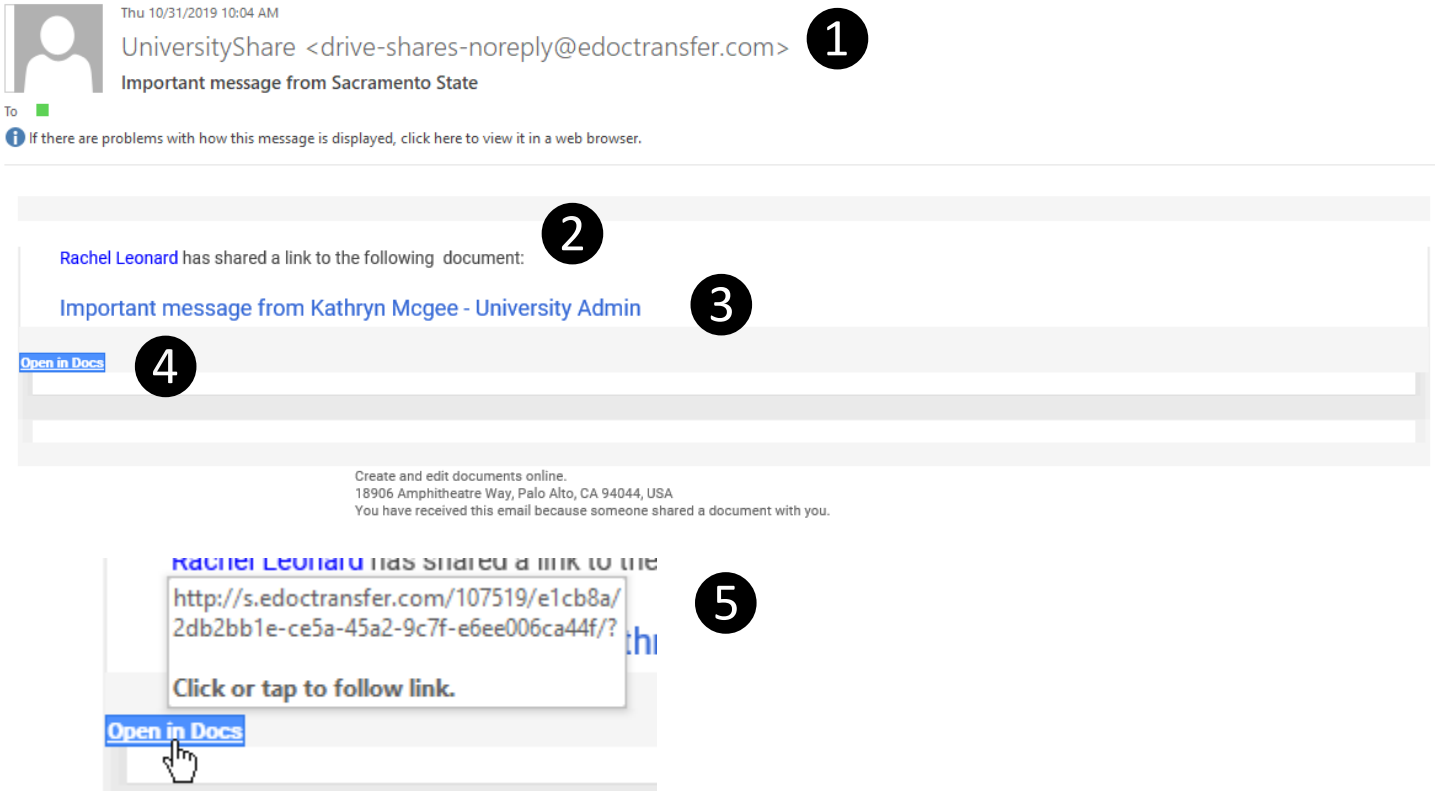
Fake Shared Document Phishing Awareness Campaign – October 2019

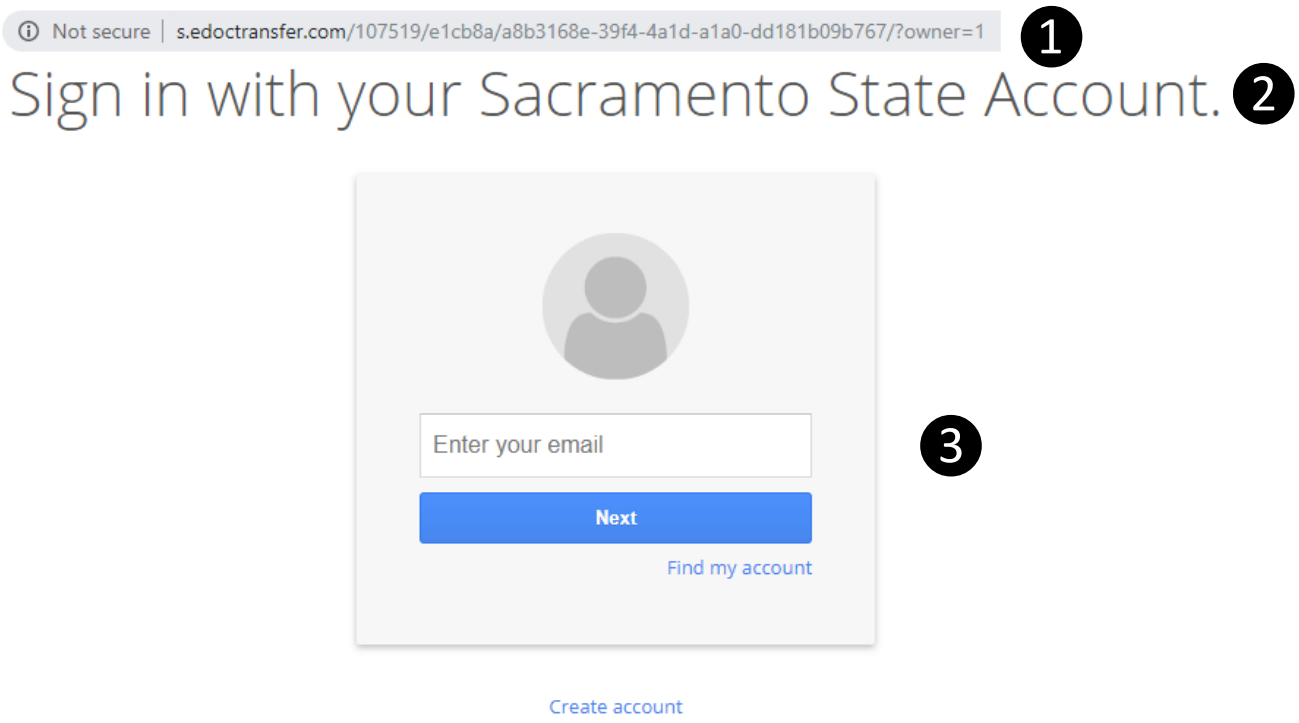
On October 31, 2019 IRT sent Cofense PhishMe training emails to Faculty, Staff, Auxiliary Employees, and Students. Why? Phishing email messages are the number one security breach for organizations. They account for 91% of all breaches. The messages and the education page that accompanies them, are meant to teach the Hornet family how to avoid real phishing scams.

How did we do?

Below is a graphic of the simulated phishing email sent to students, faculty, staff, auxiliary employees, and 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.



1. Not a valid Sacramento State email address (username@csus.edu).
2. Message was not send by an actual Sac State employee.
3. Do you recognize the name the message if from? If not, don't open the message. If so, verify with the sender that they sent the message.
4. Generic "Docs" branding. Even if actual branding was used, you still need to use caution.
5. If you hover over the "Open in Docs" link, it shows that it is not going to a Sacramento State web page.



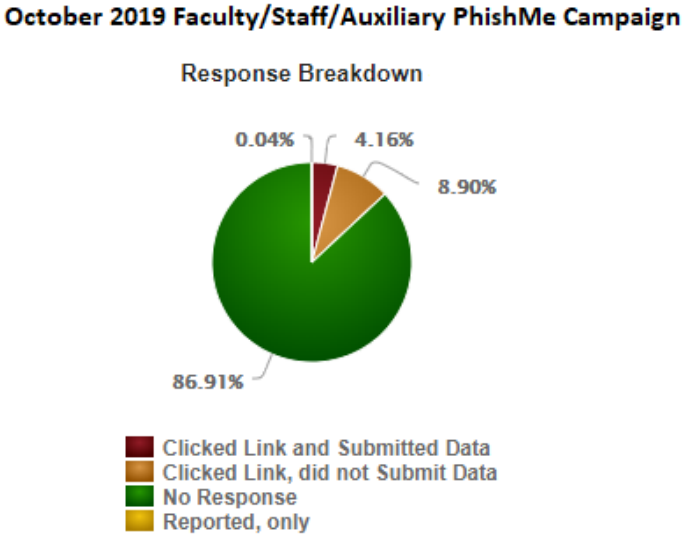
1. The URL for the page is http://s.edoctransfer.com/ and not our branded https://idp.csus.edu/idp/profile/cas/login?execution=e1s1 page.
2. The site is not a Sacramento State site but is asking you to use your Sacramento State account.
3. Use extra caution when a page asks for your username and password. Check the page out carefully to ensure it is a legitimate site.

Results of the October 2019 PhishMe Faculty/Staff/Auxiliary Phishing Simulation

Of 4,640 recipients, 606 (18.06%) clicked the link in the test phishing email. 193 (4.16%) 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.

606 of 4,640 Users Found Susceptible to Phishing

Unique Recipients:	4,640
Clicked Link, did not Submit Data:	413
Clicked Link and Submitted Data:	193
Reported, only:	2

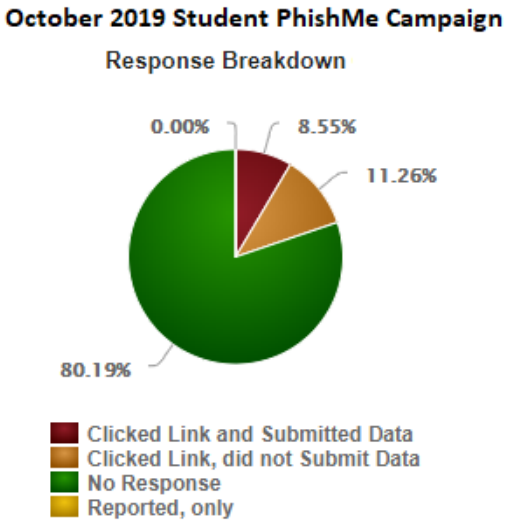


Results of the October 2019 PhishMe Student Phishing Simulation

Of 39,770 recipients, 7,877 (19.81%) clicked the link in the test phishing email. 3,400 (8.55%) went further and gave their login credentials on the second screen.

7,877 of 39,770 Users Found Susceptible to Phishing

Unique Recipients:	39,770
Clicked Link, did not Submit Data:	4,477
Clicked Link and Submitted Data:	3,400



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.