KELLOGG COMMUNITY credit union

Kellogg Community Credit Union (KCCU) knows that keeping your personal information secure is an important responsibility. To assist you in keeping your information safe, we wanted to share these tips from the National Commission on Aging.

Tips on Avoiding Scams

1. Be aware that you are at risk from strangers—and even from persons closest to you.
2. Always tell salespeople that come to your door or call you on the phone: "I never buy from (or give to) anyone who calls or visits me unannounced. Please send me your information in writing."
3. Shred all receipts with your credit card number.
4. Sign up for the "Do Not Call" list (*donotcall.gov*) to prevent telemarketers from calling and take yourself off multiple mailing lists. If you do not have internet access you can also call 1-888-382-1222.
5. Use direct deposit for benefit checks to prevent checks from being stolen from the mailbox. The KCCU team would be happy to assist in setting up your direct deposit, simply call 800.854.5421.
6. Never give your credit card, banking, Social Security, Medicare, or personal information over the phone unless you initiated the call.
7. Be skeptical of all unrequested offers and thoroughly do your research if you are seeking any type of services. Also be sure to get references when possible.

Tips for Protecting Your Identity

1. Monitor your bank and credit card statements. Check your accounts regularly, so you can catch any purchases made on your credit or debit card by persons other than yourself. The same goes for cash withdrawals.
2. Understand what internet scams are and do not respond to any attempts. Do not click on the links in emails.
3. Beware of telephone scams. Never give out personal information over the phone to someone who claims to represent your bank, credit card company, or other organization. People are not always who they claim to be. If in doubt hang up and call the company back at their main phone number.
4. Be careful with your mail. Sometimes identity thieves will steal your mail right out of your mailbox in order to obtain your personal information. To reduce this threat, try not to let incoming mail sit in your mailbox for a long time. If you're going to be away for extended periods of time, have the post office hold your mail for you. When sending out sensitive mail, consider dropping it off at a secure collection box or at the post office.
5. Be careful when using account information in public. Whether punching in your PIN number at an ATM or filling out forms with personal information on it, be sure to cover the keypad or complete paperwork in a private setting. Also, don't give out credit card information over the phone while you are in a public place.
6. If you suspect that you have been a victim of identity theft:
    - Contact your bank(s) and credit card companies immediately.
    - File a report with the police. The police may not be able to do very much themselves, but companies you work with to clear up identity theft issues may want to see a copy of this report.
    - Put out a fraud alert to the credit-reporting agencies:
        - Experian: 1-888-397-3742 (TDD 1-800-972-0322)
        - Equifax: 1-888-766-0008 (TDD 1-800-255-0056 and request connection to Auto Disclosure Line at 1-800-685-1111)
        - Transunion: 1-800-680-7289 (TDD 1-877-553-7803)

KELLOGG COMMUNITY credit union

Tips on Avoiding Telemarketing Fraud

It's very difficult to get your money back if you've been cheated over the telephone. Before you buy anything by telephone, remember:

1. Don't buy from an unfamiliar company. Reasonable businesses understand that you want more information about their company and are happy to comply.
2. Always ask for and wait until you receive written material about any offer or charity. If you get brochures about costly investments, ask someone whose financial advice you trust to review them. But beware—not everything written down is true.
3. Always check out unfamiliar companies. Check them with your local consumer protection agency, Better Business Bureau, state attorney general, National Fraud Information Center, or other watchdog group. Unfortunately, not all bad businesses can be identified through these organizations.
4. Obtain a salesperson's detailed information. Ask for their name, business identity, telephone number, street address, mailing address, and business license number before you transact business. Some con artists give out false names, telephone numbers, addresses, and business license numbers. Verify the accuracy of these items.
5. Find out where your money will go. Before you give money to a charity or make an investment, find out what portion of the money is paid in commissions and what portion will actually go to the charity or investment.
6. Look for a guarantee. Before you send money, ask yourself a simple question: "What guarantee do I really have that this salesperson will use my money in the manner we agreed upon?"
7. Don't pay in advance for services. Pay services only after they are delivered.
8. Be cautious of companies that want to send a messenger to your home. Some fraudulent companies want to send someone to pick up money, claiming it is part of their service to you. In reality, they are taking your money without leaving any trace of who they are or where they can be reached.
9. Always take your time making a decision. Reasonable companies won't pressure you to make a snap decision.
10. Don't pay for a "free prize." If a caller tells you the payment is for taxes, he or she is violating federal law.
11. Know your limits. Before you receive your next sales pitch, decide what your limits are—the kinds of financial information you will and won't give out on the telephone.
12. Wait, think, and discuss before you decide. Be sure to talk over big investments offered by telephone salespeople with a trusted friend, family member, or financial advisor. It's never rude to wait and think about an offer.
13. If you don't understand, don't respond. Never respond to an offer you don't understand thoroughly.
14. Never send money or give out personal information such as credit card numbers and expiration dates, bank account numbers, dates of birth, or Social Security numbers to unfamiliar companies or unknown persons.
15. Realize that your personal information is often brokered to telemarketers through third parties.
16. Be cautious of help with losses. If you've been victimized once, be wary of persons who call offering to help you recover your losses for a fee paid in advance.
17. Always report fraud. If you have information about a fraud, report it immediately to state, local, or federal law enforcement agencies.

For more information on how to help protect your KCCU accounts from fraud, visit kelloggccu.org, click on the Tools and Resources tab, then Member Security.