

High School Identity Theft Activity

Items Needed

- Download and print copies of OKMM's *Your Money Matters* high school guide for each student.
- Download and print copies of Friend or Foe? worksheet as shown in this activity.
- Provide highlighters.

Opening Activity / Dialogue

- Have you or someone you know ever been a victim of identity theft?
- Do you worry about becoming an identity theft victim?
- Some studies cite that 20-29 year olds are heavily targeted as identity theft victims. Why do you think that's the case?

Content

Identity theft occurs when someone uses your personal information, like your name, Social Security number (SSN) or debit or credit card number, without your permission to commit fraud or other crimes.

Through this lesson you'll show your students:

- How to prevent identity theft.
- The importance of using strong passwords for online accounts.
- The reason they should be cautious when giving out personal information.

Use the content on page 13 of the high school *Your Money Matters* guide to educate your students about avoiding identity theft. Ask your students to read this information and be prepared to discuss the following questions.

- Why are you cautioned against putting personal information on social media sites? How could an identity thief use this information?
- Besides not carrying around your Social Security card, what are some ways you can protect your Social Security number?
- How can checking your credit report protect you from identity theft?
- How can you create and remember strong passwords?
- How can you protect your identity when shopping online?

Application

Now that your students have a basic understanding about avoiding identity theft, use the Friend or Foe? worksheet to help them better understand how information posted on social networking sites can be used by identity thieves. This exercise isn't intended to discourage them from using these sites; the purpose is to help them think twice about the information they willingly share with friends and anyone else who's looking.

Encourage them to work in groups of two or more and highlight keywords or information that could be used to help someone fraudulently use their personal information.

Activity Answers

Your students may have highlighted the following words:

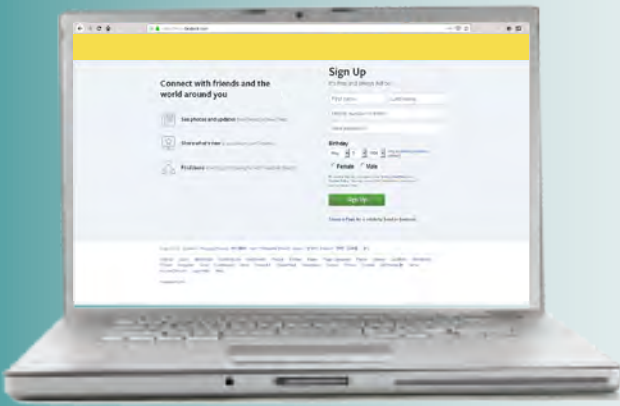
- Nikki Green: Of course, you can't avoid using your name; however, students can avoid using middle initials that might make obtaining information easier for an identity thief.
- Birthday: Encourage students to only use the date, not the year. However, even with just the date, a savvy thief could guess the year you were born.
- Hometown, school name and mascot: Many websites, like banks and credit card companies, have additional security questions that often include the high school you attend(ed) or mascot name.
- Tattoo, Terrier named Oreo: Students who don't use strong passwords may turn to easily memorable options such as TattooHappy or IHeartOreo for their passwords.
- Pampered Chef: When calling to switch services or change account information, some institutions may ask you to verify your place of employment.
- About: Much of the information listed in this paragraph could be used to gain access to more personal information. Security questions often involve your favorite animal (dog), favorite pastime (reading) or particular interest (politics).

Again, remind your students that this exercise isn't meant to scare them away from social media. They just need to be aware of the information they are making public and how it can be used to gain access to their personal finances.

To learn more about OKMM, visit our website,
OklahomaMoneyMatters.org.



Friend or Foe? Identity Theft Activity



Social media sites are great ways to share pictures and news with your friends and family, but they can also be great places for identity thieves to locate personal information and steal your identity. Many times identity thieves aren't strangers; they have relationships with their victims! You don't have to completely ban the use of social media for fear of becoming an identity theft victim, but you do need to take precautions to make sure you aren't over-sharing.

Use the following screenshot--based on a social media profile--and highlight words, sentences or phrases you think could be used to help an identity thief gain access to your information.

A screenshot of a social media profile for a user named Nikki Green. The profile includes a search bar at the top, a profile picture, and an 'About' button. The main content area is divided into several sections: 'Work and Education', 'History by Year', 'Living', 'About Nikki', 'Family', and 'Basic Info'. The 'Work and Education' section lists 'University of Central Oklahoma' and 'The Pampered Chef'. The 'History by Year' section shows a timeline of events from 1981 to 2012. The 'Living' section shows current and hometown locations. The 'About Nikki' section contains a bio. The 'Family' section lists two family members: Allen Miles and Renee Chandler. The 'Basic Info' section provides details like 'Interested In', 'Sex', and 'Phone'.