TOPIC CONNECTIONS:

Connects with ***Money Smart*** curriculum in the classroom: Lesson 5 (Choosing a Banking Partner), Lesson 11 (Risk Management and Insurance), Lesson 18 (Estate Planning), Lesson 19 (Financial Resources), and Lesson 20 (Consumer Protection).

TOPIC OVERVIEW:

With so many resources available online, it's tricky to know whom and what to trust when we're overloaded with ads, opportunities, and "get rich quick" schemes. Even though teens are growing up with technology all around them, knowing what personal information is OK to share and what information should remain private is still sometimes unclear. Creating a financial shield also means thinking about what risks you might encounter now and in the future, and thinking ahead for unforeseen circumstances through insurance and planning.

FROM THE CLASSROOM:

How do financial institutions protect money? The Federal Deposit Insurance Corporation (FDIC) insures all deposit accounts, including checking and savings accounts, money market deposit accounts, and Certificates of Deposit (CDs). Deposited money in insured financial institutions is guaranteed up to the maximum amount allowed by law ($250,000 per depositor, per bank) if the financial institution goes out of business and cannot pay you your money. The National Credit Union Administration (NCUA) provides similar coverage of deposits in NCUA-insured credit unions.

What financial resources are available? You are your greatest resource! You are in the driver's seat of your financial car, so it is important to teach yourself how to find answers to your questions. Start with free resources from governmental agencies such as the FDIC. Other federal, state, and local government agencies also publish information and have staff and resources that can help answer questions on money matters. Visit www.mymoney.gov, the federal government's one-stop resource for personal financial information. Financial institutions, consumer organizations, and the news media publish personal finance tips you can find by searching the Internet. You can also work with professionals, such as financial advisors and accountants, who can guide you in financial decision making.

How do you know what resources to trust? There are sometimes red flags for untrustworthy websites, including poor writing style, spelling or grammar errors, and lack of information about the author of the site. However, not everything written well on the web is a trustworthy site. Paying attention to other details such as domain names can offer some clues to the credibility of a website (for example: ".gov" means it is a government website, and ".edu" means it is an educational institution). It's also important to review credibility of financial professionals you choose to work with. A financial advisor is someone who offers financial advice, but if he or she is promising a return on your investment that sounds too good to be true, then it probably is! Financial experts should also be transparent with actions and fees, and you should be able to track down their credentials (for example: what type of education, training, and certifications they hold). For more information, visit the Securities and Exchange Commission at **http://www.sec.gov**, Financial Industry Regulatory Authority at **http://www.finra.org**, and Certified Financial Planners Board of Standards at **http://www.cfp.net**.

What types of insurance do you need? Insurance helps minimize financial risk when unforeseen events occur, like medical emergencies, a car accident, or even natural disasters such as hurricanes. People get insurance to help protect themselves in different situations, including health insurance, life insurance, auto insurance, and property insurance.

What is an estate plan? And why do you need one? Who has control over your social media accounts and online identity if you die? Who should get your cash, retirement savings, and bank accounts? Who should have your jewelry, your car, and your mementos? These are all difficult questions, but ones that are answered in an estate plan, which includes a will and power of attorney. An estate plan gives you an opportunity to outline ahead of time what should happen with your possessions and money in the event of your death.

What is identity theft, and how do you protect yourself? Identity theft is when someone illegally uses someone else's personal information, like full name and Social Security number, to get credit or money. Protecting yourself means paying attention and being alert to offers that sound too good to be true, acting quickly if you think your personal information is compromised, and taking precautions to limit opportunities for thieves to gain your data (for example: shredding old financial documents and "junk mail" credit offers, not oversharing on social media, keeping bank passwords to yourself, and creating strong passwords for online accounts).

WORDS TO KNOW:

Auto Insurance: A contract between you and an insurance company in which you agree to pay a fee (premium) and in return, the insurance company agrees to pay for certain expenses associated with an accident or other covered losses on your vehicle.

Claim: Request to an insurance company for payment for a covered loss under an insurance policy.

Deductible: The dollar amount or percentage of a loss that you have to pay before the insurance policy begins to pay.

Disability Insurance: Protects a person from loss of income due to a covered illness or injury.

Estate Planning: Planning for what will happen with assets or property after death.

Health Insurance: A contract that requires your health insurer to pay some or all of your health care costs in exchange for a premium (money paid).

Homeowner's Insurance: An insurance policy that covers a homeowner's house, other structures on their property, and personal contents against losses caused by such things as windstorms, fire, and theft. It generally also provides liability coverage (for example: this coverage would be applicable if you are found responsible for the injury of a friend who injures themselves while visiting you).

Identity Theft: When someone steals another person's identity to commit fraud, such as by using his or her name or Social Security number to get something. Identity theft is a crime.

Insurance: A contractual relationship that exists when one party (the Insurer), for a fee (the premium) agrees to reimburse another party (the Insured or third party on behalf of the Insured) for a specific loss.

Life Insurance: A form of insurance that will pay money to a beneficiary if the policyholder dies.

Medicare: A health insurance program for people who are 65 or older, certain younger people with disabilities, and people with permanent kidney failure requiring dialysis or a transplant. This program is financed by deductions from wages and managed by the federal Social Security Administration.

Pharming: Redirecting Internet requests to false Web sites to collect personal information, which is generally then used to commit fraud and identity theft.

Phishing: When fraudsters impersonate a business or government agency to try to get you to give them personal information, such as through an email or text message. Can also be thought of as "fishing for confidential information.

Power of Attorney: A legal instrument authorizing someone to handle the financial or other business affairs of another person.

Premium: The amount of money that has to be paid for an insurance policy.

Property Insurance: Insurance to protect you against damage that may occur to your property.

Text Message Spam: Similar to e-mail spam, but on your cell phone. Criminals often text offers of free gifts or low-cost credit offers to try to get you to click on a link so they can install malware on your phone or get you to give them information they can use to commit fraud.

CONVERSATION STARTERS...ASK YOUR TEEN:

- **What types of personal information do you think are OK to share with others, and why?**
- **What kind of insurance will you need when you live on your own?**
- **Why do you think it's important to think today about your finances in the future?**
- **How do you decide whether a resource or website is trustworthy and credible?**

WHAT IF MY TEEN WANTS TO...:

What if my teen wants to open a social media account? Most social media sites require users to be a certain age before creating an account. If your teen is of age and you feel he or she is ready to manage the responsibility of being online, discuss what information is OK to share and what information should be kept private. For instance, make sure your teen knows that under no circumstances should personal, identifying information like full name, address, Social Security number, and account passwords or numbers ever be shared. Talk with your teen about being selective with his or her "friends" online just as he or she would in real life. Some criminals may pretend to be "friends" or relatives in order to obtain personal information. For more information, read *Avoiding Fraud, Protecting Your Privacy: Best Practices for Young Adults* by FDIC Consumer News at **https://www.fdic.gov/consumers/consumer/news/cnfall12/avoidfraud.html**. Additionally, keep discussions open by talking about the permanence of social media and how one post, even if deleted, never really goes away.

What if my teen wants to play an online game? Like setting up social media accounts, your teen should comply with the legal age of use set by the game. If you feel your teen is responsible enough to play, monitor use closely. Does the game require a credit card in order to play? Does the game include communication and interaction with other players that your teen may or may not know in real life? These are all important elements to consider before determining whether your teen is ready to play online.

What if my teen has already shared personal data? If your teen has shared personal data, be on alert for warning signs of identity theft. If a criminal has obtained personal information such as a Social Security number, they can use it to open bank and credit card accounts, apply for government benefits, or apply for a loan. For a list of warning signs, visit the Federal Trade Commission's (FTC) Child Identity Theft website at **http://www.consumer.ftc.gov/articles/0040-child-identity-theft#Warning**. If you are certain that your teen's identity has been stolen, the first step to take is to place a fraud alert immediately. Taking action quickly minimizes the damage that can be done if an identity thief has stolen personal data. The FTC outlines the immediate steps to take to repair identity theft at **http://www.consumer.ftc.gov/articles/0274-immediate-steps-repair-identity-theft**. Once a fraud alert is set, you will want to order your teen's credit report and then create an identity theft report, instructions for which can be found at the website above.

FAMILY ACTIVITIES:

Wallet Review: If your teen carries a wallet or purse, go through it together and discuss what information he or she may be carrying that could potentially cause financial stress if stolen (for example: a driver's license, debit card, Social Security card). Or use your own wallet or purse as an example.

Shred "Junk Mail": Have your teen help you sort and shred financial documents that are old or that you don't need. For example: you could shred "junk mail" credit offers or even old receipts and papers that list your address and other personal information. Discuss why it's important to shred instead of throwaway personal papers.

Learn How You're Protected: Arrange a meeting to take your teen with you to visit a bank representative and discuss what type of protection and services the bank provides in response to identity theft.

Meet an Insurance Agent: If you work with an insurance agent, take your teen with you to review your current insurance policy, and encourage your teen to ask questions about coverage, cost, and protection. If visiting an agent isn't possible, you may also show your teen your family's insurance policy when paying bills and use it as an opportunity to discuss the costs and protection for different policies.

Social Media: If your teen is already on social media, use his or her account(s) to discuss positive and negative instances of social media participation (you may also use your own social media account or use an Internet search engine to locate news stories about oversharing online). Use real-life examples to discuss why oversharing personal information can be harmful and how it exposes you to identity theft.

Internet Search: Have your teen use an Internet search engine to type in his or her name and see what search results appear. Use the results as an opportunity to discuss with your teen how easy it is to get information on oneself online. You may also try searching your name and those of family members to further reinforce the availability of information about ourselves on the Internet.

RESOURCES:

ARTICLES:

- *4 Ways to Protect Your Teen from Identity Theft* by Abby Hayes, U.S. News: Read tips for how to avoid identity theft. **http://money.usnews.com/money/blogs/my-money/2014/06/22/4-ways-to-protect-your-teen-from-identity-theft**
- *Shopping for Auto Insurance* by the American Institute of Certified Public Accountants: Learn how to shop for auto insurance; from determining how much coverage you need to comparing value. **http://www.360financialliteracy.org/Topics/Insurance/Cars-and-Auto-Insurance/Shopping-for-Auto-Insurance**
- *Comparing Health Insurance Plans* by the American Institute of Certified Public Accountants: Learn how to compare and contrast health insurance plans. **http://www.360financialliteracy.org/index.php/Topics/Insurance/Health-Care-and-Health-Insurance/Comparing-Health-Insurance-Plans**
- *Writing a Will* by USA.gov: Read about what goes into writing a will, as well as how to write a social media will to describe how you would like your social media accounts handled in the event of death. **http://www.usa.gov/topics/money/personal-finance/wills.shtml#Write_a_Social_Media_Will**
- *Understanding Trusts* by USA.gov: Read about types of trusts and reasons for setting one up. **http://www.usa.gov/topics/money/personal-finance/trusts.shtml**
- *Prepare Your Estate Plan* by eXtension.org: Read an overview of how to create an estate plan. **http://www.extension.org/pages/15749/prepare-your-estate-plan#.VCqGiWRdVNt**
- *What You Can Do to Avoid Investment Fraud* by Investor.gov: Read tips on how to avoid being a victim of investment fraud. **http://investor.gov/investing-basics/avoiding-fraud/what-you-can-do-avoid-investment-fraud#.VCqIwWRdVNt**
- *Types of Fraud* by Investor.gov: Read about different types of investment fraud and how to avoid them. **http://investor.gov/investing-basics/avoiding-fraud/types-fraud#.VCqI-GRdVNt**
- *Taking Charge: What to Do if Your Identity Is Stolen* by the Federal Trade Commission: Read about immediate and next steps to take if you believe your identity has been stolen. **http://www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf**
- *When a Criminal's Cover Is Your Identity* by the Federal Deposit Insurance Corporation: Read an overview of identity theft and a prevention checklist. **https://www.fdic.gov/consumers/privacy/criminalscover/index.html**

ONLINE TOOLS:

- *Life Insurance Calculator* by the American Institute of Certified Public Accountants: Use this online calculator to determine how much life insurance you need. **http://www.360financialliteracy.org/index.php/Topics/Insurance/Life-Insurance/Life-Insurance-Calculator**
- *Financial Fraud in the United State* by SaveAndInvest.org: Review statistics on identity theft and fraud and learn how to protect yourself. **http://www.saveandinvest.org/web/groups/sai/@sai/documents/sai_original_content/p339651.pdf**

- The Federal Trade Commission offers resources that describe the warning signs of child ID Theft, how to check for your child's credit report, steps to go about repairing a child's credit damage, how to prevent and protect against ID Theft, and what to do when a child turns 16. **http://www.consumer.ftc.gov/articles/0040-child-identity-theft**
- *StopFraud.gov* by the Financial Fraud Enforcement Task Force: Learn about what financial fraud is and how to protect yourself from it, as well as what to do if you think your personal information has been compromised. **http://www.stopfraud.gov**

GAMES/APPS:

- *ID Theft FaceOff* by OnGuardOnline.gov: A quiz-style game reviewing what to do if your identity has been stolen. **http://www.onguardonline.gov/media/game-0005-id-theft-faceoff**
- *Spam Scam Slam* by OnGuardOnline.gov: A quiz-style game reviewing types of spam and scams. **http://www.onguardonline.gov/media/game-0012-spam-scam-slam**
- *The Case of the Cyber Criminal* by OnGuardOnline.gov: You work to stop a spy from stealing your personal information in this game. **http://www.onguardonline.gov/media/game-0013-case-cyber-criminal**
- *Phishing Scams* by OnGuardOnline.gov: Practice avoiding the bait of phishers in this game. **http://www.onguardonline.gov/media/game-0011-phishing-scams**