

Internet criminals use high tech scams, product offers or fear tactics to deceive consumers into disclosing credit card numbers, bank account information or social security numbers.

## Recognize the signs that may indicate a scam:

- You receive an email that claims to be law enforcement, the IRS or some other government agency stating you owe money and must immediately call a number, purchase gift cards and so forth to pay your debt.
- You receive an urgent email telling you your account with your credit union or bank is in some type of jeopardy and needs your immediate response including critical account or other numbers.
- You are sent an email-only offer that sounds too good to be true and is only available by responding immediately.
- The website does not offer a secure connection when processing sensitive information such as your credit card number, address, etc. (only use https:// sites)
- You receive a call or email from someone claiming to represent your financial institution, asking for sensitive account or personal information.
- You are promised a quick turnaround and easy money through a work-at-home opportunity.

## What you should do if you suspect a scam:

- If you sense a problem, call the credit union or bank sending the email. Use a number other than the one provided in the email to verify if the message sent to you is legitimate.
- If you do not recognize the sender's name, delete the email without reading it. Remember, legitimate institutions do not use email to deliver critical news about your account or financial status. Assume any solicitation email is a scam until you can verify it.
- Never provide bank account numbers, social security numbers or other identifying information in response to unsolicited emails.
- Never allow anyone to take control of your computer or download any apps on your phone that allow a third party access to your device.
- Never click on a link sent with an email until you verify it's a legitimate email.
- If you decide to make a purchase via the internet, make sure you know the following before you buy:
  - <sup>o</sup> The company from whom you are buying.
  - <sup>o</sup> The specific product you are buying.
  - The company's shipping and handling charges.
  - The company's return policy.
  - ° The privacy policy regarding your purchase.
  - <sup>o</sup> The site is secure.

If you fall victim to a scam call the Credit Union immediately so we can help protect you and your account from any additional fraudulent transactions.



