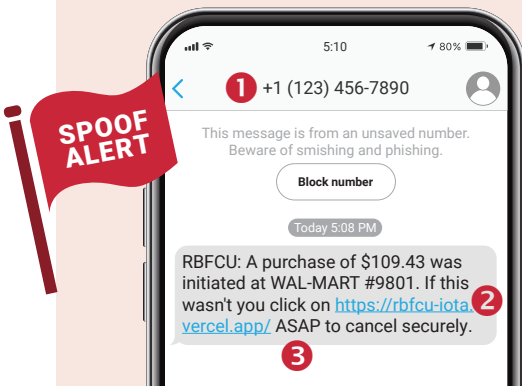


Learn how to identify valid RBFCU Text Alerts

With fraud on the rise, RBFCU wants to help protect you from potential scams. Fraudsters will try to trick you by posing as reputable companies in order to obtain your personal information, such as passwords or credit card numbers.



Red flags that could signal a fake RBFCU Text Alert include:



1 Phone number or email address

Fake messages usually originate from full phone numbers or email addresses instead of shortened phone numbers

2 Suspicious link

Fake website – RBFCU's website is rbfcu.org

3 Urgent call to action

Fake messages may alert you to an urgent situation and pressure you to take immediate action to resolve it, like sign in to the RBFCU website or make a transfer from your RBFCU account

Bonus Tip: Fake messages are usually unsolicited – meaning you didn't apply for an RBFCU loan, open an RBFCU account or contact RBFCU for assistance first

If you receive a text message that appears to be from RBFCU and meets the red flag criteria, do not respond to it or click any links. Send a screenshot of the text message to abuse@rbfcu.org, and then delete it.

Green flags that may indicate a legitimate Alert include:



1 Short code¹

RBFCU text messages usually originate from shortened phone numbers, also known as short codes

2 Text messages from RBFCU alerting you to fraud will never include links to websites²

Most text messages sent from RBFCU are sent after an action was taken on your account, like when you make a transaction, apply for a loan, open an account or contact us for assistance first

However, you may get an unsolicited text message from RBFCU alerting you to fraud, but beware: Fraudsters use this tactic, too! It's OK to call RBFCU to confirm it's a legitimate text before acting – we'd rather you be cautious

Remember: RBFCU and RBFCU employees will never initiate a phone call, email or text message to anyone – members or non-members – asking for your sign-in information, including usernames, passwords, security questions and answers, multifactor authentication (MFA) codes, MFA recovery codes and one-time passcodes (OTP), or other personal information, like account, credit card, debit card or Social Security numbers. Also, RBFCU employees will never need to sign in to your Online Banking account on your behalf. If someone contacts you claiming to be an RBFCU employee and asks you to approve a sign-in request for them, do not respond.

If you believe your account, username or password has been compromised, you should immediately contact RBFCU at 210-945-3300 for assistance. Additionally, members should monitor their accounts regularly and report any suspicious transactions.



For more information, visit rbfcu.org/security

¹ The format of RBFCU text message Alerts may vary based on the Alert type.

² Some RBFCU products and services, like MemberSafe, may use full-digit phone numbers to send text message alerts with links to members after they've taken action to apply for a product or enroll in a service. Insurance products are not deposits; not NCUA insured; not an obligation of Randolph-Brooks Federal Credit Union (RBFCU); and not guaranteed by RBFCU or any affiliated entity. Visit rbfcu.org/membersafe to learn more.
RN5594355

Online security is important for all RBFCU members



The security of your information is one of our top priorities. Here are some things you can do to help keep you and your family secure while online.



Use a complex password for your Online Banking account. A combination of 16 or more letters, numbers and symbols is most secure.



Change your Online Banking password on a regular basis, at least every 90 days.



Don't reuse your Online Banking username and password to sign in to other websites.



Enable multifactor authentication (MFA) for your Online Banking account. MFA provides an extra layer of security so a cracked password isn't as likely to compromise your account. Sign in, select the profile icon and then "Security Center" to set up MFA.



Never provide security questions and answers, one-time passcodes (OTP) or MFA codes to anyone. Your financial institutions and other companies will never ask you for these codes.



Avoid using public Wi-Fi networks, especially when accessing your Online Banking account. If you must use public Wi-Fi, install a virtual private network (VPN) app on your device.



Protect your computer and mobile device by updating your operating system, apps and antivirus software as soon as updates are available.



Turn off your computer when you're not using it.



Go to Online Banking at rbfcu.org or the RBFCU Mobile® app and tap the ? icon to find "Review Account Security" for measures you can take to keep your account even more secure.



Never open email attachments from people you don't know, and be wary of forwarded attachments – even from friends and family.



Use a lock screen on your phone to prevent thieves from gaining access to your accounts if your phone is lost or stolen.



Check an app's reviews before downloading it to your phone to help make sure it's trustworthy.



For more information, visit rbfcu.org/security