It's Me 247

Mobile and Desktop Online Banking

2023 Update

SecuriKey

LEGAL DISCLAIMER

The information contained in this document does not constitute legal advice. You should retain and rely on your own legal counsel, and nothing herein should be considered a substitute for the advice of competent legal counsel. These materials are intended, but not promised or guaranteed to be current, complete, or up-to-date and should in no way be taken as an indication of future results. All information is provided "as is", with no guarantee of completeness, accuracy, timeliness or of the results obtained from the use of this information, and without warranty of any kind, express or implied, including, but not limited to warranties of performance, merchantability and fitness for a particular purpose. In no event will CU*Answers, its related partnerships or corporations, or the partners, agents or employees thereof be liable to you or anyone else for any decision made or action taken in reliance on the information provided or for any consequential, special or similar damages, even if advised of the possibility of such damages.

LOGIN CONTROLS

Cross Site Forgery Prevention. Inputs are sanitized, and session tokens are used to prevent cross site forgery.

Session Timeout. Members are automatically logged out of **It's Me 247** after fifteen minutes of inactivity or page refresh (five for login and security screens). At login and security screens, if the user has an idle screen for 3 minutes the user will get a pop-up advising 2 minutes are left. If the user maintains activity, the session will continually extend itself. Activity is mouse/keyboard actions on the active browser window.

MOP Restrictions based on Session. Users cannot jump ahead or go back on certain pages, and verify, fund, and enroll processes are restricted to single use (even when multiple windows are opened to the same page).

Dynamic API keys for External Access. Keys needed for external access to MOP are constantly changed, rather than a static set of keys that could be lost or stolen.

256 Character Password Limit. Minimum limit is 6 characters.

Challenge Question. Members must answer a challenge question at login.

Incorrect Login. Account is disabled if three incorrect passwords are entered, or three incorrect answers to challenge questions.

Temporary Password. Controls are in place to control the length of time a temporary or unused password is available to the member if the member has not logged into **It's Me 247**.

Password Expiration. Online banking passwords can be configured to expire.

Red Flag Warnings. When credit union employees enter selected screens (such as Teller, Inquiry and Phone Operator), they receive a warning message noting how many changes have been made to the member's personal information items in the last 30 days.

DATA TRANSMISSION

Encryption. Information entered by the member is encrypted through 256-bit encryption.

Data Storage. Username and password information is "salted" (random data added) and hashed.

PIB LAYERED CONTROLS (OPTIONAL)

Geographic Controls. Allows or blocks access based on the PIB profile.

PC Registration Controls. Members can require that a computer be registered before it can be used to sign on to **It's Me 247**.

Days and Times Available. Members can use these to establish what is "normal" for them, blocking access during days and times when they will never be using **It's Me 247**.

Confirmation Codes. Members can set a confirmation code, which is essentially an additional password for EFT transactions and transfers, and for loan applications.

Secure Message Center. If changes have been made to a member's PIB Profile, or if someone has attempted to access the member's **It's Me 247** accounts in violation of a PIB profile setting, a message is sent to the member's **It's Me 247** secure Message Center.
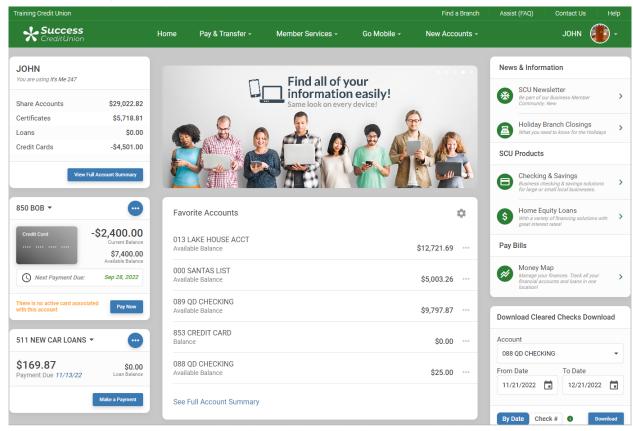
CU*ANSWERS

OVERVIEW:

IT'S ME 247 ONLINE AND MOBILE BANKING

It's Me 247 is an online and mobile banking product designed to safeguard your members' money and privacy. To further ensure security, these protective technologies have been applied in layers to address each phase of any online transaction.

Both **It's Me 247** Online Banking and Mobile Banking use the same authentication features. Enhanced authentication options are available via PIB for Online Banking, and Multiple Authentication Choice Options ("MACO") for Mobile Banking.

USING SECURIKEY: Credit unions may be asked by examiners or auditors to provide an Online or Mobile Banking risk assessment, documenting **It's Me 247** safeguarding of authentication information. While this document is intended to assist credit unions in their risk assessments, note that not all features and tools listed are automatic. Many security tools must be specifically activated by the credit union. For example, many of the security features are available in Personal Internet Branch (PIB). **SecuriKey provides descriptions of the controls used to protect sensitive information and verify identity**.

USERNAME AND PASSWORD FEATURES

It's Me 247 Online and Mobile Banking offers many controls for managing the passwords used by members to gain access to their accounts.

Usernames. Usernames can contain a letter or a combination of letters and numbers. Usernames are not case sensitive. Usernames can include spaces and cannot contain special characters. Usernames cannot contain the account number, nor the member's first and last name.

Password Disabled. Three incorrect attempts disable the password.

Password Length. Online banking passwords can be up to 256 alphanumeric characters, including special characters.

Password Characteristics. Passwords are case-sensitive (i.e., *Ds443&sld* is different from *dS443&SLD*). Passwords can include a blank space. Credit unions can specify a minimum number of characters. 6 characters are the minimum required. Maximum length is 256 characters. Passwords are not stored on the system.

Password Complexity. Credit unions can require members to follow complex password rules (requires three of the four following: uppercase letter, lowercase letter, number, and special character).

Hide Typing. When logging into **It's Me 247** members have the option of selecting a "Hide my Typing" feature so that when they enter their password and security question answer, asterisks appear on the screen in place of the actual characters that they type.

RED FLAG WARNINGS

When credit union employees enter selected screens (such as Teller, Inquiry and Phone Operator), they receive a warning message noting how many changes have been made to the personal information items in the last 30 days.

AUTHENTICATION INFORMATION

Authentication information entered by the member is encrypted. Transmission security is provided by using 256-bit encryption. Passwords are then "salted" for additional security, hashed, and the 256-bit string is compared to the value stored in the database.

CHALLENGE QUESTION

It's Me 247 requires users to answer a challenge question in addition to supplying a password each time they login to online banking. Members set up these questions and answers the first time they use online banking. Since answers can be a maximum of 30 characters, this gives the member an opportunity to create a longer, harder to guess passphrase to work in tandem with the password. The challenge question rotates for each login. Three incorrect challenge question answers require the credit union to reset the account in CU*BASE.

ABNORMAL ACCOUNT ACTIVITY

Credit unions can monitor high risk online banking activity through the Abnormal Account Activity Monitoring function. This allows a credit union to define the ranges (number of transactions and dollar amount) of a month's worth of transaction activity considered normal, abnormal, and high risk for the group.

Online banking activity that can be monitored (among other transactions) include:

Share Draft from Bank Process. This includes all checks posted to member accounts via daily share draft processing, including member checks processed via **It's Me 247** Bill Pay.

ACH Network Processing. ACH activity, including debits for online bill payments that are processed via **It's Me 247** Bill Pay.

TEMPORARY PASSWORD

Credit unions have four configurations to select from for their temporary password, including: Last four digits of SSN (current option), first four digits of SSN and last two letters of last name (all CAPS), 4-digit birth year and first two letters of last name (all CAPS), last four digits of SSN and 4-digit birth year. Temporary passwords expire after 24 hours.

Additional access controls are in place to control the length of time a temporary or unused password is available for access to **It's Me 247.**

Non-Use Expiration. If a member fails to log into **It's Me 247** within the allowed time, the member will need to call the credit union to reset the password for access. A temporary password reset by the credit union is valid for 24 hours.

Online banking passwords can be configured to expire after a certain period of non-use, either a configured number of days (1-90) or select 999 days to never expire passwords due to non-use.

Immediate Change. Once new members log in to **It's Me 247** the member will be required to immediately change their online banking password.

New Memberships. New memberships can set how long a period (from one to seven days) that the new member temporary password is valid.

Temporary Code. First-time members have the option to receive a temporary code via text or email instead of using one of the configured formulas.

PERSONAL INTERNET BRANCH (PIB)

The Personal Internet Branch (PIB) System provides layered security controls and member personalization for the **It's Me 247** Online Banking application. The configuration of PIB settings involves two parts: the PIB default profile configuration itself, and the master ARU/Online banking configuration settings that control the availability of certain features for the credit union. PIB default profile configuration allows individual members to make decisions about their security, rather than having security unwillingly forced on every member.

Geographic Controls. **It's Me 247** uses geolocation technology to determine where the computer is located when the member logs in, and then allows or blocks access based on the PIB profile. If someone tries to log in from a PC that is in a different country, city, or state, the PIB profile will restrict access.

PC Registration Controls. Members can require that a computer be registered before it can be used to sign on to **It's Me 247**. This registration technology uses a "persistent cookie" that contains encrypted data that is stored on the user's hard drive for use by the browser software. When a member attempts to log in to **It's Me 247**, the system looks for that cookie on that computer and will not allow the member to log in the cookie does not exist on the user's system.

Days and Times Available. Members can use these to establish what is "normal" for them, blocking access during days and times when they will never be using **It's Me 247**. This provides another layer of security by narrowing the window when the accounts could potentially be accessed by an unauthorized person.

Confirmation Codes. Members can set a confirmation code, essentially an additional password for EFT transactions and transfers, as well as loan applications.

Secure Message Center. If changes have been made to a member's PIB Profile, or if someone has attempted to access the member's **It's Me 247** accounts in violation of a PIB profile setting, a message is sent to the member's **It's Me 247** secure Message Center.

PASSWORD SECURITY

The credit union can select minimum number of characters. This minimum must be at least 6 characters with a maximum of 256.

The credit union can optionally select to force complex password rules. This requires three of the four of the following: uppercase letter, lowercase letter, number, and special character. Regardless if complex passwords are required, members can use numeric, alphabetic, and special characters in the passwords. Passwords are case-sensitive.

TEMPORARY PASSWORD

This system-generated password used for new members, members whose password is reset by a credit union employee, or the password used during a promotional campaign for **It's Me 247**.

The credit union selects one of the four temporary password settings. They include: birth year and first two letters of last name (all capital letters), last 4 of SSN and birth year, last four of SSN, or first 4 of SSN and first two letters of first name (all capital letters). First-time members have the option to receive a temporary code via text or email instead of using one of the configured formulas.

Temporary passwords are only available for 24 hours. If the member does not log into online banking and change the password within 24 hours, the password expires and the member must have the password reset again.

The member is required to change the temporary password immediately after logging into online banking for the first time. The member is not allowed to set a new password that matches the temporary password.

Notes: The password is not visible to member or credit union staff and is encrypted in CU*BASE files.

RESTRICTED PASSWORD AND SECURITY QUESTION RETRIES

Members are only allowed 3 attempts to enter the correct password and security question answer combination before the password is disabled. This feature is used to prevent someone from trying to guess a member's password or security question.

RESET OF DISABLED PASSWORD

Once password is disabled, a credit union employee can reset the disabled password to the default password setting (see previous section on credit union options). Member is required to change password upon first access.

Member can also use the "*I forgot my password*" feature to reset their password. The member must answer all three security questions correctly to reset their password.

SECURITY QUESTIONS AND ANSWERS

Members must answer a security question and a password each time they log into online banking.

Members set up three questions and answers the first time they log into online banking. The member is given the option of composing both the question and answer for one security question.

Security questions can also be set up in Mobile Web Banking (for example on the member's phone during the membership opening process). Security question answers can be a maximum of 30 characters, allowing members to create a phrase as an answer.

Security questions are also used when members reset their passwords through the "I forgot my password" feature. Members must answer all three security questions correctly to reset their password.

Member Service representatives can delete security questions and answers (first following credit union policies). In this case, the member will set up security questions next time the member logs into online banking.

Notes: The security question answer is available to credit union staff in Query; member can elect to hide answers when typing it in a public area.

MEMBER NOTIFICATION OF PASSWORD CHANGE

Members receive an email notification and a message in their Secure Message Center in online banking every time their password is reset, regardless of who resets the password. A password might be reset by a credit union employee in CU*BASE or by the member in online banking. Additionally, members can see these password changes in online banking to self-monitor activity on their account.

CREDIT UNION MONITORING OF PASSWORD CHANGES

The *Member Password Change History* report and online management dashboard lists all online banking password changes.

Both features indicate the reason for the change. Two examples are that a credit union employee reset the password in CU*BASE or member locked the account with three incorrect entry combinations and used the "*I forgot my password*" feature to rest the password.

"NON-USE" PASSWORD EXPIRATION

Passwords can be configured to "expire" automatically after a certain number of days of non-use. Credit unions can select the number of days (1 – 90 days) for password expiration. If a member logs in during this time period, a member's password will not expire. Members may contact the credit union to have password reset when the password expires. Or members can use the "*I forgot my password*" link and answer three security questions to reset the password themselves.

Credit unions can select to never expire a password due to non-use by entering "999" days.

HIDE MY TYPING

Members can select to use the "Hide my Typing" feature to type the answers to their security answers as asterisks (instead of the actual text of the answer).

REMINDER WHEN MEMBER HAS NOT CHANGED PASSWORD IN THE LAST 30 DAYS

It's Me 247 displays an automated "soft" warning message to encourage members to change their password, without making the password change mandatory. This message will appear when the member has not changed the password for the last 30 days. Members can elect to change their password or ask to be reminded again in 30 days.

The member's selection is recorded in CU*BASE for auditing purposes. Members can also see their selections online.

DEACTIVATE ACCESS AT MEMBER'S REQUEST

The credit union can deactivate a member's password altogether so that no access is allowed to online banking.

EVALUATION OF ACTIVATED BUT INACTIVE MEMBERS

The CU*BASE auditing report helps evaluate risk of inactive members. The auditing menu lists members who are activated but have not logged in for a selected date range.

USERNAME

Usernames are used in place of account numbers when the member logs into **It's Me 247**.

Usernames are defined by members in **It's Me 247**. Usernames can also be set up in Mobile Web Banking (for example on the member's phone during the membership opening process).

A credit union employee cannot set up a username in CU*BASE for a member.

The first-time members log into online banking, their account number is used since a username is not yet defined.

Usernames may not include the member's account number. They may be 1-20 characters, cannot be all numbers, cannot contain the member's first or last name, and are not case sensitive.

Credit union employee can view username of member and assist member who forgets (after first confirming identity of member).

Credit union employees can delete usernames (after confirming identity of the member). In this case the member will use the account number until another username is configured by member.

*Notes: The username can be displayed to credit union staff in CU*BASE.*

REQUIRED USERNAMES

Credit union can elect to require usernames instead of account numbers. In this case all members are required create a username and use it in place of their account numbers when they login to online banking.

PERSONAL PREFERENCES AND SECURITY CONTROLS

Personal preference configurations available to the member include personal information update, password changes, username changes, and eStatement options.

NEW MEMBERS ACCESS

The credit union can elect to activate **It's Me 247** automatically for new members. They can also require member to request access before manually activating.

The credit union can define the number of days a new member can access online banking with the system generated temporary password before the password expires. Expiration length for new member password can be set to a configured 1-7 days. First-time members have the option to receive a temporary code via text or email instead of using one of the configured formulas.

The temporary password follows the rules defined by the default temporary password.

The member is required to change the password immediately after the first access to online banking. Members are not allowed to set a new password that matches temporary password setting.

ONLINE BANKING USE AGREEMENT (MEMBER INDEMNIFICATION)

Members are required to accept the "*It's Me 247* *Online Banking Use Agreement*" the first time they access **It's Me 247**. The acceptance date is recorded in CU*BASE.

CONFIRMATION EMAIL AND SECURE ONLINE BANKING INFORMATION FOR PERSONAL INFORMATION CHANGES

Members receive confirmation emails and secure message center messages whenever a personal item, such as address, email address, or code word is changed either via **It's Me 247** by the member or via CU*BASE by a credit union employee. If the email is changed, the member receives and email to the old and new email address.

No personal information is shared in the email. Members receive notification of what element has changed but not the actual change itself.

WRONG EMAIL MESSAGING

If member's email address is flagged as a wrong email address, member will see a message encouraging them to change their email address immediately upon logging in and each time thereafter until the email address is updated.

Members can click to save the address if it is mistakenly marked as invalid.

TRANSFER CONTROLS

Must first activate transfers to other credit union accounts. Transfer Control is used to limit the member accounts to which funds can be transferred. Requires password access on the "from" account only.

The credit union can select either of the transfer controls or require both:

(1) Transfer control configuration restricts transfers to select to: accounts. These relationships must be set up by credit union employee.

(2) Transfer control configuration allows for optional restriction to require member to enter specific to: account information (acct # with 3 characters of the last name for confirmation).

ADDITIONAL CONFIRMATION REQUIRED WHEN MEMBERS MAKE ACCOUNT-TO-ACCOUNT TRANSFERS

If A2A is activated, members must select an additional confirmation checkbox before authorizing an A2A transfer. Members are then provided a page where they can print the transaction for their records.

USAGE STATISTICS FOR CREDIT UNION EMPLOYEES ON MEMBER ACCESS

Displayed via CU*BASE Inquiry, Phone Op, Teller; shows logons used during the current and previous month and other self-service status (bill pay, eStatements).

Management dashboard show stats for online/mobile web banking, mobile text banking, and audio-response banking). Shows logons used during the current and previous month and other self-service status (bill pay, eStatements).

USAGE STATISTICS TO MEMBER

This CU*BASE menu details times are logged into online banking as well as access point: online banking, mobile banking, or jump from other accounts.

STAND-IN PROCESSING FOR 24x7 AVAILABILITY

Stand-in processing makes online banking services available even during nightly and monthly CU*BASE processing.

TIMEOUT NOTIFICATION
SESSION TIMEOUT

Members are alerted after twelve minutes of inactivity or page refresh with a pop-up window that counts down the remaining three minutes.

If the member clicks "*Continue This Session*" the timer will be reset and the page will not be refreshed so the member will not lose anything they have done on the page.

If the user does not respond or clicks "Log me out," the person is automatically logged out of **It's Me 247** or mobile web banking.

eALERTS

Credit unions can elect to allow members to subscribe for eAlerts online through **It's Me 247.** CU*BASE features are also available for credit union staff to maintain for members and view alerts sent.

Member receives the alert via the **It's Me 247** Secure Message Center.

Member can optionally select to also receive an email notification alerting them that an alert has been sent. The notification can be configured with a "short option" where no account details are included in the email, or a "long option" containing more detailed information.

If Mobile Text Banking is activated at the member's credit union, and the member is enrolled in Text Alerts, members can also select a fourth option, to receive the text of the alert in the form of a text to their mobile phone.

eAlert balance notifications (email and text message) are evaluated on a 30 minute cycle. Other emails and text messages are sent according to request, for example ACH Transaction alerts are sent when ACH transactions are posted.

eNOTICES

Allow the credit union to send an electronic version of a printed notice to the member. Members can view their eNotices in their Secure Message Center in Online Banking.

Content of an eNotice is the same as a printed notice, except that member's private information is masked in the eNotice for additional security.

Members can select to have an additional email notification sent when the eNotice is sent. Also, having the notification sent via text message is also available if the member is enrolled in Mobile Text Banking. (NOTE: Only a notification is sent; the notice text is not included in the notification.)

E-Notices email notifications and text messages are sent when notices are printed by the credit union.

VERSION CONTROL

VERSION	DATE	CHANGE	TEAM
1.0	June 14, 2018	First published	Internal Audit
2.0	May 23, 2021	Revised for clarity	Internal Audit
3.0	Janaury 30, 2023	Revised for clarity	Internal Audit

LEARN MORE

Review a video introducing **It's Me 247** here.

Additional videos about **It's Me 247** can be found here.

Detailed **It's Me 247** Online and Mobile banking materials are located in one convenient location here.

Keep up-to-date with online materials about **It's Me 247** here.

SecuriKey