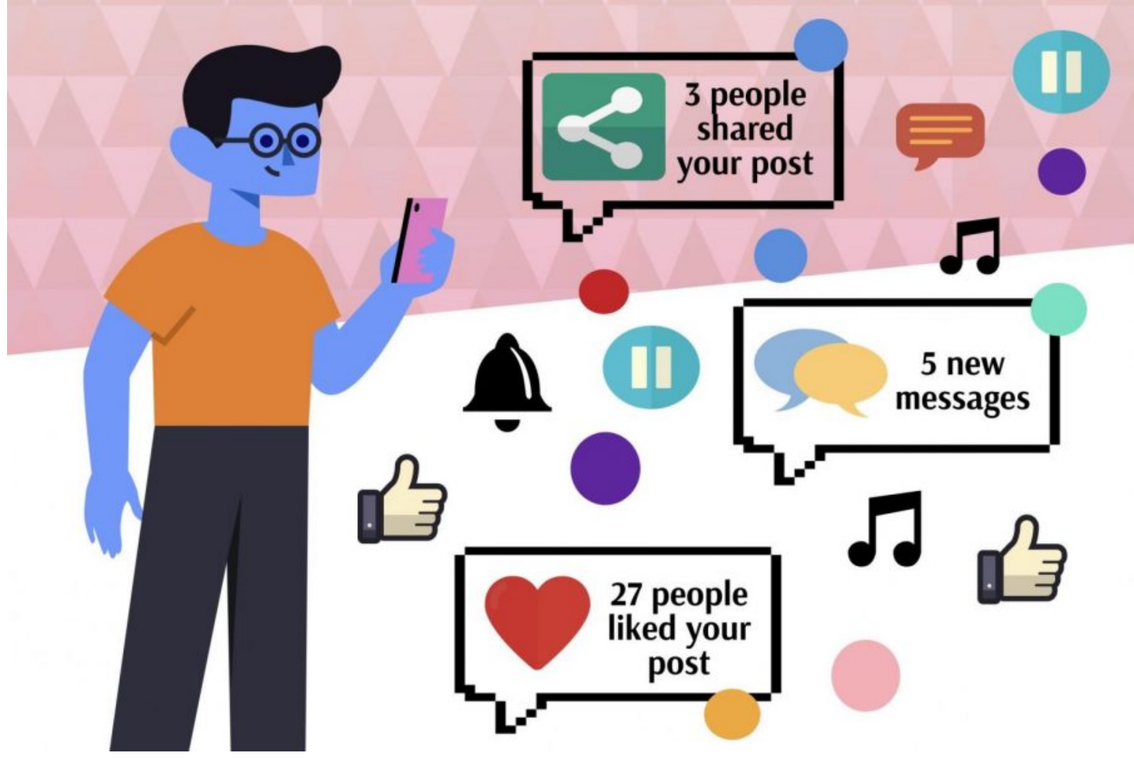
resolution

Your identity at risk Our solutions at work



Social Media & Child Identity Theft

96% of Child Identity Fraud victims within the past six years were active users of Social Media when their identities were compromised, and they subsequently suffered a monetary loss through fraud or a scam.

Social Media continues to be the two edged sword, especially with regards to children, as it combines opportunity for education, creativity and fun alongside acute dangers of identity theft and fraud.
Studies show children aged 8-12 spend an average of 5-6 hours daily on digital devices, with a large portion of this time on social media. TikTok, Instagram, Snapchat, and YouTube are the most widely used platforms among children and teens

How Social Media Enables Identity Theft

- Children may unknowingly share sensitive details, such as their full name, birthdate, school name, or location, which can be exploited by cybercriminals.
- Scammers can use photos or publicly shared information to create fake identities or accounts in a child's name, potentially leading to fraud.
- Children are more likely to fall victim to fake messages or links that ask for personal details, passwords, or other private information.
- Platforms storing user data are sometimes hacked, exposing sensitive information, including that of young users.
- Many children and teens are unaware of privacy settings or the potential consequences of their online actions, making them more vulnerable to identity theft.
- Freezing a child’s credit is one of the most effective tools ways to prevent a child’s identity from being used by cybercriminals to fraudulently open new accounts. But criminals can pursue many avenues of identity fraud for which credit freezes offer no protection, as in the case of fraudulent tax returns, fraudulent applications for government/medical benefits, and fraud created using synthetic identities.

How Can We Try and Protect Them?

- **Educate Children About Privacy**: Teach them to avoid sharing personal details online, including their full name, address, or school name.
- **Set Privacy Controls**: Use parental controls and ensure accounts are set to private, limiting access to approved friends or followers.
- **Monitor Activity**: Regularly review children's online interactions, posts, and followers.
- **Use Secure Passwords**: Encourage strong, unique passwords for social media accounts and avoid reusing passwords. Also, shore up authentication by relying more heavily on physical biometrics (fingerprint or retina scans when available) and other passwordless authentication methods to detect synthetic identities.
- **Check Credit Reports**: Parents can monitor their child’s credit by requesting a credit freeze or regularly checking for unauthorized activity.
- **Limit Oversharing**: Be cautious about posting children’s personal information, such as birthdates or school details, on your own social media accounts.
- **Suspicious Activity Alerts**: Are critically important for consumers who use peer-to-peer payments (Zelle, Venmo etc) and those with minors who have custodial accounts. Alerts are often among the first indicators to consumers that something is awry with their accounts, and alerts keep consumers, even young accountholders, engaged.

To learn more and to watch a very informative video on this issue, Scan the QR Code or go to:

https://idresolution.net/social-media-child-identity-theft/

Questions? Call Us at 877-308-9169