People's CREDIT UNION

LOCATIONS & HOURS

Protecting You From Fraud & Scams

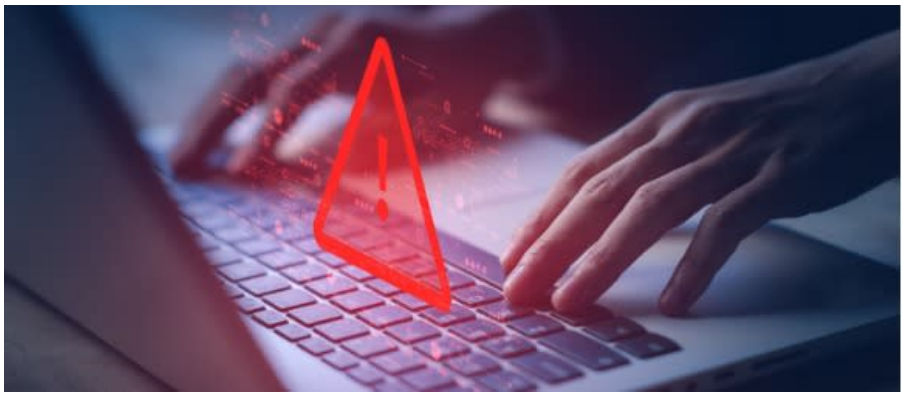
Welcome to your Fraud and Scams Prevention newsletter. With an increase in fraud and scams, we have put this together to provide information on the most recent fraud schemes, risks, and preventive strategies. We aim to increase awareness and promote good practices that can help protect our members and help you stay informed, alert, and empowered to safeguard your assets and personal information.

PCU Members: Beware of Fraudulent Letters!

There has been a recent surge of letters received by our members and those at other financial institutions that appear to be jointly sent from your credit union or bank and any number of governmental agencies or computer software companies. These letters request that you supply personal information such as account information, online banking logins, and security passkeys or even directly request funds. They often contain links to fake websites that will appear to be valid but are only set up to steal your credentials. Some links even contain malware, which installs spyware on your computer to discover allegedly nefarious content that can lead to extortion.

These letters are a scam. We will never send you a letter in conjunction with the IRS, Federal Trade Commission (FTC), Credit Reporting Bureaus, or Microsoft. Only a fraudster would extort money and ask you to throw it in the trunk of a car or give it to an Uber driver.

If you do receive a letter from People's or another one of your financial institutions that includes the logo of another company or government agency, do not hesitate to contact your nearest branch for review by our Risk Management department.



It's NOT All Relative

Watch out for scammers pretending to be family.

If you get a call or letter from someone saying they're a family member or close friend who needs you to send money right away via courier because they're hurt or incarcerated, it is a scam.

They may say it's urgent and that you're the only one who can help. They may know your name, where you live, and other information they could have found on social media sites. They may tell you it's important to keep it secret from other family members and friends. They will always say you have to pay right away.

Don't do it!

Never give a stranger your address or personal information, and do not provide them with cash via courier. No bail bondsman, hospital, or attorney will ever request that you withdraw currency from your PCU account and send the cash by Uber OR through a driver in an unmarked car that comes to your house. If you are instructed to do this and for your personal safety call the police immediately!

Earning Your Trust… Every Day

More and more of our older members are being targeted by scammers who are warning them not to trust their financial institutions or the people that work there. These fraudsters falsely advise our senior friends that “The bank or credit union is embezzling” or are “under investigation and can’t be trusted.” In some cases, they’re even instructing members to lie to tellers.

The goal of these scammers is to destroy your confidence in your financial institution and send them your hard-earned money instead. They are directing members to withdraw all of their funds in currency from the Credit Union and deposit the money into a fraudulent Bitcoin ATM, but once the funds are in that ATM, they’re gone and unrecoverable!

Their mission is to steal your money. Our mission is to serve your best interests and protect your assets. Be assured -- your money is safe with us. We adhere to strict regulatory requirements imposed for your protection by the National Credit Union Administration as well as a number of state and federal agencies. We are also regularly audited by the RI Department of Business Regulation. Internally, People's maintains a robust audit program, including monitoring employee activity.

Spot and Prevent Elder Financial Abuse

Each year, millions of senior citizens are victimized by financial fraud or theft of money, property, or valuable personal information. Often, an adult child or other relative is responsible. Other situations may involve trusted individuals such as caregivers, legal guardians, investment advisors, or new “friends.”

Since the types of abuse may differ widely, it is important to take a variety of precautions.

- Be careful with powers of attorney. A power of attorney can be easily misused because it allows the appointed person to step into your shoes and do everything you can do.
- NEVER give out your bank account numbers, Social Security numbers, personal identification numbers (PINs), passwords, or other sensitive information unless you initiate the contact.
- Keep your checkbook, account statements, and other sensitive information in a safe place. Shred paper documents containing sensitive information that is no longer needed.
- Closely monitor your credit card and bank account statements for unauthorized or suspicious transactions.
- Review your credit report through credit agencies like Equifax, Experian, and TransUnion.
- Be aware of scams involving reverse mortgages. They can be complex products with a variety of risks and costs.
- Do not comply with requests from strangers to deposit a check into your account

and wire some or all of it back.

Finally, and sadly, grandparent scams are on the rise. If you use social media, many security experts advise against posting the names, addresses, birthdates, and daily activities of relatives because a thief looking for personal information can use that information to call or email an elderly person and pretend to be a relative in distress—such as a grandchild being injured, in jail, or lost in a foreign country—and needing money sent fast.

Financial fraud is on the rise. Knowing how to spot and prevent it will help you protect yourself and your finances.

Be on the Lookout for Fake Card Readers!

Overall, credit and debit cards equipped with security tools and features are very safe to use. But when you're using the card reader at an ATM, gas pump, or local grocery, convenience, and department stores, watch out for illegally installed credit card skimmers. When you swipe your credit or debit cards, these fraudulent devices scan or skim your information and, with the help of Bluetooth devices, send your stolen information to the thief's computer or phone.

According to the FBI, these devices are costing financial institutions and consumers more than $1 billion each year. These skimmers aren't always easy to spot, but there are a few signs that a skimmer has been installed:

- Does the card reader look intact? Is there any piece of the machine that's out of alignment or looks to be covering another part?
- Does the machine feel like it's coming apart in some places or isn't properly installed?
- Is the pump panel open, or is the security seal near the card reader broken?
- Does the card slot and keypad on your reader look different than others around you?

While credit cards and debit cards are typically both safe options, credit cards may have slightly more protection than debit cards if fraud were to occur. Debit cards, you must report fraudulent activity within 60 days of your statement date to avoid liability for your loss.

As always, checking your card transactions regularly and setting up account alerts can help you spot fraudulent transactions.

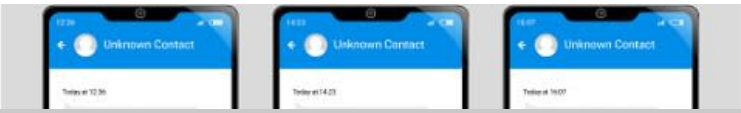
The Latest in Identify Theft – Account Takeover

Account takeover fraud (ATO) is a form of identity theft that occurs when a cybercriminal gains access to your login credentials to steal funds or information. ATO is a top threat to financial institutions and their customers and members.

These cyber thieves often try to change your account information, password, and even notifications so you won't know they've compromised your account. They will often steal money from a bank account by making a payment to a fraudulent company or by transferring funds to another account. They are also now able to make a request for a new credit card, new account, or another financial product. In addition to these types of actions, they have the power to carry out any number of unauthorized transactions that cause financial harm.

There are some signs of account takeover fraud. If multiple users suddenly request a password change or if there is an accumulation of unsuccessful login attempts, these could be indicators of account takeover fraud. You are alerted via email or SMS text message when a password change is requested.

To reduce your risk of account takeover fraud, be meticulous with passwords, use multifactor authentication, safeguard your credit, and consider identity theft protection.



Contact us:

Email: memberservice@peoplescu.com

Phone: 800.498.8930

Follow Us:

** By clicking the above social networking links, you will be re-directed to a Web site not directly controlled by People's Credit Union. We do not endorse or guarantee the products, information or recommendations provided by the linked Web site, and we are not liable for any products, services, or content advertised on those linked Web sites.

When You Encounter a Scammer (and You Will!)

It's important to be aware of scammers and know how to protect yourself. If you receive a call or email or visit a website that seems suspicious, the best thing to do is to ignore it. Refrain from providing any personal information or sending any money until you have confirmed that the source is legitimate. If a scammer has already contacted you, you can report them to the Federal Trade Commission to help prevent them from contacting you or others in the future.

If you have sent money to a potential scammer, acting as soon as possible is essential. Contact your bank or credit union and inform them of the situation. Cancel your card or account if necessary. If the scammer can access sensitive information, such as your social security number, you can find helpful guidance on the FTC website.

Scammers are continually developing new ways to steal information and money. Visit the FTC website to stay informed about the latest scams and learn more about how to stay safe.

To learn more about ways to protect yourself from ongoing fraud and scams, click here.

Thank you for being a valued member of People's Credit Union.

Sean Daly
Head of People's Credit Union