



### Be vigilant.

If something seems too good to be true, it is. If you aren't sure what you are looking at is real, show it to a trusted friend or family member, or bring it to the credit union so we can advise you.

Don't be afraid to ask for help! It is better to be overly cautious than to lose your hard-earned money to a scam.

When talking to strangers, be wary. People may seem trustworthy, but if things are getting too serious too fast, that is a red flag. Don't give your personal info out to people you don't know, especially online.

## Watch out for these scams:

### Think before you click.

Email About a Strange Refund or Purchase

- It's a scam! They might try to get you to visit a fake website or take over your device to prove the transaction is real. Then, they'll ask you to buy gift cards and send them the codes to make things right. Once that is sent, you are out all of that money.

"Just Pay Shipping" for a Prize

- This is also a scam. It may be a small charge at first, but scammers will use your card info to make unauthorized transactions—sometimes hundreds or even thousands of dollars.

### Protect yourself over the phone.

Calls Pretending to Be From PSCU

- Scam alert! We will never call and ask for your account number or full credit/debit card information.
- If you're ever unsure, hang up and call us directly at 260-432-3433.

Urgent Requests or Legal Threats

- Don't panic. Scammers use fear to pressure you into giving up personal information. Always verify first—don't share anything on the spot.

Beware of Text Message Scams

- Get a text saying that you owe unpaid tolls or have a package that couldn't be delivered? Do not click any link! These messages often lead to fake websites that steal your payment information or install malware.

## FRAUD & SCAMS



## YOUR GUIDE TO STAYING SAFE ONLINE



**PUBLIC SERVICE**  
CREDIT UNION

[www.mypscu.com](http://www.mypscu.com)

260.432.3433 888.432.3433

# WHAT DO I DO?

Getting scammed can be overwhelming, especially when you don't know what your next steps are. This guide below will walk you through what we recommend you do to protect yourself and your personal information. Follow the steps below depending on what kind of information was compromised.



## Credit/Debit Card Number

If you gave out your card number to someone that seems suspicious, or you see a transaction on your account that you know was not done by you, follow these steps:

- Lock your card immediately by logging into your mypscu mobile app. Go to the More Menu and click Manage My Cards.
- Review each account's transaction history for any additional suspicious activity.
- Request a new card by completing a Debit Card Request Form in online or mobile banking or calling 260-432-3433.
- File a dispute for any charges that are fraudulent by completing a Cardholder Dispute form online or by calling 260-432-3433.

## Member/Account Number

If a scammer gained access to your online banking, took control of a device, or if you gave your account number to someone suspicious, follow these steps:

- Call the credit union immediately at 260-432-3433 to request a freeze on your account and get a new account open for you.
- If your device was hacked or compromised, it may need a factory reset. This will remove all of the data including the scammer's access to your device. You can complete this yourself or take it to your service provider or Best Buy's Geek Squad.
- Be sure to update your new account number with your employer, Social Security, and any services that bill you—like utilities or insurance.

## Social Security Number

If your Social Security number was leaked or you provided it to someone suspicious, follow these steps:

- Freeze your credit. This can be done on their websites or via phone. You will want to freeze your credit with all three bureaus.
  - Experian(888-397-3742)
  - Equifax (888-298-0045)
  - TransUnion (800-916-8800)
- Contact the credit union so that we can note your account to not use your social security number as a means of verifying your identity.
- Report the fraud at [identitytheft.gov](https://www.identitytheft.gov).
- Sign up for an account at [ssa.gov](https://ssa.gov) so that you can monitor activity associated with your social security number.