Password tips and recommendations

A strong password helps you protect your account.

To create a strong password, keep in mind the following guidelines:

- Create unique, original passwords
- Use the longest practical password
- Use a mix of upper and lower case letters
- Include one or more numbers
- Do not use repeating or adjacent characters
- Use at least one of these special characters: `~!@#$%^&()_+={}|[]:”?,./\
- Avoid using software or toolbars that store your password
- Change your password regularly

Remember to avoid the following password pitfalls:

- Do not choose passwords or security codes that others can easily guess.
- Do not reuse passwords for multiple sites.
- Never use your account numbers.
- Do not use personal contact information, such as addresses or phone numbers.
- Do not use personal information, such as your name, birthday, Social Security Number, passport number, or the names or information for family members or friends.
- Do not use sequences of characters such as *1234567* or *abcdefg*.
- Do not rely on look-alike substitutions of numbers or symbols alone. Passwords like *P@ssw0rd* are easy to guess, but can be effective when you also change the case of the letters, the length of the words, and misspellings, or when you use multiple unrelated words in a phrase.
- Do not use dictionary words.

Registering a browser or device

A conventional authentication system relies on two forms of identification to prove your identity: your Login ID and your password. Multi-factor authentication uses multiple forms of identification to make it harder for attackers to access your account. The multiple forms of identification can include something that you know, such as a password, and something that only you have.

In online banking and the mobile banking app, we can send a Secure Access Code to a contact address that you configure. The code is only valid for a single use and it expires after a short time. You choose one of the following ways to deliver the code:

Secure Access Code delivery methods

Method	Details
Phone	The system calls the telephone number on file. You answer the phone normally and make a selection to hear the code. If necessary, you can repeat the code. The system does not leave the code on voice mail. If you miss the call, you can request a new code.
Text (SMS)	The system sends a text message with the code. Standard text messaging fees apply.
Email	The system sends a short email with the code. Depending on the configuration of the filters on your mail server, the message may be in your junk or spam mailbox.

Whenever possible, you should configure phone and text delivery methods, and leave email unconfigured. Attackers can use viruses or other malicious activity to compromise your email and view the Secure Access Code. If you do not configure an email address as a Secure Delivery Contact, you can help prevent this type of attack.

Note: Depending on your security needs, we may configure your account to use codes from Symantec™ Validation and ID Protection (VIP) Service Tokens. If your account uses a token, you enter the code from the token instead of a Secure Access Code. You enter the code from the token every time that you log in.

If you have never used a particular browser or device to log in, you may need to enter a Secure Access Code to use it. If the browser or device is one that you plan to use again, you can register it. By registering a browser or a device, you confirm that it is under your control and that you intend to use it to access online banking or the mobile banking app.

Tip: Multiple users can register the same browser or device.

You register your browser or device again in the following circumstances:

- You use a different browser on your desktop
- You delete and reinstall the mobile banking app
- Your browser does not save browser cookies
- You clear existing browser cookies
- We reset registration for all users for security reasons

Caution: Only register a browser or device if it is under your control. Do not register a browser on a public computer.