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.

Extended Fund Holds Protect Our Elder Members

In 2023, scams targeting Rhode Island residents aged 60 and over continue to rise. The most common financial scams targeting older people include government impersonation, sweepstakes, and robocall scams. These crimes can be devastating, often leaving victims with no way to recoup their losses. So remember, do not send funds to anyone you recently met on the Internet.

To better serve our members and maintain their financial safety, as permissible by law, People's Credit Union may place an extended hold on any transactions where we suspect elder financial exploitation. In accordance with RI General Law, we have 14 days from the date of detection to hold the funds and release them on the 15th day if no fraud is detected.

Fraudsters and con artists go after older adults because they believe this population has plenty of money in the bank. But it's not just wealthy older Americans who are targeted; older adults with low income are also at risk for fraud.

Financial scams often go unreported or can be tough to prosecute, so they're viewed as a "low-risk" crime. If you believe you're a victim of fraud, contact your local police, and then, if money has been taken from your accounts, call our Member Service Center at 800.498.8930. Sharing your experience can help prevent it from happening to another older adult.

You Don't Need to be Online to Get Scammed!

Being on high alert for online fraudsters is crucial, but you also need to be on your toes outdoors as well. In smash-and-grab scenarios, scammers often target municipal recreation areas such as tennis courts, playgrounds, and hiking paths. Activities that prompt people to lock their purses, wallets, or checkbooks in their vehicle for safekeeping are higher risk because the thief will smash your car window, steal what's inside, and then speed away within seconds.

A woman in Texas was targeted when she dropped her toddler off at school. She returned to her car and noticed that her front passenger window was shattered and her purse was stolen. The thief went right to a drive-through lane of a local bank to cash a fraudulent check. These individuals will keep hitting banks with the stolen information until finally, someone recognizes them as a fraud and asks them to come inside to verify their account information.

To avoid becoming a victim, NEVER leave personal identification, debit cards, or credit cards locked in a car in a public parking lot. If you are victimized by a thief, immediately call the police. As soon as possible, contact our Member Service Center at 800.498.8930. We will assist you with confirming that your account has not been accessed and will take steps to protect your identity by updating any potentially compromised banking information. You should also contact your other financial institutions and credit card companies so they

can put an alert on your accounts.

New Scams Are Turning Up Every Day

As quickly as local and federal law enforcement and financial institutions identify a new scam and alert the public on how to defend against it, fraudsters seem to devise new ways to steal your personal information and your money. Here are just a few to be aware of:

Gift Card Scams:

Con artists have latched onto gift cards as an easy scam. A criminal talks their target into believing they need to make an urgent payment to solve a problem like an imminent utility shutoff, an issue with a Social Security account, or a grandchild who needs bail. The criminal then directs the victim to purchase a gift card, load a specific amount of money on the card, and then share the information on the back. From there, they can access and drain the funds.

If someone you met online requests you purchase a gift card and then send them the activation code and number, please contact our Member Service Center at 800.498.8930 before purchasing the gift cards. They will put you in touch with our Risk Department.

Student Loan Scams:

Payments are starting back up for federal student loans that were paused during the Pandemic, and scammers have jumped into action. If you get an unscheduled call, text, e-mail, or message on social media about your federal student loan, keep the following in mind:

- Never pay an upfront fee to reduce or eliminate your student loan debt.
- Never give out your Federal Student Aid ID, Social Security number, or other personal information to anyone contacting you.
- Don't sign up for quick loan forgiveness. Scammers might say they can get rid of your loans, but they can't.

The Biden administration's plan to forgive student loans has faced some roadblocks on the way to approval, but that hasn't stopped scammers from trying to take advantage of people who may not have heard it's on hold. They've built phony application sites aimed at stealing applicants' Social Security numbers and bank information, and sometimes, they contact targets by phone, pressuring them into applying and charging a fee for their help.

If a scammer contacts you, report it at ReportFraud.ftc.gov. and keep up to date on the status of the student loan forgiveness program at the Department of Education's student aid website.

Tech Support Scams:

Criminals posing as online tech support to save people from fake computer viruses isn't anything new. But these scams have spiked in recent years as scammers continue developing new tactics.

These criminals gain access to your computer by inserting fake virus pop-up warnings. When you contact the "hotline" to fix the virus, these scammers request remote access to your computer, allowing them to steal your personal information and bank account login credentials. They also utilize text messages, emails, or robocalls to tell their targets that their security software has expired or even claim that child pornography has been implanted on their computer, all the while asking for hefty fees to fix the "problem."

If scammers have invaded your computer, you may want to hire a trusted professional to address the problem. When in doubt, shut your device down or unplug from your internet connection. You may lose data and documents, but it's a small price to pay.

It's extremely important to report these crimes. If you spot or have been the victim of a scam, report it to your local police and the FTC at reportfraud.ftc.gov and the Federal Bureau of Investigation's Internet Crime Complaint Center at IC3.gov.

Outsmart Fraudsters with These 5 Tips

1. Know who you're dealing with.

If you've never done business with someone before, check their credibility with your state or local consumer protection agency and the Better Business Bureau (BBB) before conducting any transactions with them. Always call the number listed on the entity's website to ensure the phone number they gave you is legitimate.

2. Use credit cards for online purchases.

Credit cards are the safest way to pay for online purchases because you can dispute the charges if you have yet to receive the goods or services promised or the offer was misrepresented.

3. Guard your personal information.

Only provide your credit card or bank account number over the phone if you are paying for something, and you know to whom you are sending payment. Your social security number should only be necessary if you are applying for credit. Fraudsters often pretend to be from a familiar company trying to verify your personal information, so be especially suspicious if someone asks for information that you know a business already has on file.

4. Stay safe online.

Don't send sensitive information, such as credit card numbers, by email because it's not secure. If you are asked to provide your financial or other sensitive information, the letters at the beginning of the address bar at the top of the screen should change from "http" to "https" or "shttp." Your browser may also show that the information is being encrypted or scrambled so no one who might intercept it can read it.

5. Be cautious about unsolicited emails.

Unsolicited emails are often fraudulent. If you are familiar with the company or charity that sent you the email and don't want to receive further messages, reply asking to be removed from the email list. However, responding to unknown senders may verify that yours is a working email address, resulting in even more unwanted messages from strangers. The best approach is to delete the email.

Contact us:

Email: memberservice@peoplescu.com

Phone: 800.498.8930

Follow Us:

added protection.

- **Sign up for account alerts.**
  - Inside your Online and Mobile Banking, you can add card alerts and controls to help keep your account secure.
- **Secure your devices and networks.** Do not use public wifi, use VPNs, and install a screen lock and password on your smartphone and computer.
- **Protect your credit.** Check it often using our free credit reporting and score platform via SavvyMoney.

Guard Your Login Credentials

If cybercriminals steal your login credentials, they can access your accounts and find your personal or professional information.

Avoid Oversharing on Social Media