ConnectSafely
Smart Socializing Starts Here™

Tips for Protecting Kids and Teens from Identity Theft

You might think that you have to be an adult to be an identity theft victim, but that's not the case. Children are also at risk. One reason is most kids have squeaky clean credit ratings since they have never taken out credit. Another is that identity thieves know that the crime can go undetected for years, until a child is 17 or 18 and applies for a student loan or credit card. Identity theft can not only interfere with a child's ability to get a loan, it can hurt his or her chances for a job or internship or cause trouble with the law or at school, which is why it's so important to take steps now to protect your child's identity.

Know how your child's school protects student data. Schools typically have a great deal of information about students, so check with school authorities on how they protect your child's data. This includes directory information like home addresses and phone numbers, and any surveys the school has conducted. Also check with school clubs or organizations that might have their own privacy policies that could differ from the school's. There are strict federal guidelines for how schools manage student data, outlined in the Family Educational Rights and Privacy Act (FERPA). You'll find lots more about this in ConnectSafely's free booklet A Parents' Guide to Student Data Privacy (ConnectSafely.org/privacy).

Protect your child's Social Security number. Don't give it to anyone — even trusted sources — unless they have a legitimate need. Even doctors, who may ask for this information, don't need it since they are not extending credit to your child.

Know how your child's personal information is being used. There are times when you must share confidential information about your children including at school, medical facilities, day care centers and sometimes even school clubs, youth groups and sports organizations. Only give them the information they need (it is rarely necessary to share a child's Social Security number) and ask how they protect that information.

Secure your child's devices. Smartphones, laptops, tablets and even media players can contain confidential information that could jeopardize your child's identity. There is also a risk of someone harassing or bullying others from your child's device and having it blamed on your child. Be sure that all of your family's devices are protected with a password, confidential PIN or fingerprints. Only use trustworthy apps and make sure that you have the latest versions of apps and operating system software, which means you'll have the latest security updates.

Even if your devices are secure, you need to develop safe online habits. Beware of phishing — fraudulent websites or apps that look legitimate that ask you to enter personal information. You'll find more on protecting phones in A Parents' Guide to Mobile Phones, free from ConnectSafely (ConnectSafely.org/mobile).

Be careful on social media. Social media is a great way to share lots of information but, if you or your child aren't careful, data posted online could lead to identity theft. And it's also possible for people to impersonate your child on social media and perhaps abuse others in your child's name — another form of ID theft that can get your child into trouble.

Make sure your child is using strong, secure and unique passwords as well as dual factor authentication as outlined in our Tips for Strong, Secure Passwords (ConnectSafely.org/passwords). Teach them from a young age to never share passwords, even with trusted friends, and to keep private certain confidential items including Social Security numbers, driver's license numbers, bank and credit card information. ConnectSafely has a series of guides on ConnectSafely.org to help parents understand privacy and security tools for major social networking services.

Be careful in the physical world. Paper remains one of the "technologies" used to steal identities. Be sure to shred any papers that contain Social Security numbers or sensitive financial, academic, legal or medical information. Don't carry around your or your child's Social Security card or anything with highly sensitive information. Make sure potential employers, landlords and others protect any information and documents with your information.

Get your child's credit report. The three major credit reporting agencies are required to offer a free annual credit report for anyone, including children. The Federal Trade Commission recommends that you run your child's report when they get close to their 16th birthday. The credit reporting agencies may (legitimately) require your child's Social Security number, birth certificate and proof of address. Don't, however, assume that a clean credit report means your child is not a victim. It is quite possible that the report may not reveal identity theft has taken place. You can access these reports from AnnualCreditReport.com, which is recommended by the FTC.

Not just strangers: Sadly, children can be victims of their own relatives or friends of the family who have access to information they can use to steal the child's identity. Youth can also be victimized by friends, current or former roommates and people who have access to their mail, among other things.

Vulnerable youth: Not all young people are equally vulnerable. Foster children, according to the Identity Theft Resource Center, are at a higher risk for identity theft than other youth. Sometimes it's related to their own parents' economic problems but it can also result from the child's data being passed around between agencies and foster homes.

Look for warnings signs. The FTC says to watch for the following signs that your child may have had his or her identity stolen:

- Being turned down for government benefits because the benefits are being paid to another account using your child's Social Security number
- Getting a notice from the IRS saying the child didn't pay income taxes, or that the child's Social Security number was used on another tax return
- Getting collection calls or bills for products or services you didn't receive