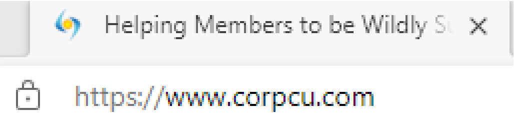
How to Protect Yourself and Your Credit Union from Fraud

Verify you are on a vendor/partner's correct webpage.

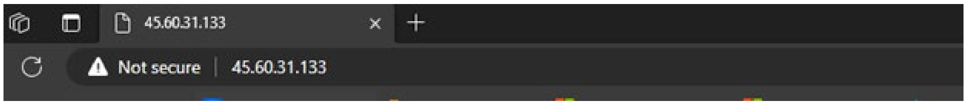
- The correct company logo is present.
- The correct URL (e.g. https://www.corpcu.com) is present.
    - Be vigilant in checking for the correct spelling.
- The lock symbol and a URL starting with 'https' mean that your web browser's connection to the website server is secure and encrypted. However, bad actors can acquire SSL certificates cheaply or at no cost.
    - For further confirmation a website is secure, you can access a website's SSL certificate through a few easy steps. Learn about it here.



Helping Members to be Wildly S ×

https://www.corpcu.com

    - If you see a "Not secure" warning, you should refrain from going to the site.



45.60.31.133 × +

Not secure | 45.60.31.133

This information may look different depending on the browser you are using. When a third party has verified the website you are accessing, you will see a message on the site letting you know you are on a verified website.

Do you think you have shared sensitive information with a bad actor?

Sign into Beastro (https://beastro.corporatecu.com/) and check your account information. If you notice suspicious activity in your accounts, please notify us immediately by calling (800) 242-4747 or emailing memberservices@corpcu.com. If you think you may have mistakenly given sensitive information (such as your account number, password, or PIN) in an email, text, phone call, or website that might be fraudulent, call us right away. We will help secure your account.

If at any time you do not feel your username or password is secure, you may also contact your User Administrator to change your security profile in Beastro. Reference this helpful knowledgebase article for more information.

Protect your personal login credentials.

You can protect yourself and your account by recognizing and preparing for online banking threats. Here are a few ways to keep yourself and your information safe:

- **Be careful about giving out your username and passwords.** Corporate Central will never ask for this sensitive information over the phone or through email.
- **Be creative with your password and consider using a password management service.** It is important to use a highly secure password for all your financial accounts. The most secure

passwords combine letters, numbers, and special characters. Never use your pet's name, your child's name, or anything else that a fraudster could easily find out, like your address, phone number, or birth date. A password management service can suggest randomized passwords and store them in a secure, cloud-based application.

- **Use multifactor authentication (MFA).** MFA is a multi-step account login process that requires users to enter more information than just a password. For example, along with a password, you might be asked to enter a numerical code sent via text or email, scan a fingerprint, touch a physical pass key, or answer a secret question.
- **Be careful on social media.** It is better to be cautious about the information you share on social media. Do not use information from your social media account for your password.
- **Do not be fooled by phishing attempts.** Phishing is when an imposter tries to trick you into providing your personal information. They might impersonate Corporate Central in an email, phone call, or text and ask you to confirm your information. They may even purport that an issue with your account has been identified and they need you to verify information. These scams often involve a sense of urgency or alarm.
- **Think before you open.** Do not open email attachments or links, even if it appears to be from a known contact, unless you are expecting the communication and know what it contains. Use different means to verify the communication before taking action.

If you think you have received a suspicious email or phone call from Corporate Central, please call us right away at (800) 242-4747 or forward the suspicious email to phish@corpcu.com.

For additional resources on fraud prevention and cybersecurity, please refer to this helpful article from mycreditunion.gov.