April 2026

Blazon

FIREFIGHTERS CREDIT UNION • 726 MASSACHUSETTS AVE. • INDIANAPOLIS, IN 46204 • 317-636-5581 • www.fire-cu.org

Let the Sun Set

ON YOUR OLD AUTO LOAN.

Refinance your auto, motorcycle, RV or boat loan from another institution for a 1% APR* reduction on your current rate!

FIREFIGHTERS CREDIT UNION

EQUAL HOUSING LENDER

YOUR SAVINGS INSURED TO $250,000 PER ACCOUNT
AMERICAN SHARE INSURANCE
This institution is not federally insured. Members' accounts are not insured or guaranteed by any government or government-sponsored agency.

*APR = Annual Percentage Rate. This offer is not valid on loans currently financed with Firefighters Credit Union. Payment example based on $25,000.00 financed at 4.99% for a 72-month repayment term is estimated at $402.53. Will not go lower than 4.99%. Must provide proof of existing rate. Subject to credit approval. Standard underwriting policies and guidelines apply. Terms and conditions subject to change without notice.

35th ANNUAL SCHOLARSHIP GOLF OUTING

The 35th Annual Scholarship Golf Outing has been scheduled for Monday, August 10th, at Valle Vista with a 9AM start time.

Please join us for this fun-filled day that helps many students with college expenses. Last year we raised $4700.00.

Applications are available at Firefighters Credit Union. For more information contact Madison at 317-636-5581 ext. 252.

Scholarship Applications are available on the website at www.fire-cu.org or you can pick one up in the office. Applications are due in the credit union by August 14th. Winners will be notified after the drawing.

in this ISSUE

holiday CLOSINGS

Firefighters Credit Union will be closed for the following holidays:

GOOD FRIDAY
Friday, April 3, 2026
Closes at noon

FDIC
Friday, April 24, 2026
Closes at noon

MEMORIAL DAY
Monday, May 25, 2026

JUNETEENTH
Friday, June 19, 2026

EQUAL HOUSING LENDER

YOUR SAVINGS INSURED TO $250,000 PER ACCOUNT
AMERICAN SHARE INSURANCE
This institution is not federally insured.

ANNUAL MEETING ELECTION RESULTS

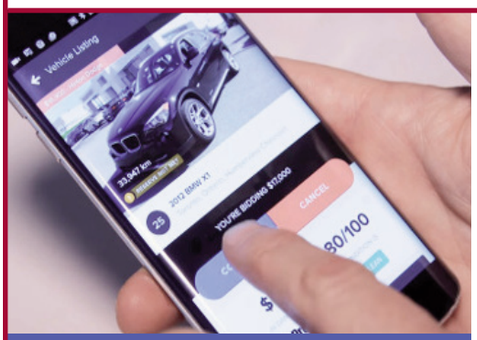
The 70th Annual Meeting was held March 31st, 2026. Voting was conducted for the volunteer Board of Directors and Supervisory Committee.

REINSTATED TO THE BOARD OF DIRECTORS

Gregg Harris
Jason Smith
Ron Kautsky

REINSTATED TO THE SUPERVISORY COMMITTEE

Peter Downing
Shawn Cross



VEHICLE SCAMS

In recent years, fake vehicle listings have been on the rise.

Cybercriminals have been creating fake listings or websites presenting too-good-to-be-true deals. Often, they are hard to verify due to the supposed rarity of the vehicles.

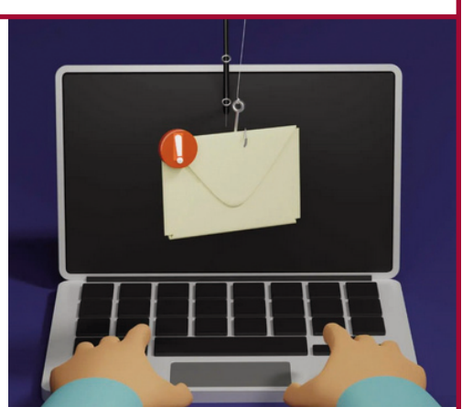
A fake vehicle history report may even be included to lend credibility to their listing. To avoid these scams research the seller, insist on seeing the vehicle in person, and proceed with caution if asked to pay through unusual or untraceable methods.

1) **Mobile Payment Apps:** Be aware of fake text messages from payment apps asking you to enter account information or click on a link. Do not send money to people you don't know. If someone you know requests money, always contact them beforehand to ensure they haven't been hacked.

2) **One-Time Password (OTP) Bots:** Receiving an OTP message out of the blue, usually means someone else was trying to log-in to your account. The cybercriminal may pretend to be with a legitimate company and ask you to provide the OTP sent to your phone. They also may ask you to enter the code if you did NOT authorize a change to your account. If you give them the code, they will be able to access your account.

3) **QR Code Scams:** Cybercriminals are taking advantage of the popularity of QR codes. QR codes provide touchless options for payment, as well as access to restaurant menus, business cards, and more. Scammers are using QR codes to lead people to fake payment screens or infect their devices with malware. Avoid QR codes posted in public places such as parking meters or sent in unsolicited emails.

IMAGE-BASED PHISHING



Cyber attackers may use images to perform a phishing attack. Clicking an image or graphic included in an email may execute malware, initiate a malicious download, or send you to a website intended to steal your credentials or financial information.

Imaged-based scams are more likely to make it through email filters since some services cannot catch suspicious wording in an image.

In some cases, the attacker composes a message, turns the content into an image and sends the image to unsuspecting recipients. The email might look slightly stretched or blurry and might use colors that seem slightly off from the brand's color scheme. Not realizing they are viewing a screenshot of text, a recipient may click the image which could contain embedded malicious links, fake login pages, or other fraudulent content.

To avoid these scams, always compare the sender's email address to past communications. Never scan a QR code from an unsolicited message, as they can be used to disguise malicious links.