Prevención de fraudes

Prevención de fraudes (Resolución CRC 5111 de 217. Artículo 2.1.10.7.)

A continuación, relacionamos las practicas que se debe tener en cuenta:

- 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 WiFi es importante crear claves difíciles de identificar, recuerde cambiarlas frecuentemente llamando o dirigiéndose a nuestras oficinas más cercanas. 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 cómputo.

- 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 conocidas.

- 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).