Financial Aid Phishing Awareness Campaign – February 2020

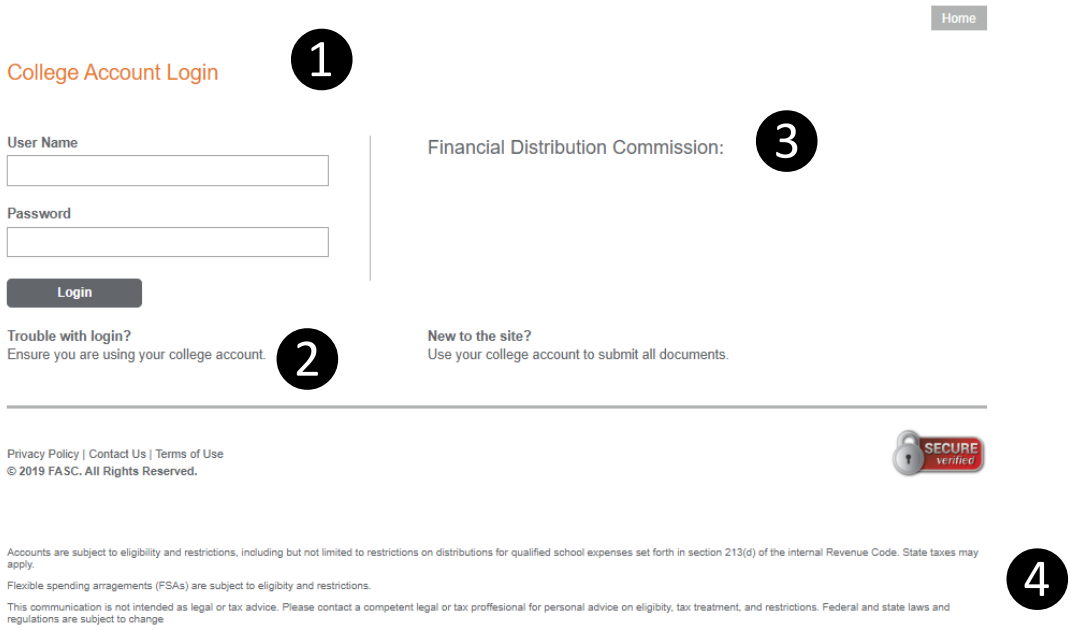
On February 26, 2020 IRT sent Cofense PhishMe phishing simulation email messages to all students. Why? The U.S. Department of Education has reported an increase in phishing attempts aimed at stealing credentials to gain access to student financial aid awards. The messages and the education page that accompanies them, are meant to provide awareness about this serious phishing threat and to teach the Hornet family how to avoid real phishing scams.

How did we do?

Below are graphics of the simulated phishing email sent to all students and the log in page that was displayed when clicking the link in the email. The graphics contain call-outs to the items that help identify a phishing message. The results of the campaign follow the graphics.

1. The message was not sent by a Sac State employee or department. The sender email address is not a valid Sacramento State email address (username@csus.edu).
2. Use extra caution when email messages use words like “urgent” and “you must respond.” Phishing scammers try to rush you so you do not stop to think.
3. The line, “You have not responded to our request!” is demanding, pushy, and not professional.
4. If you hover over the “here” link, it shows that it is not going to a Sacramento State web page.
5. The message does not contain official Sacramento State branding. Even if actual branding was used, you still need to use caution because this can be spoofed, but not containing any branding is a tip off.
6. The message is signed by “Financial Distribution” which is not a Sacramento State department.

Those who clicked the link in the email were presented with the following web page.



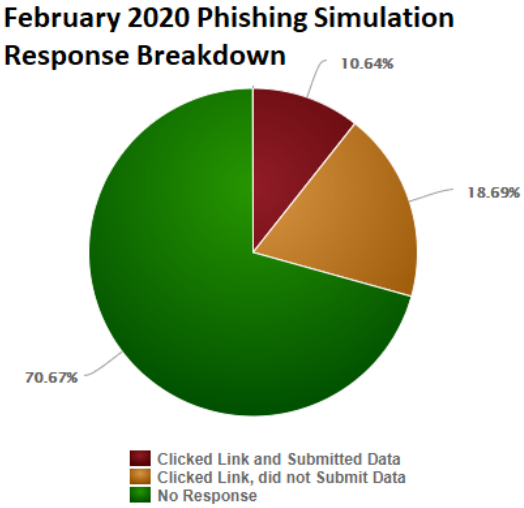
1. The page does not contain official Sacramento State branding. Similar to an email, even if actual branding was used, you still need to use caution because this can be spoofed, but not containing any branding is a tip off.
2. In addition to the lack of branding, the site requires you to log in using your "college account," rather than expressly mentioning Sacramento State or SacLink. This is another tip off that it is not a legitimate Sacramento State web site.
3. The "Financial Distribution Commission" is not a Sacramento State department.
4. There are misspellings and grammatical errors in the fine text, such as "arragements."

Results of the February 2020 PhishMe Student Phishing Simulation

Of 38,233 recipients, 11,215 (29.33%) clicked the link in the test phishing email. 4,068 (10.64%) went further and gave their login credentials on the second screen.

11,215 of 38,233 Users Found Susceptible to Phishing

Unique Recipients:	38,233
Clicked Link, did not Submit Data:	7,147
Clicked Link and Submitted Data:	4,068



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.