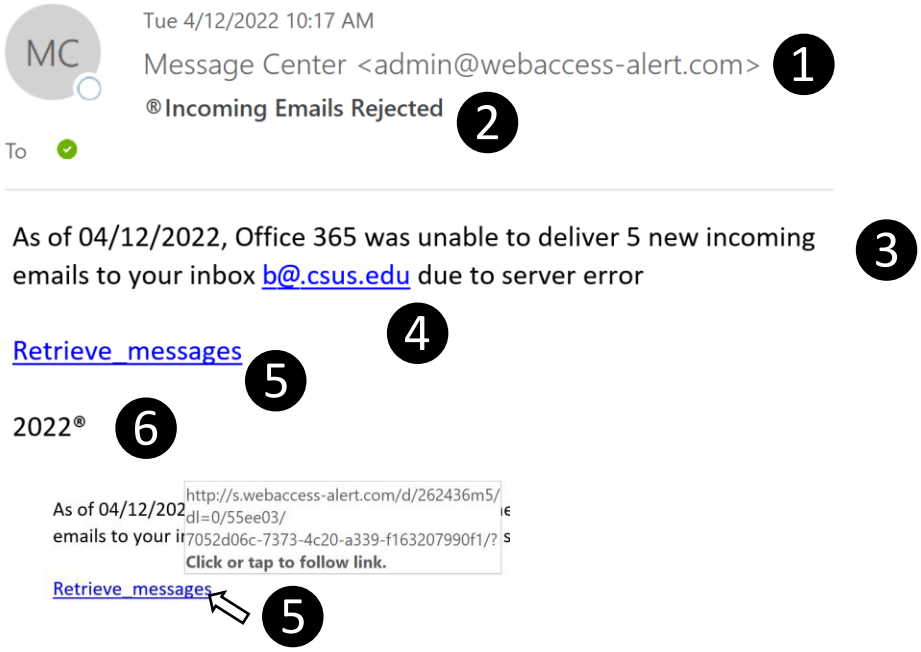
On April 12, 2022 the IRT Information Security Office sent Cofense PhishMe phishing simulation email messages to all faculty, staff, and students. Why? Phishing messages account for the over 90% of security breaches. Many cyber security agencies such as the FBI and the Cybersecurity & Infrastructure Security Agency (CISA) recommend sending phishing simulation campaigns as part of awareness efforts to help reduce the number of breaches. The messages and the education page that accompanies them are meant to provide awareness to the campus community about the seriousness of phishing threats and 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 all faculty, staff, and students. The graphic contains call-outs to the items that help identify a phishing message. The results of the campaign follow the graphics.



1. Check email addresses thoroughly to ensure they match the agency they are claiming to be associated with. Scammers use many addresses including @gmail.com, @yahoo.com, etc. Email addresses can be spoofed but when they are not, it is a real tip off. Sacramento State email addresses end with @csus.edu.
2. Use extra caution when email messages have a sense of urgency. They will use exclamation marks or use words like “rejected” and “you must respond.” Phishing scammers try to rush you so you do not stop to think.
3. The message language is vague and poorly worded.
4. Sometimes phishing scammers try to establish legitimacy by using your email address in the message. This is easy for them to automate. Do not let that trick you.
5. The link is very suspicious, and if you hover over the link, it shows where the link will actually go. This one points to a suspicious site.
6. Check the signature line in messages. This one is very odd.

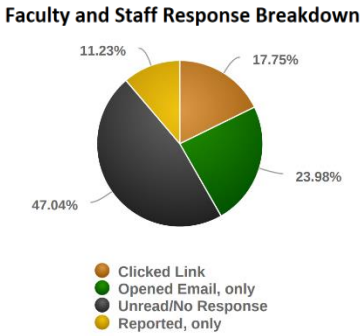
Results of the April 2022 Phishing Simulation

Results of the April 2022 Faculty and Staff Phishing Simulation

Of the 5,363 recipients, 952 (17.75%) clicked the link in the test phishing email. 602 (11.23%) used the Report Phishing Button to report the message.

952 of 5,363 Found Susceptible to Phishing

Unique Recipients:	5,363
Clicked Link:	952
Reported Only:	602

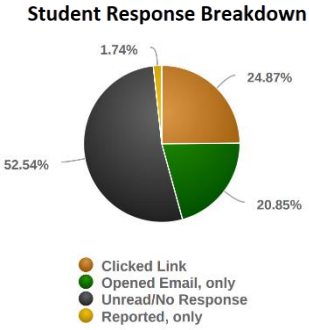


Results of the April 2022 Student Phishing Simulation

Of the 37,644 recipients, 9,361 (24.87%) clicked the link in the test phishing email. 655 (1.74%) did not click and used the Report Phishing button to report the message.

9,361 of 37,644 Found Susceptible to Phishing

Unique Recipients:	37,644
Clicked Link:	9,361
Reported Only:	655



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.

Learn more at csus.edu/phishing.

Why PhishMe Training?

1. To protect and educate. Cofense 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 or (916) 278-7337.

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