All One
CREDIT UNION
Partnership • Trust • Community

Is This Text Real or a Trap?

May 2025 | Issue No. 21

If you have a mobile phone, you've probably received texts from friends and family. If you've opted to receive texts from retailers, you get these too. But what do you do when you receive a text, and you question the source?

The answer matters because your response to a questionable text might keep you safe from a scammer – or lead you into a trap.

How Text Scams Work

Below is a simplistic example of how a spoofed message can be sent to you.

Step One: Threat actors find your phone number on the Dark Web or they generate your number with an auto-dialer tool.

Step Two: The scammer creates a message. Scam texts sound urgent to get victims to react without thinking – "invoice overdue" or "your account has been breached" are common rues.

Step Three: The scammer sends the text and hopes that you take the bait.

Prevention Tips

Don't reply to unexpected text messages. The text may push you to react quickly, but it's best to stop and think it through.

Never click links in unexpected messages. You might download malicious software (malware) that will compromise your device, and scammers often create real-looking websites to draw you deeper into the trap.

Don't assume a text from a known company or organization is legit. Double check by contacting the company. Don't use information from the text – get the phone number or email address from the company's website.

Filtering Unwanted Texts

There are ways to filter unwanted text messages or stop them before they reach you.

On your phone	Your phone may have an option to filter and block spam or messages from unknown senders.
Through your wireless provider	Your wireless provider might have a tool or service that lets you block calls and text messages. Check out ctia.org, a website from the wireless industry, to learn about options from different providers.
With a call-blocking app	Got to ctia.org for a list of call-blocking apps or search for an app online.

Take Action – Report Texts

- Forward spam messages to 7726 (SPAM). This helps your wireless provider spot and block similar messages.
- Report potential scams on either the Apple iMessages app or Google Messages app.
- Report potential scams to the FTC at Reportfraud.ftc.gov.

If you have lost money to a scam, reach out to the company that transferred the money right away to see if there's a way to get your money back. Then report the scammer at ReportFraud.ftc.gov.

If You're a Victim?

Immediately change any passwords you might have revealed. Consider reporting the attack to the Internet Crime Complaint Center, (https://www.ic3.gov), the police, and file a report with the Federal Trade Commission. (https://www.identitytheft.gov)

Getting Help

If you need help and have identified suspicious activity involving All One Credit Union, contact us immediately at 800-649-4646.