

How to Verify Emails, Text Messages and Links from Radiant Credit Union

Radiant Credit Union uses email, text messages and digital links to help members access and complete certain services. Because fraudulent messages can sometimes appear legitimate, it's important to verify communication before clicking a link or providing information.

Before You Click: Check Three Things

- 1. Sender**
Confirm that the email address or text message came from an official or recognized Radiant source.
- 2. Purpose**
Consider whether the message relates to something you requested, a recent interaction with Radiant or an activity you recognize.
- 3. Destination**
Before clicking, verify that the link directs you to Radiant's official website or a trusted service. On a computer, you can hover over a link before clicking to see its destination.

Radiant May Send Links For

Radiant may send links related to:

- Payment requests
- Secure document uploads
- Insurance verification
- Secure document signing
- Online banking services
- Fraud alerts requiring you to log in
- Fraud disputes

Radiant Will Never Ask You To

- Provide your password or one-time verification code by email, text or over the phone.
- Move money to a "safe" account.
- Act immediately to prevent your account from being closed.
- Install remote-access software at our request.

Never provide passwords, PINs, one-time passcodes or Secure Access Codes through a link or in response to an unexpected text or email.

Not Sure? Contact Radiant Directly.

If you aren't certain that a message came from Radiant, don't click the link or use the contact information contained in the message.

Instead:

- Open the Radiant Mobile App.
- Type radiantcu.org directly into your browser.
- Call the number on the back of your Radiant debit or credit card or use the contact information provided on Radiant's official website.

When in doubt: Sender. Purpose. Destination. Verify Before You Click.