Community Alliance Credit Union Online Banking Security Tips

What Members Need to Know

As internet usage has continued to increase, so has internet fraud. Criminals have continued to develop and deploy more sophisticated, effective, and malicious methods to compromise member authentication and gain unauthorized access to members' online accounts. As a result, the need to protect your identity online has become increasingly important. At CACU, the security of member information is a priority. We are strongly committed to the safety and confidentiality of your records. One of the best ways to avoid fraud is to become an educated consumer and we would like to help you in this endeavor.
Please take a moment to read this important information on how to keep you safe when conducting business online.

Rights and Responsibilities

With respect to online banking and electronic fund transfers, the Federal government has put in place rights and responsibilities for both you and the credit union. These rights and responsibilities are described in the Account Opening Disclosures you received when you opened your account with us. Ultimately, if you notice suspicious account activity or experience security-related events, please contact the credit union immediately at 734.464.8079.

Requesting Member Credentials

CACU will never contact you and request your personal information such as user ID, etc.

Protecting Yourself Online

Here are some great tips from ***OnGuardOnline.gov***, a website managed by the Federal Trade Commission, in partnership with several other federal agencies to help keep you safe online.

- **Use Security Software That Updates Automatically -** Criminals constantly develop new ways to attack your computer, so your security software must be up to date to protect against the latest threats. Most security software can update automatically; set yours to do so.
- **Treat Your Personal Information Like Cash -** Don't hand it out to just anyone. Your Social Security number, credit card numbers, and bank and utility account numbers can be used to steal your money or open new accounts in your name. **Every time** you are asked for your personal information – whether in a web form, an email, a text, or a phone message– think about whether you really can trust the request.
- **Give Personal Information Over Encrypted Websites Only -** If you are shopping or banking online, stick to sites that use encryption to protect your information as it travels from your computer to their server. To determine if a website is encrypted, look for **https** at the beginning of the web address (the "s" is for secure).
- **Be Careful Using Public Access Computers-** There are risks in using a publicly accessible computers (e.g., at hotels, libraries, etc.) to access your accounts. Computers

accessible to the public may be infected with viruses and/or malicious software, such as Trojans and key loggers.

- **Protect Your Passwords -** Here are a few principles for creating strong passwords and keeping them safe:
  - o The longer the password, the tougher it is to crack. Use at least 10 characters; 12 are ideal for most home users.
  - o Mix letters, numbers, and special characters. Try to be unpredictable – don't use your name, birth date, or common words.
  - o Use phrases with a combination of characters instead of easy to guess words
    - Example "Pass Go and collect $200"– p@$$GOandCLCt$200
  - o Don't use the same password for many accounts. If it's stolen from you – or from one of the companies with which you do business – it can be used to take over all your accounts.
  - o Don't share passwords on the phone, in texts or by email. Legitimate companies will not send you messages asking for your password. If you get such a message, it's probably a scam.
  - o Keep your passwords in a secure place, out of plain sight.

Who to Contact
If you notice suspicious activity on your credit union account or feel your personal information has been compromised in some way, please contact CACU at 734.464.8079 for assistance.