

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.

Neighbors or Scammers?

Who is Really On Your Neighborhood App?



With the growing popularity of “neighborhood watch” apps, such as Nextdoor, Neighbors by Ring, and Front Porch Forum, scammers use these apps to take advantage of you and your trust in your neighbors. These scammers tend to target people that are more likely to trust their neighbors and respect the business recommendations that are posted on these apps without doing a thorough background check on who they’re hiring.

How Does It Work?

For example, scammers use the Nextdoor and Neighbors by Ring apps to pose as fraudulent contractors to charge people money before performing their tasks. However, instead of doing the job they were paid to do, they avoid all further contact with the customer. Alternatively, some scammers will complete the job even though they are not qualified after claiming they are. This forces families to spend more money on the new damages caused to their property by the “business” they hired.

How To Avoid These Scammers?

While this can be alarming and unsettling, there are still ways to protect yourself and your information on these Neighbor Apps. To help you stay safe, here are some tips:

Check with the Better Business Bureau. If you are skeptical about a business being suggested or if the deal sounds too good to be true, verify that the business is real with the Better Business Bureau.

Have a face-to-face conversation with your neighbors. Having a face-to-face conversation with your neighbors eliminates the risk of coming in contact with a scammer pretending to be a client of the business in question. Going straight to the source is better than falling victim to a scam.

Do not overshare. Oversharing can allow scammers to know what types of services you need. They may use that information to trick you into giving them your personal information or money.

Never give out sensitive information over the phone, online, in email, or on an app. Only share your personal data once you know the person you speak with is legitimate. They should be able to prove that they are qualified to provide the services discussed.

Know When It's Time to Hang Up. Don't Fall Victim to These New Phone Scams.



Recently, it was discovered that new phone scams are making the rounds. These scams play on our fears (a scammer favorite), are tough to spot, and are after your money. Knowing how they work and when it's time to hang up is always wise. Looking at these scams can help save you and those you know from falling victim to them. The following statistics help show the financial severity of phone scams and who's more likely to fall for them.

Jury Duty

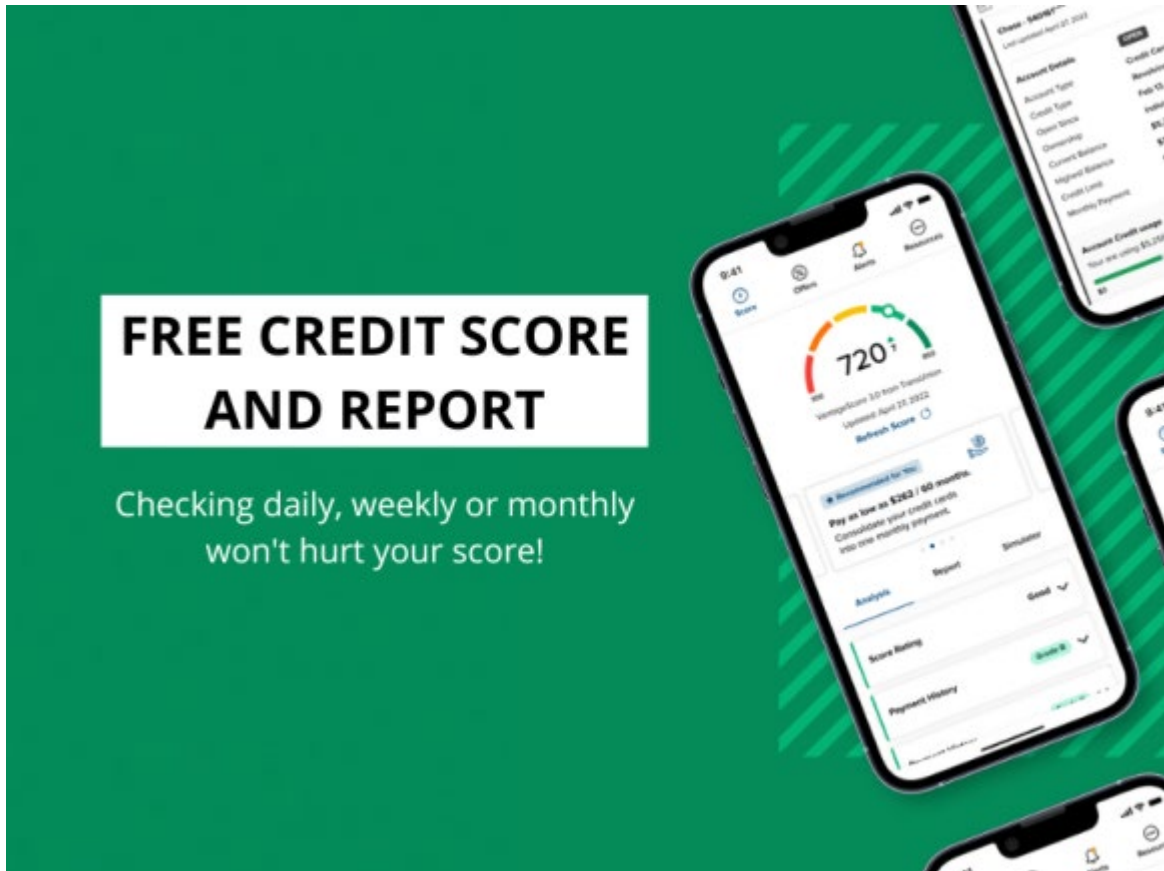
This phone scammer tells the potential victim that they've missed their designated jury duty and there's a fine to pay for that. The victims believed the call was legitimate and followed the scammer's instructions on paying their fine using gift cards. Paying with gift cards is one of the most common signs that the phone call is a scam—time to hang up.

Caller ID Reads "Police Department"

Seeing this message on your phone is enough to worry most scam targets that something could be wrong, and that's exactly what scammers count on to pull you in. However, the phone number left on the voicemail differs from the caller ID left on the phone.

When victims call back, they're told the police have a warrant for them. From there, they're likely told the warrant needs paying, and the victim's financial information is needed. It's not only time to hang up but also to call the actual number for the police and find out if there's any truth to the phone call. This also makes police aware that this scam is going on.

Did you know 1 out of 3 credit reports have errors?



**FREE CREDIT SCORE
AND REPORT**

Checking daily, weekly or monthly
won't hurt your score!

Over one-third of consumers have found at least one error on their credit report.

Mistakes in your credit report can impact your score and your lending power. Some of the common errors found on credit reports are:

- Personal Information Errors.
- Errors such as wrong name or address.
- Account Errors.
- Credit accounts that consumers did not recognize as being theirs.

To provide our members with benefits that enhance their security and financial education we partnered with a free credit score solution myCreditHealth with SavvyMoney, you can review

and download your free credit report for errors and dispute any errors you might see right within the tool. You can check your credit score daily without any impact to your score, receive real-time credit monitoring alerts and learn about the factors that make up your credit score.

Enroll now in [Online](#) or [Mobile](#) Banking and check your credit report today!

Tips to Protect your Personal Information

Let's look at ways that you can protect your personal information.

- **Always verify.** If you're contacted by an institution (bank, broker, government entity), hang up the phone and call that institution directly.
- **Use two-factor authentication.** It may take a little longer, but it's worth it for the 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

Social media can be used to update friends and family about your life, but cybercriminals can also use your accounts as an easy source of information.

Know the Information on Your Credit Report

As part of our Online and Mobile Banking, we offer myCredit Health with free access to our partner SavvyMoney to monitor your credit score and report as often as you would like.

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
President & CEO

Contact us:

Email: memberservice@peoplescu.com

Phone: [800.498.8930](tel: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.