

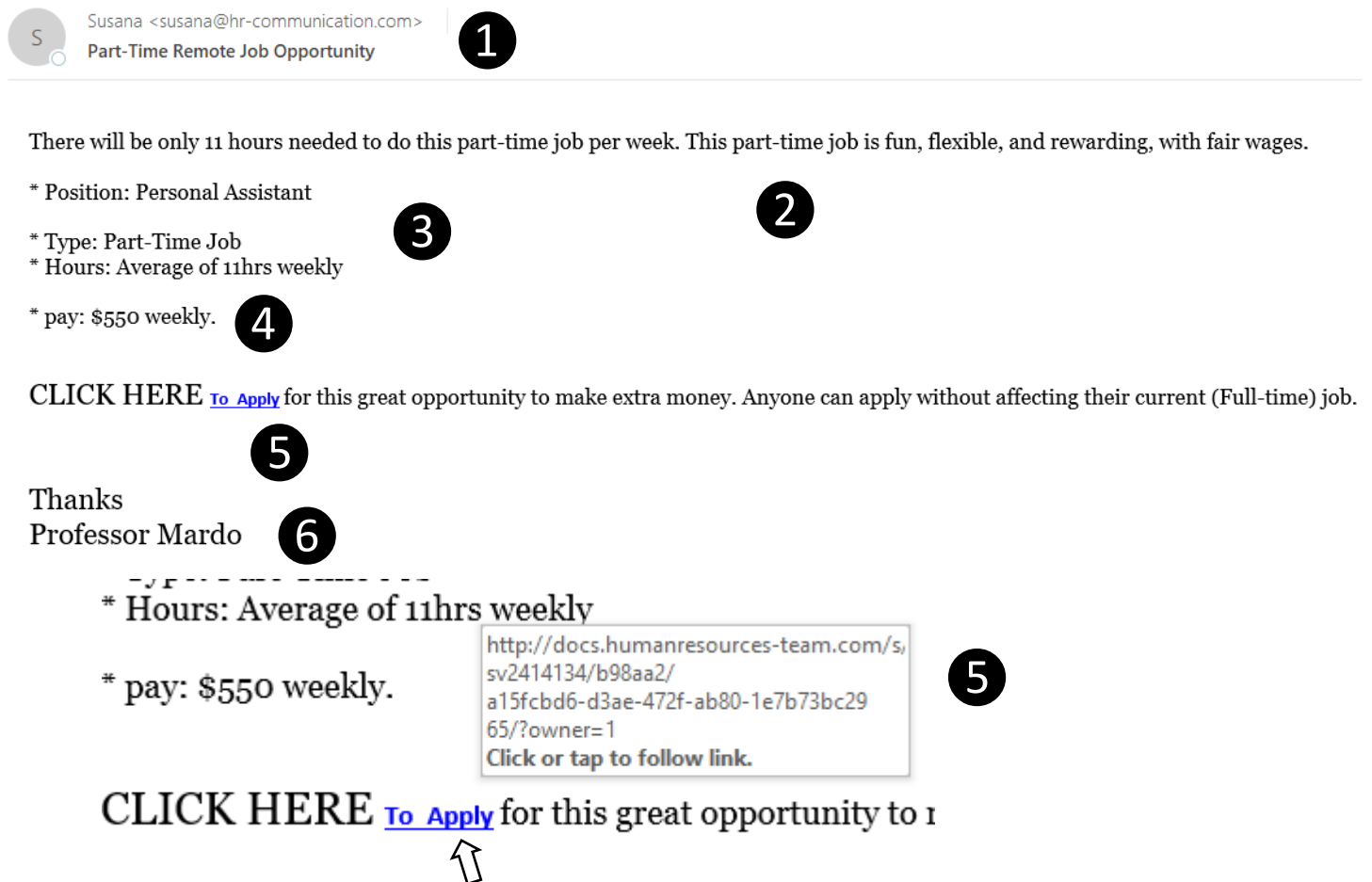
On September, 2023, IRT sent Cofense PhishMe phishing simulation email messages to all Students and all Faculty, Staff, and Auxiliaries. Why? Ninety-one percent of security breaches are caused by phishing messages.

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.

We sent students a separate campaign than we did to faculty and staff to provide awareness pertinent to those groups.

Student Campaign

This campaign mimicked a part-time job scam that is similar to one sent to the campus. Part-time job scams continue to be sent to our campus. This campaign is targeted to spread awareness about this type of scam. Below is a graphic of the simulated phishing email sent to all students. The graphics contain call-outs to the items that help identify a phishing message. The results of the campaign follow.



1 Susana <susana@hr-communication.com>
Part-Time Remote Job Opportunity

There will be only 11 hours needed to do this part-time job per week. This part-time job is fun, flexible, and rewarding, with fair wages.

* Position: Personal Assistant **2**

* Type: Part-Time Job **3**

* Hours: Average of 11hrs weekly

* pay: \$550 weekly. **4**

5 CLICK HERE [To Apply](#) for this great opportunity to make extra money. Anyone can apply without affecting their current (Full-time) job.

Thanks

Professor Mardo **6**

* Hours: Average of 11hrs weekly

* pay: \$550 weekly. **5**

<http://docs.humanresources-team.com/sv2414134/b98aa2/a15fcbd6-d3ae-472f-ab80-1e7b73bc2965/?owner=1>
Click or tap to follow link.

5 CLICK HERE [To Apply](#) for this great opportunity to

↑

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 message greeting is not personalized for Sacramento State.
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 pay rate is high and the hours are only 11 hours a week.
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 is not from an official Sacramento State or CSU individual or office.

Faculty, Staff, and Auxiliary Campaign

This campaign simulated a credential stealing phishing scam that was recently sent to campus. Credential stealing scams continue to be sent to campus. This campaign is targeted to spread awareness about this type of scam. Below is a graphic of the simulated phishing email sent to all faculty, staff, and auxiliaries. The graphic contains call-outs to the items that help identify a phishing message. The results of the campaign follow the graphics.

The image shows a simulated phishing email. At the top left is a circular profile picture with the initials 'FM' and the name 'Fred Murry <fredmurry@hr-communication.com>'. To the right of the name is a callout circle with the number '1'. Below the name is the subject line 'Our administrator has begun the process' with a callout circle '2'. The main body of the email contains the following text:

Your office 365 account appears to have two different logins with two different universities' portals.

To avoid termination within 24hrs, we expect you to strictly adhere to and address it. 3

Please give us 24 hours to terminate your account OR verify your account at www.csus.edu/enrollment-management

Failure to Verify will result in the close of your account. 4

nd address it.

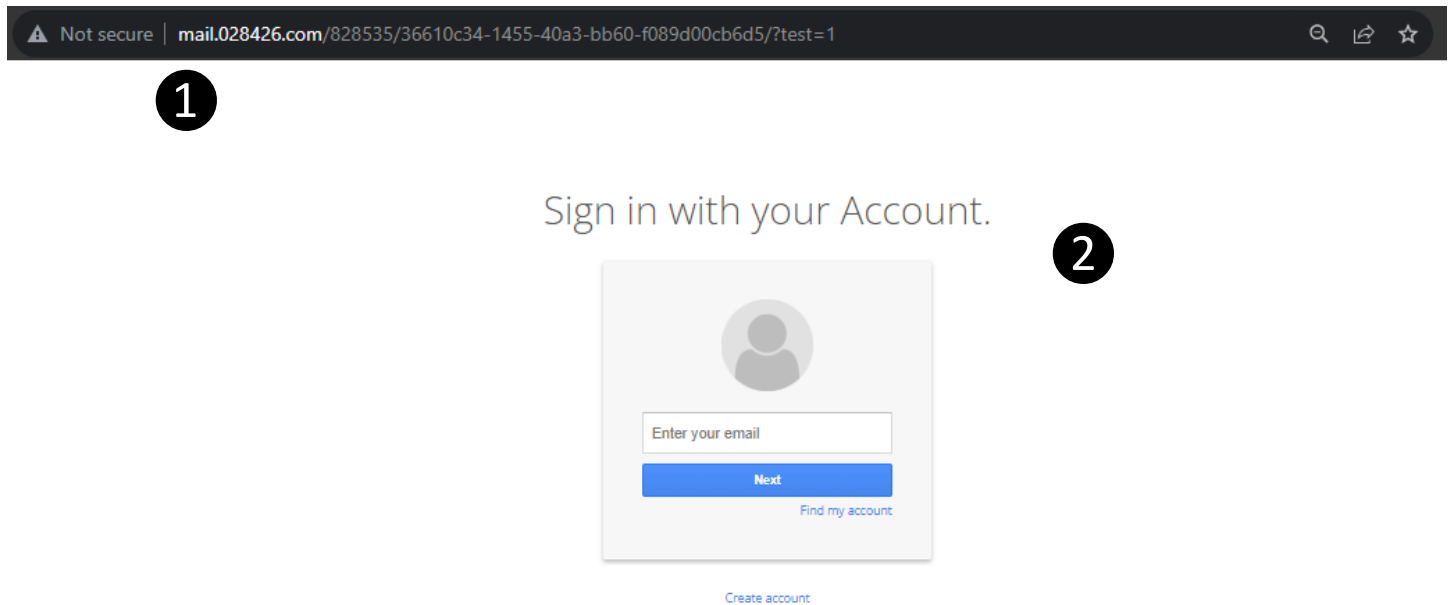
at www.csus.edu/enrollment-management

A callout box with a white border and a shadow points to the URL. It contains the text: `http://mail.028426.com/41e81b/c4c7b2ce-11ee-4e3f-8e2d-f8050d7471ba` and the instruction 'Click or tap to follow link.' A callout circle with the number '4' is positioned to the right of this callout box. A white arrow points from the bottom of the callout box to the URL in the text below.

1. Check email addresses thoroughly to ensure it is coming from a legitimate source. 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.
2. The subject line is odd and not specific.
3. The timeframe of 24 hours is trying to add urgency to make you act fast. We will not give you only 24 hours to keep your account.

4. Even though, the hyperlink says it points to a Sac State site, if you hover over the hyperlink, it shows that it is not going to a Sacramento State or CSU web page.

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



1. The web address is not a Sac State or Office 365 address.
2. The page does not contain Sacramento State or official system branding. 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.

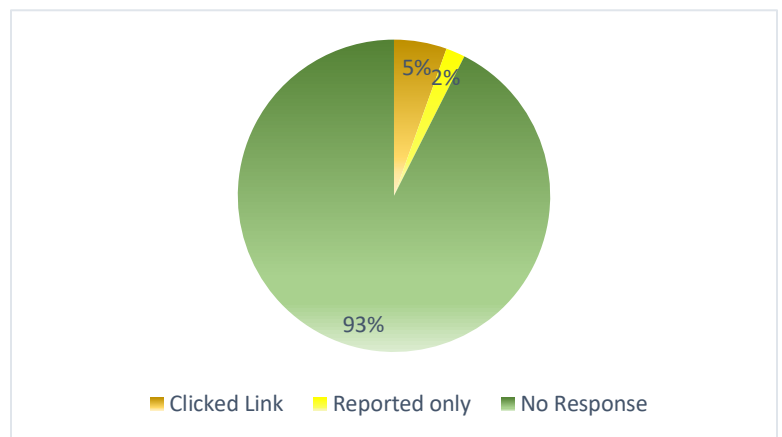
Results of the September 2023 Phishing Simulation

Results of the September 2023 Student Phishing Simulation

Of the 42,561 recipients, 2,323 (5.4%) clicked the link in the phishing simulation email. 844 (1.9%) used the Report Phishing Button to report the message.

2,323 Found Susceptible to Phishing

Unique Recipients:	42,561
Clicked Link:	2,323
Reported only:	844

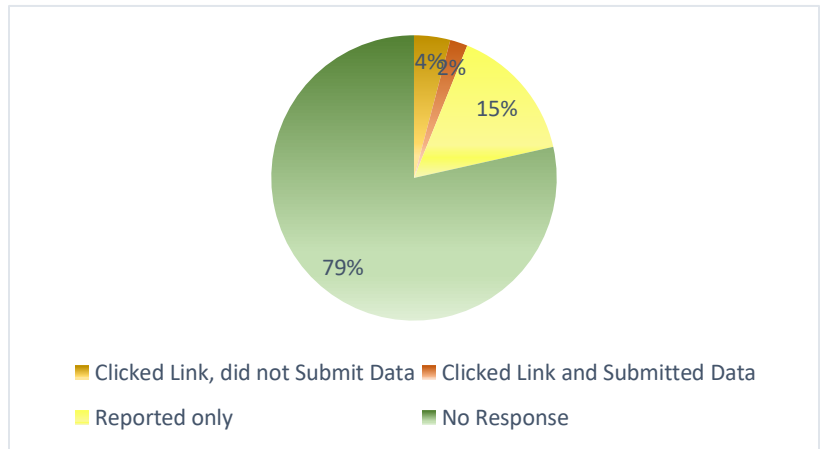


Results of the September 2023 Faculty and Staff Phishing Simulation

Of the 5,520 recipients, 343 (6.2%) clicked the link in the phishing simulation email. 231 who clicked the link did not submit data (4.1%) and 112 clicked the link and submitted data (2%). 868 (15.7%) used the Report Phishing button to report the message.

343 Found Susceptible to Phishing

Unique Recipients:	5,520
Clicked Link:	343
Clicked link did not submit data:	231
Clicked link and submitted data:	112
Reported only:	868



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.

