$CAM PREVENTION

You work hard for your money. We work hard to keep your accounts and personal information secure. Learn how you can help protect your money and personal information from savvy scammers.

Bedford IN *– Somebody claiming to be from the Hoosier Hills Credit Union fraud department called Raymond. He insisted Raymond (not his real name) had been hacked. Scam, Raymond thought. He hung up immediately and called the consumer line (800.865.2612 or after hours at 800.472.3272, or the number listed on the back of his card) at Hoosier Hills Credit Union. Raymond's money was safe.*

On the same afternoon another member, Robert (not his real name), got a similar call. This member panicked, giving out credit card, social security, and debit card numbers. After about 40 minutes, he realized something was very wrong. By the time Robert hung up and called the HHCU fraud line, it was too late.

Gone in an instant: $6,500

Two different outcomes but the same high-stakes lesson: vigilance and skepticism keep cyber-thieves at bay. As crooks team up and become more sophisticated, Credit Union Members and their families need to be extremely careful.

In 2023, according to the Federal Trade Commission (FTC), Americans filed 2.6 million fraud reports and lost a record-setting $10 billion - an increase of 14% over 2022.

The FBI's Internet Crime Complaint Center logged a record-setting 880,000 complaints in 2023, costing Americans $12.5 billion.

You can protect yourself and your loved ones: be vigilant, skeptical, and take the time to reach out to us for questions or insight.

Don't Fall For It

There is a big legal difference between a fraud and scam, though both involve deception and harm. Fraud is unauthorized access to personal information without the victim's knowledge or consent.

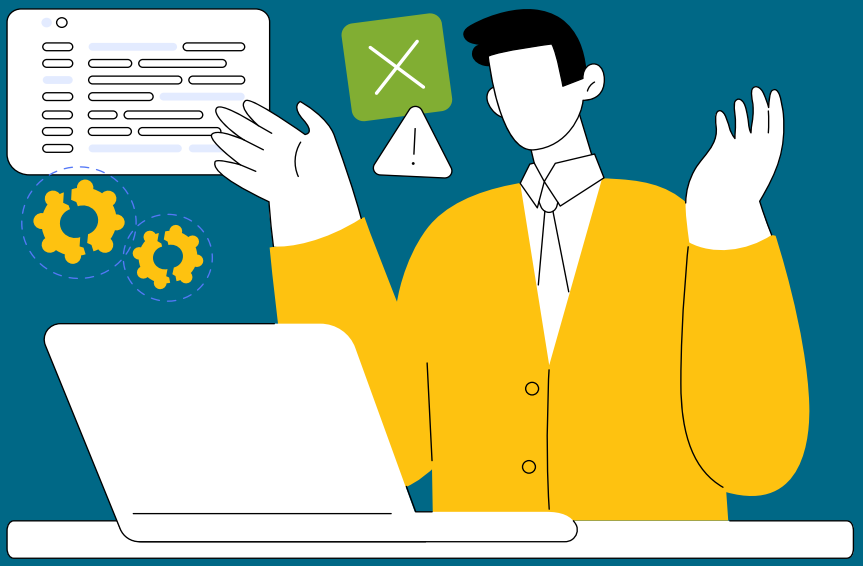
Scams manipulate victims into willingly providing information, and there is almost no chance of restitution from a scam because the information was freely given out.

HHCU informs our Members about fraud and communicates ways people can protect themselves, but ultimately, HHCU cannot absorb losses from scams when Members choose to share personal information with fraudsters.

Fraud is unauthorized access to personal information without a victim's knowledge or consent.
A **scam** is when a victim willfully provides personal information, usually under false pretenses or coercion.

Hoosier Hills CREDIT UNION

NEW SCAMS CREATED DAILY



Though the variety of scams are endless, here are some common ploys:

- **Phishing:** One of the most common social media scams. Using social media sites, messages, or emails to target individuals, "phishing" tricks victims into handing over personal information.
- **Catphishing:** Hackers pretend to be someone they're not and use fake but familiar profiles. An individual was purchasing a home and received a spoofed email from their supposed attorney instructing them to wire $426,000 to a financial institution to finalize the closing. Two days after the wire, parties realized instructions came from a spoofed email. Early notification allowed authorities to freeze the fraudulent recipient's financial bank account and return the money for a rare happy ending.
- **Phony job openings:** Get rich from working from home is the promise. But criminals harvest social security numbers or other personal information during sign-up and your money vanishes.
- **Online buy from fake stores:** You place an order with a fraudulent company fronting as an online store using your credit or debit card. Since the company is fake, you never receive the goods you ordered, and fraudsters now have your personal information to misuse.
- **Cryptocurrency deals:** Since cryptocurrency is relatively new and largely unfamiliar, unknowing investors are easily duped into risky deals that never pay off.
- **Fake vacation or apartment rentals:** Beware the fake dwelling. Study all reviews. Is the rental legit?
- **Deceptive checks/money orders:** Cashier's check scams depend on a check or money order that looks real - genuine. The scammer asks you to deposit the check then wire money back to start the company. After you make the deposit, send the money and pay a starter fee, you learn the money order was phony.

YOUR MONEY. YOUR LIFE.

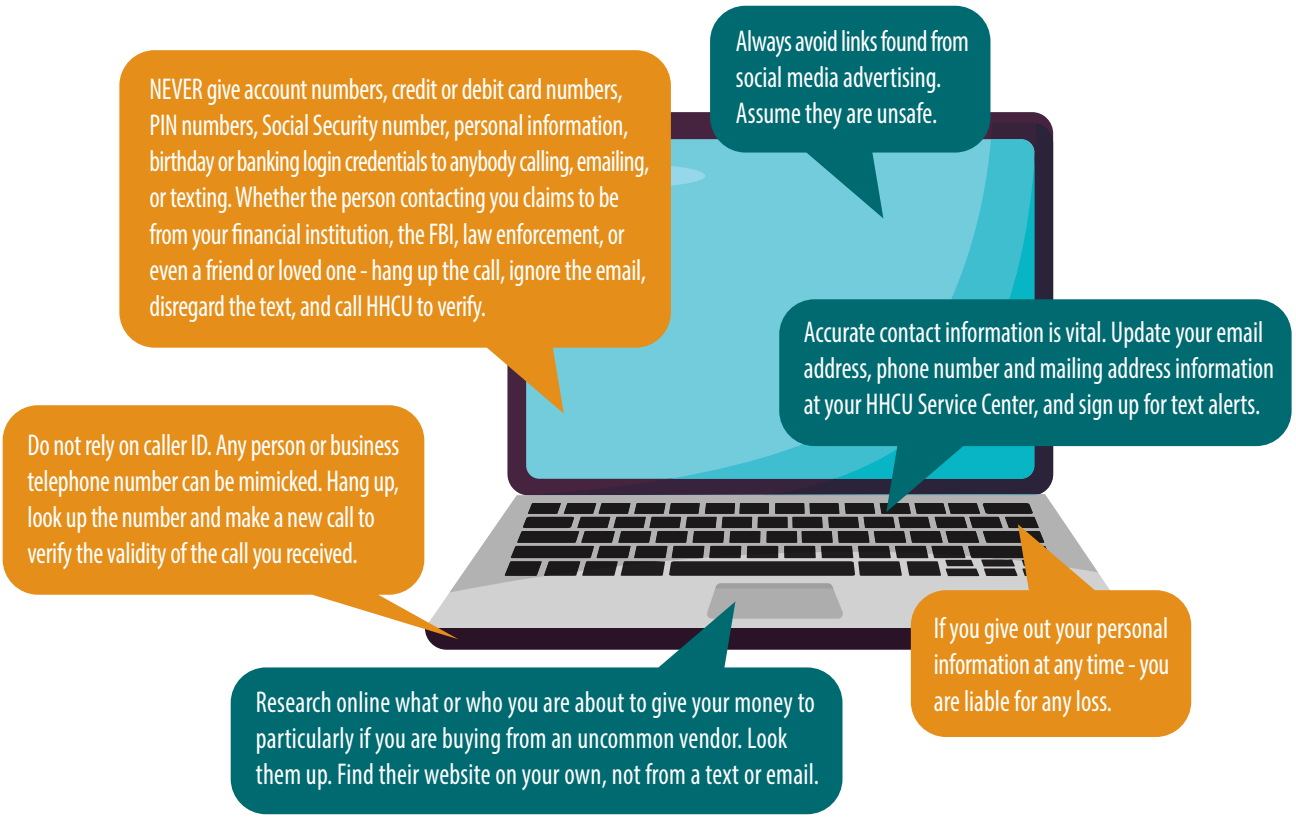
- **Romance:** Don't fall for an online friendship or romance with somebody who soon asks for money. You can't buy love. A legitimate person will never send you money to have you send to someone else…. this is called being a "mule." Don't end up holding the bag and with a broken heart, too.
- **Loan fees:** A legit institution will never ask for advance fees for a future loan.
- **Mystery shopper swindle:** You are selected as a "mystery shopper," receive a cashier's check and are told to deposit the check into your account. You are instructed to use a portion of your funds to purchase items at designated stores, transfer some to a third party using a wire service company, and then keep the rest. The cashier's check is fake and you lose money you spent and sent.
- **FBI or Phony Sheriff Marshals:** TV shows aside, marshals do not threaten large fines for missing a grand jury or petit jury summons. FBI agents do not offer to mitigate charges via a fine structure. Don't fall for it!
- **Fake credit repair:** Offers of debt relief that seem too good to be true...are too good to be true.
- **Beware fake log-ins:** Always open a new browser window for www.hoosierhills.com to access your online accounts. Do not use a link to our website or to the login portal that was sent to you via email or text as it could be from a scammer.

YOU CAN PROTECT YOURSELF

UPDATE YOUR EMAIL ADDRESS

Update your email address on file to ensure you receive fraud warnings and scam updates as quickly as possible.

800.865.2612 info@hoosierhills.com Visit your local Service Center



✓ Any financial institution fraud alert (email or text) will not have a link for you to click on. If any fraud alert email or text contains a link, DO NOT CLICK ON IT. Contact the financial institution directly.

✓ Online banking login and password information is strictly confidential; NO FINANCIAL INSTITUTION WILL ASK FOR THAT INFORMATION in an email, text or phone call! Never move your money when told you need to protect it. That's a swindle.

✓ If you get a call, piece of mail, or text stating you have won something: don't believe it. Ask questions: did you enter? If not, then how did you win? If you did enter a contest, a legitimate company will never need your banking information, nor will you ever have to pay money to get the prize.

✓ Pushy callers asking for secrecy? Be concerned! Talk to your financial institution, friend, or family member before you invest or act.

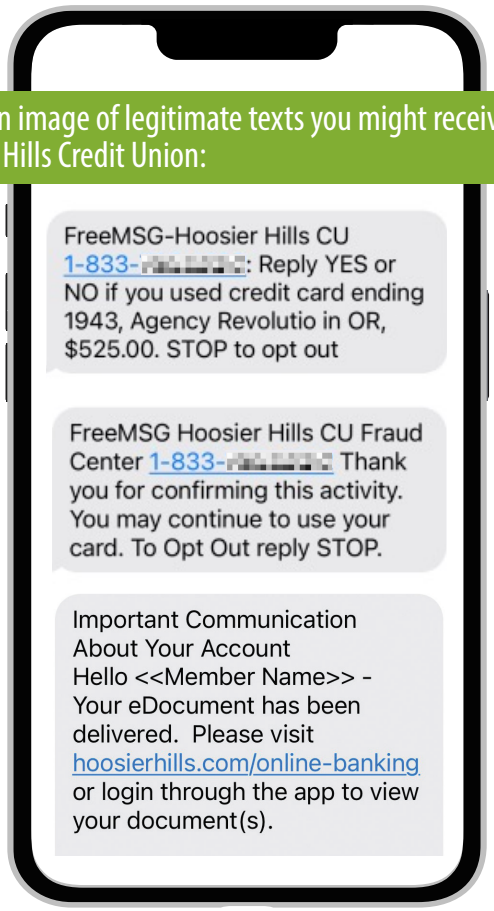
Never hesitate to reach out to **HHCU**.

We are here to help and guide.

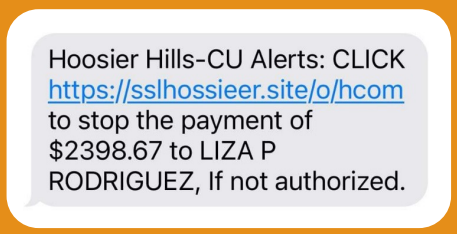
Hoosier Hills Credit Union will never call, email or text asking for you to verify any of the information listed above. Call us immediately, please, at 800.865.2612 if this happens. For a lost, compromised or stolen credit card, call 800.865.2612 during business hours or after hours at 800.472.3272

All cards are enrolled in a powerful financial monitoring system used by banks and financial institutions worldwide to detect and prevent fraud. We will reach out to you if a questionable purchase is made, but you must have text alerts established.

Here's an image of legitimate texts you might receive from Hoosier Hills Credit Union:



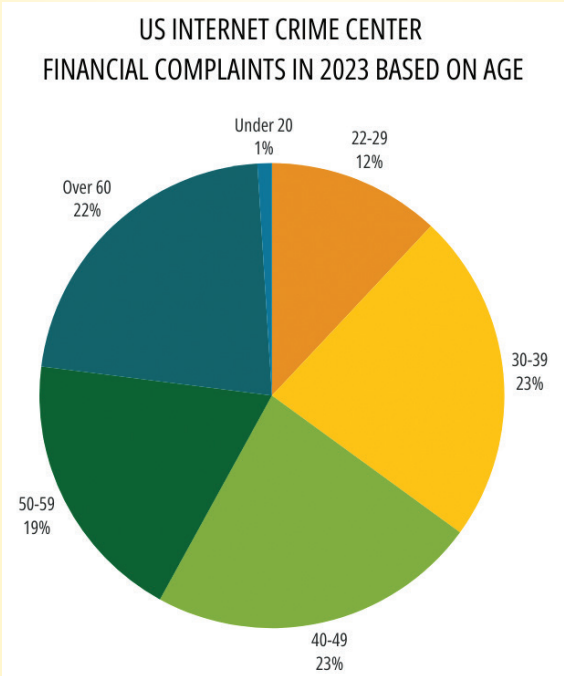
This is an image of a text that YOU WILL NOT RECEIVE!!!!! Note the fraudulent and misspelled website:



No matter your age:

YOU ARE A TARGET

The FBI registered 29,096 financial crime complaints in 2023



FRAUD WATCHDOG AGENCIES

AARP Fraud Watch Network™

FBI Common Scams and Crimes

FBI Scams and Safety

HHCU Fraud Center

FTC Report Fraud

Internet Crime Complaint Center

FOLLOW US ON SOCIAL MEDIA

@hoosierhillscreditunion

@hoosierhillscreditunion

@hoosierhillscreditunion

NCUA

EQUAL HOUSING LENDER

Hoosier Hills
CREDIT UNION

800.865.2612 | hoosierhills.com