|  |  |  |
| --- | --- | --- |
| |  | | --- | |  |  |  | | --- | |  | |
| |  |  | | --- | --- | | |  | | --- | | **Steps You Can Take to Protect Your Children’s Identity**  **Young children and teens can become easy prey to fraud. Parents need to know how to protect them and understand what happens if they don’t.**  In our digital age, it’s not unusual to find young children spending time on the internet. As they age, they may become even more avid users of apps and websites that can be quite risky. There are simple steps you can take to help your kids stay safe from scams, fraud, and identity theft.  **Institute a credit freeze.** A security freeze of your child’s credit report prevents anyone from opening an account under your child’s name. A parent can place a freeze on the credit reports of children up to age 16. If a credit report for your child doesn’t already exist, requesting a hold on a credit report automatically creates a credit report for your child and a security hold is immediately placed on it. Parents should request holds from all three major credit bureaus – Equifax, TransUnion, and Experian. Be prepared to provide proof of your own identity and that you are the child’s parent.  **Protect children’s information at school.** Many schools ask children to provide Social Security numbers (SSNs) for various reasons, such as tracking scores. If those numbers get stolen, your child will be easy prey for identity theft. You have the right to withhold SSNs except under certain circumstances, like filing taxes or buying health insurance. Protect your child’s SSN and other private information by not giving it out except where required by law. Read about the Family Educational Rights and Privacy Act1 for more information about prohibiting information disclosure.  **Protect computers and tablets.** Unfortunately, many computers can be vulnerable to malware that can steal information and cripple files. You can fight back by ensuring all household computers have up-to-date software that protects against viruses, adware, and spyware. You can use parental controls that limit children’s access to websites. Password vaults can generate hard-to-crack passwords and keep them safe from spyware. You might consider investing in software that periodically monitors the internet for the suspicious appearance of your household’s personal information.  **Teach your children well.** If they’re old enough to use a computer or smartphone, they’re old enough to learn safe online behavior. Educate your child about threats to personal security and what information should not be shared online. Most importantly, make sure your kids know never to click links on emails, even if they think they know the sender. Consider using computer monitoring software to ensure your children are not misusing their devices or taking unnecessary risks.  **Children require a lot of care.** As a parent, you want to keep your kids safe from all sorts of harm, whether physical, emotional, or financial. Protection from identity theft is one of your responsibilities. Contact me today for a review of your financial plans with a special emphasis on shielding your children from current and future financial threats. | | |
| |  | | --- | | [LET'S CONNECT](mailto:##AdvisorEmail##) | |

|  |  |
| --- | --- |
|  | Tracking #1-05034053 Expiration 07/23 |

1 [2.ed.gov/policy/gen/guid/fpco/ferpa/index.html](https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html) [3/1/18]