Digipadres

UNA INICIATIVA DE saferkidsonline by eset

El robo de identidad
también afecta a los niños

De vez en cuando, nuestro equipo de ciberseguridad de ESET recibe consultas sobre casos en que la identidad de un menor fue suplantada en Internet, y sus familiares y amigos están buscando ayuda para saber cómo proceder.

Lo que a simple vista podría parecer un incidente breve y desagradable, en la mayoría de los países se considera un delito, por lo que los padres o tutores legales de las víctimas jóvenes de robo de identidad **deben comunicarse con la policía local o buscar asesoramiento legal**. Recomendamos que lo hagan, ya que, lejos de ser un incidente menor, **el robo de identidad puede tener un impacto grave en el futuro financiero de tus hijos.**

El robo de identidad afecta incluso a niños muy pequeños

El robo de datos personales online es muy común. Quizá pienses que los datos de tus hijos no son de mucha utilidad. Pero cuando sean mayores, tendrán un historial crediticio limpio sin antecedentes penales, algo que los estafadores pueden aprovechar en beneficio propio.

Aunque se pruebe legalmente que quien sacó un préstamo o recibió una multa fue un tercero que utilizó indebidamente su nombre, sus hijos **tendrán problemas administrativos que les costará mucho papeleo resolver.**

Cuidado con la ingeniería social

Los ladrones de identidad generalmente intentan robar los nombres, las direcciones, los números de pasaporte o identificación y, en ciertos casos, los datos financieros de víctimas anónimas. Algunos compran estos datos en la Dark Web (sitios que no puedes encontrar en Google) y otros utilizan malware o tácticas de ingeniería social para obtenerlos por sus propios medios.

Una vez que logran infectar los dispositivos de las víctimas con malware, los ciberdelincuentes pueden extraer los datos personales almacenados en los dispositivos o navegadores de Internet. Si usan un malware para registrar las pulsaciones, todo lo que la víctima escribe en su dispositivo infectado se envía directamente al atacante, incluyendo números de tarjetas de crédito y contraseñas.

También hay otra forma de ataque más rentable para los estafadores online: la ingeniería social, que consiste simplemente en **engañar a las víctimas para que ellos mismos proporcionen sus datos personales, ya sea haciéndose pasar por otra persona o fabricando un sitio web falso.**

Esto es peligroso para los niños que muchas veces no tienen las herramientas para diferenciar estas situaciones. Pero, si sigues estos pasos sencillos, fortalecerás la protección de los datos personales de tus hijos.

Cómo proteger a tu familia del robo de identidad

1 Enséñales a tus hijos a no compartir datos innecesariamente

Trata de conversar con ellos sobre cómo usan las redes sociales y lo que normalmente les gusta publicar. Explícales por qué no deben ingresar la dirección de su casa al aceptar solicitudes de amistad de personas que no conocen.

2 Es imprescindible crear buenos hábitos de uso de contraseñas

Enséñale a tu familia a crear contraseñas largas, difíciles de adivinar y únicas, o a usar un administrador de contraseñas. Recuerda que no se deben reutilizar las contraseñas para diferentes servicios o sitios web.

3 Protege todos los dispositivos de tu familia

Y solo envía datos personales online cuando tu conexión a Internet sea segura. Esto significa que debes evitar usar las redes de Wi-Fi públicas o cualquier conexión a Internet que no sea de confianza. En una conexión no segura, los estafadores pueden interceptar fácilmente todos los formularios que envías.

4 Desecha los documentos confidenciales en forma segura

Si necesitas deshacerte de documentos físicos viejos que contienen datos personales, destrúyelos. No olvides que los dispositivos electrónicos y de almacenamiento de datos que ya no usas también contienen mucha información personal. Algunos de ellos ofrecen una función de borrado para desechar de manera segura todos los datos guardados.

5 Enséñales a tus hijos a identificar mensajes sospechosos

O sitios web que podrían intentar engañarlos para que envíen sus datos personales. Considera usar un Anti-Phishing, que puede incluirse como parte de una solución de seguridad cibernética. De esta

forma, si algún miembro de la familia intenta abrir un sitio web de phishing, la solución antimalware te lo advertirá.

Próximos pasos

¿Pero qué debes hacer si descubres que los datos personales de tu hijo ya fueron robados y se utilizaron para una actividad ilícita? No lo dudes: contacta a la policía local. De una forma u otra, en la mayoría de países y regiones, el robo de identidad es considerado un crimen.

Cuando te comuniques con la policía, **ten en cuenta que es posible que no estén familiarizados con todos los aspectos de esta rama de la ley.** Si te sucede eso, no dudes en volver a presentarte con un abogado.

Aunque no pasa siempre, en algunos casos existe una fuerte conexión entre el fraude y el bullying, esto significa que, en algunos casos, puede ser que el atacante conozca personalmente a tu hijo. En este sentido, es importante comunicarse con la escuela y con la familia para saber si hay que proceder de alguna otra forma.

El robo de identidad es subestimado por muchas personas, por eso, si sospechas que tu familia es víctima de uno de estos casos, te recomendamos consultar con organizaciones de tu país que brinden asesoramiento legal general o específico en seguridad informática.

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

¿Estás listo para acompañarnos en este desafío?

www.digipadres.com