Check Point software destaca que la formación en ciberseguridad desde la infancia es una herramienta vital: el 72% de los niños en el mundo han experimentado al menos un tipo de amenaza cibernética

Tan solo un 40% de los padres saben que sus hijos han sufrido amenazas cibernéticas. El 90% de los niños mayores de 8 años ya utiliza Internet

La educación es un pilar fundamental, ya que es la que permite progresar como sociedad e inculcarles a las nuevas generaciones los valores y conocimientos fundamentales. En una sociedad cada día más digitalizada y, sobre todo, teniendo en cuenta que los niños y niñas cada vez hacen un mayor uso de las tecnologías y desde edades más tempranas, es fundamental que la educación ponga foco en cómo usarlas de manera segura. Si bien la tecnología les ofrece numerosas ventajas a nivel educativo, cultural y como divertimento, también presenta ciertos riesgos que deben conocer.

El informe "Por qué los niños están inseguros en el ciberespacio " del Foro Global de Ciberseguridad ha detectado que un 72% de los niños en el mundo han experimentado al menos una vez un tipo de amenaza cibernética. Estos datos se vuelven preocupantes ya que pueden afectar a la salud, integridad y privacidad de los más pequeños. El informe atestigua las crecientes dificultades que se están encontrando a la hora de proteger a los niños en el ciberespacio en unos tiempos en los que el 90% de aquellos que tienen más de ocho años ya están activos en la red.

Check Point® Software Technologies Ltd. (NASDAQ: CHKP), un proveedor líder especializado en ciberseguridad a nivel mundial, estima que si bien los esfuerzos para responder con mayor concienciación y generar nuevas medidas de protección están aumentando, siguen sin ser suficientes. Las amenazas a las que se enfrentan en la red los niños y niñas son muy diferentes, y en la mayoría de los casos ellos no son conscientes de que las están sufriendo, ni los padres son conocedores de estas amenazas. Es urgente tomar medidas preventivas para que no estén en peligro cuando naveguen por la red. Estas son algunas de las medidas principales que se proponen para proteger a los menores:

1. Aprender ciberseguridad a través del juego: el juego siempre es una herramienta fundamental a la hora de enseñar a los más pequeños, ya que aquello que se aprende desde la diversión, se adquiere de una manera más eficaz. En este sentido, se pueden proponer ejercicios prácticos en los que se simulen amenazas para que aprendan a protegerse. Se pueden diseñar aplicaciones y juegos online para que adquieran estos conocimientos, reconozcan las amenazas y sepan proteger sus datos personales.

2. Etica como estandarte: la educación en ciberseguridad siempre viene acompañada de un componente ético y es que es fundamental inculcar principios éticos para el desarrollo de futuros ciudadanos responsables. El desarrollo de las habilidades tecnológicas debe venir acompañado de un uso consciente de las mismas.

3. Desmitificación del hacker: es importante que los más pequeños entiendan todas las complejidades de esta figura, ya que además de ciberdelincuentes que vulneran los sistemas y generan actos vandálicos, también existen los hackers buenos o "White Hats" que usa sus conocimientos en informática de manera ética para detectar posibles brechas o errores en el sistema de las empresas y arreglarlos para prevenir los ataques.

4. Asignatura en los colegios: una de las estrategias principales para prevenir las amenazas que afectan a los menores es la educación en ciberseguridad por parte de las escuelas. La ciberseguridad está pendiente en los colegios, y sería de gran utilidad para concienciar a los niños y niñas de los riesgos, además de enseñarle habilidades para protegerse. Para ello, es fundamental que estas instituciones cuenten con formadores con conocimientos digitales y también es muy recomendable que ofrezcan charlas para que los padres también cuenten con unos conocimientos básicos.

5. Crear una red segura: los menores también tienen que saber cómo crear redes seguras para poder prevenir las posibles amenazas, una de las más comunes es el phishing. Esta amenaza consiste en usar un correo electrónico para intentar engañar a las personas para que hagan clic en enlaces o archivos adjuntos maliciosos. Estos pueden ser especialmente difíciles de detectar para los niños porque un email a menudo parece llegar de una persona conocida, como un amigo o familiar. Esto también puede hacerse a través de una aplicación de mensajería o mensaje de texto. Es por esta razón que cada vez es más necesario que aprendan a detectar cuando un ciberataque puede estar vulnerando su red, a emplear contraseñas seguras que sean una barrera adicional, a proteger sus redes sociales en las que pasan numerosas horas y a saber detectar los ataques de phishing.

"El hecho de que los niños y niñas se vean expuestos a los riesgos cibernéticos a edades tan tempranas puede ser muy perjudicial, ya que se podría poner en peligro su salud emocional, su integridad física y su privacidad", explica Eusebio Nieva, director general de Check Point Software para España y Portugal. "En este sentido, consideramos que es fundamental que reciban formación en ciberseguridad para saber identificar las amenazas y tener herramientas para darles respuesta. De este modo, los más pequeños podrán sentirse más seguros en la red y además, a través de la educación, construir una sociedad más consciente y responsable con el uso de las nuevas tecnologías".