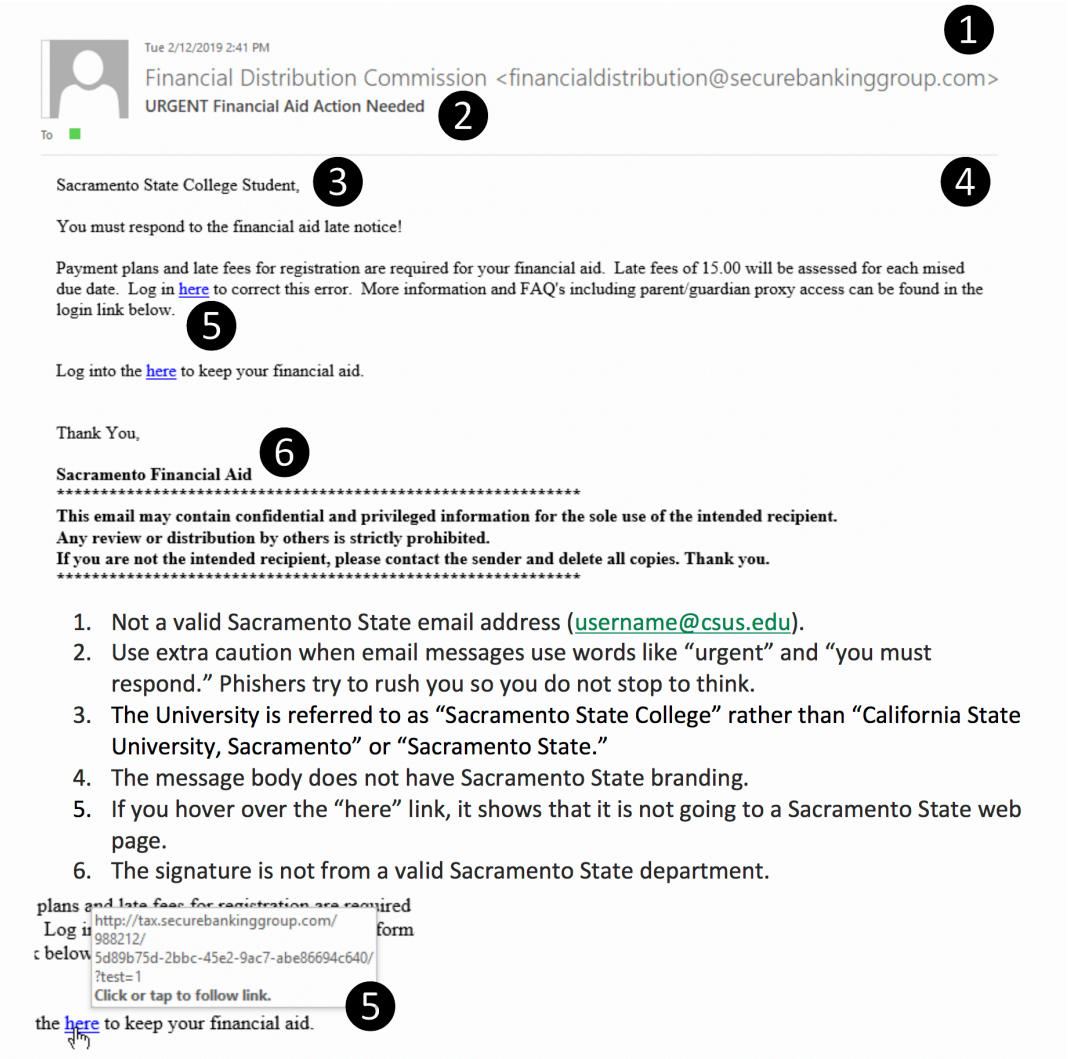
Financial Aid Phishing Awareness Campaign

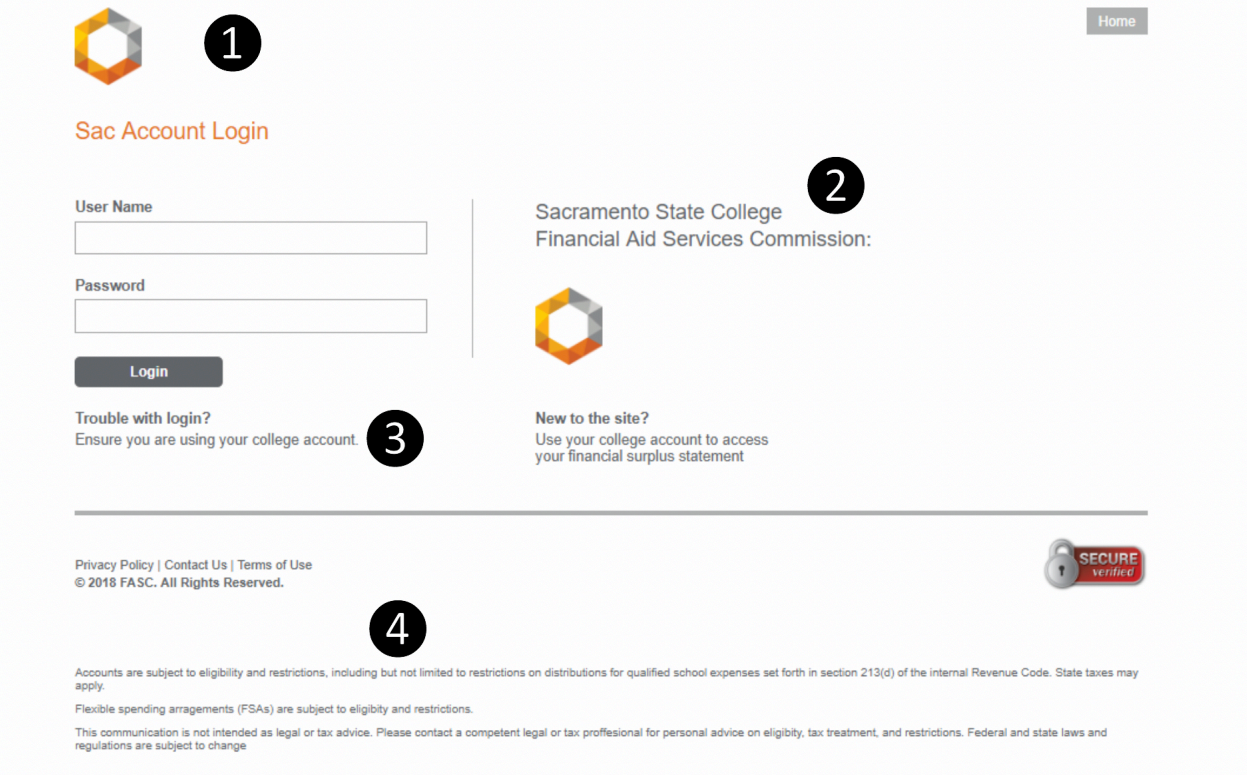
On February 19, 2019, Student Affairs and IRT teamed up to send a Cofense PhishMe training email to all students. Why? The U.S. Department of Education has been reporting an increase in phishing attempts aimed at stealing credentials to gain access to student financial aid awards.

How did we do?

Below is a graphic of the simulated phishing email sent to students, with call-outs to alert you to the items that can help you identify a real phishing email. Scroll down for the full results.



SIMULATED PHISHING EMAIL SENT OUT.



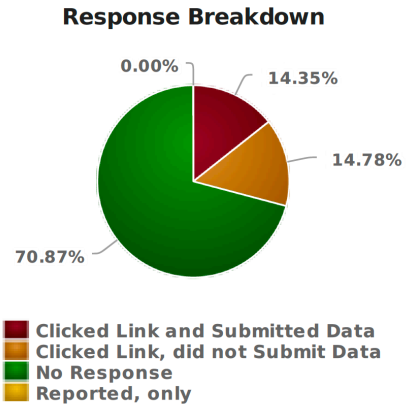
1. If you click on the click, it will direct you to an unfamiliar page. The logo and title of the page do not match My Sac State.
2. The University is referred to as "Sacramento State College" rather than "California State University, Sacramento" or "Sacramento State." The Financial Aid Services Commission is not a legitimately named institution.
3. It requires you to log in using your "college account," rather than specifying your "SacLink Username" or simply "Username" as on the legitimate Sacramento State login page.
4. There are misspellings and grammatical errors in the fine text, such as "arragements."

Results of the Phishing Simulation

Of 36,051 recipients, 10,502 (29%) students clicked the link in the test phishing email. 5,174 (14.35%) of students went further and gave their login credentials on the second screen. If this had been a real phishing email, you can imagine the type of damage that could result.

Summary Report

Scenario Name:	2019 February All Student - Financial Aid Campaign
Unique Recipients:	36,051
Emails Delivered:	36,051
Emails Bounced:	0
Clicked, did not submit:	5,328
Clicked Link and Submitted Data:	5,174
Started:	Tue February 19, 2019 at 10:00 AM
Ended:	Sun February 24, 2019 at 10:00 AM
Duration:	5 days
Scenario Type:	Data Entry



RESULTS OF THE PHISHING SIMULATION FOR STUDENTS PIE CHART

What is Phishing?

Phishing emails are designed to steal your identity. They can look very official, with familiar logos or messaging, and ask you to click links to confirm or update information such as logins, account numbers, or other personal information. You can usually identify them because they convey urgency, make claims or threats about the security of your account, or just seem suspicious.

Why PhishMe Training?

1. To protect and educate. PhishMe training is designed to help protect and educate, not to trick you. Not to worry, results of this training are kept confidential.
2. Knowledge is power. The simulated emails provide hands-on experience in what a phishing email looks like. If you click a link in one of these simulated phishing emails, you'll instantly see that it was a training exercise. Educational materials will help improve your 'phish finding' abilities.

Future Campaigns

We hope this campaign helps to protect you and campus data by improving phishing awareness and leading to fewer compromised accounts. Through Cofense Phishme, we will periodically send additional campaigns to help increase awareness.

If you need assistance or have any questions, please contact the IRT Service Desk Team at servicedesk@csus.edu, (916) 278-7337, or drop by at AIRC 2005.

Have feedback on these phishing awareness campaigns? Email iso@csus.edu.