SEGURIDAD EN APLICACIONES MÓVILES

Seguridad en Aplicaciones Móviles

1. Descargue la APP únicamente a través de Google Play o APP Store, en donde la encontraras como: LC virtual

2. Para acceder a la APP Móvil se le solicitará la clave y usuario de acceso de la cooperativa Virtual (la que utiliza a través de la página web).

3. Al efectuar transacciones se le enviará un código de seguridad (OTP) a su número celular y correo electrónico registrado en la Cooperativa.

4. Es responsabilidad del socio/usuario que tenga su información actualizada en la Cooperativa, con el fin de que toda notificación de transacción realizada a través de canales electrónicos pueda ser conocida de inmediato a través de mensajes de texto a su número celular y correo electrónico.

5. Recuerde que la cooperativa no solicita contraseñas de correo electrónico, dispositivos móviles o medio de uso personal por ningún medio.

6. Si se registra 3 intentos de ingreso fallidos a su cuenta con claves incorrectas, el sistema procede a bloquear el acceso. Para desbloquear el dispositivo deberá ingresar en el botón «Cuenta bloqueada» y seguir los pasos indicados.

7. Le recordamos que su clave de acceso y el celular son parte de tus bienes personales por tanto su prolijo cuidado y uso es su responsabilidad.

8. Al terminar el uso de nuestro sistema Virtual y APP Móvil es necesario que cierre la sesión, para evitar inconvenientes.

9. Cooperativa de ahorro y crédito se reserva el derecho de modificar, suspender o interrumpir el servicio del aplicativo móvil o parte de este, no obstante, informará a los socios a través de redes sociales o página web de dicha decisión.

CONSEJOS DE PREVENCIÓN

Le brindamos una lista de las amenazas más frecuentes:

• Phishing. - Zonas que falsifican sitios corporativos legítimos con el objetivo de obtener información confidencial financiera, u otro tipo de información de los usuarios.

• Bot. - Aplicaciones relacionadas, que se han infiltrado en las computadoras de los usuarios con fines maliciosos, por ejemplo, acceso remoto o robo de información.

• Keylogger. - Programas que se ejecutan de fondo y registran todos los movimientos del teclado, y que pueden enviar dicha información posiblemente contraseñas o información confidencial a un tercero externo.

• Software Malicioso. - Diseñado por una persona externa para atacar o manipular la máquina o la red, ya sea para causar daño, utilizar información y recursos en forma no autorizada.

• Spyware. - Software utilizado para registrar e informar sobre la actividad de una computadora de escritorio sin el conocimiento del usuario, excluye hardware y cookies.

• Pharming. - Es la explotación de una vulnerabilidad en el software de los servidores DNS (Domain Name System) o en el de los equipos de los propios usuarios, que permite a un atacante redirigir un nombre de dominio (domain name) a otra máquina distinta. De esta forma un usuario que introduzca un determinado nombre de dominio que haya sido redirigido, accederá en su explorador de internet a la página web que el atacante haya especificado para ese nombre de dominio.

• Troyanos. - Los troyanos son programas maliciosos que están disfrazados como algo atractivo que invitan al usuario a ejecutarlo ocultando un software malicioso. Este software puede tener un efecto inmediato y consecuencias indeseables, por ejemplo, borrar los archivos del usuario, instalar programas indeseables o maliciosos.