(Resolución CRC 5111 de 217. Artículo 2.1.10.7)

Optinetv S.A.S comunica las consideraciones que deben tener en cuenta nuestros usuarios con la finalidad de salvaguardarse ante fraudes que se puedan presentar por el uso y disfrute de nuestro servicios.

Artículo 2.1.10.7. Prevención de Fraudes. Los operadores tienen la obligación de hacer uso de herramientas tecnológicas adecuadas para prevenir que se cometan fraudes al interior de sus redes y debe hacer controles periódicos respecto a la efectividad de estos mecanismos. Cuando el usuario presente una PQR (petición, queja/reclamo o recurso) que pueda tener relación con un presunto fraude, el operador debe investigar sus causas; y en caso de que determine la no existencia de un fraude, le debe demostrar al usuario las razones por las cuales no procede su PQR Disposiciones analizadas por Avance Jurídico Casa Editorial Ltda.© Página 15 de 59 (petición, queja/ reclamo o recurso). Sin embargo, si se demuestra que el usuario actuó diligentemente en el uso del servicio contratado, no habrá lugar al cobro de los consumos objeto de reclamación.

A continuación tenga en cuenta las siguientes consideraciones:

- No suministrar información personal por medio de correo electrónico o portales web que el cliente no conozca o sospeche que no son legales.
- Para su red WI-FI es importante crear claves difíciles de identificar, recuerde cambiarlas frecuentemente llamando o dirigiéndose a nuestra oficina más cercana. Memorice las claves, no las escriba ni guarde en lugares de fácil acceso. No permitas que terceros vean o conozcan sus claves.
- Si recibe ofertas o información de premios vía SMS, MMS, vía telefónica o de cualquier otro medio solicitando cualquier datos o información personal, verifique la fuente de la solicitud a través de nuestras líneas de atención telefónica, antes de dar cualquier información o realizar cualquier transacción, para garantizar su seguridad.
- Proteja la interfaz de administración remota (Anydesk, Teamviewer). Utilice conexiones VPN temporales.
- Bloquee en el firewall de su computador los puertos TCP/IP de acceso remoto que no utilice.
- Use antivirus reconocidos en sus dispositivos y equipos de computo.
- Mantenga seguro los buzones de correo y elimine los que no utiliza.
- Utilice un sistema de detección de intrusos (IDS) y herramientas de protección en sus dispositivos.
- Cuando sus dispositivos y equipos de cómputo requieran soporte se sugiere contratar el servicio técnico con empresas legalmente establecidas, que posean la suficiente experiencia y reconocimiento en el campo.
- Acceso únicamente desde direcciones IP y web conicidad.
- No use la dirección IP pública para acceder remotamente aplicativos o cámaras de seguridad, preferiblemente utilice NAT y conexiones seguras a través de VPN (red privada virtual).