How We Protect You

Isabella Community Credit Union (ICCU) is committed to protecting your privacy across all communication channels. ICCU employs proven technologies and trains staff regularly to protect your personal and financial information.

In addition, under federal law, Regulation E (Electronic Fund Transfer Act) provides certain protections to consumer members when there is unauthorized account activity. Regulation E covers electronic fund transfer activity through a checking, savings or other consumer account used primarily for personal, family or household purposes. All of the protections provided by Regulation E are incorporated into our Electronic Fund Transfer Agreement.

Special Note to Commercial (Business) and Organizational Account Holders: Many of the protections afforded through Regulation E do not apply to you. Furthermore, **It's*Me*247** online banking is designed with consumer accounts in mind. Therefore, ICCU recommends that you conduct your own risk assessment and evaluate your internal controls regarding online transactions and other account access methods. You may request to disable access to online banking or bill pay at any time by contacting the credit union.

Individualized Password & Username

During your initial login to **It's*Me*247** online access, ICCU asks you to create your own password. ICCU requires a complex password that includes any three of the following four options: upper case letter, lower case letter, number and special symbol. Ideally, it should be something you can remember and not write down. **It's*Me*247** will only allow three invalid password attempts before a password is disabled. If this happens, the member must contact the credit union to reset (after proper identification). This provides extra protection against unauthorized entry. Your password may be changed at any time while logged in to **It's*Me*247** by going to the *Info Center*, then selecting *Password* under *My Preferences*.

While **It's*Me*247** defaults to your account number as the username, ICCU recommends that you create your own, customized username to use during login instead of your account number. To create a new username, log in to **It's*Me*247**, go to the *Info Center*, and then select *Username* under *My Preferences*.

ICCU may verify a member's **It's*Me*247** username to assist with troubleshooting online banking login problems, but only after authenticating the member's identity by other means. ICCU will never ask for your online banking password and will never contact you by telephone, mail or email to request your login credentials.

Security Questions

During your initial login to **It's*Me*247** online access, ICCU asks you to establish three security questions in addition to your password. To log in successfully to **It's*Me*247** on future visits, you must correctly enter not only the correct username and password, but also the answer to one of these questions, asked at random. These questions may be changed at any time while logged in to **It's*Me*247** by going to the *Info Center*, then selecting *Security Questions* under *My Preferences*. If you click *I forgot my password* on the login page, you will be asked to answer all three of your security questions. If they are all answered correctly, we will know it is you and will allow you to specify a new password.

Timed Log Off and Disabled Due to Inactivity

While it is important that you always log out when your **It's*Me*247** visit is completed, ICCU has configured time-out values into **It's*Me*247** to protect your account information should your computer become unattended. **It's*Me*247** will timeout after 9 minutes of inactivity on transaction or settings pages and after 6 minutes on login and menu pages. Account history and research pages allow up to 12 minutes before timeout, while sales information and links allow 15 minutes. Applicable timeout values are displayed on each page of **It's*Me*247**.

To prevent unwanted, online account exposure, **It's*Me*247** passwords expire after 90 days of nonuse. Password resets expire after 24 hours if a login is not successfully completed. New accounts are disabled for online access if not activated within 7 days. In any of these situations, members must contact the credit union to reactivate.

Firewall

It's*Me*247 employs redundant, state-of-the-art firewall technology and hardened server configurations to block unauthorized entry and internet-based attacks. Segregated network architecture separates the online banking servers from systems that contain member data. Consequently, member data may only be exchanged between these systems following a successfully authenticated member request as described above. Furthermore, data exchanged with **It's*Me*247**does not include personal identifying information, such as social security number, birthdate, driver's license number, etc.

Encryption

It's*Me*247 employs 128-bit encryption. From the moment account information leaves your computer to the time it enters our system, all **It's*Me*247** online access and Bill Pay sessions are encrypted. This encryption turns your information into a coded

sequence with billions of possible variations, making it virtually impossible for unwanted intruders to decipher. **It's*Me*247** then applies the proper formulas to turn this code back into meaningful information to complete your transaction or setting request.

Look for a "closed-lock" icon in your browser (e.g. Microsoft Internet Explorer, Firefox, Safari or Chrome) or "https://..." to determine whether encryption is being used on any web page you are viewing. Any web address beginning with "https://..." indicates that the page you are viewing uses encryption. The "s" stands for "secured."

System Monitoring and Technology Updates

To ensure that **It's*Me*247** security measures continue to resist constantly evolving online threats, the system employs proven industry standards for technology to protect your account security. Furthermore, it is reviewed on an ongoing basis by expert security consultants and regulators, plus is monitored closely by network engineers.

Fraud Net for Bill Pay

CU*EasyPay, ICCU's online bill pay product, deploys an algorithm-driven technology to monitor all bill pay activity. It is designed to detect abnormal activity and prevent fraudulent payments. If a transaction is suspect, Fraud Net will alert key credit union personnel so that the activity can be reviewed prior to posting.

Additional Security Measures

ICCU's layered approach to online security extends beyond a unique username and password, challenge questions, 128-bit encryption, redundant firewalls and diligent monitoring. We have additional security measures that may be activated in response to certain activities or events. If we are suspicious of any online behavior, we may restrict online access to accounts or prevent certain types of transactions. These measures safeguard your identity and accounts. Further proof of identity may be required before online access is restored. If you are ever concerned about your account activity, please contact our member service department.

OnGuard Online | YOUR SAFETY NET™

7 PRACTICES FOR SAFER COMPUTING

1. **Protect your personal information.** *It's valuable.* To minimize your risk of identity theft, don't share your personal information unless you know how it will be used and protected. Don't reply to or click on links in any email asking for your personal information.
2. **Know who you're dealing with.** When shopping online, look for a seller's physical address and a working telephone number. Before downloading free software, read the fine print – some downloads come with spyware.
3. **Use anti-virus and anti-spyware software, as well as a firewall.** Update them all regularly; many update automatically. Look for anti-virus software that removes or quarantines viruses, and for anti-spyware software that can undo changes spyware makes to your system. Make sure your firewall is on and set up properly.
4. **Be sure to set up your operating system and Web browser software properly, and update them regularly.** Select security settings high enough to reduce your risk of being hacked. Make sure to regularly update your system with the latest patches.
5. **Protect your passwords.** Keep your passwords in a secure place, and don't share them on the Internet, over email, or on the phone.
6. **Back up important files.** If you have important files stored on your computer, copy them onto a removable disc and store it in a safe place.
7. **Learn who to contact if something goes wrong online.** Visit OnGuardOnline.gov and click on "File a Complaint" to learn how to respond if problems occur when you're online.

To learn more, visit OnGuardOnline.gov

STOP • THINK • CLICK™