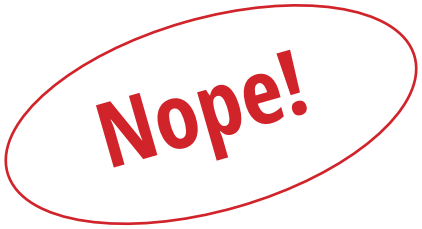
Identity theft and fraud: What to watch for and how to protect yourself

Identity theft is when a scammer steals your personal information and pretends to be you for their own financial gain. Fraud happens when a scammer uses your money for purposes other than what you intended.

Aren't I too young to be a victim of ID theft?



Teens are actually one of the biggest targets for identity theft! ID thieves are looking for targets that won't notice their identity has been stolen. People under the age of 18 do not have credit or credit reports to check, so it is easy for someone to use credit under the minors social security number.

Fraud Tactics

Here are a few popular ways the bad guys get your information:

- **Phishing** - When a scammer uses an email disguised as a legitimate company to get a persons information.
- **Smishing** - Similar to a phishing email, but smishing is through text messaging.
- **Dumpster Diving** - Scammers will go through your trash to find any documents that you may have thrown away with sensitive information, such as your social security number, credit card numbers, birthdays, etc.
- **Shoulder Surfing** - Be aware of who is around you when inputting personal information into a computer or ATM. Scammers will lurk over your shoulder to try and get any information they can.

Signs someone has stolen your identity

- Unexpected bills (or phone calls)
- Bills from companies you don't use
- Denials of credit you didn't apply for, or being denied credit
- Charges on financial statements you don't recognize
- Incorrect information on your credit reports, or if you under 18, having a credit report

Sounds like a scam...

Scams come in a lot of different forms. If it sounds good to be true, IT PROBABLY IS! Below are some examples of common scams that are targeted at young adults:

- **Job applications:** signs of a fake job application are a high hourly pay for limited hours and the employer sending you a check only to have you send some of the money back. If you apply for a job online, verify the job and the application before submitting any information. A call to the employer can prevent you from submitting your information to a scammer.
- **Social media:** social media is a great place for an ID thief to steal your information; birthday, full name, phone number, etc. Lock down your social media accounts so only people you approve can see that information. Better yet, don't post anything too personal. If you receive a duplicate friend request from someone you are already friends with on that platform, do not accept the new request. It is usually a scammer.
- **Online shopping:** The internet is full of ads, especially ads with deals that sound,you guessed it, too good to be true. If you shop online, be sure you are shopping from a reputable website that has many good customer reviews. Shopping with a credit card ensures better protection if fraud occurs.
- **Student Loan Repayment:** There are some legitimate student loan repayment programs. These programs take years before they will pay off. If a company offers you complete repayment for a one time, or monthly fee, that is a scam. Your student loan servicer will be able to give you details on legitimate student debt repayment plans.

Name the scam

Below are some common scam tactics and examples of how they are enacted. Match the tactic to the correct example.

Phishing

Smishing

Shoulder Surfing

Hacking

- You're at an ATM and there is someone in line behind you, standing suspiciously close...
- You receive a text message claiming you've won a $1,000 from a prize drawing you did not enter
- While you are on your computer, connected to the WIFI at your local coffee shop, you notice the mouse starts to move on it's own and someone is opening windows
- Netflix emails you asking you to email back your credit card information or else they will cancel your subscription

How can you better protect your identity?

List out 5 things that you are going to do now to protect yourself from identity theft, and then go do them!

1.

2.

3.

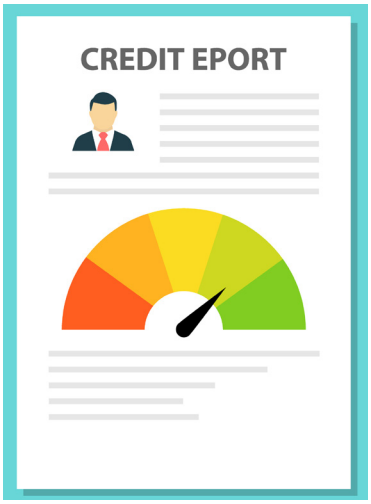
4.

5.

How do you know if you have been a victim?

- You receive bills, per-approved credit offers, or other mail in your name for accounts that you didn't open
- You are denied when you try to open your own bank accounts or accounts already exist in your name
- You have a credit report in your name

Checking your credit reports for fraud



If you are worried you have been a victim of identity theft, your guardian can check with the three credit bureaus. You can check your credit reports at www.annualcreditreport.com

- **Transunion**: www.transunion.com, https://www.transunion.com/credit-disputes/child-identity-theft-inquiry-form
- **Experian**: www.experian.com, https://www.experian.com/consumer-products/free-child-identity-theft-scan.html
- **Equifax**: www.equifax.com

What can I do to protect myself?

- Don't share perosnal information on social media- your phone number, birthday, full name and address are just a few of the things you should not share with the world
- Have your guardian look for a credit report in your name when you turn 16. If they cannot find anything, you are good to go!
- Use strong passwords on all of your accounts. Try to use a different password for each account, that way if a scammer hack one of your accounts, they can't use that password to access all of your accounts.
- Sign your debit cards and use RFID sleeves to protect them
- If you get an email or text message, even a letter in the mail, that doesn't look legitimate, don't respond to it!
- Don't carry your social security card with you. It should be locked away in a safe place at home.