TECHNICOLOR
Federal Credit Union

Frequently Asked Questions

(818) 973-4900 or info@technicolorfcu.org
Mon. – Fri. 8:30 a.m. – 4:00 p.m.

Why are you changing the security standards?

We care deeply about keeping your money safe while providing you with easy access to your accounts. With the continued growth of online banking, there are increased needs for greater security standards to keep you and your money well protected. In addition, the government issued new guidelines, calling for enhanced security measures for online banking. Thus, we are upgrading our security procedures to provide you with the best protection available. Our new security standards will make it even safer for you to monitor and manage your money while safeguarding against unauthorized access to your accounts.

How do I update my user ID and password?

To update your user ID and password, go to the User Options page and click on the link for “Change User ID” and “Change Password,” respectively. Then, create a new ID and password that meet the following requirements:

User ID criteria:

- Must be between six and 20 characters long
- Must contain one letter
- Can contain numbers and/or the following special characters: @$*_-=.!~
- Must NOT contain any spaces (including before, in the middle of, or after the user ID)

Password criteria:

- Must be between six and 32 characters
- Must contain a combination of:

Letters and numbers
or

Letters and any special characters
or

Numbers and any special characters

- Must NOT contain any spaces (including before, in the middle of, or after the password)
- Cannot be a substring of the user ID
- Other items to note about passwords:

  Passwords are case-sensitive

  Passwords do not expire

What will I experience when I log in to my online banking account the first day after the security upgrade?

You will be guided through an easy three-step process:

Step 1: The system will check your current user ID and password to see if they meet the new security standards stated above. If the user ID and/or password need to be updated, you will be prompted on screen to make the change before proceeding. Otherwise you will see a message stating that your login is fine.

Step 2: The system will check if your phone number(s) are registered. If any phone numbers are identified, the system will display them and allow you to review and edit these numbers if desired. If you do not have any phone numbers registered, you will be prompted to enter up to two phone numbers. These numbers will be used to send you a one-time passcode via a voice call or SMS text message (you choose the method). If you do not have a phone, then you can elect to receive your one-time passcode through email. You will be able to click a link to provide an email address during this step. By default you will be shown the email address within your online banking profile, and any change to this email address will be saved as your primary email address within your online banking profile.

Step 3: Finally, you will need to respond to a secondary challenge with any of your registered devices from Step 2. You will have the opportunity to go back to Step 2 to provide a new device if you realize you have made an input error. Once you have successfully completed the secondary challenge, you will see a confirmation message and you will have the option to have your computer (or mobile device) remembered so that you can skip this step in the future. **Note:** If you enabled a phone number for SMS in Step 2, you will not be challenged again given that SMS enrollment requires you successfully complete a challenge there; instead, you will be presented with a success message and can choose for your device to be remembered before entering online banking.

What information is contained in the automated voice call or SMS text message?

Information within an automated voice call:
*"Hello, this is your financial institution***.*
Please press pound to receive your 6 digit access code."
** Press pound **
[1.5 second pause and your unique one-time passcode will be provided]. Press # to repeat.

Information within a SMS text message:
[your financial institution*****] Access Code. Your access code is xxxxxx. Reply HELP for help.

******the automated call or SMS text you receive will use our financial institution name.*

If I am traveling internationally, can I receive a one-time passcode via SMS text or automated voice call if I access my online banking account from an unrecognized computer?

If you have a US-based mobile phone, you can use it to receive a one-time passcode via SMS text or automated voice call as long as your wireless carrier and your current wireless plan is supported within the country you are visiting.

How will using my phone make my account safer?

We are implementing what is known as “multifactor authentication” which makes it more difficult for phishers and attackers to access your accounts without you knowing it. While this might seem unfamiliar, you actually use it every time you visit an ATM. When you access your account from any ATM, you need both your ATM card (something that you have) and PIN (something that you know). We’re implementing the same type of protection by using both your user ID and password and your phone to access your account. By doing this, even if an phisher or a attacker manages to steal your password and tries to use it to log in, they would be unsuccessful because they would need your phone as well.

Is there anything I need to do?

If your user ID or password does not currently meet the new standards, update this information now. If you do not complete the update before the security upgrade goes live, then you will be prompted to strengthen your user ID and password upon your first login after the security upgrade. At that time, you also must have a cellphone or a landline phone and provide the phone number to receive your one-time passcode. You will need this phone every time that you need to receive an access code.

Will I always need to use both my user ID and passcode and my phone from now on?

The first time you attempt to log in from a new computer, you will need to use both your password and the access code you receive on your phone in order to log in. If you are accessing from a private computer that you personally use, you can opt for the system to remember your computer for future logins. By doing this, you will not need to repeat the step of obtaining an access code via phone, and you will only need your user ID and password in the future to log in. For the best security protection, we suggest that you always use both your phone and your password. If you do opt to have your computer remembered, we recommend that you do so only on computers that you personally own and that have the latest updates and virus protection software installed on them.

How about if I log in from another computer or mobile device?

The first time you log in from another computer or mobile device, you will need to use both your password and a new one-time passcode code to log in. However, you can choose to have your new computer/mobile device remembered on the system so you only need your user ID and password for future access to your account online.

What browsers do you support?

We support Internet Explorer 8 and 9, the latest versions of Firefox and Chrome and the latest versions of Safari for Mac OS X. As of January 2012, we no longer support Internet Explorer 7.