RIESGOS RELATIVOS AL SERVICIO DE INTERNET

Malware: Es el acrónimo en inglés de software malicioso (malicious software). El objetivo de este tipo de aplicaciones es dañar la computadora. En la mayoría de los casos, la infección ocurre por "errores" realizados por los usuarios, al ser engañados por el atacante. Existen muchas herramientas (antivirus, antispyware) y buenas prácticas, que reducen el riesgo de infección, ante todas las variantes de códigos maliciosos.

Ciberacoso: Es una conducta hostil que puede ser practicada hacia los niños. La víctima de este tipo de acosos es sometida a amenazas y humillaciones de parte de sus pares en la web, cuyas intenciones son atormentar a la persona y llevarla a un quiebre emocional. Estas prácticas pueden ser realizadas a través de Internet, así como también, teléfonos celulares y videoconsolas.

Sexting: Proviene del acrónimo formado entre Sex y Texting. Inicialmente, y como lo indica su nombre, se trataba del envío de mensajes con contenidos eróticos. Posteriormente, dado el avance tecnológico, esta modalidad evolucionó hacia el intercambio de imágenes y videos convirtiéndose en una práctica habitual entre adolescentes y niños.

Phising: es una estafa de correo electrónico o comunicaciones dirigida a personas, organizaciones o empresas específicas. Aunque su objetivo a menudo es robar datos para fines maliciosos, los cibercriminales también pueden tratar de instalar malware en la computadora de la víctima.

Robo de información: Toda la información que viaja por la web, sin las medidas de precaución necesarias, corre el riesgo de ser interceptada por un tercero. De igual modo, existen también ataques con esta finalidad. La información buscada, normalmente apunta a los datos personales.

¿CÓMO PREVENIRLO?

Para prevenir las vulnerabilidades y los riesgos en la red, el usuario debe tener en cuenta las siguientes acciones:

- Proteger adecuadamente los Dispositivos.
- Instalar una herramienta antivirus para que detecte posibles aplicaciones maliciosas que intenten colarse en el dispositivo.
- No intercambiar información privada o confidencial.
- Nunca responda a solicitudes de información personal a través de correo electrónico.
- Utilizar contraseñas fuertes y protegerlas.
- Mantener protegido el dispositivo de acceso a la red de manera adecuada.
- Instalar en el dispositivo un antivirus y mantenerlo actualizado para que detecte las últimas amenazas que circulan por la red.

Por su lado la empresa TELCOSUR cuenta con mecanismos de protección del CORE de la Red, como son: Firewalls y filtrado perimetral, lo cual, evita y elimina todo riesgo de acceso no autorizado a la data correspondiente al servicio de correo masivo de sus usuarios.

De igual manera cuenta con una plataforma especializada en el bloqueo de páginas y redirección a portales cautivos, dando cumplimiento a lo establecido por la normatividad vigente, se filtran las páginas de pornografía infantil publicadas por el ministerio de Comunicaciones Ley 679 (Esto se hace a través de los URLs reportados en la página).