Extra login security with multifactor authentication

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

An extra step at login not only helps prevent scammers from accessing your accounts and data—even if they somehow manage to steal your password—it can also give you a heads-up if someone is trying to log in to your account without your permission.

Multifactor authentication (MFA) options

Set up fast and secure logins with a passkey
Passkeys provide a fast, secure, and password-less way to log in to your Fidelity® account.

- **Fast, convenient logins:** Logging in is easy. You can log in the same way you unlock your device—with a fingerprint, face scan, or device PIN.
- **High security:** Passkeys help protect against tricks scammers commonly use because they only work with the real website and don't use things scammers can steal, such as a password or a security code.

Passkeys can be created and stored directly on your device, such as a laptop or mobile device, like hardware keys. You can also use a password manager that supports passkeys, which allows for syncing across multiple devices. After setting up a passkey, you can use it to log in quickly and securely.

Approve logins with the Fidelity NetBenefits® app

Approve or deny a login on your mobile device when you receive a notification about a login attempt for your account on the Fidelity website. If you're enrolled in biometrics on the Fidelity Investments® mobile app—such as facial ID or fingerprint recognition—and have push notifications enabled, you'll receive notifications.

Make sure you've downloaded the Fidelity NetBenefits® mobile app and have set up biometrics, like facial ID or fingerprint recognition, at login and that you've enabled notifications.

Connect an authenticator app

Authenticator apps provide you with a unique code to enter after your username and password. These codes change frequently in your authenticator app, so they are resistant to phishing scams and other fraudulent activities. We allow connections to most authenticator apps, including ones that are widely used, such as Google Authenticator, Microsoft Authenticator, and Passwords app for iOS.

You can connect an authenticator app in your security settings or to the Fidelity NetBenefits app.

More ways to secure your login

Trust your personal devices

When you log in on a personal device that you trust, you can skip MFA for future logins. Select the "Remember this device" checkbox when you log in to add it to your trusted device list, which you can view and manage in your security settings. Trusted devices only require MFA occasionally. For your security, MFA will still be required for certain sensitive transactions.

Never choose to remember public devices, like a library computer, or a device using a public, unsecured Wi-Fi network to access your account.

Make sure your contact information is up to date.

Accurate contact information supports security by allowing you to receive real-time alerts for updates to your profile information and important transactions, such as a request to transfer money from your account.

Confirm or update your email address and mobile phone number in your profile so you can receive important security information.

Passkey FAQs

Q: How do passkeys strengthen my account security?
A: Passkeys only work on real websites and do not use things a scammer could steal, such as a password or a security code. This provides protection against common tricks scammers use when attempting to gain access to accounts.

Q: Can I still log in with my password after setting up a passkey?
A: A passkey is designed to let you log in to your account without having to enter a username and password. If you have set up a passkey and enter a username and password, you may be prompted to complete your login using your passkey.

Q: Do I need to set up passkeys on all my devices?
A: If your passkey is synced through the cloud, you only need to set it up once. You can use it on any device logged in with the same account where the passkey is stored.
If your passkey is only saved on one device, it won't automatically be available on your other devices. In that case, you can:

- Use the device that has the passkey to help you log in on another device, or
- Create additional passkeys on your other devices so you can log in more easily in the future.

Q: What happens if I lose my device where I store my passkey?
A: If you set up another strong login option, such as an authenticator app or push notifications, you may be able to use it to log in and regain access to your account.

If you're unable to log in, contact us for help restoring access to your account.

If your passkey was synced to the cloud, you may be able to recover it by following the recovery instructions provided by your password manager provider.

Multifactor authenticator FAQs

Q: Which authenticator app should I use?

A: If you already have an authenticator app that you use for work or other personal accounts, you can connect your Fidelity® account directly. If you aren't already using one, you can search for "authenticator app" in your mobile device app store to find one that works for you. Fidelity allows you to use most of them, including Google Authenticator, Microsoft Authenticator, and Passwords app for iOS.

Q: Do you have to enter an authenticator app code each time you log in?

A: By default, yes, you will enter a code from your authenticator app each time you log in. However, you can skip this step by selecting "Remember this device." We will then trust the device and won't require you to go through multifactor authentication at log in—but that extra step may still be required for certain transactions. You can manage your trusted devices in your security settings.

Q: What should I do if I get a new mobile device?

A: When getting a new mobile device, set up and connect your authenticator app before disposing of your old device. Some authenticator apps make it easy to transfer connections to a new phone by scanning a QR code on your old device.

Q: How do I prevent losing access to my authenticator app?

A: Options vary across apps, but saving any recovery code from your app in a secure place is suggested.

Q: How do I stop using an authenticator app?

A: If you decide to stop using the authenticator app, go to your security settings to remove it as a multifactor authentication option before deleting the app from your device.

Q: What should I do if I lose access to my device or authenticator app?

A: Give us a call, and we'll get you back into your account.

Q: How can I protect my authenticator app account?

A: Be sure to enroll in the security options your authenticator app offers. You can also protect the device the app is on by keeping it in a safe place, installing software updates when available, and using biometrics (facial ID or fingerprint recognition) to log in.

Q: What transactions require extra security steps?

A: You will be prompted to verify your identity when you perform sensitive transactions such as setting up new bank instructions or changing your contact information. It is possible that you may not get prompted for additional verification during such a transaction because we will have already verified your identity when you logged in.

Q: What if I am not seeing the "Remember this device" checkbox?

A: Check your security settings to see if 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 the one-time security code doesn't work?

A: Make sure you're using the security code that's in the text message itself, not the incoming number from the sender. If this doesn't solve the problem, select "Request a new code."

Complete the steps for requesting a new code. If you're receiving the code by phone, make sure you are near that phone. We can only send text messages to a mobile number.

Third-party trademarks and service marks are the property of their respective owners. All other trademarks and service marks appearing herein are the property of FMR LLC or an affiliated company and may be registered.

Google is a trademark of Google LLC.

Fidelity Investments Institutional Operations Company, LLC, 245 Summer Street, Boston, MA 02210
© 2026 FMR LLC. All rights reserved.
1283543.1.0