

## **RECOMENDACIONES PARA PREVENIR MAL USO DE LA LINEA O DEL TELEFONO**

### **Para Usuarios que acceden al servicio de Larga Distancia Internacional a través de de redes móviles:**

- No preste su tarjeta SIM o su teléfono a otras personas, recuerde que usted es totalmente responsable por el uso de estos y de las llamadas de LDI que se generen.
- En caso de pérdida o robo de su teléfono o tarjeta SIM, reporte este hecho inmediatamente a su operador para bloquear los servicios.
- Active el código de seguridad para uso del teléfono (vea manual de su teléfono) y el código de acceso PIN de la SIM CARD (vea documento que acompaña su SIM CARD). Para activar el PIN es necesario consultar el documento que acompaña la Sim Card. Lo anterior le ayudará para que otra persona no use su teléfono sin su autorización.
- Mantenga desactivadas las conexiones “infrarrojo”, “wi-fi”, “bluetooth” y cualquier otra conexión alámbrica o inalámbrica mientras no las requiera. Si usted mantiene activadas permanentemente conexiones mientras no las requiere, puede ser susceptible a consumos no autorizados de su línea celular y otros problemas de seguridad.
- Si recibe ofertas o información de premios vía SMS, MMS, vía telefónica o de cualquier otra manera conocida o por conocer a través de su celular solicitando cualquier dato o información personal o del servicio, o solicitándole realizar cualquier tipo de transacción o llamada, 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.
- No genere llamadas a números desconocidos puede tratarse de una llamada de Larga Distancia Internacional.
- Consulte las tarifas que aplican para LDI para que lleve el control de sus consumos antes de realizar las llamadas.
- Si usted no hace llamadas internacionales, pida a su operador el bloqueo de las mismas.
- Hay números de teléfonos internacionales que tienen la misma cantidad de dígitos que los de larga distancia nacional; pero, en realidad, corresponden a otro país. Si no está seguro de si el número es nacional o de otro país, antes de llamar consulte con su operador.

### **Para Usuarios que acceden al servicio a través de de redes Fijas:**

Compruebe que no existan derivaciones u otras conexiones desde el cable que va de la entrada de su vivienda sea casa o edificio hasta el gabinete o armario principal donde se conecta el teléfono. Exhorte a la administración de su edificio a tomar todas las medidas de seguridad pertinentes con respecto a las redes telefónicas.

- Denuncie situaciones sospechosas como: pérdidas constantes de tonos en su línea, escucha de conversaciones al momento de levantar el auricular, repiques cortados de teléfono cuando esta colgado, si al momento de estar realizando llamadas usted escucha cruces de llamadas, ruidos extraños o interrupciones.
- Informe a su operador lo antes posible (inmediatamente) en caso de notar (observar, apreciar) comportamientos sospechosos en personas con o sin identificación que ese

encuentren manipulando las redes telefónicas o que se tenga indicio de robo o daño de cable e infraestructura en las redes de telecomunicaciones.

**Dialers:** se trata de un programa que marca un número de tarificación adicional (NTA) usando el módem, estos NTA son números cuyo costo es superior al de una llamada nacional. Estos marcadores se suelen descargar tanto con autorización del usuario (utilizando pop-ups poco claros) como automáticamente. Además pueden ser programas ejecutables o ActiveX.

En principio sus efectos sólo se muestran en usuarios con acceso a la Red Telefónica Pública Básica Conmutada (RTPBC) o Red Digital de Servicios Integrados (RDSI) puesto que se establece la comunicación de manera transparente para el usuario con el consiguiente daño económico para el mismo. Aunque la tarificación no funcione con los usuarios de PLC, Cable módem, etc. afecta al comportamiento del ordenador ya que requiere un uso de recursos que se agudiza cuando se está infectado por más de un dialer.

Los marcadores telefónicos son legítimos siempre y cuando no incurran en las malas artes que lo ha definido como Malware que son los siguientes trucos:

1. No se avisa de su instalación en la página que lo suministra.
2. Hace una reconexión a Internet sin previo aviso, o lo intenta.
3. Se instala silenciosamente en el ordenador utilizando vulnerabilidades del navegador, programa de correo electrónico (email), otros programas de acceso a Internet o el propio sistema operativo.
4. Puede dejar un acceso directo al escritorio sin conocimiento del usuario.
5. Puede instalarse unido a otros programas como barras de mejora para el navegador.
6. No informa de los costos de conexión.

Afortunadamente hay varios programas que pueden detectar y eliminar los dialers, entre ellos la mayoría de los antivirus actuales, sin olvidar los programas gratuitos que podemos encontrar en los enlaces que se pueden encontrar en esta misma página.

### **TAMBIÉN ES IMPORTANTE QUE TENGA EN CUENTA MODALIDADES DE FRAUDE COMO LAS SIGUIENTES PARA QUE LAS PREVENGA:**

**Fraude de Suplantación de Identidad o Nombre:** Sucede cuando una persona toma un servicio de telecomunicaciones bajo el nombre de otra persona o utiliza un nombre falso, documentación falsa, dirección falsa, etc. Esta modalidad de fraude puede utilizarse para realizar acciones delictivas y/o usos inadecuados de los servicios de telecomunicaciones ofrecidos por su compañía y lo afecta directamente pues se generan grandes cobros a nombre de la persona afectada que traen consigo reportes en las centrales de crédito por mora y hasta acciones judiciales en su contra. Con el fin de disminuir este riesgo, asegúrese de proteger toda su información personal de manera cuidadosa nunca entregándola a desconocidos y en caso de pérdida o robo de su documento de identidad reportarle inmediatamente a las autoridades pertinentes.

**Fraude con PBX:** Sucede cuando se recibe una llamada de alguien que dice ser empleado de la empresa de teléfonos, el cual se encuentra investigando problemas técnicos con su línea, o verificando llamadas de Larga Distancia que supuestamente se hicieron desde su línea. El individuo que llama le pide que colabore ya sea marcando un código especial o transfiriéndolo a una línea externa antes de colgar. Al hacer esto, es posible que usted le permita al individuo que llama hacer llamadas fraudulentas que luego se facturan al número de teléfono. Este fraude sólo funciona si su teléfono es atendido por una central telefónica privada (PBX, por sus siglas en inglés). Para evitar este fraude:

- Pida a la persona que llama se identifique con nombre, número de documento de identidad y teléfono.
- Comuníquese a la persona que llamó que se va a llamar a la compañía telefónica, con el fin de que ellos determinen si su línea tiene o no problemas.
- No marque ningún código ni transfiera llamadas a líneas externas.
- Reporte a su empresa de teléfonos estas llamadas sospechosas.

**Cambios de Servicio:** Se efectúa cuando sobre una cuenta de teléfono, terceros realizan adiciones sobre artículos o servicios que usted no autorizó o recibió. Las compañías de teléfono locales deben facturar las llamadas realizadas a través de otras compañías cuyos cargos aparecen en páginas separadas de su cuenta de teléfono local. A veces, los cargos parecen números de teléfono comunes y no tienen explicación. Es posible que se incluyan cargos no autorizados en su cuenta por aceptar llamadas por cobrar de un desconocido, llenar inscripciones en loterías o rifas o responder a indicaciones verbales engañosas durante una llamada. Con el fin de evitar esto tenga en cuenta:

- Verificar cuidadosamente su factura telefónica, en caso de tener dudas sobre algún cobro, llame al proveedor del servicio.
- Notificar a su compañía de teléfono acerca de los cargos que desconoce.
- Esta práctica puede afectar negativamente su historial de crédito.