CIBERSEGURIDAD PARA LOS CONSUMIDORES FINANCIEROS

AGENTES DE

MEDIDAS Y RECOMENDACIONES DE SEGURIDAD Y CIBERSEGURIDAD PARA LOS CONSUMIDORES FINANCIEROS

Para que puedas utilizar con tranquilidad los servicios de Giros & Finanzas C.F. S.A., te brindamos las siguientes recomendaciones que te servirán en tu día a día para protegerte de ciertos riesgos:

PORTAL TRANSACCIONAL

1. El sitio autorizado para ingresar al portal transaccional de Giros & Finanzas, es mediante la dirección o **URL: www.girosyfinanzas.com,** escribirla siempre directamente en el navegador.

2. Verifica que el dominio del sitio al que estás accediendo sea: **https://www.girosyfinanzas.com** y que veas por seguridad, el candado cerrado al lado de la URL.

3. El portal transaccional de Giros & Finanzas cuenta con un certificado digital emitido por DIGICERT, entidad que verifica y autentica la identidad del portal en internet.

4. Evita ingresar al portal transaccional de Giros & Finanzas a través de enlaces recibidos por el correo electrónico, mensajes de texto, entre otros; ya que pueden enviarte a sitios no seguros.

5. Siempre que realice transacciones, efectúelas desde equipos confiables, como tu computador personal u oficina; evita conectarte desde sitios públicos, dónde terceros puedan obtener tus claves secretas.

6. Aprende en lo posible de memoria las credenciales **(usuario y contraseña)** de acceso al portal transaccional de Giros & Finanzas; recuerde que no debe compartir con nadie esta información y mantenla en total reserva.

7. Cambia con frecuencia la contraseña de acceso al portal transaccional de Giros & Finanzas de lo contrario el portal por cuestiones de seguridad le solicita de manera automática cambiar la contraseña cada tres meses.

8. Para cerrar o finalizar sesión de manera segura dentro del portal, ubica los **botones de salida** que hay en cada sitio. Por ejemplo: “Salida Segura”. Asegúrate que no quede tu usuario activo.

CORREO ELECTRÓNICO

1. El correo electrónico no es un canal utilizado por Giros & Finanzas para:

- Solicitar usuarios, contraseñas, códigos de seguridad, claves o información personal.
- Solicitar la actualización de datos de servicios o productos.

2. No hagas clic en mensajes de correo que contengan vínculos (links) al portal transaccional de Giros & Finanzas de los cuales no conozcas su origen.

3. Las claves son personales, confidenciales e intransferibles, no las compartas por correo electrónico, así proteges tu información confidencial y de igual forma, evitas fraudes.

TUS REDES SOCIALES

1. No publiques demasiada información personal, incluyendo datos financieros.

2. No publicar una imagen (foto) tuya frontal completa (tipo documento). Puede usarse para elaborar un documento de identidad falso y lograr así robar tu identidad.

3. Evita la publicación de fotos (tuyas o de familiares) que puedan dar mayor información sobre tu forma de vida.

5. Evitar publicar tu ubicación, esto puede provocar que facilites situaciones no deseadas.

6. No publiques nada que más adelante vayas a lamentar. Nada de lo publicado en internet al borrarse desaparece por completo. ¡Piensa muy bien antes de hacerlo!

SEGURIDAD EN INTERNET

1. Códigos Maliciosos

Hace referencia a programas no autorizados en tus dispositivos o en sitios en internet para realizar actividades maliciosas y obtener información privada. Los códigos maliciosos o también llamados malware incluyen entre otros: troyanos, spyware, gusanos y ransomware.

2. Ingeniería social

El arte de manipular personas usando la fuerza persuasiva para eludir la seguridad de su información, haciéndose pasar por otras personas o incluso empresas y obtener información privada usando para ello el celular, teléfono fijo, correo electrónico, redes sociales, correo tradicional o el contacto directo.

3. Phishing

Es una técnica de ingeniería social que usa correos electrónicos fraudulentos de una supuesta “entidad confiable”, pero que realmente provienen de delincuentes pidiendo claves, solicitando llenar formularios o enviando vínculos a sitios web falsos, donde la información puede ser hurtada.

4. Pharming

Modalidad de fraude que contamina los dispositivos por medio de programas maliciosos para obtener acceso sin su consentimiento, modificando los archivos o haciendo que al digitarse una URL sea redirigido a un sitio web fraudulento para que al usuario ingrese sus datos y estos sean robados.

5. Robo de identidad

Es un tipo de delito donde se obtienen y usan los datos de otra persona de forma ilícita implicando fraude, engaño o delito, para beneficio económico propio o de terceros.

6. Registrador de teclas (Keylogger)

Tipo de software (programa) o hardware (dispositivo) que registra las pulsaciones del teclado, los clics del ratón o toma capturas de pantalla para almacenarlas en un archivo o que sean enviadas por correo electrónico o a internet, permitiendo que otras personas tengan acceso a la información privada.

OTRAS RECOMENDACIONES DE SEGURIDAD

1. Instale y mantenga actualizados una suite de programas de seguridad (licenciados en lo posible) que incluya: Antivirus, Antimalware, Antispam, Antiphishing y firewall personal, para protegerse contra amenazas como phishing, pharming, keyloggers entre otros códigos maliciosos.

2. No almacenes o guardes las contraseñas en ninguno de los navegadores que utilices.

3. Evita instalar software, programas o aplicaciones que provengan de procedencia dudosa.

4. Aplique con periodicidad en sus dispositivos las últimas actualizaciones y parches de:

- Los sistemas operativos como: Windows, Linux o MacOS.
- Las aplicaciones que utilices.
- Los programas que tenga instalado en sus dispositivos.
- Los navegadores/browsers como: Internet Explorer, Edge, Firefox, Chrome, Opera, Safari.

5. Al realizar transacciones por internet, utilice una cuenta de usuario “estándar” o que tenga privilegios limitados y no utilice nunca una cuenta “Administrador”, para una protección adicional.

6. No realices operaciones financieras desde dispositivos con conexiones a internet en lugares públicos, ya que son inseguros. Utilice preferiblemente su plan de datos que tenga con su operador de telefonía móvil.

7. Evite conectarse a redes inalámbricas abiertas en lugares públicos (centros comerciales, bares, restaurantes), ya que pueden estar interferidas o creadas por delincuentes y al realizar operaciones bancarias es posible que roben su información personal.

8. Si es inevitable el conectarse a una red inalámbrica abierta (sin contraseña) en lugares públicos para realizar operaciones bancarias, confirme que sea la red oficial del lugar donde se encuentre ubicado.

MANTÉN TU SISTEMA OPERATIVO, APLICACIONES Y PROGRAMAS ACTUALIZADO

Estas son algunas recomendaciones al momento de hacer uso de dispositivos para realizar operaciones bancarias:

1. Programas Antivirus y Antimalware

Programas de seguridad para dispositivos, cuyo objetivo es: buscar, detectar, bloquear, prevenir, desinfectar y eliminar virus y códigos maliciosos.

2. Programas Antiphishing

Programas de seguridad para dispositivos que identifican el contenido del Phishing en sitios web, correos electrónicos o formularios comúnmente desde internet, y bloquear su contenido.

4. Firewall personal

Programas de seguridad que funciona como un centinela monitoreando las conexiones (entrantes y salientes) a internet con capacidad de “distinguir” las legítimas de las que no lo son y en conjunto con el antivirus y antimalware, brindan un mayor grado de seguridad posible.

5. Actualizaciones y parches del sistema operativo, software y aplicaciones

Es importante siempre tener al día las actualizaciones y parches del software, las aplicaciones y el sistema operativo porqué estas:

- Arreglan agujeros de seguridad
- Corrigen errores
- Mejoran su rendimiento
- Incrementan la estabilidad

- Aumentan la seguridad
- Añaden nuevas funciones
- Implementan las últimas mejoras
- Mejoran la experiencia del usuario.