RECOMENDACIONES DE SEGURIDAD PARA PROTECCIÓN EN NUESTROS PUNTOS DE ATENCIÓN

- No permitas que ninguna persona se acerque a CAJAS cuando realices alguna transacción.
- Mientras estas realizando tu transacción no te retires de CAJAS.
- Al realizar tus transacciones en cajas, antes de retirarte debes verificar el efectivo.
- No descuides el dinero durante la permanencia ni al salir de la Cooperativa.
- Tu vida nos importa, por lo que, si pese a haber tenido todo el cuidado posible, resultas ser víctima de un atraco es mejor no ofrecer resistencia.

SEGURIDAD DE LA INFORMACIÓN

La información es tu activo de mayor valor, te damos algunos consejos para cuidarla:

- Cambia tus contraseñas periódicamente de tu Banca Móvil.
- Nunca proporciones datos personales, claves u otros datos confidenciales a través de correos electrónicos, medios de comunicación instantánea o por teléfono.
- Nunca publiques en redes sociales tus datos personales.
- Mantente informado sobre los Fraudes por Internet es tu mejor arma.

CONSEJOS DE LA COMUNICACION MEDIANTE EL USO DE INTERNET

- Somos una Cooperativa de atención personal y cumplimos con las medidas de bioseguridad. Nunca solicitaremos tus datos personales o confidenciales por correos electrónicos o medios digitales.
- El ingreso a nuestra página web siempre sea a través de un navegador de internet “https://cactri.com.bo/”, nunca por medio de enlaces que reciba de terceros.
- Nunca enviaremos enlaces que lo inviten a actualizar y/o validar tus datos. Todo será bajo nuestra página web https://cactri.com.bo o de manera presencial en nuestros puntos de atención.
- Verifica siempre el origen de las herramientas o programas antes de realizar descargas o instalaciones en tu equipo o celular.

PHISHING

¿De qué se trata?
Captar datos personales y de cuentas bancarias enviados a través de enlaces de correos electrónicos o páginas

Web fraudulentas, que aparentan pertenecer a una entidad financiera u otra entidad real.

¿Cómo ocurre?

La persona recibe mediante correo electrónico un mensaje con indicaciones, en las que mediante un enlace solicitan actualizar datos mediante un procedimiento o instrucción. Una vez la persona hace clic en el enlace, se abre el navegador con una página muy similar a la real; al ingresar los datos solicitados en la página fraudulenta y presionar el botón "Aceptar", los datos son capturados con el fin de realizar fraudes con esta información.

Consejos para minimizar el Phishing

Siempre ingresa a nuestra página web digitando la dirección: "https://cactri.com.bo/", nunca por medio de enlaces que reciba de terceros.

SMISHING

Qué es? Es una variante del phishing pero con el uso de los mensajes a celulares mediante mensajes cortos de texto o SMS.

Cómo Funciona?

Los estafadores por medio de mensajes de texto con ofertas de trabajo, suscripciones falsas u otro mensaje con engaños, tienen como objetivo criminal, obtener a través de estos introducir spyware o programas con intenciones maliciosas sin consentimiento.

Consejos para minimizar Smishing

Ser cuidadoso con los datos que resguarda en tu teléfono móvil. Sospecha de mensajes de texto no solicitados y, no respondas mensajes de texto que soliciten esa información. No suministres información personal o financiero a través de SMS.

Cuidarnos de volvernos paranoicos, sólo mantenernos informados y alertas de aquello de te que ocurre para saber cómo cuidarnos.

En caso de que tengas dudas acerca de la página puedes reportarlo al siguiente correo electrónico:

cactri@entelnet.bo