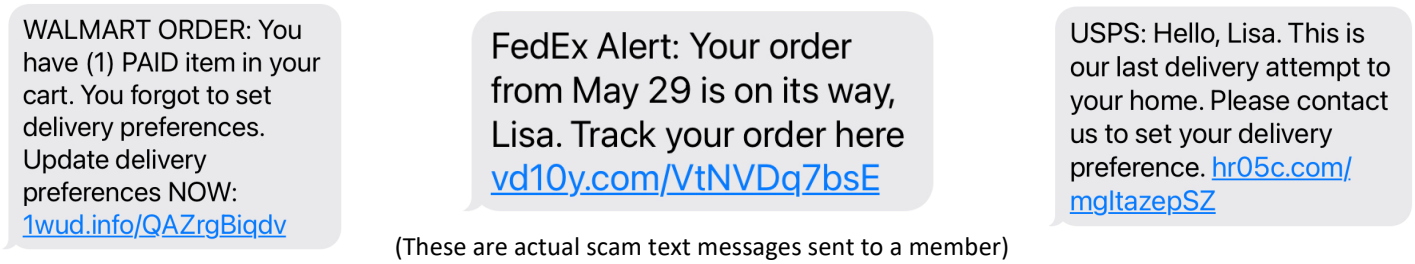
Fake Purchase Scams



(These are actual scam text messages sent to a member)

WARNING: Scam Targeting Consumers

Several Members have reported a new scam tactic that attempts to take over devices as well as coerce members into withdrawing funds from their accounts.

Fake purchase scam

The scam goes something like this:

The member receives an email or text stating that their purchase is scheduled to be delivered that day. Typically, the dollar amount is usually high—something like $899. The communication advises the member to contact the merchant if they did not make this purchase at the number provided in the communication. When calling the number, the operator will answer as the merchant's Customer Service department. The member will be told that their account has been compromised—both their merchant account and their CFCU account.

They will ask you to download an app in order to re-establish your merchant account. While it may be a legitimate application, the scammer uses it to gain control of your device including personal information, usernames and passwords. It is not required, nor necessary, to download any app other than the merchant's official app.

Next they will tell you that they are connecting you with a fraud specialist with CFCU. The individual often knows the last few transactions to your card or account, which make them seem to be a legitimate representative from the credit union. That individual then advises the member to withdraw a significant amount of cash from their CFCU account and either: 1) deposit it at a non-CFCU ATM or 2) purchase gift cards and send them. They will advise you to avoid going to your local branch due to suspected internal fraud.

Sometimes there is a link in the email or text for the member to click on to resolve the issue. After clicking a phishing link, the sender knows the member is a valid target. The attacker receives some basic data like approximate location, devise statistics and any information voluntarily provided. A phishing link may download malware. If a member has clicked on a link they should immediately take precautionary measures.

If you clicked on a phishing link, it is **critical** to stop interacting with the page and delete any downloaded files. Search for the intended target site using a search engine. Compare the legitimate web address and content to the phishing site. Watch for suspicious account activity, calls or texts.

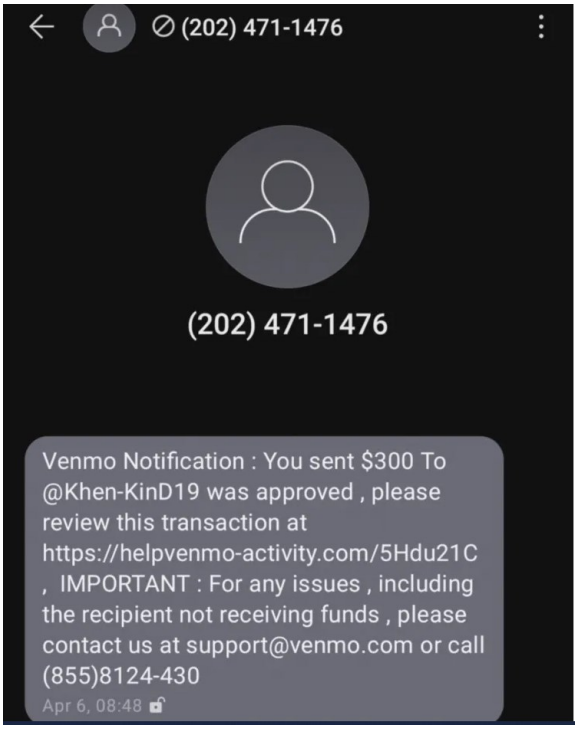
Now is the perfect time to be super suspicious and selective about all your online activities.

Can my smartphone be hacked by clicking on a phishing link?

A smartphone can be hacked by clicking a link found in an email, text message, or software. Tapping or opening a phishing link can expose users to automatically downloaded malware. Sometimes, the malicious link may redirect a user to a website or application controlled by hackers designed to collect user information or infect a mobile phone.

A cybercriminal doesn't need to obtain your smartphone to infect it with malware. If your phone is connected to the internet, hackers can infiltrate your device through phishing links. Sometimes, the messages can seemingly come from legitimate companies or reputable organizations as a notice about their services or apps. Clicking or tapping on these phishing links can open a pathway into your smartphone.

Can you identify the 5 suspicious parts that should set off alarms?



1. **Hook:** Many people would be worried about losing $300 unexpectedly.
2. **Curiosity:** The text doesn't say who the user is, but the transaction was approved.
3. **Urgency:** "Venmo" wants the member to review the "transaction" (picture me using air quotes) for any problems. The attacker legitimized the message by using the correct support email and phone.
4. **Copy-Cat Link:** The link has the word Venmo, but it's clearly not help.venmo.com (the correct URL).
5. **Bad Formatting:** Companies the size of Venmo ensure their notifications are well-formatted.
    a. The grammar is incorrect.
    b. The toll-free phone number has the dash in the incorrect place, not following the formatting of US or Canadian telephone numbers.
    c. There are odd spaces before the commas and colons.

It is also possible that the text message originates from an out-of-service or disconnected phone number, making it unwise to call it.

Signs this is a scam

Unsolicited communications

Have you signed up for text or email alerts for purchases from this merchant?

Transferring your call to your financial institution

Merchants do not have direct connection to your financial institution. If they tell you they can transfer your call to your financial institution, it is likely a scam.

Directing you to download an app

If they advise you to download any app other than their primary store app, it is likely a scam.

Asking you to withdraw funds

If you are asked to withdraw cash and deposit it to another financial institution or purchase gift cards, it is absolutely a scam.

Telling you to avoid branch employees

If they tell you to avoid local credit union employees, it is a scam.

What to do if you get a suspicious text or email

Check your merchant account

Log in to your merchant account **directly** from your mobile app or the store's website. Don't rely on links in texts or emails which can be faked.

Review your order history to see if there is an authorized purchase. If there is, contact the merchant directly at their official customer service phone number, email, or chat.

Check your credit and debit card history

Log in to your financial institution account(s) to check for unauthorized charges. If you have an unauthorized charge contact your financial institution by phone or chat to dispute the charges.

Steps to protect your accounts

Never download unfamiliar applications

Always download apps from your device's app store or directly from the merchant's site.

Never call the number provided in the text or email

Look up the merchant's number and dial it directly to ensure you are being connected to the merchant and not a scammer. Always contact Cheney Federal Credit Union personally. We'll be happy to review the scenario with you to identify and resolve fraudulent activity.

Set Alerts on the merchant's site

Set alerts on the merchant's site so you know when purchases are made. This can also help you become familiar with what a legitimate notice from the merchant looks like (though scammers can often replicate them well).

Guard your card

Enroll in Cheney Federal Credit Union's eAlerts! You can learn more at CFCU Convenience : Cheney Federal Credit Union (cheneyfcu.com) ; cheneyfcu.com/for-your-convenience/

Set alerts on your accounts

Sign up for and actively use mobile and online banking. You can set alerts for activity to ensure you're immediately aware of any new transactions posted to your accounts.

Update and strengthen passwords

It's a good idea to update passwords often and use strong, hard to guess passwords.

Don't share personal information on social media

Many seemingly innocent interactions are actually intended to gather information that could be used to compromise your accounts, such as:

- Your first concert
- Your first car
- The last purchase you made
- Your favorite food

At Cheney Federal Credit Union, we're always here to help! If you suspect any suspicious activity please give us a call and we'll work with you to identify whether or not it's a scam and, if necessary, resolve any fraudulent activity on your CFCU accounts.