Glosario riesgos de internet

bq

GLOSARIO RIESGOS DE INTERNET

En este documento, podemos consultar los conceptos trabajados durante las sesiones de Uso y seguridad en Internet que hacen referencia a los riesgos que se pueden encontrar en la red. Se pueden dividir en 3 niveles:

- Riesgos para los dispositivos: son los que afectan al software de los dispositivos (ordenador, tablet…). Los principales riesgos son:
  - **Malware**: es cualquier programa cuyo objetivo sea dañar un dispositivo o alterar su funcionamiento normal. Dentro de este grupo podemos encontrar: virus, troyanos, gusanos, ransomwares, rogues, etc.
  - **Gusano**: programa que se copia o reproduce a sí mismo y cuyo objetivo es impedir el trabajo de los usuarios colapsando las redes y los dispositivos.
  - **Ransomware**: programa que restringe al usuario el acceso a determinados elementos o archivos de su dispositivo, con el fin de que el atacante obtenga un beneficio para desbloquear el acceso a dichos elementos.
  - **Rogueware o rogue software**: programa de seguridad falso o antivirus ficticio cuyo objetivo es infectar el dispositivo en el que se instala.
  - **Troyano**: programa cuya apariencia es la de una aplicación normal, pero al ejecutarlo permite un acceso remoto del atacante al dispositivo del usuario.
  - **Virus**: programa cuyo objetivo es alterar el funcionamiento del ordenador sin que el usuario se dé cuenta.

Con el fin de estar protegidos contra estos ataques se pueden utilizar antivirus o antimalware, así como utilizar una configuración de seguridad alta del dispositivo que impida instalar programas de creadores desconocidos y el acceso a determinadas páginas.

- Peligros de robo de datos o información: En este nivel se engloban aquellos riesgos o elementos que intentan sacar información del usuario. Podemos encontrar los siguientes:
  - **Hacker**: persona que se dedica a descubrir las debilidades de un dispositivo o red, sin que resulte dañino para el usuario.
  - **Cracker**: son hackers pero con la diferencia de que estos debilitan o rompen sistemas de seguridad con el fin de causar daños.
  - **Keylogger**: programa que se encarga de registrar lo que el usuario escribe en su teclado y almacenarlo en un archivo que es enviado a través de Internet, con el fin de obtener información y datos del usuario al que está atacando.
  - **Phishing**: robo de información confidencial (personal y/o financiera). Este método utiliza el correo electrónico que parece de confianza con el fin de que el usuario envíe sus datos o información o los introduzca en una página y se envíen al atacante.
  - **SCAM**: engaños que se llevan a cabo a través de Internet. Son muy diversos, desde algunos que intentan convencer al usuario para

que introduzca sus datos en una página hasta otros que ofrecen un servicio que no es verdad (premios, aplicaciones, servicios bancarios,etc.).
  - **SPAM**: correos electrónicos remitidos por un desconocido que se envían sin solicitarlo. Un ejemplo de ello son los correos publicitarios.
  - **Spyware**: tipo de malware que recopila información de un ordenador y la envía al atacante o sitio externo sin el consentimiento del usuario.

Una posible solución contra este tipo de peligros es el firewall. Un cortafuegos (firewall) es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas. Además, se podrán tener filtros en el correo electrónico que eliminen o almacenen dichos correos en una carpeta en vez de en la bandeja de entrada.

- Riesgos personales en Internet: En este último nivel están englobados todos aquellos peligros que causan daño, tanto físico como psicológico al usuario. Se pueden encontrar:
  - **Bullying o ciberacoso**: conducta que pretende humillar o amenazar a una persona a través de Internet. La víctima y el agresor suelen tener aproximadamente la misma edad, es decir, son pares.
  - **Cyberstaking o ciberacecho**: uso de Internet para acosar a un individuo o grupo haciendo falsas acusaciones sobre él.
  - **Grooming**: conducta en la que un adulto intenta persuadir a un menor, con el fin de ganarse su confianza y crear una conexión sentimental, para poder abusar sexualmente de él.
  - **Sexting**: difusión o intercambio de contenidos (vídeos, fotos…) de tipo sexual, enviados por el usuario utilizando un teléfono móvil o cualquier otro dispositivo, como una webcam.
  - **Sextorsión**: amenazas de una persona hacia otra para difundir un contenido (imagen o vídeo) personal (desnudo, realizando actos sexuales, etc.) que la persona no quiere que se haga público.

Para evitar estas conductas, se deberá adoptar un especial cuidado con los contenidos personales que se publican o envían y en caso de que ocurra, se deberá denunciar.