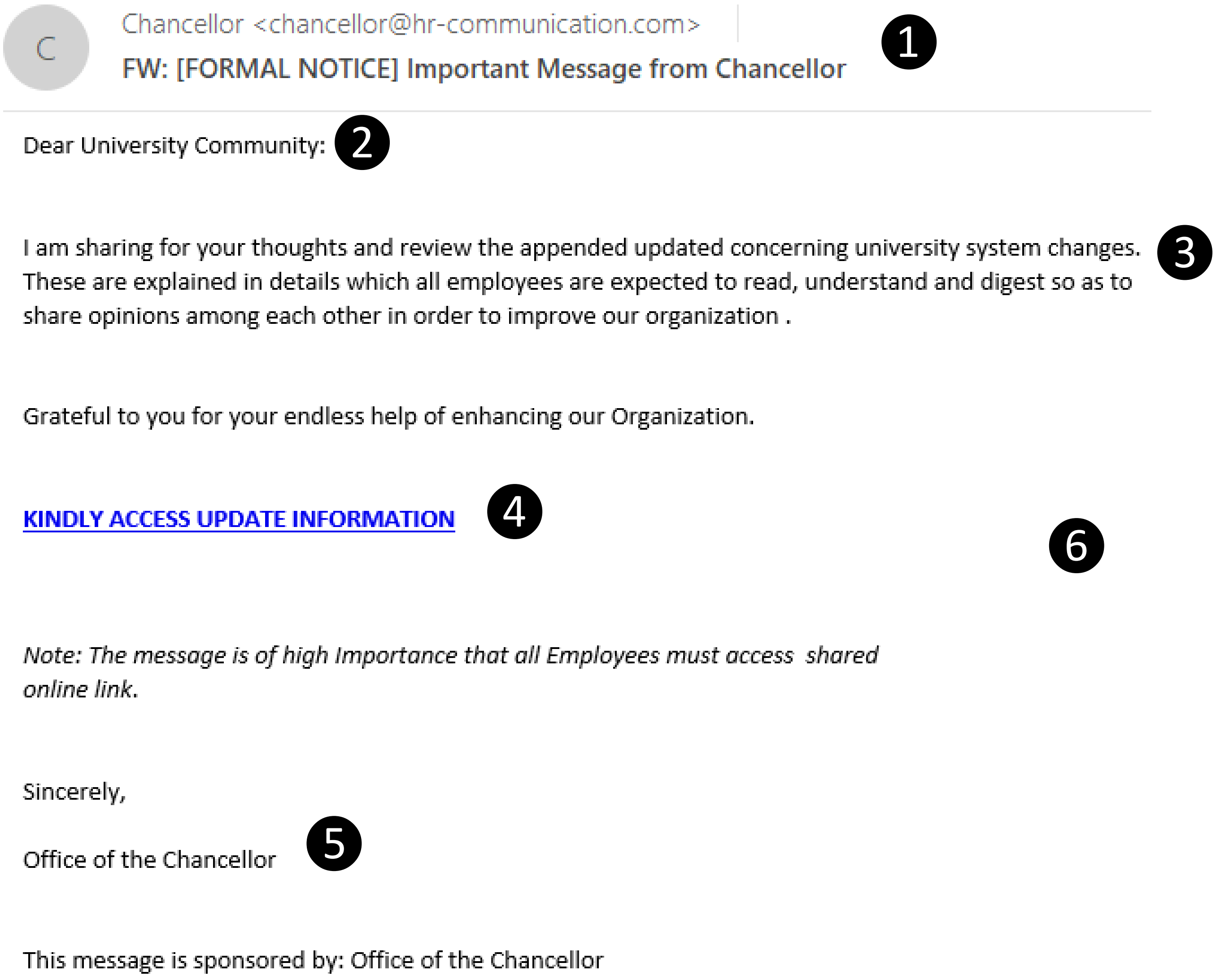
SACRAMENTO STATE
INFORMATION RESOURCES & TECHNOLOGY

Financial Aid Phishing Awareness Campaign – May 2020

On May 5, 2020, IRT sent a Cofense PhishMe phishing simulation email message to all Faculty, Staff, and Auxiliaries. Why? Ninety-one percent of security breaches are caused by phishing messages. The phishing simulation messages and the education page that accompanies them are meant to provide awareness about this serious security 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 Faculty, Staff, and Auxiliaries, as well as 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.



Chancellor <chancellor@hr-communication.com>

FW: [FORMAL NOTICE] Important Message from Chancellor

Dear University Community:

I am sharing for your thoughts and review the appended updated concerning university system changes. These are explained in details which all employees are expected to read, understand and digest so as to share opinions among each other in order to improve our organization .

Grateful to you for your endless help of enhancing our Organization.

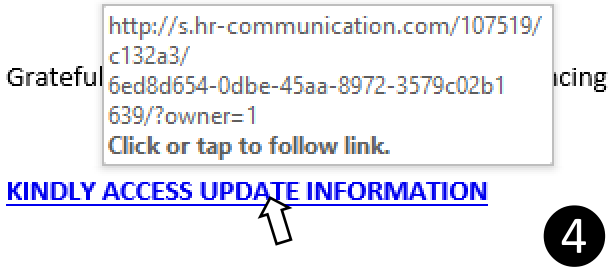
KINDLY ACCESS UPDATE INFORMATION

Note: The message is of high Importance that all Employees must access shared online link.

Sincerely,

Office of the Chancellor

This message is sponsored by: Office of the Chancellor



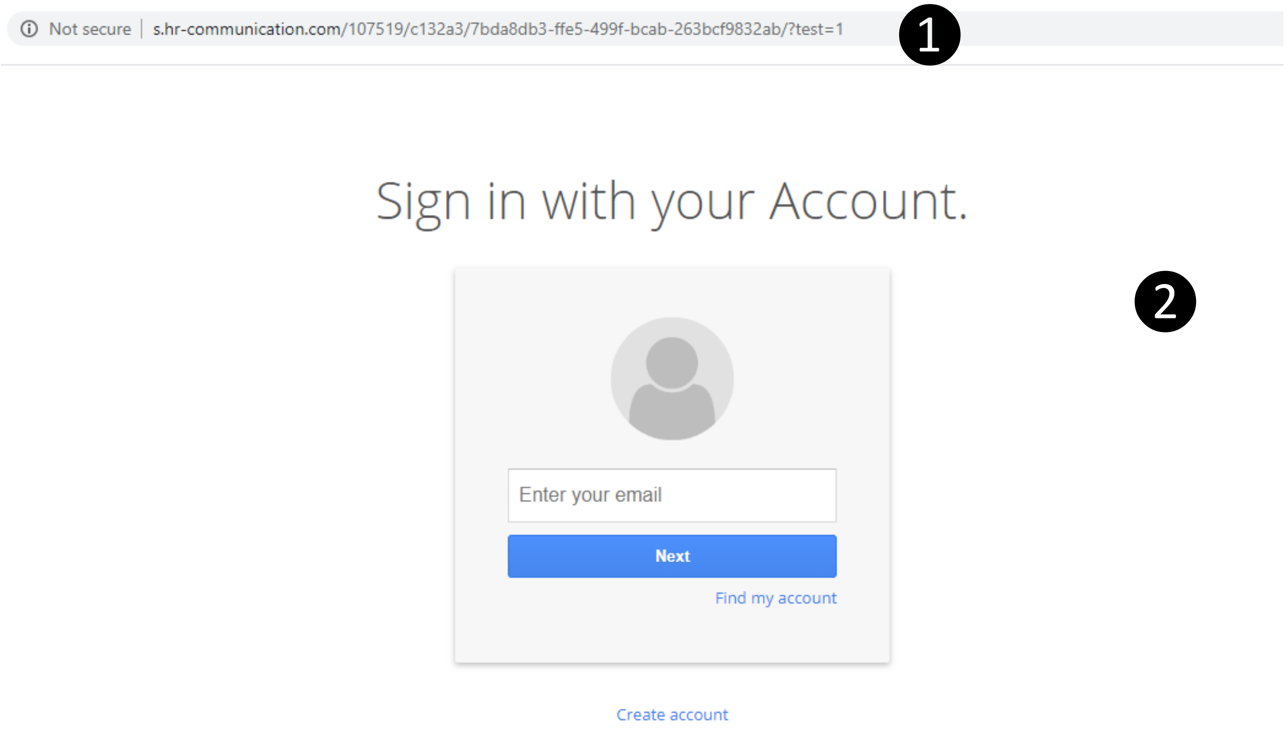
Grateful ncing

http://s.hr-communication.com/107519/c132a3/6ed8d654-0dbe-45aa-8972-3579c02b1639/?owner=1
Click or tap to follow link.

KINDLY ACCESS UPDATE INFORMATION

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)
2. The message greeting is not personalized for Sacramento State.
3. The message is oddly worded.
4. If you hover over the hyperlink, it shows that it is not going to a Sacramento State or CSU web page.
5. The message signature is not specific to an official Sacramento State or CSU individual or office.
6. 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.

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



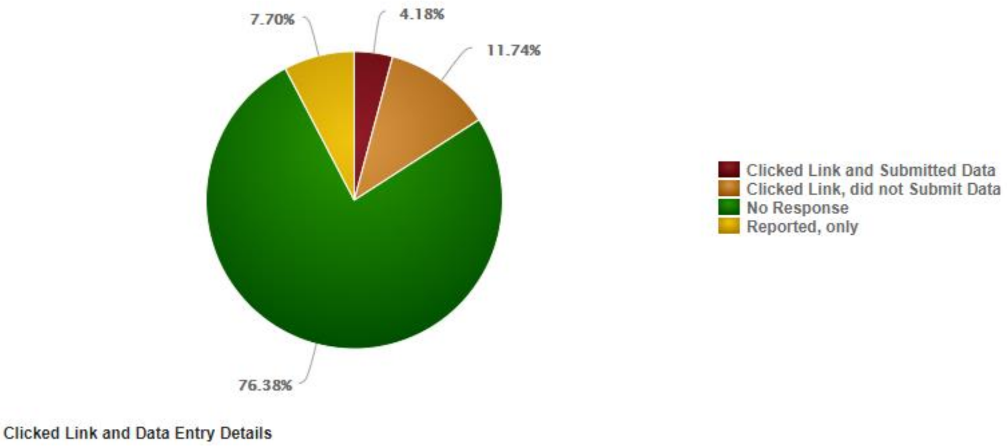
Not secure | s.hr-communication.com/107519/c132a3/7bda8db3-ffe5-499f-bcab-263bcf9832ab/?test=1

Sign in with your Account.

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 May 2020 PhishMe Faculty, Staff, and Auxiliary Phishing Simulation

Of 5,000 recipients, 385 used the new Report Phishing tool to report the phishing simulation. 796 (15.9%) clicked the link in the phishing simulation email. 209 (4.18%) went further and gave their login credentials on the second screen.



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 and instructions on how to alert the ISO about a suspicious message (including the new PhishMe Reporter button in your Outlook menu!) will help improve your 'phish finding' and reporting abilities.

Future Campaigns

These campaigns are designed to help protect you and campus data by improving phishing awareness and leading to fewer compromised accounts. Through Cofense PhishMe, we will periodically send additional campaigns as training, and we encourage you to bookmark csus.edu/phishing to learn more, and see what current phishing scams are being reported.

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.