Blazon

July 2026

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

AUTO • MOTORCYCLE • BOAT • RV

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 valid on new or used auto, motorcycle, boat, and RV loans. Loans currently financed with Firefighters Credit Union are not eligible. Terms and conditions subject to change without notice. Motorcycle loan payment sample based on $20,000.00 financed at 4.75% for 60 months is estimated at $375.19 and assumes a 720 credit score on a 2026 motorcycle with loyalty and auto pay discounts. Credit approval required.

35th Annual Scholarship Golf Outing

It's not too late to sign up for this year's Golf Outing!
The 35th Annual Scholarship Golf Outing is scheduled for Monday, August 10th, at Valle Vista with a 9:00 a.m. start time.

Last year we raised $4700.00 to help students with college expenses! To join us or donate please contact Madison at 317-636-5581 ext. 252

Scholarship Applications

College Scholarship Applications are available on our 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.

Member Appreciation

Save the Date!

This year's Member Appreciation will take place on October 23rd from 8:30am to 2pm.

Stop by the credit union for refreshments and prizes!

in this ISSUE

Seize The Day Loan Promotion

35th Annual Scholarship Golf Outing

Scholarship Applications

Membership Appreciation

Passphrases

Cloud Storage Message Scams

Dangers of the Data Marketplace

How Hackers Crack Passwords

holiday CLOSINGS

Firefighters Credit Union will be closed for the following holidays:

LABOR DAY
Monday, September 7th, 2026

COLUMBUS DAY
Monday, October 12th, 2026

EQUAL HOUSING LENDER

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

Over the years people have been urged to create complex passwords comprised of letters, symbols, and special characters. These pass-words can be difficult to remember and, with the rise of AI technology, surprisingly easy for scammers to crack.

Passphrases are a safer alternative to traditional passwords. A passphrase is a string of unrelated words put together. *(An example would be: BlueRiverSunshineBus!)* Not only are passphrases easier to remember, but their length makes them difficult for automated systems to decode.

Here are some tips to create strong passphrases of your own:

- Use at least 12-16 characters
- Combine unrelated words
- Avoid common phases/words such as famous quotes or song lyrics
- Add a number, symbol, or capitalization as required by your system.

Cloud Storage Message Scams

Receiving an email or text saying you're out of cloud storage can be alarming. With our digital footprint becoming greater, people rely on cloud storage to back up their data. While many companies offer this service to their customers, how can you be sure the message isn't a scam?

Scammers send phishing emails designed to pressure you into clicking a link. Via these links scammers can steal your personal information or install malware on your device. If the message comes from a company you don't have cloud storage with, the message is probably a phishing scam. Do not click any links or interact with the sender. Delete the message.

If the message comes from a company you do use for cloud storage, proceed with caution. Do not click any links or respond to the message. Instead, contact the company directly. Reach out using a number or website you know is real. You can also log into your account from a secure location to verify the status of your cloud storage.

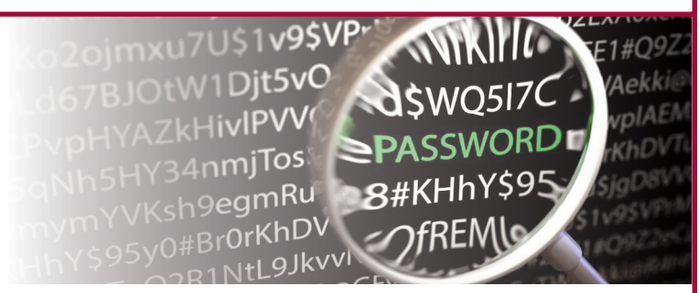
Dangers of the Data Marketplace

Data Brokers have built their industry on the collection, packaging, and sale of personal data. Most often they gather data from things such as:

- Public Records
- Social Media
- Online Purchases
- App Usage
- Loyalty Programs
- Location Date
- Website Cookies

This information allows Data Brokers to compile a profile that is specific to you and your habits. With this data they can estimate your income level, political views, health conditions, shopping habits, debt likelihood, and more. This valuable date is sold often to legitimate parties. Advertisers want to pinpoint their audience to optimize sales. Political campaigns want to expand their influence amongst their constituents. Scammers, however, want the advantage this data can give them. Once there is a data breach, this valuable information can fall into the wrong hands. To keep yourself safe, be mindful of what data you share online.

How Hackers Crack Passwords



Hackers don't need luck to guess your password. With a little help from automation, data leaks and even patterns in human behavior they can access your account. Here are some of the ways modern hackers are cracking passwords.

BRUTE FORCE ATTACKS
These attacks occur when automated tools test every possible password combination. Short passwords, and accounts with no login limits are especially vulnerable to these types of attacks. Consider using longer passwords, and Multi-Factor Authentication to protect your accounts from these sorts of attacks.

CREDENTIAL STUFFING
Data breaches are a treasure trove of stolen usernames and passwords. Hackers test these credentials across different websites and systems. Since password use is extremely common, it's easy to access other accounts after one has been compromised. To lower your risk, consider using a password manager to store and create different passwords for each of your accounts.

DICTIONARY ATTACKS
Many people use common words, predictable keyboard patterns, or familiar combinations (Password123, BusinessName1). Attackers have pre-built lists of common passwords, phrases, and more. These lists make simple passwords susceptible to dictionary attacks. When creating a password think outside the box. Using words that are unrelated or a long phase phrase can make your account less vulnerable.

PASSWORD SPRAYING
This is when attackers try one common password across many accounts. This tactic avoids account lockouts, while pinpointing users with simple passwords. Change your passwords frequently and use complex passwords to avoid falling victim.