blue
FEDERAL CREDIT UNION

NCUA

EQUAL HOUSING OPPORTUNITY

blue
FEDERAL CREDIT UNION

Fraud Facts

It's important to educate yourself

Scams, identity theft, viruses, worms, and credit card fraud are happening more frequently today than ever before. Be sure to stay vigilant to protect yourself from fraud and identity theft and always stay aware of what is happening with your account.

How to protect yourself

1. Be sure to use two-step authentication for smart devices and mobile apps.

2. Make sure you have unique and complex passwords for your most sensitive logins, including access to your account(s). Also be sure to use various passwords instead of using a duplicate password for all logins.

What if you fall for a scam?

1. Change your passwords on all important websites and phone apps.

2. Contact your financial institution immediately, and give as much detail as you can.

3. Freeze your credit at all three credit agencies. It's free and it can save you from identity theft.
   - www.experian.com
   - 1 (888) 397-3742
   - www.transunion.com
   - 1 (800) 916-8800
   - www.equifax.com
   - 1 (888) 548-7878

4. Contact your local law enforcement.

Concerned about a potential scam from your Financial institution?

- Contact your financial institution to verify that an employee actually reached out to you regarding your account.

- Never call the phone number that is provided to you through suspicious email, text message, or over the phone.

Scan Now to stay up-to-date on current fraud and scams

Scan the QR code below to see the FBI's page on commonly occurring fraud and scams.

Types of Fraud

Account Take-Over:

Occurs when a scammer obtains the victim's online credentials and accesses their online banking profile. The scammer then transfers money out of the victim's account(s) into the scammer's own account. Account take-over is one of the most common forms of fraud that financial institutions experience.

Account take-overs occur in various ways. Examples include: data breaches, compromised multi-factor authentication, and compromised information.

PayPal, Venmo, and Zelle:

These channels are known as peer-to-peer (P2P) channels, which means that individuals can send money to other individuals directly.

Scammers try gaining access to the victim's account by impersonating the victim's financial institution's fraud department. The scammers typically contact victims through a phone call, text message, and/or email.

Gift Card Scams:

It is important to remember that gift cards are a gift and not a way to exchange money. Scammers will request that the victim obtain gift cards at locations such as Walmart or Target. Scammers can be persuasive and manipulative, but also use scare tactics to pressure the victim to obtain and send the gift cards.

Romance Scams:

Scammers will target vulnerable individuals by developing a relationship through social media or online dating sites. Over time, the scammer will gain the victim's trust and begin to create stories of desperation to get the victim to send money to them. The scammer may also convince the victim that they want to meet and need funds for travel expenses.

Other Channels for Fraud:

There are many other tactics that scammers use to gain an individual's banking information. Other channels of fraud to be aware of are Craigslist, social media (Facebook, Snapchat, Instagram, Twitter), SIM card swapping, employment, and secret shopper.

IMPORTANT: Never give out your credentials to anyone, even if it is someone you trust.