Cooperativa de Ahorro y Credito
15 de Abril

SEGURIDADES WEB 15 ONLINE

PROCEDIMIENTOS DE SEGURIDAD

Bloqueo de Usuario:

- *Luego de 3 intentos errados en el inicio de sesión.*
- *Al ingresar 3 veces de manera incorrecta la respuesta a las preguntas de seguridad.*
- *Al ingresar 3 veces de manera incorrecta la clave temporal.*

Reactivación:

- *El sistema validará las preguntas de seguridad.*

Cancelación:

- *Anule su usuario llamando a nuestro Call Center all número 2590040 opción 1, o también acercándose a cualquiera de nuestras oficinas de servicio de atención al cliente.*

CONSEJOS DE SEGURIDAD

Es importante que conozca que es el FRAUDE ELECTRÓNICO y como debe de protegerse.

Fraude electrónico es una manera de estafar a las personas a través de Internet, con la finalidad de obtener información confidencial, de usuarios del sistema financiero.

COMO OPERA ESTE TIPO DE ROBO?

La forma de operar este tipo de robo es muy simple. Llega un correo electrónico a su computador supuestamente de una institución bancaria donde le solicita que actualice sus datos personales y de esta manera acceder a tus cuentas bancarias.

PHISHING

Es la capacidad de duplicar una página Web para hacer creer al visitante que está en la página original de la institución. En forma genérica se realiza para obtener datos personales de los usuarios para luego realizar robos de sus cuentas bancarias o de sus tarjetas (Debito y Crédito)

PHARMING

Es una práctica delictiva en la que un pirata informático desvía el tráfico de Internet del sitio web original hacia otro sitio web fraudulento con apariencia similar, con la finalidad de engañar a los usuarios para obtener sus nombres y contraseñas de acceso, que se registrarán en la base de datos del sitio falso y así obtener acceso a cuentas bancarias, robar datos identificativos o cometer estafas suplantando a usuarios.

Recomendaciones para evitar ser víctima

La pagina de la Cooperativa cuenta con un certificado de seguridad VerySign, la cual los estafadores no pueden adquirir por ende lo más factible es que la página fraudulenta no lo posea y también que opere siempre bajo el contexto de una conexión no segura (sin https) por lo que el usuario notara que no es una página segura y es fraudulenta.

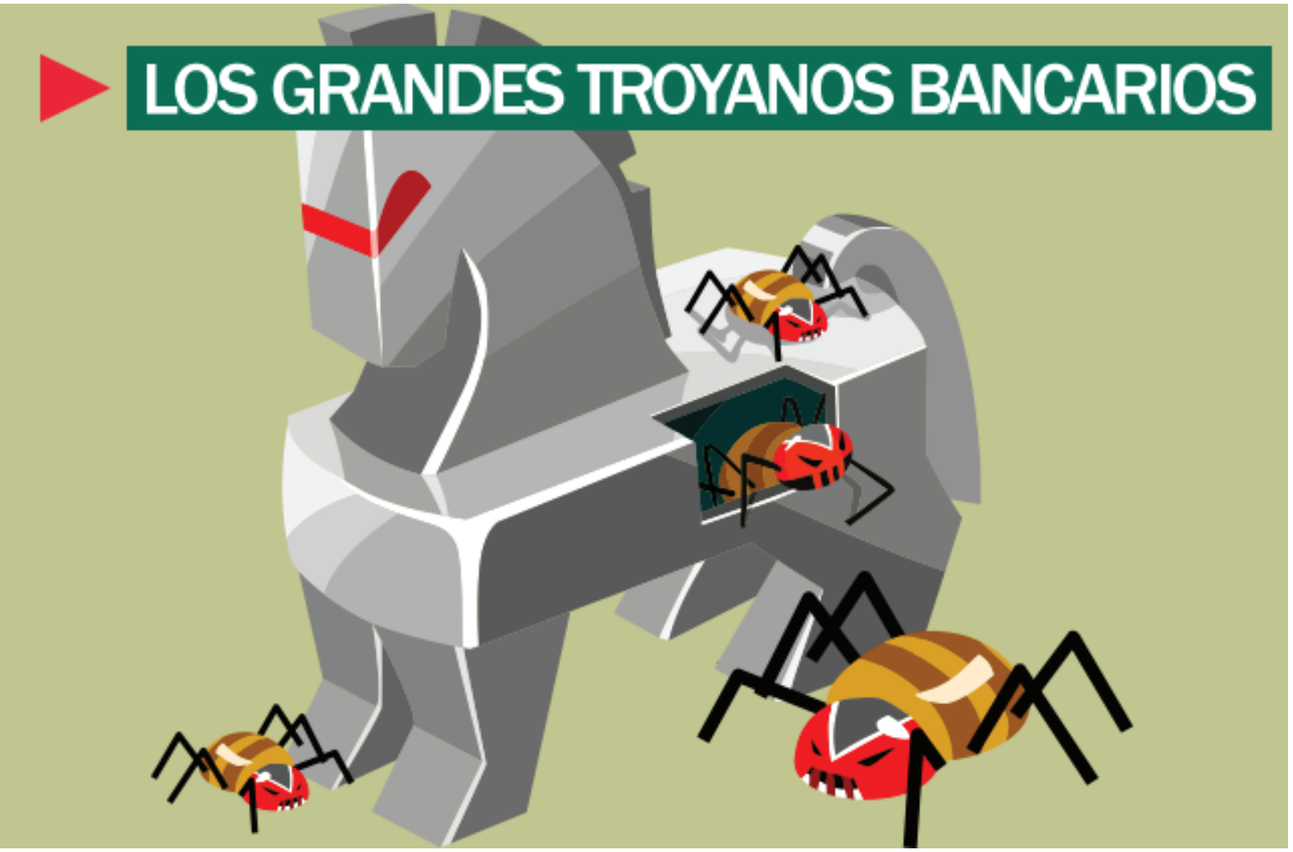
Usar software antipharming que se instala en el computador.

CLICKJACKING

Son sitios que contienen botones invisibles u ocultos sobre otros botones y hacen que los navegantes acepten enviar información o instalar programa y al hacer clip esta instala un descifrador de passwords en su computador.

Recomendaciones para evitar ser víctima

No acceda a su sitio de confianza desde links publicados en sitios desconocidos. Dichos links pueden estar montados sobre botones falsos que lo llevarán al sitio o archivo malicioso



TROYANOS BANCARIOS

Los troyanos son programas maliciosos que se instalan en su computador con o sin su consentimiento para capturar sus datos personales y financieros como números de identificación, NIT y claves de acceso.

ROBO DE IDENTIDAD

El robo de identidad consiste en recibir correos de remitentes desconocidos, que con la promesa de un premio, le solicitan datos personales. Información que posteriormente usarán para acceder a sus cuentas bancarias.

Recomendaciones para evitar ser víctima

Guarda en lugares seguros sus documentos personales. No deje información valiosa en su escritorio o desprotegida en su computador.
Rompa siempre los documentos que bote a la basura.
Cambie frecuentemente sus claves personales.

Ejemplos de mensajes que inducen al socio o cliente acceder a enlaces para ingresar en la supuesta página web de la cooperativa

Problemas de carácter técnico y necesitamos actualizar nuestra base de datos.
Recientemente hemos detectado algunos fraudes y necesitamos actualizar sus datos.
Nuevas recomendaciones de seguridad y por su tranquilidad queremos actualizar sus datos.
Cambios en la política de seguridad de la entidad y necesitamos actualizar su datos.