjetas de iTunes
- Fraude de Oferta de Sobrepago/ Craigslist
- Fraude de Comprador Secreto
- Fraude de Envoltura de Auto
- Fraude de Romance
- Fraude de Herencia Inesperada
- Fraude Telefónico de Tarjeta de Crédito

Contáctenos
206.398.5500 | 800.334.2486 | TTY 206.398.5697
1521 1st Ave S, Ste 500, Seattle, WA 98134 | seattlecu.com

Your savings federally insured to at least $250,000 and backed by the full faith and credit of the United States Government
NCUA
National Credit Union Administration, a U.S. Government Agency
EQUAL HOUSING OPPORTUNITY