

How 2-Factor Authentication Works

To help prevent unauthorized access to your Fidelity NetBenefits® account, we use an enhanced security feature to verify your identity.

HOW IT WORKS



WHAT IS 2-FACTOR AUTHENTICATION?

With 2-factor authentication, an extra layer of security is added to your NetBenefits account to prevent someone from accessing your account or performing certain transactions within your account, even if they have your password. This extra security measure requires you to verify your identity using a randomized 6-digit code. Each security code is used only once. It is *not* a password that you need to create and remember.

While 2-factor authentication for key NetBenefits transactions and at-risk logins is automatically enabled, we recommend that you turn on 2-factor authentication for all logins (find out how below). This will require 2-factor authentication on every login unless coming from a remembered device.

NEXT STEPS

Please take a moment to log in to NetBenefits.com. Navigate to *Profile*, and under *Personal & Contact Information*, verify that your contact information is current. To opt into 2-factor authentication challenges at every login, visit the *Security Center* in *Profile* and select the *2-Factor Authentication* link. Please note that to take advantage of this feature, you must have at least one phone number on file in NetBenefits.



Frequently Asked Questions

Q: Why is this extra step required for key transactions and at-risk logins?

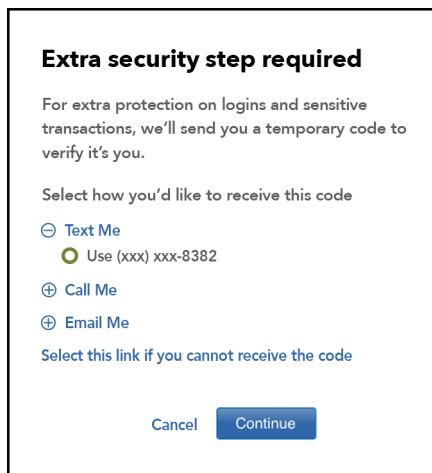
A: Common online activities, such as downloading apps or using the same password on multiple sites, can put your information at risk. Phishing emails and data breaches at companies where you have previously done business can also pose a threat. We use the 2-factor security code as a second level of verification to help prevent unauthorized access to your account (for example, in situations where your username and/or password may have been compromised).

Q: What constitutes a key transaction or login for which I might receive a challenge?

A: Examples of key transactions include but are not limited to profile changes, such as cellphone number or email address updates, or certain financial transactions. Examples of at-risk logins may include logging in from an unusual location or using a new device.

Q: What will the 2-factor authentication experience look like?

A: Review the sample screens below:



Extra security step required

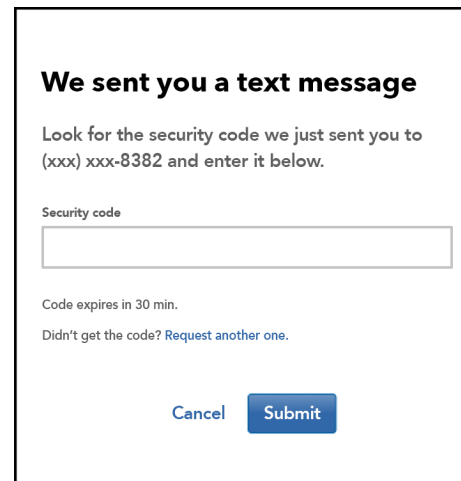
For extra protection on logins and sensitive transactions, we'll send you a temporary code to verify it's you.

Select how you'd like to receive this code

- Text Me
- Use (xxx) xxx-8382
- Call Me
- Email Me

Select this link if you cannot receive the code

Cancel Continue



We sent you a text message

Look for the security code we just sent you to (xxx) xxx-8382 and enter it below.

Security code

Code expires in 30 min.

Didn't get the code? Request another one.

Cancel Submit

Q: How do I update my contact information?

A: You can update your contact information on NetBenefits by visiting *Profile* after logging in.

Q: Why did I receive a 2-factor challenge at login even though I did not enable it?

A: You will receive a 2-factor challenge at login if certain risk criteria are met. This may be because you are logging in from a new device or location.

Q: Why am I going through 2-factor authentication every time I log in to the site?

A: You are enrolled in 2-factor authentication at login. You can choose to remember a device when you are challenged for 2-factor authentication.

Q: I did not receive a code. What should I do?

A:

- If you choose to receive the code via text message, ensure that your phone is capable of receiving texts.
- If you still do not receive a code, consider having the code sent via an alternate method, such as an email or a voice call.

Q: My code does not work. What should I do?

A: First, make sure to enter the security code that is in the message itself and not the hyphenated six-digit incoming number. If this doesn't solve the problem, do the following:

1. Select *Request a new code*.
2. If you receive multiple codes, enter the most recent one.

Q: You asked for my security code. Does this mean someone tried to access my account?

A: No, it's just a security best practice we implement to help prevent unauthorized access. We take security very seriously and employ the latest measures to help protect your information.

Q: Can I access my account from different devices?

A: Yes, although you may be asked for a security code if you are accessing your account(s) from a device you have not used before.

Q: Is there a way to restrict email from receiving 2-factor authentication security codes?

A: Yes, if you opt in to 2-factor authentication for all logins, we will only send security codes via phone.

Q: Where can I learn more about how Fidelity protects me from fraud?

A: Visit the [Security Learning Center](#) to learn more, and read our [Customer Protection Guarantee](#), which reimburses you for losses from unauthorized activity in covered accounts occurring through no fault of your own.

Screenshots are for illustrative purposes only.

Fidelity Brokerage Services LLC, Member NYSE, SIPC, 900 Salem Street, Smithfield, RI 02917

© 2022 FMR LLC. All rights reserved.

765241.9.0

44136_01