La seguridad en Internet

El estar conectados a la Internet ya nos hace vulnerables. El objetivo es establecer reglas y medidas que usar contra ataques en la web.

Internet representa un canal inseguro de intercambio de información incluyendo un alto riesgo de intrusión o fraude. Se han estado utilizando diferentes métodos para proteger la transferencia de datos, incluyendo el cifrado de información.

Un usuario puede ser engañado o forzado a descargar programas en su computador, tableta, celular, etc., con intenciones dañinas. Dichos programas pueden aparecer de distintas formas, tal como virus, troyanos, spyware o gusanos;

Algunos de estos son:

Malware, abreviación de programa malicioso, es cualquier programa utilizado para cambiar o dañar la forma en la que opera el computador, tableta, celular, etc.

Virus Informáticos, son programas que pueden replicar sus estructuras o efectos infectando otros archivos o estructuras en un computador, tableta, celular, etc.., El uso más frecuente de un virus es robar información.

Ransomware, restringe el acceso al sistema del computador, tableta, celular, etc.., demanda al usuario el pago de un rescate para que se elimine dicha restricción.

Scareware, es un programa de estafa, normalmente con un beneficio limitado o inexistente, que se vende a los consumidores a través de estrategias de marketing poco éticas. Se utiliza el shock, la ansiedad o el miedo que produce a los usuarios para lograr su objetivo.

Spyware, son programas espía que monitorizan la actividad de un computador, tableta, celular, etc., envían la información obtenida a otras personas sin el consentimiento del usuario.

Troyano, es en términos generales, un programa que se hace pasar por inofensivo para que el usuario lo descargue en su ordenador.

Ataques de denegación de servicios, también llamado ataque DoS (siglas en inglés de *denial of service*), es un intento para hacer que uno de los recursos de un computador, tablet, celular, etc., quede inutilizado para su usuario. A pesar de que

los motivos, las formas de llevarlo a cabo o las víctimas de un ataque DoS pueden variar, generalmente consiste en hacer que una página de Internet o un servicio web concreto deje de funcionar correctamente de forma temporal o indefinida.

Phishing, ocurre cuando el atacante se hace pasar por una entidad segura, ya sea vía email o a través de una página web. Las víctimas son guiadas hacia webs falsas que aseguran ser totalmente legítimas a través de email, mensajería instantánea y otros medios.

Firewalls, es un programa que controla el acceso entre redes. Generalmente consiste en varios accesos y filtros los cuales varían de un firewalls a otro, leen el tráfico de una red y son capaces de bloquear parte de ese tráfico si considera que puede ser peligroso. Los firewalls actúan como servidor intermediario entre las conexiones de SMTP y HTTP.

Spam, El correo masivo supone actualmente la mayor parte de los correos electrónicos intercambiados en Internet, siendo utilizado para anunciar productos y servicios de dudosa calidad. Usualmente los mensajes indican como remitente del correo una dirección falsa. Por esta razón, no sirve de nada contestar a los mensajes de *spam*: las respuestas serán recibidas por usuarios que nada tienen que ver con ellos. El antispam es un programa que permite a los usuarios prevenir o restringir la entrega de correos no deseados, analiza automáticamente todos los correos electrónicos entrantes enviados a un buzón de correo detecta y eliminar el spam y los correos no deseados.