

Don't Fall Victim to Fraud.

Here are more safety tips to help you become more aware and better protected against fraud and identity theft.

1. At home, keep personal information safe, especially if you have roommates or are having any work done in your home. Don't keep Personal Identification Numbers (PINs) near your checkbook, ATM card, or debit card.
2. Shred any papers with confidential information before you throw them out - even the junk mail. Anything with an account number can be used in identity theft. This includes prescreened credit card offers, receipts, canceled checks, credit union statements, expired charge cards, doctors' bills, and insurance documents.
3. Don't give out any confidential information - such as your credit card number, social security number, or PIN number unless you initiated the contact with a business. Be careful of unexpected emails that look as if they are from a legitimate company seeking you to enter some information at a linked website; sometimes phony websites can look real.
4. Check your credit union and credit card statements regularly to make sure there is no unexplained activity.
5. Consider canceling credit cards you haven't used in a long time.
6. Keep track of when your bills usually arrive. If a bill does not arrive on time, call the company to make sure no changes have been made to your account. Often, identity thieves will change the address of a bill so that it will take you longer to figure out the scam.
7. Carefully check your credit reports regularly. Your credit reports are important tools for limiting the amount of damage a thief can cause.
8. When choosing a Personal Identification Number (PIN) for your ATM or for other purposes, use one that is hard to guess. Avoid the last four digits of your social security number, your mother's maiden name, birth dates, names of pets, or even the name of your hometown baseball team. Try to mix numbers, letters, and symbols.
9. Make it harder for thieves to use your account. NEVER write your passwords on credit card, credit union, and phone accounts. GPCE Credit Union offers members many security features such as Falcon on your MasterCard credit card, Enhanced Internet Account Authentication, and ALERTME: online credit monitoring service. These services help to protect your financial accounts from fraud.
10. Use only secure sites when making online purchases. Secure pages begin with "https:".
11. Don't print your social security number or drivers license number on your checks.



Tips continued.

12. Be suspicious of any email or phone calls with urgent request for personal financial information. Never give out financial information such as checking and credit card numbers, or your Social Security number, unless you know the person or organization you are dealing with, even someone claiming to be from your credit union. Your financial institution will **NEVER** call and ask for this type of information.
 13. Notify your credit union of suspicious phone inquiries such as those asking for account information to “verify a statement” or “award a prize”.
 14. Don’t use the links in an email to get to any web page and do not reply to the email.
 15. Report lost or stolen checks **IMMEDIATELY**. Always review new deliveries of checks to make sure none were stolen in transit.
 16. Closely guard your Personal Identification Number for your credit and debit cards and online banking access. Check your monthly statements to verify all transactions.
 17. Notify your credit union, bank, or credit card issuer **IMMEDIATELY** if you discover any erroneous or suspicious transactions on your statements.
-

For information on the latest identity theft scams and more information on identity theft, check out these websites:

<http://ftc.gov/>

<http://www.ic3.gov/>

<http://www.consumer.gov/idtheft/>

<http://www.fraudtech.bizland.com/>

http://www.nabihq.org/en-us/cons_and_scams

<http://www.snopes.com/snopes.asp>

