Seguridad en Internet (Vocabulario)

Contenido:

- Vocabulario propio del tema.

Malware: *una variedad de software hostil, intrusivo o molesto. El término virus informático suele aplicarse de forma incorrecta para referirse a todos los tipos de malware.*

Navegador: ***p****rograma que permite navegar por internet u otra red informática de comunicaciones. La mayoría de los navegadores permiten también enviar y recibir mensajes de correo electrónico.*

Buscador: ***u****n buscador es una página web en la que se ofrece consultar una base de datos en la cual se relacionan direcciones de páginas web con su contenido. Su uso facilita enormemente la obtención de un listado de páginas web que contienen información sobre el tema que nos interesa. Existen varios tipos de buscadores pero todos ellos tienen en común que permiten una consulta en la que el buscador nos devuelve una lista de direcciones de páginas web relacionadas con el tema consultado.*

Router: ***s****e trata de un producto de hardware que permite interconectar computadoras que funcionan en el marco de una red. Se encarga de establecer qué ruta se destinará a cada paquete de datos dentro de una red informática.*

Gusano: *es un malware que tiene la propiedad de duplicarse a sí mismo.*

Los gusanos utilizan las partes automáticas de un sistema operativo que generalmente son invisibles al usuario. Los gusanos informáticos se propagan de computadora a computadora, pero a diferencia de un virus, tiene la capacidad a propagarse sin la ayuda de una persona. Lo más peligroso de los gusanos informáticos es su capacidad para replicarse en el sistema informático, por lo que una computadora podría enviar cientos o miles de copias de sí mismo, creando un efecto devastador a gran escala.

Los gusanos casi siempre causan problemas en la red (aunque sea simplemente consumiendo ancho de banda), mientras que los virus siempre infectan o corrompen los archivos de la computadora que atacan

Virus*: un virus es un malware que tiene por objetivo alterar el funcionamiento normal del ordenador, sin el permiso o el conocimiento del usuario. Los virus, habitualmente, reemplazan archivos ejecutables por otros infectados con el código de este. Los virus pueden destruir, de manera intencionada, los datos almacenados en una computadora,*

aunque también existen otros más inofensivos, que solo producen molestias.

Spayware: *el spyware es un software que recopila información de un ordenador y después transmite esta información a una entidad externa sin el conocimiento o el consentimiento del propietario del ordenador.*

Adware: *se trata de un tipo de software que, de modo automático, exhibe al usuario anuncios publicitarios. De este modo, el fabricante del software obtiene ganancias a partir de estas publicidades.*

Phishing: *es utilizado para referirse a uno de los métodos mas utilizados por delincuentes cibernéticos para estafar y obtener información confidencial de forma fraudulenta como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria de la víctima.*

Spam: *correo electrónico no solicitado que se envía a un gran número de destinatarios con fines publicitarios o comerciales*

Troyano: *un troyano es un tipo de virus cuyos efectos pueden ser muy peligrosos. Pueden eliminar ficheros o destruir la información del disco duro. Además, son capaces de capturar y reenviar datos confidenciales a una dirección externa o abrir puertos de comunicaciones, permitiendo que un posible intruso controle nuestro ordenador de forma remota. También pueden capturar todos los textos introducidos mediante el teclado o registrar las contraseñas introducidas por el usuario. Por ello, son muy utilizados por los ciberdelincuentes para robar datos bancarios.*

Sexting: *es el envío de mensajes, fotos o vídeos de contenido sexual por medio de teléfonos celulares. Evidentemente, esta práctica tiene muchos riesgos.*

Ciberbullying: ***e****s el uso de los medios telemáticos (Internet, telefonía móvil y videojuegos online principalmente) para ejercer el acoso psicológico entre iguales. No se trata aquí el acoso o abuso de índole estrictamente sexual ni los casos en los que personas adultas intervienen.*

Cibergrooming*: el cibergrooming es un método formado por un conjunto de estrategias que una persona adulta desarrolla para ganarse la confianza de un menor de edad a través de Internet y las nuevas tecnologías (TIC), para conseguir su control a nivel emocional, con el fin último de obtener concesiones de índole sexual.*

Grooming: *igual que el anterior pero se da sin intermediarios como las redes sociales, es decir, el adulto se gana la confianza del menor en directo, mediante encuentros físicos, para luego desembocar en los mismos actos.*

Rootkit: *un RootKit es un programa o conjunto de programas que un intruso usa para*

esconder su presencia en un sistema y le permite acceder en el futuro para manipular este sistema.Para completar su objetivo, un Rootkit altera el flujo de ejecución del sistema operativo o manipula un conjuntos de datos del sistema para evitar la auditoría.

***PopUp (ventana emergente)**: es una ventana nueva que aparece de repente en la pantalla de tu ordenador.Verás pop-ups, por ejemplo, cuando abras un programa nuevo, cuando cambies de un programa a otro (eso es multitareas), y cuando utilices un menú desplegable.*

***Cookie:** son pequeños archivos que algunos sitios web guardan en tu ordenador.*

Las cookies almacenan información sobre tí, como nombre de usuario o información de registro, o preferencias de usuario, pero no espían, como el spyware. Si tienes una cookie de un sitio web al que vas a menudo, la cookie recuerda cosas que harán tu próxima visita a esa página un poco más fácil, e incluso hace que las páginas se carguen un poco más rápido.