NORTHERN INDIANA
FEDERAL CREDIT UNION

FINANCIAL SERVICES BUILT FOR HARDWORKING PEOPLE

Fighting Fraud

At NIFEDCU, we prioritize your financial well-being and are dedicated to helping you safeguard your assets. It is crucial to remain vigilant and proactive in preventing fraud. By staying informed and taking necessary precautions, you can protect yourself from potential scams. Here are three popular scams taking place in Indiana.

Phantom Hacking - Fraudsters are using technology so that their phone numbers appear on your caller ID as though they are calling from a reputable source such as a financial institution, state police, etc. By making you feel as though they are trustworthy and that you have been hacked or are in some sort of danger, they will then ask you to "verify" personal information like social security numbers, financial account information, etc. No one should be asking you for this information. It is best to deny their requests, find the actual number for the business that was calling you and call them back directly.

Phishing - Fraudsters utilize this form of scamming by sending out emails/text message that look like they are from legitimate businesses in the hopes that you will click on a link and input personal information such as account numbers and passwords. These messages can say that your password is about to expire, that a large purchase was made on one of your accounts, etc. Be on the look out for emails/texts that say you must act immediately and ones that have bad grammar/misspellings. Do not open any links or attachments. Instead, call the business and ask them if this is an actual correspondence sent by their company.

Card Skimmers - Skimming is when a fraudster places an illegal device over a gas pump card reader, ATM or any other point-of-sale (POS) terminal. When you insert your card, these devices collect your card and PIN numbers. Though they do blend in well, there are ways to spot a card skimmer. They are usually bulky where you insert your card, might have a sticky glue like substance around it or the pin pad will be slightly off center and have buttons that are hard to push. You can wiggle/pull on the card reader and if it moves at all there is probably a skimmer attached to it.

Stay vigilant by monitoring your transactions and financial statements regularly for any unusual activity.

Remember, we are here to support you every step of the way. Keep an eye out for suspicious activities and never hesitate to reach out to us for guidance and assistance. Let's work together to ensure the security of your finances.