**CONTACT**

**Cherie Kistner**

**OCCU Corporate Communications**

**541.681.6016**

[CKistner@MyOCCU.org](mailto:CKistner@MyOCCU.org)

**Date: Aug. 31, 2023**

**Oregon and Washington credit union security experts warn about impostor texts – fraudulent texts impersonating credit unions**

**Eugene, Oregon –** One of the latest scams in cyberthieves’ bags of tricks is a text message designed to look like it’s from a well-known local credit union.

These impostor text scams are on the rise, racking up millions in losses and swamping credit union call centers. One Oregon credit union reports that during an active text scam, it can receive 200-400 calls about them per day.

The fraudsters use the name and logo of a credit union and blast a geographical area with thousands of these text messages aimed at tricking people into providing personal information. Anyone with a mobile number in the area can be a recipient whether or not they have accounts with that credit union. These texts are not an indication of a security breach or that member information has been compromised.

Text scams, also known as smishing, are particularly effective because people are more likely to glance at a text message and respond quickly, often while on the go. It is estimated that users read 98% of text messages and respond to 45%.

Security experts from Oregon and Washington-based credit unions want to educate consumers about these and other scams with tips on how to stay safe in our fast-moving digital world. These experts are available for interviews about this or any cyber-financial security issue. They include:

* + - Matthew Wilson, SVP Risk and Administration, OCCU (Eugene, OR), [MWilson@MyOCCU.org](mailto:MWilson@MyOCCU.org)
    - Jordan Lehrman, Chief Technology Officer, iQ Credit Union (Portland, OR/Vancouver, WA), [Jordan.Lehrman@iqcu.com](mailto:jordan.lehrman@iqcu.com)
    - Colleen Boccia, SVP Chief Marketing Officer, Columbia Credit Union (Vancouver, WA/Portland, OR), [ColleenB@columbiacu.org](mailto:ColleenB@columbiacu.org)
    - Rodney Beard, Information Security Officer, Rivermark Community Credit Union (Portland, OR and surrounding communities), [RBeard@rivermarkcu.org](mailto:RBeard@rivermarkcu.org).

\*\*For more information or to make interview arrangements with an expert in your area, contact one of the above directly or the sender of this release.

The article below is for your use as-written, with adaptations or as interview prompts with one the experts reference above.

# # #

**Fraudulent impostor texts: How to spot the latest texting scams and keep yourself safe**

Scammers are always trying to find new ways to extract your personal financial information to steal your money or your identity.

One of the latest scams is the fake text message that looks like it came from a well-known local credit union. The text messages look legitimate, often including the credit union’s logo and an official-looking link or phone number.

The scammers send these texts to every mobile phone number in a region. Anyone with a mobile number based in the same area as the credit union can be a recipient whether or not they have accounts with that credit union.

Because the texts are going to all mobile phones in a region, the texts are not indicators of a security breach at the credit union or that member information has been compromised. If you have a phone that receives text messages, you’re a target.

Text scams, also known as smishing, are particularly effective because people are more likely to respond to a text, often while on the go. It is estimated that users read 98% of text messages and respond to 45%.

Many consumers also have already caught on to phone or email scams that appear to be from reputable sources. As these avenues become less effective for cyber thieves, they are turning to text messages instead.

Fake text messages and similar scams cost victims more than $52 million in 2022 alone, with more than 300,000 complaints nationwide, according to the [FBI’s Internet Crime Complaint Center](https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf).

Keep reading to find out what you need to know, how to spot scams and how to protect yourself.

**How impostor text scams work**

The text messages usually sound urgent, indicating things like a suspicious transaction has occurred or that your account has been locked.

The message will include either a phone number that redirects to the fraudsters or a hyperlink to a fake website that looks very similar to the credit union mentioned in the text.

If you respond, the hacker will use your information to commit fraud or sell your stolen data on the dark web.

“Most impostor text scams invoke a temporal element that warns of negative consequences should you fail to respond or act quickly: your card is being shut off, fraudulent charges are pending, etc.,” said Matthew Wilson, senior VP of risk and administration for Eugene-based OCCU. “The messages usually include a link to click that will then prompt you for credentials, which then the malicious actor uses against you.”

**How to avoid falling for a smishing scam**

The key to sidestepping a scam is to stay alert and refuse to respond to any texts that are unexpected or otherwise feel “off.”

“If you’re unsure whether the message is legitimate, **take a deep breath** and call or visit the site or service in question manually — ideally, by typing the company’s exact URL,” Wilson says. “Be cautious and **reach out to the company from another source**, outside of the phone numbers or links provided in the suspicious message, to validate legitimacy.”

Here are a few things you should always keep in mind when reading or responding to text messages:

* Legitimate financial institutions will notcontact you via text message and ask you to provide login information such as passwords, codes or other credentials. In fact, you can safely assume that no reputable organization or service provider would ever do so. This is an essential security policy that all responsible organizations share precisely for the purpose of protecting you and your identity.
* When in doubt, go straight to the source. **Do not respond to the text message**.
  + If you do not have a relationship with the impersonated organization, delete the text and report it as spam.
  + If you do have a relationship with the impersonated organization, use another method to verify the status of your accounts — such as online banking or the mobile app or call the organization and ask whether it’s legitimate. It’s probably not.
* Do not respond to or click on links from anyone you don’t know or that are purportedly from an organization with whom you do not already have a relationship.

**What to do if you’ve been scammed**

If you’re involved in a scam, the first thing you need to do is give yourself a break. It’s not your fault — we all get caught unaware sometimes. The next thing you need to do is report it immediately. Contact your financial institution right away and ask about canceling fraudulent transactions and blocking future charges.

“If you are concerned that you’ve fallen victim to a social engineer using smishing methods, **don’t be embarrassed!**” Wilson says. “Get on the phone with your financial institution and let them know so that we can assist in monitoring your accounts for fraudulent transactions.”

The next step is to consider freezing your credit reports and notifying the [**Internet Crime Complaint Center**](https://www.ic3.gov/), Wilson adds.

Above all, be as wary of text messages as you are of email and phone spam. Social engineers may be clever, but they’re not that hard to spot if you stay on the lookout.