Reports of financial aid scams are on the rise this holiday season, and Chico State students are being targeted by threat actors who have been stealing personal banking information by promising funds through a fraudulent “financial aid relief” grant. While Chico State’s cybersecurity infrastructure catches and quarantines the majority of these messages, some of these threat actors succeed at their phishing attempts by quickly moving the conversation to another communication medium, such as a phone call, Zoom, or personal email.

Please remain vigilant about identifying these scams and watch out for the following red flags that signal you are being targeted by a threat actor:

- Many threat actors pretend to be from Chico State, but will give a department name that does not exist. Always verify information you receive on the official Chico State website.
- Chico State campus will be closed from 12/22/23 through January 1. Do not call or text any phone number claiming to be from “financial aid relief” during that time, even if the email is sent from a Chico State email address, as Chico State staff will be off duty during winter break.
- Be leery of job offers that sound too good to be true, such as remote work offering compensation for working very few hours a week. Students who have been responding to this scam have been contacted by an agent who has asked for their personal email in order to take the phishing scam offline, where Chico State technicians can no longer detect their fraudulent activities.
- Do not trust phone numbers that you see in emails or texts claiming to be Financial Aid Relief/Award notices. Always go directly to the official Chico State website and look up departments, contacts, and phone numbers yourself.
- Ignore text messages pretending to be from Chico State ITSS (Information Technology Support Services) claiming that your Microsoft Outlook account will be terminated if you do not respond.
- If you suspect that your campus email received a fraudulent message, immediately report the message using the PhishAlert button within your Outlook client and never correspond with the threat actor. More information about the PhishAlert button can be found on our Knowledge Base.
- If you have already engaged with a threat actor and feel you may be a victim of fraud, contact the University Police Department (UPD) by calling (530) 898-5555.

Division of Information Technology
California State University, Chico

https://www.csuchico.edu/it