idwatchdog®

Child Identity Theft

WHAT PARENTS NEED TO KNOW FROM BIRTH TO TEENAGE YEARS

Many parents assume that their child is safe from identity theft because of their young age and lack of credit history. In fact, the opposite is true.

For identity thieves, children can be the perfect mark.[1]

While adults may be targeted by thieves for the money in their accounts, a child represents an entirely different type of opportunity—a clean slate for opening new lines of credit that the child's parents may not notice until years down the road.[2]

One million children were impacted by identity fraud in the US in 2017, according to Javelin Strategy and Research's 2018 Child Identity Fraud Study.[3] Fortunately, there are steps that parents can take to help better protect their children from identity theft at every stage—from birth to school-aged years to young adults starting out on their own.

From Carefree Kid to Identity Theft Victim

It's admittedly hard to imagine. What could a cybercriminal possibly want with your child's identity? After all, he or she likely has no assets, no credit history, and no accounts of their own.

For a savvy cybercriminal, taking advantage of a child's identity is easier than you may think. Fraudsters can use a child's stolen identity to take out mortgages, get car loans, rack up credit card debt, or obtain fraudulent immigration documents[2]—all while parents and guardians remain unaware that their child's credit rating is being destroyed.[4]

Perhaps even more frightening, cybercriminals may share the information with other thieves, connecting multiple identities to a child's stolen Social Security number.[2] In fact, according to reports, one of the latest trends on the dark web is selling children's personal data online.[4]

Unfortunately, the identity theft of a child could go undetected for years—or even decades[5]—and the child may suffer long-term consequences as a result.[2] Until the issue is resolved, he or she may not be able to qualify for student loans, get a credit card, or rent a place to live.

Many Points of Vulnerability for Child ID Theft

Where can child identity theft happen? Practically anywhere.

According to the Identity Theft Resource Center (ITRC), schools, doctor's offices, daycare centers, and even school lunch computers have suffered data breaches, reportedly in search of children's Personally Identifiable Information (PII).[6] Essentially anywhere that a parent or guardian provides a child's Social Security number can create a potential vulnerability.[7]

Sadly, in many cases, the theft takes place in the child's own home—or close to it. It's estimated that 60 percent of child identity fraud victims personally know the perpetrator.[3]

Once an identity thief has a child's Social Security number in hand, they may use the internet to find the rest of the information they need to open accounts, such as date of birth, city of birth, and mother's maiden name.[7] Alternatively, the thief may leverage a tactic called synthetic identity theft, which is an increasingly common method of using children's stolen information.[6] In cases of synthetic identity theft, thieves create a whole new identity by combining a victim's real Social Security number with a fake name, address, phone number, and other details.

Help Better Protect Your Child from Identity Theft at Every Stage

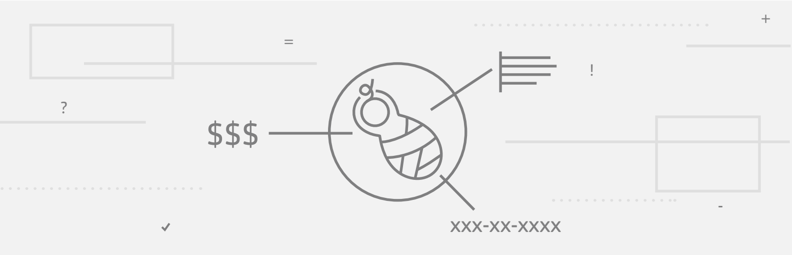
Armed with the knowledge of how identity theft can negatively impact children, let's walk through specific concerns and preventative steps to help better protect your child at every stage—from infants to school-aged children and from tweens to young adults starting out on their own.

Many of these recommendations can be applied to all ages—and even used by parents to help better protect themselves.

Infants and Young Children: The Worrying Trend of Young Children's Data Being Sold on the Dark Web

Security researchers have reported a concerning identity theft trend, especially for parents of young children. Cybercriminals have recently begun targeting children—even infants—in order to take advantage of their clean, unmonitored credit.[6]

In some cases, the stolen data is being advertised on the dark web for the purpose of committing tax fraud, but more often, criminals use it to open credit card accounts, get loans, and stain what would otherwise be the child's clean credit.[5]



For Sale On the Dark Web: An Infant's Data Set for $300

According to reports, cybercriminals have posted advertisements in online marketplaces selling children's identities.[4] In one instance, criminals advertised something called "infant fullz," encouraging potential buyers to purchase it before tax season.[5] The term "fullz" is cybercriminal slang for a full identity kit—essentially everything a thief needs to steal an identity, such as name, address, Social Security number, and date of birth.

The price? $300 worth of bitcoin for an infant's data set, in some cases.[8]

Fresher is typically better in the criminal exchange of data that often takes place on the dark web, and a young child's data may be more appealing to cybercriminals because it is less likely that it has been exploited before.[4] If, for example, a criminal can snag a child's identity before anyone else does, they may get to start from scratch in setting up a credit profile under the victim's name for the first time.[4]

Fake Dependents Can Be Profitable for Identity Thieves

One way that a criminal may attempt to use a child's stolen data is by committing tax fraud—essentially claiming the child as a dependent on a fraudulent tax return in order to take advantage of the child tax credit.[5] Given that many tax refunds are issued by the IRS well before the tax form is fully scrutinized, identity thieves could have enough time to cash in on a fraudulent dependent tax credit—and run.[9]

For a thief, that potential profit may be worth the gamble.

Case in point: an identity thief who purchases an infant's data set for $300 worth of bitcoin could then use that information to potentially earn $1,000 by claiming a dependent on a fraudulent tax return.[9]

Steps to Help Better Protect Your Infant or Young Child

Protect physical information

Try to avoid carrying documents in your wallet that disclose your child's Social Security number or other PII.[7] Instead, keep important documents locked up at home or in a safe deposit box.

Store safely or shred documents that contain your child's information

For electronic or paper documents that you need to keep, choose a safe location.[10] For documents that you can dispose of, shred them first.

Provide less information about your child on forms

Consider holding back some information, such as your child's Social Security number, middle name, and date of birth, when filling out forms.[7] In some cases, you may be able to use your own identifying information instead, which can be easier to monitor for potential problems. Also consider asking if you could use a different identifier, or use only the last four digits of your child's Social Security number.[10]

Be aware of events that may put information at risk

Pay particular attention to certain circumstances, such as having an adult in your household who might be tempted to use a child's identity to start over, losing a wallet, purse or important paperwork, experiencing a break-in at your home, or being notified of a data breach at your child's school, doctor's office, or another location.[10]

Exercise caution on social media

Be careful when sharing personal information online about your child, such as birthday or city of birth, that could be of value to an identity thief.[7]

Consider a child credit freeze or credit report lock

Consider freezing or locking your child's credit reports until he or she is old enough to use credit.[11] A credit report freeze or lock restricts access to your child's credit file, making it harder for identity thieves to open new accounts in your child's name.[12]

Consider filing taxes early

Consider filing taxes as early as possible to help prevent criminals from cashing in on your refund, including a dependent tax credit, before you do.[13]

School-Aged Children: Teaching Kids How to Safely Navigate in a Virtual World

The internet is an incredible resource for children to learn, communicate with family and friends, and entertain themselves while you're busy tackling the latest work emergency. But it can also expose children to both virtual and real-world dangers.

While children are gaming, chatting, or surfing the internet, they can stumble onto inappropriate content and images, malicious emails or file sharing programs, or even actual predators who may use the internet to find and lure heir victims.[14]

The Internet Can Be a Risky Place for Kids

When you were a child, your parents may have advised you not to talk to strangers or to be home before dark. But these days, kids have to learn how to navigate in an entire virtual world as well.

Both adults and children alike are at risk for having their information misused on the web. The difference is that a child likely doesn't understand what information is safe to share online, and they may be unaware of the myriad of scams and malicious content that are pervasive on the internet.[15]

In the more frightening scenario of cybercriminals who actually target children, the criminals may use unique tactics that are hard for kids to resist, such as links to fan sites that contain malicious links, or offers of music or movies that a child might be tempted to download and could contain viruses or malware that represent a security threat.[16]

School Data Breaches May Expose Students' Personal Data

Schools can be a tempting target for cybercriminals, as they typically store a mountain of Personally Identifiable Information of both students and staff members.[17]

The K-12 Cybersecurity Resource Center documented 122 cybersecurity incidents that impacted public K-12 school districts in the US in 2018, which equates to one new incident every three days of the calendar year.[18] And that may be just the tip of the iceberg, as it's likely that many more school breaches or attacks were either not detected or not reported.[19]

Student data was exposed in more than 60 percent of K-12 data breaches in 2018, and with the ever-growing adoption of technology in schools, K-12 cybersecurity incidents are expected to become both more frequent and potentially more significant.[18]

Tweens and Teens: The Majority of Teens Have Been Bullied or Harassed Online

Teens may face particularly difficult challenges in the virtual world in the form of cyberbullying.

One type of cyberbullying occurs when a password that a child has previously shared with friends or classmates is used to break into the child's social media account. The cyberbully can then use the account to post embarrassing messages or images, spread spam, or post links to malicious sites.[16]

Sadly, 59 percent of teenagers in the US have been bullied or harassed online.[20]

The most common types of cyberbullying were offensive name-calling and spreading of rumors, but teens also reported receiving unwanted explicit images, stalking behaviors, physical threats, and having explicit images of themselves shared without their consent.[20]

Steps to Help Better Protect Your School-Aged Child

Consider parental controls

Research the tools available that can help limit, monitor, or filter a child's internet use.[21] Depending on what's right for you and your child, you can choose tools that filter certain content, limit time on device, monitor a child's usage, or even disable outgoing content and in-app purchases.

Check privacy settings

Talk with your child about the importance of using the appropriate privacy settings, especially for social media networks and chat.[22] It's recommended to set strict privacy preferences on chat and video chat accounts, such as whether other users can see if the child is currently online and who can send the child messages.

Create a safe screen name

Talk with your child about their screen name for apps and games and what it reveals about them.[22] A safe screen name won't divulge the child's full name, age, where they live, gender, email address, or even seemingly innocent information like a sports jersey number.[23] It also shouldn't contain any vulgar or suggestive words as this can attract the wrong type of attention.

Create strong passwords and keep them private

Teach children never to share passwords, even with their friends.[16] Talk about safe password habits, such as creating a "passphrase" that would be difficult for others to guess, and using different passwords for different accounts.[24]

Talk about what information can be shared—and what shouldn't

Kids typically like to share a lot of personal details online, including pictures, videos, plans, and their location. Talk with your child about what types of information should never be shared, such as their Social Security number, street address, phone number, and financial information.[21]

Be aware of school privacy policies

Pay attention to notices from your child's school[10] that explains your rights under Family Educational Rights and Privacy Act (FERPA), including your right to approve the disclosure of personal information in your child's records.[25] Don't forget to also review the privacy policies for any extracurricular programs your child participates in, as those programs could have websites in which children are named and pictured.[10]

Consider opting out of the school directory

Student directory information may include your child's name, address, date of birth, telephone number, email address, and photo. If you want to opt out of the release of directory information to third parties, it's best to put your request in writing.[10] If you don't opt out, directory information may be available to the school community as well as to the general public.

Talk about how to avoid malicious links

Malicious links can be found on video sharing sites, in ads or invites and may lead kids to inappropriate or illegal content to third-party sites that capture sensitive information.[16] Teach kids to be wary of tempting links, like "make a new friend" or "find out who's talking about you."

Train them to recognize inappropriate online behavior by others

Educate your child on how to detect intrusive or predatory behavior online. One option is to role play with them about what they'd do if someone was asking nosy questions in person or was standing too close to them.[26] Then talk about the online equivalent of that inappropriate behavior as well as actions they should take if they encounter it.

Keep an open line of communication

A myriad of experts—from Google's Safe Search Kids[27] to non-profit KidsHealth[28] to the Federal Trade Commission (FTC)[29]—recommend one key element in helping kids stay safer online: open communication with their parents or guardians.

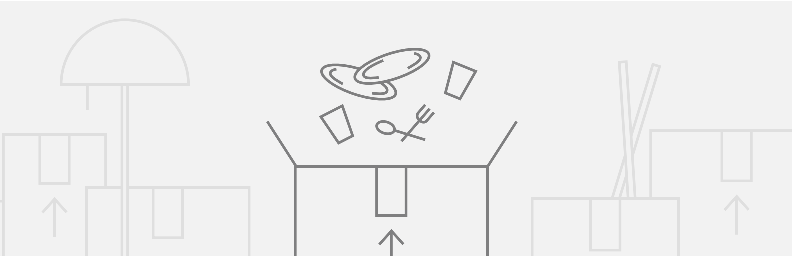
Check their credit at age 16

Check whether your child has a credit report close to his or her 16th birthday.[10] If it has errors due to fraud or misuse, you will have time to correct it before the child applies for a job, needs a loan for tuition or a car, or attempts to rent an apartment. If you placed an earlier credit freeze, you will have to lift it before the child applies for new credit.

Graduates and Young Adults: Preparing Kids to Outsmart a Lifetime of Scammers

These days, it may not be enough to send your high school graduate off to start school or tackle a new job with new clothes, a set of twin sheets, and a shower caddy. The ITRC says it's equally as important to arm them with a cross-cut shredder, a locking storage box, and knowledge about identity theft and other scams that they may encounter while living on their own for the first time.[30]

In fact, the FTC notes that 20 percent of identity theft incidents reported in its Consumer Sentinel Network Data Book in 2018 were committed against victims ages 29 and under.[31]



Big Life Changes May Mean Big Risk for Identity Theft and Scams

Many students and young people think that identity theft won't necessarily affect them, since they may not have a lot of financial assets or great credit scores.[32] But as we've learned in this paper, identity theft isn't just about stealing money—it's about stealing personal or financial information to try to open credit card accounts, secure a loan, or commit other fraudulent acts in the victim's name.[32]

The reality is that students can be a target for identity theft. During this transitional time, their identifying information may be in a lot of different places, because of life changes, such as moving out on their own, filling out background checks to sign a lease or activate utilities, or applying for jobs and completing college applications.[33] It's important to prepare young people for these life events and help them understand how the safety of their financial, medical, and personal identity may be impacted.

Financial Scams Abound on College Campuses

According to the ITRC, there are several ways that scammers target young people, and many of those tactics go hand-in-hand with students heading off to college—such as applying for colleges or employment, moving into a dorm or apartment, signing up for utilities, or getting a new credit card.[34]

College students may be vulnerable to a myriad of scams, including scholarship and financial aid scams, employment scams, imposter scams in which fraudsters pretend to be a school official or work for another trusted organization, student loan debt relief scams, or even scams related to non-existent apartments or textbooks.[35]

In one example of how criminals may target students, the ITRC warns that scammers may try to steal identities from unsuspecting students through enticing job offers.[34] These criminals may prey upon a student's money, personal information, or even physical safety.[36]

Steps to Help Better Protect Your Teenager or Young Adult

Be cautious with Social Security numbers

Advise your child to consider keeping his or her Social Security card in a locked, safe place, rather than carrying it.[30] Also, they should be thoughtful about with whom they share their Social Security number.[32] For example, some financial institutions let account holders provide an identifier other than a Social Security number when accessing or opening an account. In addition, most schools now use a student identification number instead of a Social Security number.[30]

Keep a permanent address for important mail

It may be best to avoid mailing important documents to a dorm or apartment where the mailbox may not be secure.[37] Instead, young people should consider using a parent or relative's address or getting a post office box

Don't loan identification, credit or debit cards, or signatures

As difficult as it can be to say "no" to a friend when they are in need, remind your child that loaning out their ID or credit cards, or co-signing for any cell phone, utility account, car loan, or credit card could put them at unwarranted risk.[30]

Sort and shred mail and documents

Instead of letting mail pile up where others can easily access it, consider buying them a shredder, and advising them to shred all important documents, such as bank statements, credit card offers, and anything that contains an account number or Social Security number.[32]

Secure laptops and other devices

Discuss how to safely store laptops and other devices in a locking storage box if they are left unattended in dorm room or apartment.[30] It's also a good idea to log out of secure sites, such as online banking sites, and check that web browsers aren't automatically saving login and password combinations for sensitive sites.[32]

Be cautious when sharing on social media

Young people who are comfortable sharing details about their lives on social media sites may post a lot of personal details over time.[37] Advise your child to remember that scammers may be able to mine social media networks for information that could help them answer account security questions and hack into various sites.

Surf and shop wisely

Train your child to always look for the "https" and padlock icon on websites,[32] as sites that don't use proper encryption may make them an easier target for thieves.[38] Advise them to avoid making any payments on public WiFi, as these networks may not be secure.[37]

Learn to spot phishing emails

Teach young people to be wary of emails that "phish" for information.[32] Phishing emails and texts often try to get victims to click to what appears to be a legitimate site but is actually a website controlled by cybercriminals where personal information may be recorded.

Check credit reports

Once a young person has established credit, advise them to check their credit reports with the three nationwide credit bureaus at least annually.[30] They may not have a report yet if they have never established credit. If there is a credit report in their name, they should review it to make sure that none of the information is a result of fraudulent activity. If they find suspicious activity, the FTC recommends informing the organizations where fraud occurred about the potential identity theft and placing fraud alerts, so lenders will be encouraged to take extra steps to confirm the identity before opening new credit. They might also consider placing a security freeze which could provide additional protection against unauthorized access to help better protect against identity thieves from opening new accounts in their name.[39]

How to Report a Suspected Problem

- ! If you believe you or your child has been the victim of identity theft, report the incident to the FTC at identitytheft.gov.

- ! If you believe your child's school or district has acted inappropriately with his or her data, file a written complaint with the US Department of Education.[10]

- ! If you believe a website collected information from your child or marketed to them in a way that violates the law,[21] report it to the FTC at www.ftccomplaintassistant.gov/#crnt&panel1-1.

- ! If you believe you have been a victim of tax identity theft, refer to the IRS fact sheet for taxpayers for more information at www.irs.gov/pub/irs-pdf/p5027.pdf.[40]

- ! If you or your child sees offensive online content or other criminal behavior, document the activity and report the issue to local law enforcement or the local office of the FBI.[14]

- ! If you suspect an online predator, report it to the National Center for Missing and Exploited Children's CyberTipline at www.missingkids.org/gethelpnow/cybertipline.

A Final Word of Advice on Better Protecting a Child's Identity

Perhaps most importantly, when it comes to teaching your child how to better protect their personal and financial information, lead by example.[27] One of the best lessons for a child is to see their parent or guardian model good information safety by adhering to the same ground rules that you would like your child to follow.

Sources Cited

[1] CNBC, "How to Protect Your Child From Identity Theft"

[2] FBI Portland, "FBI Tech Tuesday: Building a Digital Defense Against Child ID Theft"

[3] Javelin Strategy and Research, "2018 Child Identity Fraud Study"

[4] ZDNet, "The Latest Dark Web Cyber-criminal Trend: Selling Children's Personal Data"

[5] TNW, "The Worrying Trend of Children's Data Being Sold on the Dark Web"

[6] Identity Theft Resource Center, "One Million Kids Were Victims of ID Theft Last Year"

[7] The Washington Post, "How to Protect Your Kids—And Their Future Credit—From Identity Thieves"

[8] CNN Business, "Infant Social Security Numbers Are For Sale on the Dark Web"

[9] Consumer Reports, "Why Child Identity Theft Is a Growing Concern During Tax Season"

[10] Federal Trade Commission, "Child Identity Theft"

[11] Equifax, "Freezing Your Child's Credit Report: FAQ"

[12] USA Today story from Equifax, "Why Should I Lock My Equifax Credit Report?"

[13] ID Watchdog, "Tax-related Identity Theft: Why You May Want to Consider Filing Your Tax Return Early"

[14] The United States Department of Justice, "Children Internet Safety"

[15] Internetmatters.org, "Privacy & Identity Theft Advice Hub"

[16] ConnectSafely, "A Parents' Guide to Cybersecurity"

[17] EdScoop, "Human Error to Blame in Vast Majority of Education Data Breaches"

[18] The K-12 Cybersecurity Resource Center, "K-12 Cybersecurity 2018 Year in Review"

[19] Education Week, "Schools Suffered at Least 122 Cybersecurity Incidents Last Year"

[20] Pew Research Center, "A Majority of Teen Experienced Some Form of Cyberbullying"

[21] Federal Trade Commission, "Net Cetera: Chatting with Kids About Being Online"

[22] Federal Trade Commission, "Kids and Socializing Online"

[23] Common Sense Media, "Privacy and Internet Safety"

[24] ID Watchdog, "Expert Tips for Crafting a Stronger Password: How to Pick Passwords and (Hopefully) Remember Them"

[25] U.S. Department of Education, "Family Educational Rights and Privacy Act (FERPA)"

[26] Parent Info, "Your Child's Digital Footprint"

[27] Safe Search Kids, "How to Property Educate Your Kids on the Possible Dangers Online"

[28] KidsHealth, "Internet Safety"

[29] Federal Trade Commission, "Kids Online"

[30] Identity Theft Resource Center, "College Students and Identity Theft"

[31] Federal Trade Commission, "Consumer Sentinel Network Data Book 2018"

[32] The Balance, "College Identity Theft: A Growing Problem"

[33] Identity Theft Resource Center, "Taking the Leap to Adulthood —What Graduates Should Know About Identity Theft"

[34] Identity Theft Resource Center, "Back to School, Back to Scams"

[35] ID Watchdog, "Back to Campus: 9 Scams for College Students to be Aware of as They Head Back to Campus"

[36] University of Missouri, "Avoid Job Scams"

[37] Consumer Reports, "College Students Face a Greater Risk of Identity Theft"

[38] U.S. News & World Report, "The Very Best Ways to Prevent Credit Card Fraud"

[39] Consumer Financial Protection Bureau, "What Do I Do If I Think I Have Been a Victim of Identity Theft?"

[40] Internal Revenue Service, "Identity Theft Information for Taxpayers"