Connex CREDIT UNION

UNBANK WITH US

FAQ – Online Banking Security Changes

Why did my login page change?
Protecting members from fraud and identity theft are top priorities for Connex Credit Union. The change you are seeing on the login page is due to the enhanced security, "Multi-factor Authentication" we have implemented within Remote Banking. Multi-factor Authentication (MFA) goes beyond member ID and password verification to provide an additional level of protection against unauthorized access.

What is Multi-Factor Authentication?
Multifactor Authentication protects against online fraud by providing an additional end user authentication 'factor' beyond the username and password used today. The solution was designed to preserve the convenience and usability of your online banking channel. Previously, the MFA used by Connex was challenge questions. Currently, after the change effective February 1, 2012, MFA consists of one-time passcodes that are sent to the member via voice call, text message or email.

What is a one-time passcode?
A one-time passcode is a series of digits that is sent to you in one of the ways described above (voice call, text message, email.) It acts as an additional layer of security after you enter your user name/member number and password. It is a code that is only valid for the time you are currently logging in. Once you're logged in, that passcode is no longer valid. All of these security features reduce the changes that someone can fraudulently enter your account.

What are the benefits of MFA?

- Provides peace of mind regarding online banking authentication and reduces the opportunity for unauthorized users to enter your account.
- Easy for users – once enrolled, there is little difference in the login process or the time it takes.
- Usable anywhere at any time – users can enroll any number of computers.

Will I still have access to all the same accounts online?
Yes. This process only affects how you login, not your online banking accounts.

Will my password change?
No. The password you use to log into online banking will remain the same.

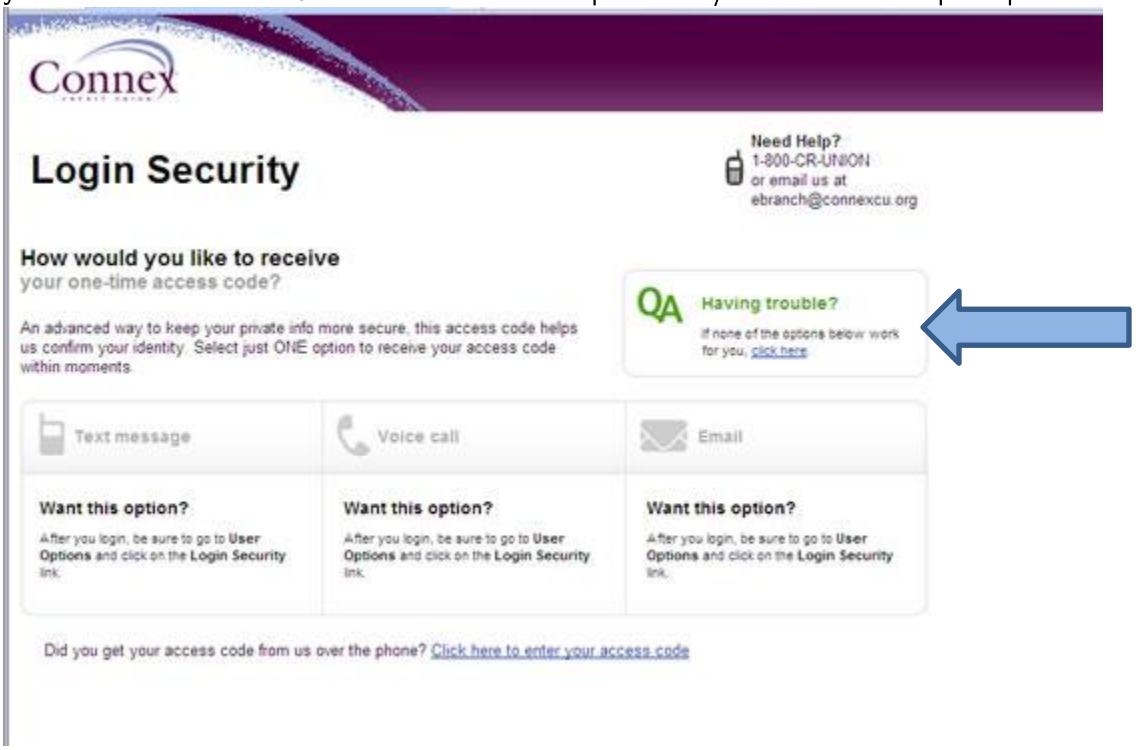
What is the difference between a one-time passcode and a password?
A password is **chosen by you** and is required to access Online Banking and the Call-24 phone system. On the other hand, a one-time passcode is a random code that is e-mailed or sent to you via phone call or text message when you attempt to log into Online Banking from a computer that you have not already designated as "private."

How will I receive my one-time passcode?

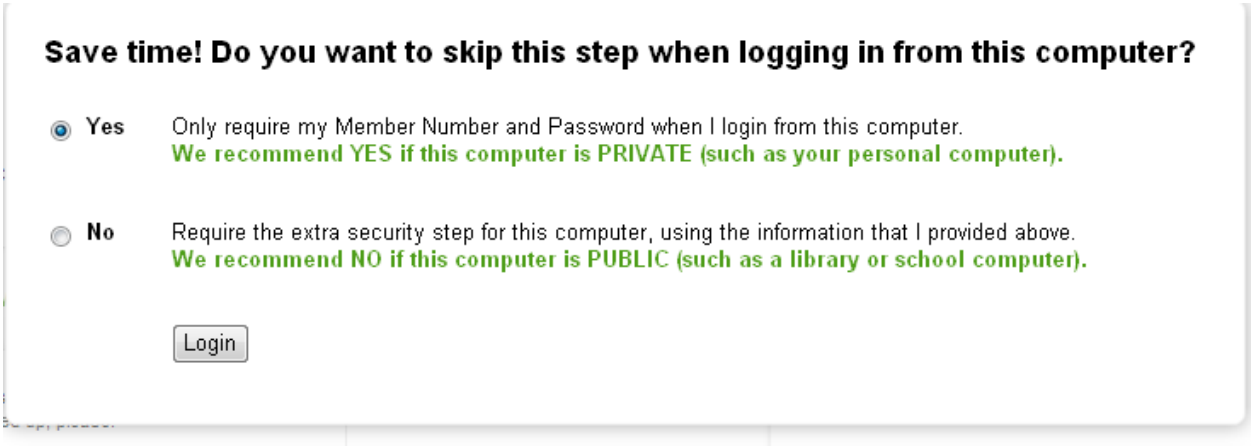
- Text Message (SMS): The member receives a short message (SMS) with a one-time access code on one of the mobile phone numbers they set up. If you do not receive a text message, you may need to check with your mobile phone provider to find out if there is a block set on numeric texts.
- Automated Phone Call: The member receives a phone call at one of the numbers that was set up with a recorded message stating the one-time passcode. If you do not receive a phone call, check to be sure you did not put your phone number in the text message phone spot.
- Email: The member receives an email with a one-time passcode at an email address that was previously set up.

How can I set up my account to receive one-time passcodes?

To set-up your account to use One-Time Passcodes, you will log into Online Banking using your current username/member number and password, then follow the prompts.



How can I avoid having to obtain a one-time passcode in the future?
As part of the security features, you can elect to register your computer during the login process. Once a computer is registered as "private", it will be recognized during future logins and you will not be prompted to receive a one-time passcode. If you elect not to register a computer, or keep the settings "public" you will be prompted receive a one-time passcode whenever you log in from that computer.



If I set my security settings to "private", will I need to receive a one-time passcode?
You will only need to receive a one-time passcode in the event you were to log onto online banking from a different computer that you have not already registered as private. If you have a program on your PC that automatically deletes cookies and internet files you will not be able to successfully select "private" and will need a one-time passcode for each login.

Are there banking applications where single-factor authentication as the only control mechanism would be adequate? Is Connex the only financial institution enhancing their online security?
Single-factor authentication alone would be adequate for electronic banking applications that do not process high-risk transactions, e.g., systems that do not allow funds to be transferred to other parties or that do not permit access to customer information. Any online banking application that allows for high risk transactions will need to update their systems to adhere to the guidelines set by the Federal Financial Institutions Examination Council (FFIEC) and many other financial institutions have already made this change.