Phishing and spoofing emails look like Members United emails and try to trick you into visiting a fake website and providing your personal account information. These emails may also ask you to call a phone number and provide account information.

Ways to identify phishing and spoofing emails include:

- **Links that appear to be Members United links but aren't.** If you place your cursor over a link in a suspicious email, your email program most likely shows you the destination URL. Do not click the link, but look closely at the URL: A URL that is formatted membersunited.fakewebsite.com is taking you to a location on fakewebsite.com. Just because "membersunited" is part of the URL does not guarantee that the site is an official Members United site.
- **Requests for personal information.** Members United emails will never ask you to reply in an email with any personal information such as your Social Security number, ATM or PIN.
- **Urgent appeals.** We will never claim your account may be closed if you fail to confirm, verify or authenticate your personal information via email.

- **Messages about system and security updates**. We will never claim the need to confirm important information via email due to system upgrades.
- **Offers that sound too good to be true.** We will never ask you to fill out a customer service survey in exchange for money, then ask you to provide your account number so you can receive the money.
- **Obvious typos and other errors.** These are often the mark of fraudulent emails and websites. Be on the lookout for typos or grammatical errors, awkward writing and poor visual design.

Thank you for bringing this suspicious activity to our attention. Members United takes any attempts to fraudulently use our brand or impersonate a credit union representative very seriously. Our team reviews all submissions; we will only reply to your message if we require additional information.