

# BOLETIN ESTRELLA



**MOUNTAIN STAR**  
FEDERAL CREDIT UNION

¡¡Una gran noticia!!

El campo de membresía se ha ampliado para Mountain Star Federal Credit Union. ¡Ahora prestaremos servicios a más comunidades no bancarizadas y desatendidas como Socorro, San Elizario, Fabens, Clint, Chaparral, Anthony, Ysleta, Tornillo, Sierra Blanca, Fort Hancock, Doña Ana con tasas de interés más bajas en préstamos!



**Start Fresh with Our Spring Loan Special!**  
Say goodbye to financial stress and hello to up to \$5,000 at an APR as low as 8.99% up to 48 months.

**MOUNTAIN STAR**  
FEDERAL CREDIT UNION

## REUNIÓN ANUAL

**Involúcrate**

**MIÉRCOLES 24 DE ABRIL DE 2024**

**HILTON GARDEN INN**

**Reunión de Negocios 6:30 p.m. – 8:00 p.m.**

**Compre su boleto para la cena hoy por \$ 1**

## Cierres por días festivos

**Memorial Day**

**Lunes, 27 de mayo de 2024**

**Juneteenth**

**Miércoles, 19 de Junio de 2024**



## LAS CONSECUENCIAS DEL FRAUDE

Los ataques de apropiación de cuentas son una de las amenazas más difíciles de detectar para una institución financiera porque a menudo el usuario y el dispositivo son confiables y genuinos. A pesar de la educación de los titulares de cuentas, las personas continúan siendo víctimas de estas estafas y las cooperativas de ahorro y crédito continúan reportando grandes pérdidas y daños a la reputación de esta actividad fraudulenta.

## CÓMO SE EJECUTA EL FRAUDE

Para apoderarse de una cuenta, los estafadores están haciendo phishing, suplantando la identidad y utilizando la ingeniería social contra los titulares de sus cuentas a través de llamadas telefónicas, mensajes de texto, correos electrónicos o chat y haciéndose pasar por el equipo de fraude de su institución financiera

**La solicitud:** El estafador solicita que el titular de su cuenta le proporcione información de autenticación múltiple, como el nombre de usuario y la contraseña de la banca en línea, el PIN, los códigos de seguridad, el código de 6 dígitos y/o el número de cuenta, en un intento de agotar el dinerotitular de sus fondos. También pueden solicitar al titular de la cuenta que verifique información como el número de tarjeta, el PIN y el CVV/CVC, proporcionando todo lo que necesita para falsificar una tarjeta. Los titulares de cuentas siguen siendo engañados al pensar que es el equipo de fraude de su institución el que quiere ayudarlos.

**La transferencia:** El titular de la cuenta puede ser manipulado por el estafador para que realice la transacción y envíe los fondos al estafador.

**La adquisición:** El estafador también puede ponerse en contacto con su institución financiera

## MEDIDAS DE MITIGACIÓN

Para evitar pérdidas, tenga en cuenta los siguientes controles:

Como su cooperativa de ahorro y crédito de confianza, le recomendamos que siempre busque un estado de cuenta en mensajes de texto y correos electrónicos cuando envíe un código de acceso para proteger la información confidencial y evitar fraudes. Este paso adicional garantiza que las cuentas de nuestros miembros permanezcan seguras y privadas. Por ejemplo: "Si no solicitaste este código de acceso, comunícate con tu institución financiera de inmediato. No compartas este código con nadie. Institución financiera emLos empleados nunca pedirán este código de acceso".

Tenga cuidado con las estafas por mensajes de texto (smishing) y llamadas telefónicas (vishing). Le recomendamos que no responda a ningún mensaje de texto o llamada telefónica, incluso si parecen provenir de su institución bancaria. Llame usando un número de teléfono confiable para cuestionar cualquier mensaje de texto, chat o llamada telefónica supuestamente de su institución bancaria.

Utilice una solución biométrica de comportamiento que busque continuamente el comportamiento digital físico y cognitivo de un usuario para distinguir entre usuarios genuinos y ciberdelincuentes.

Además, le recomendamos que registre sus dispositivos, utilice el reconocimiento de dispositivos y la ubicación geográfica.

Se establecen límites diarios para los nuevos usuarios para las primeras transacciones de aplicaciones de pago (ACH) para reducir la exposición al riesgo.

Regístrese para recibir alertas por mensaje de texto para transacciones con tarjeta de crédito/débito.

Te guiaremos y recomendaremos los pasos adecuados para congelar con las agencias de informes crediticios, limitando el uso no autorizado.

Artículo de Allied Solutions

El verano se acerca rápidamente, queremos recordarle que su tarjeta de débito tiene un límite diario de \$1,000. Si usted va fuera de la ciudad, le recomendamos que nos llame para revisar su tarjeta y evitarle interrupciones con su tarjeta de débito.

**Control de Tarjetas:** ¡una nueva función de nuestra aplicación que lo pone a cargo de su tarjeta de débito! Con solo un toque, puede activar o desactivar instantáneamente su tarjeta. Le brinda tranquilidad y control total sobre sus transacciones. Inicie sesión en nuestra aplicación y pruébelo hoy.

¡Disfrute de la comodidad y seguridad del *Control de Tarjetas*, disponible exclusivamente para todos nuestros miembros!



## Transferencias digitales

**P2P= Pago Peer to Peer (Seguro y protegido)**  
**A2A= Pago de cuenta a cuenta (conveniente)**  
**Pago de facturas**

Únase a nosotros para aprender a usar estos nuevos servicios en su banca en línea y aplicación.

A partir del 24 de febrero hasta el 27 de Abril, las clases se llevarán a cabo en nuestra sala de juntas todos los sábados de 10 a.m. a 11 a.m.