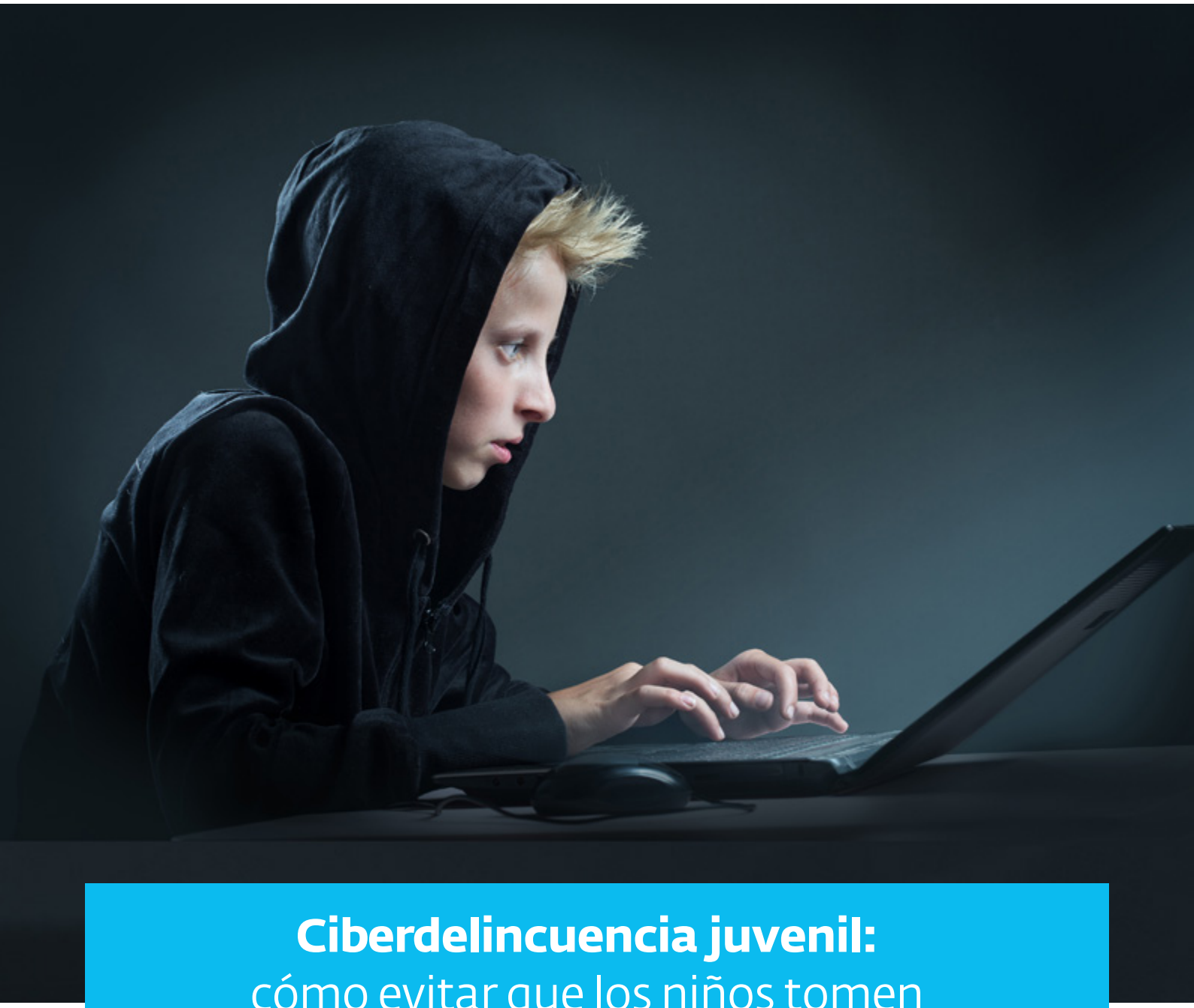
Digipadres

UNA INICIATIVA DE saferkidsonline by eset



Ciberdelincuencia juvenil: cómo evitar que los niños tomen el camino equivocado

Nunca es demasiado tarde para evitar que los jóvenes sean arrastrados al lado oscuro y garantizar que usen sus habilidades para hacer el bien.

Cuando se habla de la ciberdelincuencia y los niños, suele ser en el contexto de *proteger a los más pequeños de los peligros online*. Por ejemplo, asegurarse de que sus dispositivos cuenten con *un software de control parental adecuado*, de modo que no puedan acceder a contenido peligroso o inapropiado. O comprobar que tengan instalado un antimalware y que la privacidad esté configurada correctamente.

¿Pero qué pasa cuando el niño es el que resulta ser el "malo"? Esto es más común de lo que se cree, entre otras cosas porque, a una edad temprana, muchos niños aún no se dan cuenta de que sus actividades de "**sombrero negro**" son ilegales (en comparación con las de "**sombrero blanco**", también conocidas como "hacking ético").

La buena noticia es que, incluso si sospechas que tu propio hijo puede estar utilizando sus habilidades tecnológicas con fines maliciosos, **no es demasiado tarde para guiarlo hacia el camino correcto**. Afortunadamente, son muchas las *vías legítimas para canalizar sus conocimientos cibernéticos* y, en última instancia, ayudarlo a *iniciar una carrera en ciberseguridad*.

Cuando el hacking es un juego de niños

Aunque todo esto parezca el argumento de una película de Hollywood, la realidad es más mundana. De hecho, los hackers de edad escolar **son cada vez más numerosos, a medida que las herramientas y técnicas para cometer delitos cibernéticos se abaratan y son más fácilmente accesibles**. Algunos chicos han demostrado un asombroso dominio de la tecnología y de las técnicas de amenaza en sus ataques, mientras que otros lo hacen simplemente por la curiosidad de **ver hasta dónde pueden llegar**.

LECTURA RELACIONADA: ¿Qué motiva a algunos jóvenes a convertirse en ciberdelincuentes?

La *Agencia Nacional del Crimen (NCA)* del Reino Unido informó que los datos de su Unidad Nacional de Cibercrimen (NCCU) mostraron un **aumento del 107%** en los informes policiales de 2019 a 2020 de estudiantes que desplegaron ataques de DDoS. La edad media de las derivaciones al equipo "Prevent" de la NCCU es, al parecer, **de 15 años**, y un reciente *informe de la NCA* reveló que se descubrieron niños de tan solo nueve años lanzando ataques de DDoS. Sin embargo, los casos de niños que participan en la ciberdelincuencia no se limitan a los ataques de DDoS.

Por ejemplo:

- La alumna londinense Betsy Davies tenía solo **siete años** *cuando demostró* cómo hackear la computadora portátil de un desconocido a través de una red **Wi-Fi pública** no segura en solo 10 minutos. ¿Cómo lo hizo? Buscando una guía en Internet. En ese momento, se encontraron alrededor de 14.000 tutoriales de video solamente en YouTube.

- Elliott Gunton tenía apenas **16 años** cuando hackeó el proveedor de servicios de Internet británico TalkTalk, en un caso ahora infame que resultó en la vulneración de más de **150.000 cuentas de clientes**. Posteriormente fue encarcelado por otros delitos cibernéticos y *ha sido acusado* de delitos aún más graves en los Estados Unidos.

- Un estudiante australiano de **16 años**, cuyo nombre no se ha dado a conocer, *irrumpió varias veces en los sistemas internos de Apple*, llevándose 90 GB de "**archivos seguros**" y accediendo mientras tanto a las cuentas de los clientes. Su abogado explicó que el muchacho lo hizo porque admiraba a Apple y soñaba con conseguir un trabajo en la empresa.

¿Cuáles son las señales de alarma?

Los padres suelen ponerse ansiosos por muchas cosas en lo que respecta a sus hijos. Pero cuando se trata de una posible actividad ilegal de hacking, tienen razón al mantenerse alertas ante cualquier **cambio en su comportamiento**. Un *importante estudio de 2019* realizado por la Universidad Estatal de Michigan (MSU) puso de manifiesto algunos de los rasgos clave asociados a la ciberdelincuencia juvenil. **Entre ellos se destacan:**

- Bajo **autocontrol**.
- Relacionarse **con pares**; es decir, conocer a otros chicos que también hackean (*principalmente las **mujeres***).
- Tiempo dedicado a ver la **televisión** o a jugar con la **computadora** (*principalmente los **varones***).
- **Oportunidad**; es decir, tener su propia computadora en una habitación privada, con una **mínima supervisión de los padres**.
- **Acceso a un teléfono móvil** desde una edad temprana.
- Participación en la **piratería digital**.

PRÓXIMA LECTURA: Adicción digital: cómo alejar a tus hijos de las pantallas

¿Cómo te das cuenta de que algo anda mal?

También hay algunos indicios de que la actividad online de tu hijo puede haberse descontrolado. Por ejemplo, **puede hacer alusión a un asunto privado**, lo que te da la pauta de que estuvo leyendo tus correos electrónicos y mensajes personales; o puede hacer un esfuerzo extremo para **proteger su propia privacidad**, negándose a compartir sus inicios de sesión.

Por supuesto, esto podría indicar simplemente que son niños siendo niños. **De hecho, un interés temprano** en algunos tipos de software, como las herramientas de pruebas de penetración, **podría ser más que bienvenido**.

Pero como explica Thomas Holt, autor principal del informe de la MSU: "**Sin supervisión, los 'juegos' inocentes pueden escalar**". ¿Cuáles pueden ser las consecuencias? Según la NCA, pueden ser desde una advertencia oficial de la policía o una multa, hasta la detención e incluso el encarcelamiento en el caso de las infracciones más graves.

Hacia resultados más positivos

El *software de control parental* que se descarga en los dispositivos de los niños ayuda a detectar las primeras señales de advertencia del hacking juvenil, como los intentos de acceder a sitios específicos de ciberdelincuencia, foros de hacking y otras zonas turbias de Internet. Pero si ya han alcanzado un nivel elevado de conocimientos tecnológicos, es probable que **sean capaces de ocultar cualquier actividad de este tipo**.

PRÓXIMA LECTURA: Controlar cómo los niños usan la tecnología: ¿una medida preventiva o una invasión de la privacidad?

Por eso es más importante que nunca encontrar una alternativa positiva para sus habilidades. Por suerte, hay varios caminos que se pueden tomar. *Algunos gobiernos* organizan *programas* de ciberseguridad para estudiantes en edad escolar con el fin de poner a prueba, perfeccionar y desarrollar sus habilidades. De aquí en más, la progresión natural sería **seguir una carrera completa en seguridad cibernética**. Este sector lleva mucho tiempo sufriendo una **gran escasez de trabajadores capacitados**, lo que significa que los profesionales tienen un salario inicial elevado y **pueden aspirar a una carrera larga y gratificante**.

También hay concursos de hacking gubernamentales y privados en los que todos los participantes pueden **poner a prueba sus habilidades** frente a los mejores del mundo, con la posibilidad de **mostrar su talento** a posibles empleadores.

Pero lo más importante es **mantener las líneas de comunicación abiertas**. **Interésate por los pasatiempos de tus hijos**. Y si te preocupa que se estén desviando hacia la ilegalidad, recuérdales **cuáles son sus riesgos y anímalos a buscar oportunidades más positivas y legales**.

Aquí y *aquí* encontrarás algunos artículos útiles de la NCA que puedes compartir con tus hijos.

Para conocer más sobre los peligros a los que se enfrentan los niños en Internet y cómo puede ayudarlos la tecnología, consulta Safer Kids Online.

Queremos que más **Digipadres** potencien a los niños
y les enseñen a navegar seguros.

¿Estás listo para acompañarnos en este desafío?

www.digipadres.com