Two-Factor Authentication

Security.

Verify – Validate Your Identity

Two-Factor Authentication is a more secure method of verifying or validating your identity by requiring 'what you have' and 'who you are' in addition to the standard usernames and passwords. Two-Factor Authentication will provide more security, making it much more difficult for an attacker to impersonate you and your accounts/resources.

HOW IT WORKS

- The Two-Factor Authentication option will be managed through a new gateway user permission.
- To enroll, simply login to the administrative account and click OPTIONS then USER ACCOUNTS.
- After selecting the username to be activated you will see a checkbox to 'REQUIRE TWO-FACTOR AUTHENTICATION'.
- After selecting the box a security passphrase will be generated or you have the option to create a new HEX passphrase. It is strongly recommended that you use the randomly generated key upon activation.
- Once the permission has been activated you will then need the passphrase to be input into an external application.
- After Two-Factor Authentication has been set up and synchronized in both systems you will have to generate a key upon logging in. Each key generated on your device will remain active for 90 seconds weather or not they were used to grant access.

For more information:

Call +(599 9) 8440088
e-Mail: Hello@cxpay.global or
Visit: www.cxpay.global
FB: CXPAY

Get the App

Apple Devices

OATH TOKEN

Android Devices

Mobile-OTP

CX PAY