


On February 20, 2024 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.

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 phishing scam that is currently trending. This campaign was targeted to spread awareness about scams that mimic Teams shares. 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.

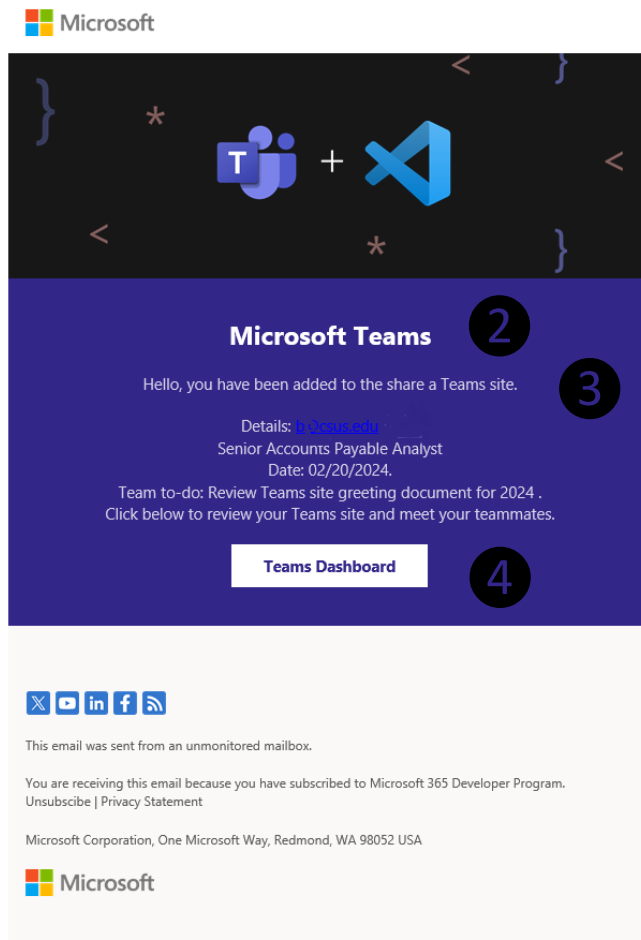
Hello b@csus.edu, you have been added to a Sac State team.

 Administrator <leah.mason@socialsmp.com>
To:  G

1

 Reply  Reply All  Forward 

Tue 2/20/2024 10:00 AM



Microsoft

Microsoft Teams

Hello, you have been added to the share a Teams site.

Details: [View Details](#)
Senior Accounts Payable Analyst
Date: 02/20/2024.
Team to-do: Review Teams site greeting document for 2024 .
Click below to review your Teams site and meet your teammates.

Teams Dashboard

This email was sent from an unmonitored mailbox.

You are receiving this email because you have subscribed to Microsoft 365 Developer Program.
[Unsubscribe](#) | [Privacy Statement](#)

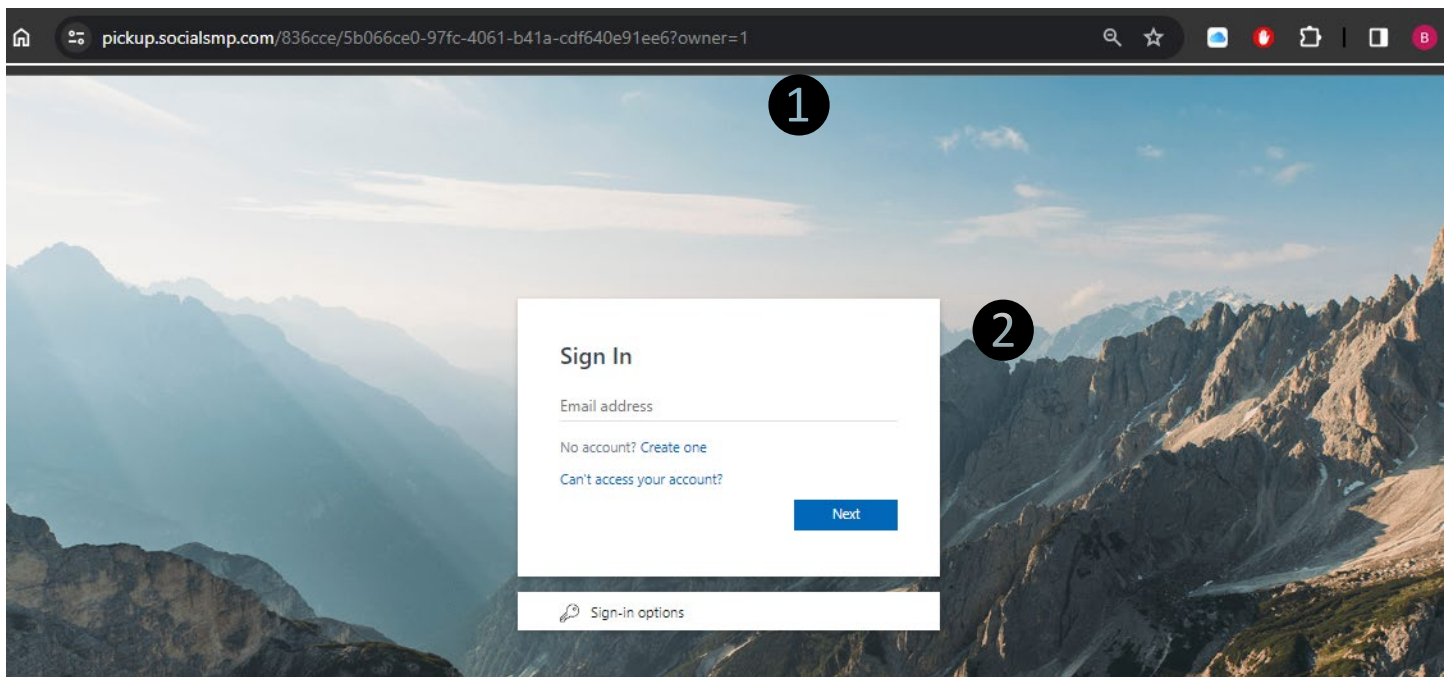
Microsoft Corporation, One Microsoft Way, Redmond, WA 98052 USA

Microsoft

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 email graphic mimics a Microsoft Teams share. Pay close attention to the name of the Team and who is claiming to share the Team with you.
3. The message contains a grammatical error.
4. When you mouse over the link, it points to a web site that is not a Sac State or Microsoft web site.



The Log In Page Displayed if the Link Was Clicked



1. The web address is not a Sac State or Microsoft 365 address.
2. The page mimics, but does not match an official Microsoft 365 log in page. Similar to an email, even if actual branding is used, you still need to use caution because this can be spoofed, but not containing any branding is a tip off.

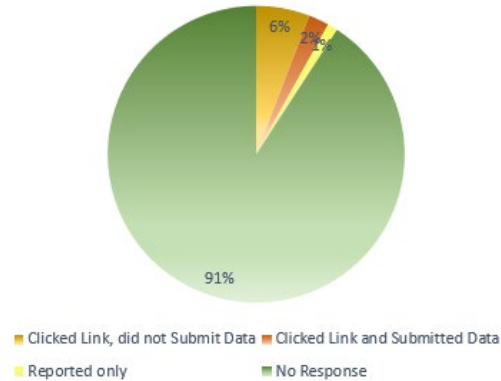
Results of the February 2024 Phishing Simulation

Student Results of the February Phishing Simulation

Of the 42,561 recipients, 3,433 (8%) clicked the link, 956 (2.2%) submitted data, and 467 (1%) used the Report Phishing button to report the message.

3,433 Found Susceptible to Phishing

Unique Recipients:	42,561
Clicked Link Only:	2,477
Clicked Link & Submitted Data:	956
Reported only:	467

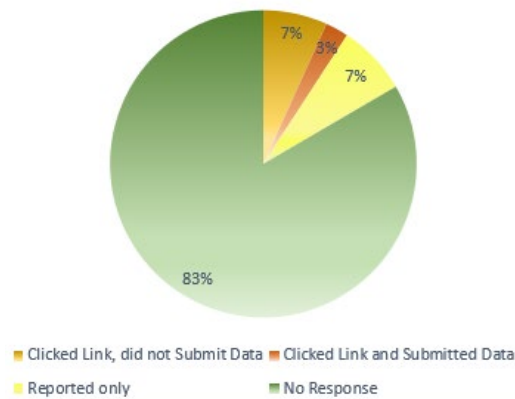


Faculty, Staff, and Auxiliary Results of the February 2024 Phishing Simulation

Of the 5,520 recipients, 373 (9.2%) clicked the link, 135 (2.4%) submitted data, and 409 (7.4%) used the Report Phishing button to report the message.

508 Found Susceptible to Phishing

Unique Recipients:	5,520
Clicked Link Only:	373
Clicked Link & Submitted Data:	135
Reported only:	409



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.

