TIPS DE SEGURIDAD

Seguridad en comunicaciones:

La Cooperativa CREA le comunicará por medio de correo electrónico y SMS únicamente información referente a:

- Contenido multimedia, videos, infografías en la página web de la Cooperativa
- Encuestas de satisfacción de servicio, en las cuales nunca solicitaremos datos personales números de tarjetas de crédito, débito o claves.
- Páginas web de promociones y alianzas especiales de la Cooperativa
- Enlaces o links para suscribirse a perfiles en Redes Sociales de la Cooperativa

Seguridad en internet:

Nuestro portal de Internet es seguro, sin embargo, para protegerte contra esta modalidad de fraude, debe tener en cuenta:

- Teclear usted mismo la dirección de la página. No siga enlaces recibidos a través de correo electrónico, mensajes o banners. Lo podrían conducir a páginas falsas.
- Nunca responda a ninguna solicitud de información personal ni confidencial a través de un correo electrónico.
- El único sitio autorizado para que ingrese a su cooperativa en internet es www.crea.fin.ec, siempre digítelo en la barra de dirección.
- Descargue e instale sus aplicaciones directamente desde las tiendas oficiales.
- Nunca almacene sus contraseñas en los navegadores que use.
- Instale en sus equipos programas licenciados de protección contra virus, troyanos, pharming, phishing y keylogger y actualízalos permanentemente.
- Ante cualquier actividad inusual como la solicitud repetitiva de sus credenciales de acceso y números generados por su token, desista de la operación y comuníquese de inmediato con la línea de atención o su asesor de la Cooperativa.
- Verifique que, en el explorador en la parte superior izquierda, la dirección del sitio web inicie con "https".
- Cambie con frecuencia sus claves desde lugares seguros.
- Realice un análisis y limpieza de sus dispositivos apoyándose en su antivirus.
- Recuerde que la Cooperativa nunca solicita información de sus claves por ningún medio.
- Cambie sus claves periódicamente, es una buena práctica y evita que éstas sean vulneradas.
- No descargue archivos provenientes de páginas web que no conozca.
- Smishing: Una forma de phishing, smishing, es cuando alguien intenta engañarlo para que le de su información privada a través de un mensaje de texto o SMS.
- Pharming: es una forma de fraude en línea a la que son vulnerables los equipos electrónicos con bajos niveles de seguridad o antivirus.
- Phishing: Esta modalidad de fraude consiste en utilizar diversos métodos (e-mails, páginas web, chat, etc.) para direccionar a la víctima a una página web falsa y convencerla de que está navegando en la página real de la Cooperativa.
- Vishing: Es el tipo de engaño en que un criminal se comunica con la posible victima para capturar su información.

- Si tiene duda de la procedencia o contenido de un mail, no lo responda y llame al call center de la Cooperativa al (07) 2881707.
- No guarde o anote su clave y usuario en lugares accesibles a otras personas. Memorícelas.
- Identifique este tipo de mensajes por el uso de lenguaje de alarma, advirtiendo sobre consecuencias si el usuario no entrega información (Bloqueos de cuentas, embargos, cargos en tarjetas de crédito).
- No instale en su dispositivo móvil aplicaciones de fuentes desconocidas o de procedencia dudosa.
- Actualice periódicamente el sistema operativo de su dispositivo móvil.
- No permita que terceros conozcan o vean sus claves al digitarlas en su dispositivo móvil.
- Ignore los mensajes que lleguen a su celular o correo electrónico, en los que solicitan datos personales como cuentas, nombres, etc. Desconfié de los enlaces proporcionados.

Seguridad en aplicación móvil:

- Nosotros NUNCA LE PEDIREMOS CLAVES NI DATOS CONFIDENCIALES a través de mensajes de texto de su celular ni llamadas a sus teléfonos fijos o celulares.
- A través de mensajes de texto, whatsapp, redes sociales o llamadas nunca le solicitaremos información confidencial como claves, números de tarjeta de débito, fechas de vencimientos, dígitos de seguridad, saldos, ni número de cuentas.
- Sospeche de notificaciones o llamadas recibidas informándole ser el ganador de premios con peticiones de consignaciones o giros para reclamarlos.
- Utilice antivirus en tu Smartphone
- En caso de pérdida de su celular que se encuentra afiliado a la APLICACIÓN Móvil llamar inmediatamente al call center de la Cooperativa al (07) 2881707.
- Tenga siempre actualizado su correo electrónico y celular en nuestra base para poder recibir las notificaciones, código de seguridad, entre otros. Hágalo exclusivamente en la agencia de su preferencia.
- Mantenga actualizado el sistema operativo y las aplicaciones de su teléfono
- Si su teléfono posee el sistema de doble factor utilícelo con su huella dactilar.
- No utilice aplicaciones modificadas por personas externas a la misma.
- La aplicación oficial nunca le va a solicitar acceder a sus fotos, registros de llamadas, contactos, etc.
- Desactive el bluetooth cuando no lo esté utilizando.
- No utilice el sistema de autoguardado de contraseñas para la aplicación de CREA.