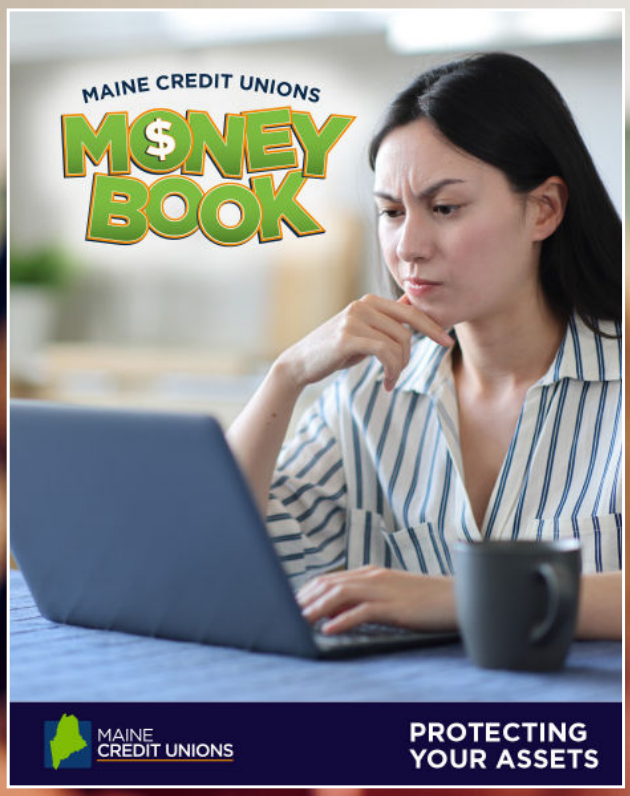


EDUCATOR GUIDE

MAINE CREDIT UNIONS

PROTECTING YOUR ASSETS

ADULT EDUCATION

MAINE
CREDIT UNIONS

A LONG HISTORY:
People Helping People.

Maine credit unions have a long history of providing financial education. Between volunteering to teach youth financial education in schools and hosting Financial Fitness Fairs, credit unions across the state collectively expose nearly 20,000 Maine students to financial literacy and money management concepts each year. Maine credit unions also provide financial education to our state's adult population––whether it be older adults, New Mainers, food pantry clients, or other groups. Maine credit unions recognize the the importance of equipping people with the knowledge and skills needed to help them manage their money effectively.

LESSON:
MONTHLY BUDGET SIMULATION

Introduction:

Greet the group. Tell them your name, describe what you do for work at the credit union, and share some fun information about yourself.

Explain to the group that you're here volunteering on behalf of your credit union, an organization that is happy to teach people of all ages about saving and spending money. Additionally, explain that your credit union is also a place where people can safely keep their money, as well as access all the latest and greatest regarding financial convenience offerings.

Volunteer Tips

When speaking to the group, remember to be yourself. People appreciate authenticity and you will establish better credibility if your personality shines through.

Encourage dialogue amongst the group as your progress through the lesson plan.

Write your introduction notes and/or talking points here:

Discussion:

While distributing the Maine Credit Unions Money Books to each participant, tell the group you're here to talk about fraud and scam prevention. Tell them that scammers are ever evolving and deceptively clever in their attempts to obtain peoples' money and personal information, and that it's important they know how to recognize, resist, and report scams.

Ask the group to turn their Maine Credit Unions Money Books to page 1, where they'll find definitions for fraud and scams. Define the following:

Scam: A deliberate scheme designed to deceive people in order to steal money, personal information, or other assets.

Fraud: When a person creates, uses, or allows a false impression to exist in order to secure money, assets, services, or other financial advantage at another's expense.

Explain that the main difference between fraud and a scam is ***permission***. Tell the group the following:

"A scam is financial theft **with one's permission or knowledge**. It's a trick that is designed to persuade people into believing false information or promises, with the goal of gaining their money, personal information, or other valuables. Scammers often manipulate their victims by exploiting their trust. Examples of scams include people pretending to be debt collectors, offering fake investment opportunities, or promising fake lottery or prize winnings. For example, a scammer could mail, call, text, or email someone to tell them they've won a prize through a lottery or sweepstakes and then ask them to pay an upfront fee to receive the rest of the money. There is no prize. The scammer simply wanted quick payment from the victim."

"Fraud is financial theft **without one's permission or knowledge**. Fraud refers to the deceptive and dishonest activities carried out with the intention of gaining financial or personal benefits–– all while breaking the law. Examples of fraud include unauthorized use of someone's credit or debit card, stealing someone's identity and opening accounts in their name, and taking over an unsuspecting person's financial accounts. Fraud is more difficult to protect oneself from than scams, as it happens without people knowing about it."

Next, ask the participants to turn their Maine Credit Unions Money Books to page 2.

Discussion:

Ask the group to raise their hands if they've received a suspicious phone call, text, or email in the past month. If there are any hands up, tell them they're not alone, as people are becoming inundated with these communications more than ever before.

Next, ask the group to raise their hands if they––or someone they know––has ever been targeted by a fraudster or scammer. Again, if there are any hands up, tell them they're not alone. Let the group know that millions of Americans fall victim every year, losing over $10 billion annually.

Ask if anyone would be willing to share a scam attempt they've experienced recently. It could be a suspicious text, email, phone call, or message on social media.

After hearing from the participant(s), reinforce that those are all classic examples, and that nobody is immune to the threat of fraud and scams. Thank them for sharing.

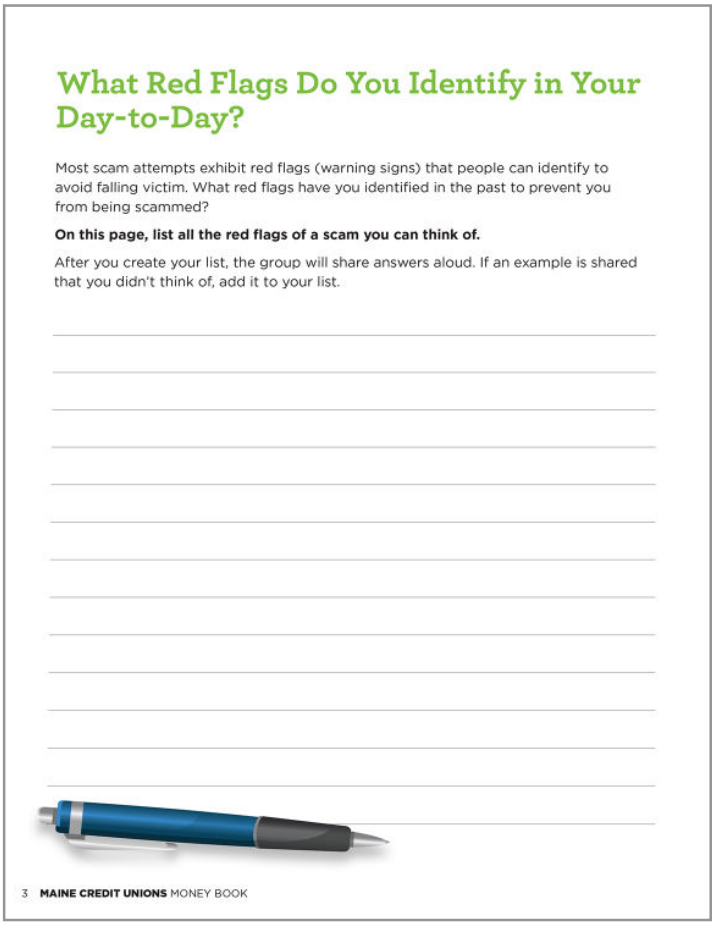
Next, ask the group to turn their Maine Credit Unions Money Books to page 3.

Activity:

Tell the group that on page 3 of the Maine Credit Unions Money Book, they will be thinking about how they're already identifying scams in their day-to-day. Explain that most scam attempts exhibit red flags (warning signs) that people can identify to avoid falling victim.

Ask the participants to spend a few minutes listing any red flags that might indicate they're being targeted by a scam.

After giving the group a few minutes, ask people to raise their hands and share an example(s) they wrote down in their Money Book.



What Red Flags Do You Identify in Your Day-to-Day?

Most scam attempts exhibit red flags (warning signs) that people can identify to avoid falling victim. What red flags have you identified in the past to prevent you from being scammed?

On this page, list all the red flags of a scam you can think of.

After you create your list, the group will share answers aloud. If an example is shared that you didn't think of, add it to your list.

3 **MAINE CREDIT UNIONS** MONEY BOOK

Discussion:

Now that the group has completed their brainstorming, highlight the following key warning signs:

You need to act fast. Acting in urgency is a warning sign of a scam. Scammers want you to act quickly and make payments without taking the time to think the situation through.

They're using fear tactics. If someone threatens to arrest you, sue you, or subject you to any other consequences if you don't pay them, it's likely a scam. Scammers know that fear can lead to poor judgement.

Unusual payment methods are requested. If you are asked to send a payment via a wire transfer, prepaid card, or cryptocurrency, do not do it. These methods are nearly untraceable, and once the money is sent, it's usually gone for good.

Pre-payment is requested. If someone offers you a prize or debt relief, if you have to pay an upfront fee or shipping costs in order to get it, it's most likely a scam.

They want your personal information. If you are contacted and asked to verify sensitive information over the phone, hang up. Never provide personally identifiable information like your birthday or Social Security number in response to an unsolicited call, email, or text message.

You need to keep it a secret. If you are asked to keep a transaction a secret, it's likely because the scammer doesn't want you to share the situation with someone who might detect it as a scam.

After reviewing the key warning signs, ask the group to turn their Maine Credit Unions Money Books to page 4.

Activity:

Tell the group that on page 4 of their Maine Credit Unions Money Book, they will try to think about the different types of scams they're aware of. On this page, ask them to list as many types as they can.

After giving the group a few minutes, ask people to raise their hands and share an example(s) they wrote down in their Money Book.

Discussion:

Now that the group has completed their brainstorming activity, highlight the following popular scams:

Lottery or prize scams: Never provide personal or financial information if you've been contacted about winning a prize, especially if you didn't enter to win one. Scammers may try to get you to pay an upfront fee or taxes before receiving the "prize," or they may ask for your account information––that way they can "deposit the money." This is likely a scam.

Imposter scams: This is when a scammer pretends to be someone else, such as a government official, police officer, credit union or bank employee, friend, or family member–– with the intention of obtaining your money or personal information. Always confirm the identity of the person contacting you. To avoid phone spoofing, hang up and call the person back directly. Your credit union won't call you for online banking information, passwords, Social Security numbers, addresses, phone numbers, or other private personal information.

Wire or money transfer fraud: Never transfer money to someone you don't know. If you are asked to send a payment via a wire transfer, prepaid card, or cryptocurrency, do not do it. These methods are nearly untraceable, and once the money is sent, it's usually gone for good.

Check scams: If you're selling something, do not accept a check for more than the requested amount. After the sale, scammers will ask you to send back the difference they "mistakenly" overpaid. The check will later bounce, and you've lost both the money and whatever item you sold.

Romance scams: These are deceptive schemes where scammers create fake online personas, pretending to be potential romantic partners, to exploit individuals looking for love or companionship. After building emotional connections with their victims over time, they gain their trust and affection. Once that trust is established, they ask for money.

Charity scams: Always verify that a charity is legitimate before donating. Check their website, look for reviews, and never donate if you're feeling pressured. You should also be suspicious if a charity asks you to make a donation via cash or wire transfer.

Debt settlement or relief scams: Don't pay upfront fees to any company that guarantees the can settle or eliminate your debts. Scammers will promise to negotiate with creditors on your behalf to settle your debts for a fraction of the amount owed, or even wipe the debt out entirely. They charge an upfront fee but fail to deliver on their promise, leaving you in a worse financial situation and without any real debt relief.

After you have highlighted the most popular types of scams, let the group know the lists of red flags and types of scams can be found in the back of their Maine Credit Unions Money Books

Next, ask the group to turn their books to page 5.

Discussion:

Tell the group that the most common end goal is for fraudsters and scammers to get your money. However, if they can't immediately get your money, what is the next most valuable thing they'll go after? Ask the group to raise their hands if they think they know the answer.

After calling on an individual(s) and hearing their thoughts, reinforce that someone's identity is an extremely valuable asset, and that your identity or bits and pieces of your personally identifiable information in the hands of a fraudster is very dangerous.

Explain that when someone's identity is stolen, there is not only a threat to threat to their finances, but there can also be other negative outcomes––including a loss of privacy and personal safety, strained relationships, reputational risks, administrative problems, and an emotional and psychological impact.

Tell the group that one's identity is an asset because their name, Social Security number, and other personal financial information can help them get a job, be approved for a loan, rent an apartment, and open an account at a financial institution––as well as a lot more.

Highlight the following documents that include very sensitive identity information:

- Social Security card
- Birth certificate
- Driver's license
- Passport
- State ID
- Student ID
- Individual Taxpayer Identification Number (ITIN)

Activity:

Next, ask the group to turn their Maine Credit Unions Money Books to page 6. On this page, they'll find a blank list. Tell them that as a group, we'll fill this list with examples of other documents or pieces of information that fraudsters could use to impersonate them.

Ask the group to raise their hands and share an example(s), and then have the group write the examples down their book as they are shared.

What Could a Fraudster Use or Reference to Impersonate Someone?

Understanding what information can be misused is the first step in protecting it. When people know which documents carry risk, they are better-equipped to safeguarding themselves and others.

On this page, list all the documents you can think of that a fraudster could use to gather personal information and potentially impersonate someone.

After you create your list, the group will share answers aloud. If an example is shared that you didn't think of, add it to your list.

in

After spending a few minutes reviewing examples, mention the following, if not already contributed:

Next, ask the participants to turn their Maine Credit Unions Money Books to page 7.

Discussion:

Tell the group that on this page, they'll learn about the ways in which they could be harmed if they had their identity stolen. Read the following to the participants:

A fraudster using a stolen identity could:

- Open up accounts in your name at financial institutions, including credit accounts, such as credit cards, personal loans, or other lines of credit.
- Access your financial accounts and steal your money.
- File a false tax return in your name, stealing your refund and reporting inaccurate information you will need to clear up.
- Use your identity to obtain prescriptions or medical treatments. This may result in medical providers billing you for services you did not receive.
- Rent property or obtain utilities using your name.
- Conduct social engineering scams, where they pose as you to deceive your friends, family, or coworkers.
- Blackmail or extort you by leveraging sensitive or private information.

Discussion:

Next, tell the group that on the bottom of page 7, they'll learn how fraudsters are able to steal identities. Read the following to the group:

Fraudsters steal identities by collecting personal information through data breaches, stolen mail, malware, or online exposure, and then use that information to impersonate someone. One of the most common methods is phishing, where criminals send emails, texts, or phone calls that appear to come from legitimate organizations (like financial institutions, employers, or government agencies) to trick people into clicking malicious links or providing passwords, account numbers, or one-time passcodes. Malware can also be installed through infected attachments or websites, allowing fraudsters to log keystrokes, capture credentials, or access stored data on a device.

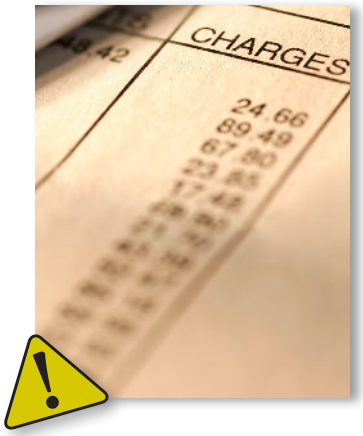
Another popular tactic is social engineering, which involves manipulating people rather than technology. Fraudsters exploit trust, urgency, fear, or authority—posing as coworkers, IT support, family members, or officials—to persuade victims to bypass security controls or share sensitive information. They often combine these techniques with publicly available data from social media or public records to sound convincing, then exploit weak passwords, reused credentials, or unsecured networks to take control of accounts and commit identity fraud.

Discussion:

Next, ask the group to turn their Maine Credit Unions Money Books to page 8. Tell them that on this page, they'll be reviewing the warning signs that someone's identity may have been stolen.

Review the following with the group:

Financial & Credit Warning Signs



- Unexpected credit card charges or account withdrawals.
- New accounts or loans you don't recognize on your credit report.
- Being denied credit unexpectedly.
- Bills or collection notices for accounts you never opened.
- Sudden drops in your credit score without explanation.
- Notifications of credit inquiries you didn't authorize.
- Debt collectors calling you to pay unfamiliar debts.

Account & Login Warning Signs

- Password reset emails you didn't request.
- Being locked out of accounts due to changed credentials.
- Login alerts from unfamiliar devices or locations.
- Two-factor authentication codes you didn't initiate.
- Account profile details (email, phone, address) changed without your knowledge.

Personal & Administrative Red Flags

- Mail stops arriving or you receive mail for accounts you don't recognize.
- Address change confirmations you didn't request.
- Calls or letters from the IRS or tax authority about unfiled or duplicate tax returns.

Medical & Insurance Warning Signs

- Bills for medical services or prescriptions you didn't receive.
- Errors or unfamiliar entries in your medical records.
- Insurance claims you didn't submit.
- Explanations of benefits (EOBs) for unknown treatments.

After reviewing the warning signs with the group, ask them to turn their Maine Credit Unions Money Books to page 9

Tell the group that on the top of page 9, they'll learn about what credit unions and other financial institutions will never contact you and ask for. Share the following with the group:

Credit union employees are trained to detect fraud and scams. It's also important to remember that credit unions and other financial institutions won't contact you and ask for your:

Activity:

Tell the group that after learning about scams and identity theft, they'll review some scenarios on the remainder of page 9 and 10. Ask that after reading each scenario, they decide whether it's a scam attempt, a warning sign of identity theft, or a legitimate communication. If they feel it's a scam attempt or a warning sign of identity theft, ask them to identify the red flags that influenced their decision.

Give them a few minutes to complete the activity.

After it looks like everyone has finished, ask a participant(s) to share their thoughts on the scenarios. Review each scenario with the group, highlighting the answers for each after the group has an opportunity to share their thoughts.

SCENARIO 1:

"ALERT: Your [Credit Union Name] account has been locked due to suspicious activity.

Click here immediately to verify your information:

http://secure-verify-cu-123.com Failure to act in **10 minutes** will result in permanent account closure."

This scenario is:

1) A scam attempt

2) An identity theft warning sign

3) Neither

What are the red flags, if any?

- **Unfamiliar link (not official URL).**
- **You need to act fast.**
- **There is a threat of "permanent closure."**

SCENARIO 2:

"[Insert name]

Your mailing address and email were successfully updated on your account.

If you did not make this change, contact customer support immediately."

**You did not make any changes.*

This scenario is:

1) A scam attempt

2) An identity theft warning sign

3) Neither

What are the red flags, if any?

- **I received an alert I didn't expect.**
- **This indicates someone has access to my login credentials.**

SCENARIO 3:

Your [credit union name] monthly account statement for September is now available.

To view your statement, please log in using your usual method (mobile app or by typing our website directly into your browser).

As a reminder, we will never ask for your password, full account number, or one-time security code by email or text.

If you have questions, contact us at the phone number listed on the back of your card or on our official website.

This scenario is:

1) A scam attempt

2) An identity theft warning sign

3) Neither

What are the red flags, if any?

There are no red flags. The communication:

- **Does not create urgency or threats**
- **Does not include clickable links**
- **Clearly states what the credit union will never ask for**
- **Directs members to use trusted access methods they already know**
- **Matches a routine, expected event (monthly statement)**

SCENARIO 4:

Your [credit union name] accont statement is ready so click this link too view it:

http://y0urcredltunion-stat3ment.com

Due to recent secuirty issues you must log in immediately to avoid service interuption.

If you have any questions reply to this message directly for help.

This scenario is:

1) A scam attempt

2) An identity theft warning sign

3) Neither

What are the red flags, if any?

- **Spelling mistakes.**
- **Grammar mistakes.**
- **A fake link.**
- **A sense of urgency.**
- **Unprofessional tone and formatting.**

SCENARIO 5:

"Grandma, it's me. I'm in trouble. I was in a car accident and I've been arrested. Please don't tell Mom and Dad—they'll freak out. The lawyer says I need **$4,000** right now. Can you go buy gift cards and read me the numbers on the back? Please hurry!"

This scenario is:

1) A scam attempt

2) An identity theft warning sign

3) Neither

What are the red flags, if any?

- **Caller says "don't tell anyone."**
- **Urgent demand for money.**
- **Request to pay in gift cards.**
- **Emotional manipulation and fear.**

After reviewing the answers to each scenario, thank the group for participating in the activity and ask them to turn their Maine Credit Unions Money Books to page 11.

Discussion:

Tell the group how they now know how to recognize the red flags and warning signs of scams and identity theft. Tell them that on page 11, they'll learn about the things they can do to limit the threat of falling victim.

Read the following to the group:

- **Slow down before responding** to any unexpected call, text, or email. Scammers use urgency to cloud your judgment.
- **Never share one-time passcodes, PINs, or passwords** with anyone who contacts you. Legitimate institutions will not ask for these.
- **Type website addresses yourself** instead of clicking on links in communications.
- **Enable multi-factor authentication (MFA)** on banking, email, and other online accounts.
- **Use strong, unique passwords** for every account. Consider using a password manager to keep them secure.
- **Set up account alerts** (transaction alerts, login alerts, card-not-present alerts) so you know immediately if something is wrong.
- **Monitor your credit reports regularly** at AnnualCreditReport.com to spot unfamiliar accounts or inquiries.
- **Be cautious with public Wi-Fi.** Avoid logging in to financial accounts or entering sensitive information unless you're on a secure network.
- **Shred sensitive documents** before disposing of them (bank statements, insurance letters, tax documents).
- **Check sender details carefully**. Their email address, phone number, spelling, and tone can show red flags of scams.

- **Hang up and call back** using a trusted phone number (like the one on the back of your card) if something feels off.
- **Never pay with gift cards, wire transfers, cryptocurrency, or payment apps** for someone you don't know personally. These are popular among scammers, as they are more difficult to trace.
- **Keep software and devices updated** to protect against malware and security vulnerabilities.
- **Review your financial statements** regularly for unfamiliar charges. Report suspicious activity immediately.
- **Limit what you share on social media.** Scammers use personal details to guess security questions or impersonate you.
- **Freeze your credit** if you want maximum identity theft protection. It prevents new credit from being opened in your name.
- **Trust your instincts.** If something feels odd, rushed, or too good to be true, it's worth pausing to think things through.

Discussion

Next, ask the group to turn their Maine Credit Unions Money Books. Tell them you'll close the lesson plan by letting them know how they can report scams and identify theft.

Read the following to the group:

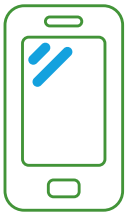
Notify your credit union or credit card issuer.

If the fraud or scam involves your credit union account, credit card, or any other financial accounts, immediately contact the institution. Inform them about the fraudulent activity and follow their instructions on how to proceed.

Document the details.

Gather all relevant information, such as emails, phone numbers, messages, receipts, or other evidence related to the fraud or scam. This will be important information to have when you report the incident.

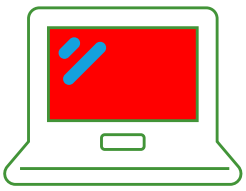
File reports.



In the United States, you can report fraud and scams to the **Federal Trade Commission (FTC)**, which collects data on deceitful activities to identity trends and patterns. You can file to report by visiting the **FTC's website** or by calling

1-877-FTC-HELP (382-4357).

Contact your local police department or law enforcement agency and file a report. Provide them with all the evidence you have gathered. Even if they might not be able to investigate every case, reporting the incident can help build a case against the scammer or fraudster by identifying patterns of criminal activity.



If your information was stolen, such as your Social Security number, credit card, account details, or other personally identifiable information, go to **IdentityTheft.gov**. On this website, you can report what happened, obtain a recovery plan, and receive guidance through each recovery step.

Safeguard your credit.

If your personal information was compromised through fraud or a scam, contact the three major credit bureaus (Experian, TransUnion, and Equifax) to initiate fraud alerts and freeze your credit. By adding a fraud alert to your credit report, it will warn lenders that you may be a victim of fraud. This is an extra precaution and will let potential lenders know they should contact you before opening any new lines of credit in your name. You can also freeze your credit for free at each of the major credit bureaus. Freezing your credit prevents any new credit accounts from being opened in your name. Even if identity thieves have accessed all of your personal information in a data breach, they can't open new accounts in your name if your credit is frozen.

Thank the group for participating and learning more about fraud and scam prevention.

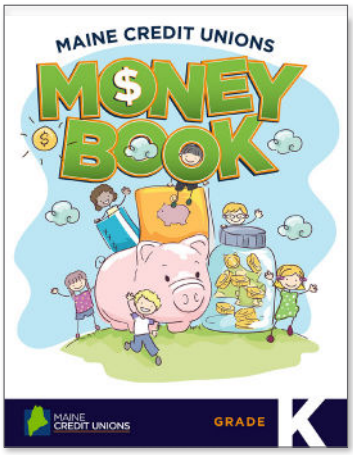
Time permitting, answer any further questions the group may have.

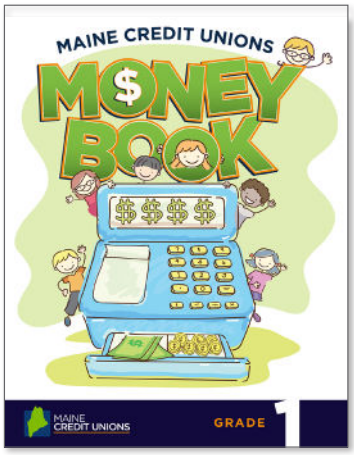
Elementary and Middle School Curriculum

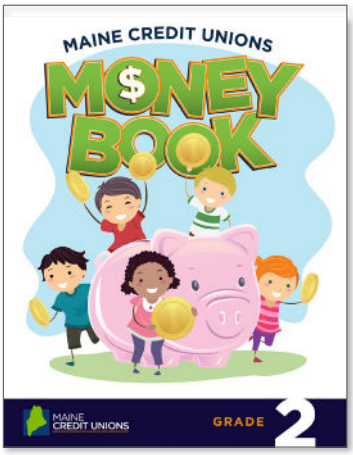
Did you know the Maine Credit Union League has lesson plans you can lead in elementary and middle school classrooms?

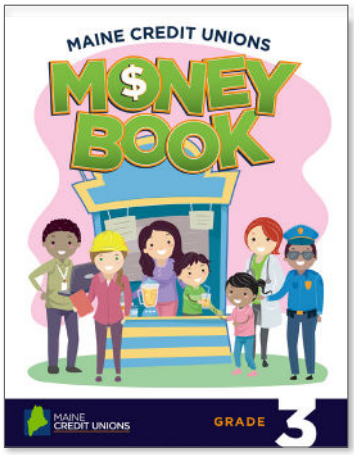
The elementary lesson plans cover the basic concept of what money is and the purpose it serves, the difference between goods and services, identifying and counting money, differentiating between wants and needs, banks and credit unions, and more.

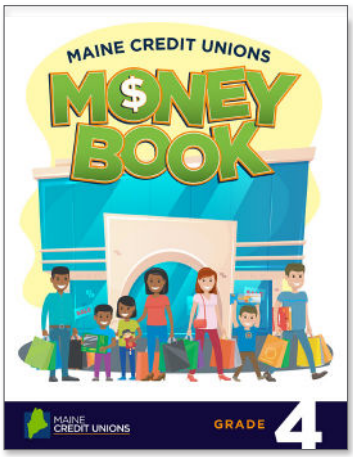
The middle school plan offers a hands-on, age-appropriate monthly budget simulation.

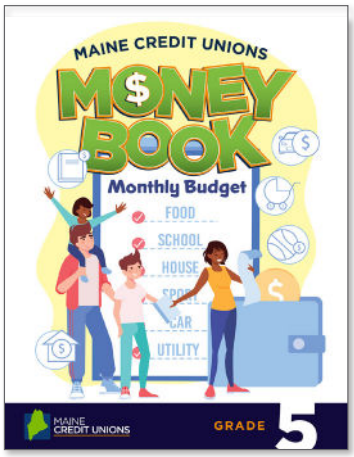


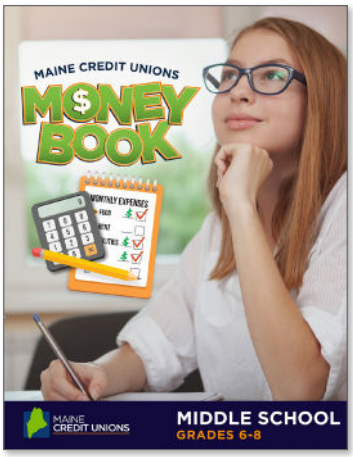










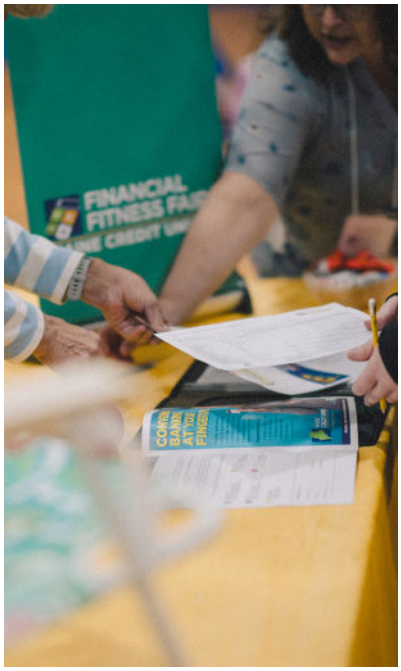


To download the turn-key, grab-and-go elementary and middle school lesson plans, scan the QR code:

Have you volunteered at a Financial Fitness Fair?

MAINE CREDIT UNIONS

Created in 2004, Maine Credit Unions' Financial Fitness Fairs are an insightful and fun budget simulation, similar to the game of "Life." Participating students choose a career and are assigned a monthly income, and then have to visit booths associated with various expenses that the average adult is faced with each month. After filling in a monthly budget form, the goal is for students to have a monthly budget that does not exceed their monthly income.



If you would like to learn more about Financial Fitness Fairs, find a schedule of upcoming fairs across the state, and learn more about what being a volunteer entails, scan the QR code:

THANK YOU,
CREDIT UNION VOLUNTEERS!

Your time and commitment to financial education are important and appreciated.