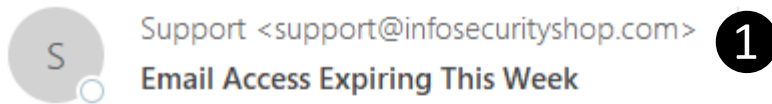


On October, 17 2023, IRT sent Cofense PhishMe phishing simulation email messages to all Students, Faculty, Staff, and Auxiliaries. Why? Ninety-one percent of security breaches are caused by phishing messages.

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.

Student, Faculty, Staff, and Auxiliary Campaign

This campaign mimicked a credential phishing scam that is currently trending. Credential phishing scams are often sent to our campus and include a fake log in page to steal passwords. This campaign was targeted to spread awareness about this type of scam. Below is a graphic of the simulated phishing email sent to all students, faculty, staff, and auxiliaries. The graphics contain call-outs to the items that help identify a phishing message. The results of the campaign follow.



Sacramento State Support-Desk

Hello bi@csus.edu **2**

Your Sign in credentials for (bi@csus.edu) are set to expire on: Friday, October 20, 2023. **3**

4

Click below to continue to access Mailbox



Sacramento State Security Team **6**



1. The message was not sent by a Sac State or CSU employee or department. The sender email address is not a valid Sacramento State or CSU email address (username@csus.edu or username@calstate.edu). Please note that even if the email is from and @csus.edu address, ensure the content matches the role that person has at the university and that there are no other issues with the message. Messages can be sent from compromised accounts and addresses can be spoofed.
2. The greeting is to an email address and not addressed to the person. Including the receiver's email address is a common trick that seems to add legitimacy but it is an easy addition.
3. The message does not have any specific information and the message does not contain official Sacramento State or CSU 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.
4. The expiration date is only a few days from when the message was sent. Our campus sends reminders that start 90 days in advance of an account expiration.
5. If you hover over the hyperlink, it shows that it is not going to a Sacramento State or CSU web page.
6. The message signature claims it is from a Sacramento State organization but does not include telephone or other information that can be used to verify the message.

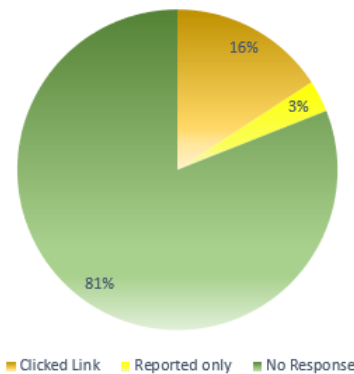
Results of the October 2023 Phishing Simulation

Student Results of the October 2023 Phishing Simulation

Of the 42,561 recipients, 6,735 (15.8%) clicked the link in the phishing simulation email. 1,357 (3.1%) used the Report Phishing Button to report the message.

6,735 Found Susceptible to Phishing

Unique Recipients:	42,561
Clicked Link:	6,735
Reported only:	1,357

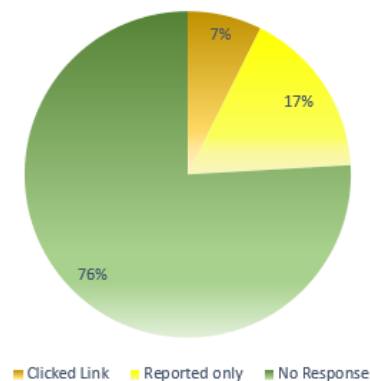


Faculty, Staff, and Auxiliary Results of the October 2023 Phishing Simulation

Of the 5,520 recipients, 406 (7.3%) clicked the link in the phishing simulation email. 924 (16.7%) used the Report Phishing button to report the message.

406 Found Susceptible to Phishing

Unique Recipients:	5,520
Clicked Link:	406
Reported only:	924



What is Phishing?

Phishing emails are designed to steal your identity, take your money, or gain access to data to sell or take for ransom. 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.

