Extra login security with multi-factor authentication

Give your account security a boost and prevent unauthorized access by adding multi-factor authentication (MFA) at login.

Using an extra step at login not only helps prevent scammers from accessing your accounts and data—even if they somehow managed to get your login information—it can also give you a heads up if someone is trying to log into your account without your permission.

To increase your security when you log in, visit your Security settings and turn on your preferred MFA method.

Make sure your contact information is up-to-date

Confirm or update your email and mobile phone number in your Profile, so we can reach you when we need to. This not only supports MFA, but also allows you to receive real-time alerts for important transactions, such as updates to your profile information or transferring money from your accounts.

Approve logins with push notifications

This convenient option relies on biometrics—which means your device recognizes your face or fingerprint—and does not require a security code. This sends a notification to your mobile device(s) that allows you to verify a login attempt—or to deny it if you believe the login attempt is fraudulent.

How to turn on push notifications

Download the NetBenefits app, turn on device notifications, and make sure you're enrolled in biometrics, such as fingerprint or facial recognition. If you do not already have MFA enabled, access your Security settings to enroll.

Authenticator apps

Authenticator apps add a layer of security to online accounts by adding a verification step beyond having just a username and password.

Once enrolled, you will be prompted to enter the time-sensitive code from your authenticator app after you enter your username and password when logging into Fidelity.

Trusted devices

A trusted device is a mobile phone, computer, or other device that you've already logged into using MFA and have asked us to remember. Once you log in and check the "Don't ask me again on this device" box, that device is added to your trusted device list.

Once a device is trusted, we won't ask you to log in with multiple steps anymore. However, we'll still rely on MFA for certain sensitive transactions.

If you no longer wish to trust a device, or if one of your devices is lost, stolen, or compromised, you can remove those devices in your Security settings.

Fidelity INVESTMENTS

One-time security code by text or call

Another option is to have Fidelity send a 6-digit security code directly to your phone (or an alternate phone number) via text or voice call. The code is not a password that you need to create and remember—simply enter the one-time code you receive to verify it's you.

Never follow links in unrequested emails or text messages or read back one-time security codes to unsolicited callers asking for this sensitive information.

Extra login security FAQ

Q: When will I be asked to complete MFA?

A: If enrolled, you'll be asked to complete MFA when you log in. You may also be challenged with MFA if you're trying to complete certain sensitive transactions or if you're logging in from a new device or location.

Q: What transactions require extra security steps?

A: You will be prompted to verify your identity when you perform highly sensitive transactions, such as setting up new bank instructions or changing your contact information. If you are signed up for extra security at login, you may not be prompted to provide additional verification during the transaction because we will have already verified your identity when you logged in.

Q: What if I am not seeing the "Don't ask me again on this device" checkbox?

A: Check your security settings to see you have already trusted the device. If the device is not trusted, try clearing your internet browser's history or cache. The process for doing this will vary depending on your specific browser.

Q: What should I do if my push notification doesn't work or if I don't have my mobile device with me?

A: Please make sure that notifications are turned on for the NetBenefits app. You can also select "Try another way" on the push notification screen to receive a text or call instead.

Q: How can I remove my trusted devices?

A: You can view and manage your trusted devices in your security settings at any time.

Q: Can I access my account from different devices once I enable MFA?

A: Yes, you can access your account from the device of your choice.

Q: What if I want to receive a one-time passcode but don't have my mobile phone with me?

A: Don't worry, you can still receive a security code. If you have an alternate phone number on file, you can have the code sent via an automated call. If you don't have an alternate number, choose "Select this link if you can't receive a code" to contact a Fidelity representative who can assist you.

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.