# Credit unions safeguard you from scams.

Credit union employees are trained to detect fraud and scams. Ask your local credit union about their fraud detection services and how they can protect your finances.

It's important to remember that credit unions and other financial institutions won't call you for:

- Online banking information
- Passwords or PINs
- Social Security Numbers
- Mother's maiden name
- Address
- Phone number

## Maine credit unions are here to help you achieve your financial goals.

To find a local credit union, visit
**mainecreditunions.org**
or scan the code below:

MAINE CREDIT UNIONS



# How to Protect Yourself from Scams

MAINE CREDIT UNIONS

*Maine Credit Unions Are Here For You*

# What is a scam?

A scam is a scheme or a trick that uses misinformation and scare tactics to obtain your personal, financial, or other important information. Scams can take place over the phone, by email, mail, and even in person.

The groups or individuals perpetrating these schemes, known as scammers or fraudsters, often pose as people, agencies, and companies that you know and trust.

## What are some signs of a scam?

**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.

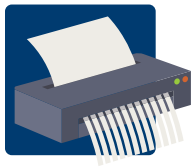
**You need to keep it a secret.**

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.

## How can you avoid scams?

**Never open unsolicited attachments or links.**

If you receive an unexpected text, email, or message that contains an attachment or link, delete it.



**Store or shred documents with personal information.**

If you have documents with your birthdate, passwords, Social Security Number, or other personal information, store them away from prying eyes or hands, or shred them before disposing of them.

**When in doubt, don't give it out.**

Trust your instinct. If someone asks for your information and you feel uncomfortable or if you believe it could be a scam, end contact with them.

**Create strong passwords and change them regularly.**

Create strong, hard-to-guess passwords for your accounts and update them regularly. Never use the same password for multiple accounts.