Riesgos técnicos: virus, troyanos, malware…

Uno de los mayores riesgos técnicos que puede llegar a sufrir un internauta es que, el dispositivo con el que se conecta a Internet ya sea ordenador de sobremesa, ordenador portátil, tableta, *smartphone*, etc., se infecte por algún tipo de virus, troyano o malware que provoquen el mal funcionamiento del equipo, pérdida de información, así como un riesgo para la seguridad de los datos contenidos en él y del propio usuario.

Los menores no quedan ajenos a este riesgo, sino todo lo contrario, ya que, por su menor capacidad de entendimiento, en general, (no siempre es así…), la ansiedad y rapidez de hacer un clic o pulsar una tecla ante pantallas llamativas y atrayentes, caen en un error y el dispositivo puede quedar infectado.

Según el Informe *NET Children Go Mobile*, establece que los virus constituyen el riesgo que se encuentran más los menores de edades comprendidas de 9 a 16 años, con un porcentaje del 23% de infecciones para ordenadores y un 5% para teléfono móvil o *smartphone* en el uso de los dispositivos por parte del menor (Garmendia M. J., 2016).

Este riesgo como otros anteriores, viene determinado por las actividades que realizan los menores día a día en Internet.

Uno de los mayores riesgos referidos a este apartado y que ha sufrido un crecimiento exponencial es el denominado *malware* (abreviatura de *malicious software*) que se podría definir como programas o códigos informáticos maliciosos que circulan por Internet y cuya función principal es dañar un sistema o causar un funcionamiento deficiente (Guilabert, 2016). Dentro de esta catalogación como *malware* se encuentran términos como virus, troyanos, gusanos (*worms*), *botnets, ransomwares, keyloggers*, etc.

Para minimizar el riesgo ante estas amenazas es primordial el comportamiento del usuario para

reducir la probabilidad de que sean víctimas de este tipo de programas. Los jóvenes realizan determinadas actividades día a día que aumentan la probabilidad de infección por *malware*. No sólo podemos proteger nuestros dispositivos con antivirus, sino advertir que ciertas actividades conllevan un riesgo mayor. También se puede reducir el riesgo asegurando nuestros equipos mediante contraseñas seguras, reducir el anonimato en la Red para poder realizar una transformación en el negocio del consumo de contenido y así hacer más atractivo el lícito del pirata (Guilabert, 2016).

Bibliografía

- Garmendia, M. J. (2016). *Net Children Go Mobile: Riesgos y oportunidades en internet y el uso de dispositivos móviles entre menores españoles (2010-2015).* Madrid: Red.es/Universidad del País Vasco/Euskal Herriko Unibertsitatea. Obtenido de Universidad del Pais Vasco: https://www.ehu.eus/documents/1370232/0/Informe+NET+CHILDREN+RED.ES+Espa%C3%B1a+2016.pdf
- Guilabert, N. G. (2016). *Actividades cotidianas de los jóvenes en Internet y victimización por malware.* Obtenido de Revista de Internet, Derecho y Política: https://idp.uoc.edu/articles/10.7238/idp.v0i22.2969/galley/3088/download/