Two-Step Authentication Frequently Asked Questions (FAQs)

What is Two-Step Authentication?

Two-Step Authentication is a new industry-wide standard that ensures safe and secure logins to Online Banking. It is an extra layer of protection to ensure you're the only person who can access your online banking or mobile app. In addition, it prevents fraudsters from being able to access your account in the event of your login credentials being compromised (lost or stolen). When you access online banking with Two-Step Authentication, you'll need to provide two things 1. Something you know, "your password," and 2. Something only you have, "a one-time verification code" sent to you by SMS text message or email to the registered mobile phone number or email associated with your online banking account.

How do I set up Two-Step Authentication?

1. Log in to your online banking account.
2. Complete the Enable Two-Step Authentication enrollment screen.
3. Enter your preferred email address or mobile phone number to receive your verification code
4. Enter the verification code sent to you by SMS text message or email *(this code will expire after 10 minutes)*

Please note that after your initial enrollment, you can edit your mobile phone number or email address used to receive the Two-Step Authentication code.

How does Two-Step Authentication work?

When you log in to your Online Banking, you will receive a verification code on your mobile phone or email, whichever you had previously chosen. Once you receive this code, you enter it to access your account. This code expires after 10 minutes. If not used within that time, another code will need to be sent.

Will I be asked to input a verification code every time I sign into online banking?

You will need to enter a verification code when added confirmation of your identity is necessary, such as when you attempt to log into online banking from an unfamiliar device or are trying to access your banking in a new location. Initially, you may need to use a verification code more frequently until your login patterns, including device safety or location, are established.

Once I sign up for Two-Step Authentication, can I go back to the old way of accessing my account?

Two-Step Authentication, also known as Multi-Factor Authentication, is a new industry security standard that most financial institutions are adopting. This technology is there to increase the security of your account. As a result, accessing your account the old way is no longer an option.

I don't have a mobile phone. Can I use my landline and receive a text-to-voice?

While you cannot register for Two-Step Authentication using a landline, you can sign-up using an email address instead. If you don't have an email address, you can choose one from one of the email providers that offer free services.

I haven't received a verification code. What should I do?

First, if you've registered for Two-Step Authentication using an email address, be sure to check your spam folder. If you haven't received a code after 10 minutes, you can click on the "Didn't receive a code" link in the Enter Your Verification Code screen to have a new code sent. Suppose you're just signing up for Two-Step Authentication and haven't received a code. In that case, you may also want to confirm that you have input your mobile phone number or email address correctly. If you find an error, you can back up a step and correct your information.

I share an online banking login with my joint account holder. How does Two-Step Verification work for me?

To help keep your information secure, we recommend that you and your joint account holder use individual logins to access Online Banking. Please contact your branch if you or your joint account holder needs to set up your login.

Does Two-Step Authentication collect or keep any of my personal information?

Two-Step Authentication does not collect or store any personally identifying information.