ISSN edición impresa: 1699-2105. ISSN edición web (http://revistas.um.es/educatio): 1989-466X

Valle, M.

Ciberseguridad. Consejos para tener vidas digitales más seguras

Madrid: Editatum, 2018

Saber utilizar la tecnología y hacer un uso seguro de la misma son algunas de las asignaturas pendientes en la escuela actual para responder a las demandas de la sociedad de la información y de la comunicación. Este hecho no se debe del todo al descuido de las instituciones educativas, sino también a la dificultad que entraña estar actualizado respecto al amplio abanico de tecnología actual, ya sea en forma de dispositivos como de servicios, lo cual implica dedicar tanto horas de formación como práctica y experiencia.

La autora de este libro, Mónica Valle, periodista y comunicadora especializada en tecnología, innovación y seguridad informática es directora de *Bit Life Media,* publicación online dedicada a la actualidad tecnológica, ciberseguridad e innovación. En este libro, la autora propone como objetivo despojar a la ciberseguridad de la complejidad que se

asocia a este tema haciéndolo así más accesible al usuario. Es de sentido común que cualquiera de nosotros puede ser víctima de un ciberataque o un delito informático, para evitarlo, según afirma Valle, simplemente hay que estar prevenido para así actuar en consecuencia.

Nos encontramos con una obra divulgativa, una guía, que explica desde la base, de una forma sencilla, comprensible y exacta la ciberseguridad a partir de los ciberataques que más nos afectan diariamente, a través de una serie de consejos dirigidos a detectar esos ataques y evitar convertirnos en víctimas de ellos. La guía está estructurada en 11 secciones donde, paso a paso y de una forma clara, se detallan todos los aspectos necesarios para entender la ciberseguridad.

En el primer y segundo capítulo se tratan los conceptos de ciberseguridad, *hacker* y ciberdelincuente, incidiendo en la diferenciación entre estos dos últimos. El tercer, cuarto y quinto capítulo enmarcan el cibercrimen en la actualidad partiendo de un recorrido histórico por los primeros virus informáticos y el inicio de internet; se explica el porqué del interés de los cibercriminales por nuestros datos, y por último, se describen los diferentes tipos de ciberamenazas como el *spam*, los fraudes y estafas a través de correo electrónico, la estafa nigeriana, los bulos, las cadenas de e-mails, el *phishing*, la ingeniería social, el *malware*, virus informáticos, gusanos, troyanos, *adware*, *spyware* y el *ransomware*. El sexto capítulo, sobre las redes sociales y la privacidad, aborda temas como los datos que compartimos, la configuración de la privacidad, los bulos y noticias falsas, la identidad digital y el derecho al olvido. El séptimo capítulo trata el acoso a través de la red, ciberacoso o ciberbullying, así como la sextorsión, entrando en el octavo capítulo en la relación entre internet y los menores, posiblemente el capítulo más importante para profesionales de la enseñanza, pero también para padres y madres preocupados por la actividad de sus hijos en la red. En este capítulo se trata el ciberbullying entre menores, el *grooming*, el *sexting*, la privacidad y el abuso de tecnología.

El noveno capítulo es muy breve y práctico, se titula *Me han ciberatacado, ¿ahora qué hago?* En él podemos encontrar unos simples pasos y direcciones a las que acudir y tratar el problema de forma efectiva, sea cual sea el caso al que nos enfrentemos entre los tantos que se explican a lo largo del libro. Los dos últimos capítulos, décimo y undécimo, a modo de conclusión, describen lo que está por venir y lo que se espera del usuario que haya concluido la lectura de esta guía. Por supuesto, uno

no deja de ser vulnerable a cualquier ataque a través del conocimiento, pero la formación en este tema hace que poco a poco contribuyamos a una vida digital segura, y a extinguir de alguna manera actos que como mínimo, hacen menos agradables nuestros momentos frente a la pantalla, pero que en muchas ocasiones pueden acarrear problemas graves y difíciles de solventar.

En conclusión, Internet, y por extensión la tecnología, son herramientas con mucho potencial, pero un mal uso puede traernos complicaciones, por tanto, es obvio que hay que aprovechar las bondades tecnológicas y comunicativas actuales, pero a partir del conocimiento de los riesgos para poder prevenirlos. Todos sabemos que pasamos mucho tiempo delante de dispositivos tecnológicos, compartiendo multitud de datos que debemos aprender a proteger, y esta guía nos ofrece, como usuarios de tabletas, móviles u ordenadores, consejos muy fáciles de aplicar y que pueden llevarnos a una vida digital segura, tanto individual como colectivamente. La aplicación de esta lectura en las aulas es muy amplia, desde la propia formación del personal de los centros educativos en las distintas áreas descritas en el *Marco Común de Competencia Digital Docente*, hasta el apoyo para el desarrollo de unidades formativas encaminadas a enseñar a nuestros alumnos a utilizar correctamente la tecnología e internet.

Sin duda, un manual recomendable e imprescindible para profesionales de la educación.

Raúl Céspedes Ventura
raul.cespedes@um.es
Universidad de Murcia, España