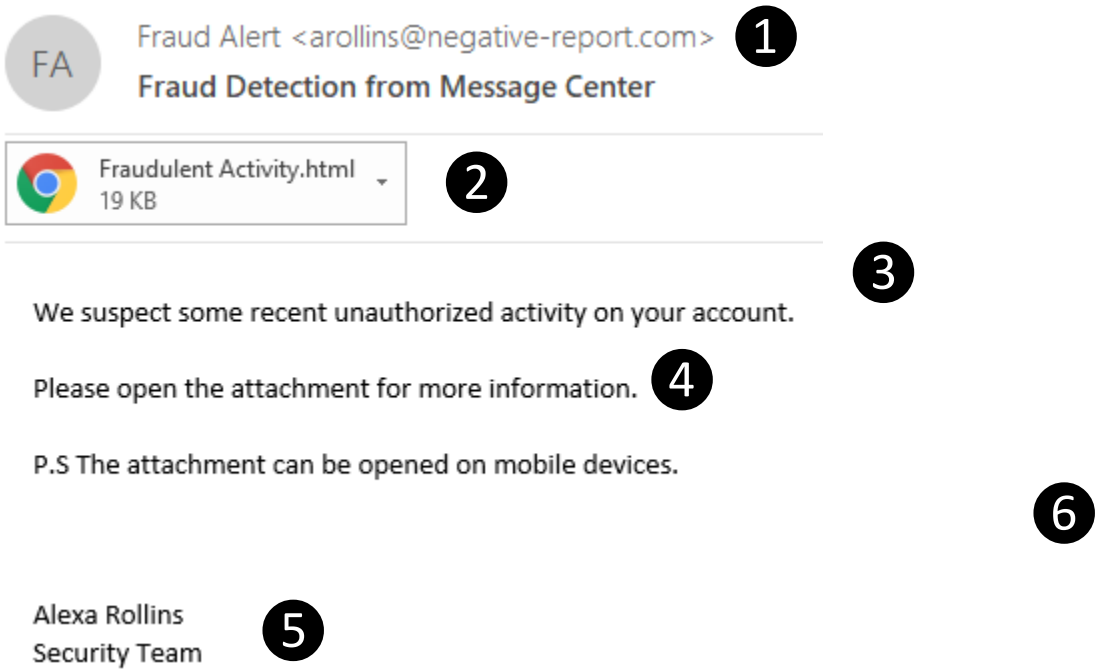
Phishing Awareness Campaign for Students, Faculty, Staff, and Auxiliaries – October 2020

IRT sent Cofense PhishMe phishing simulation email messages to all Students, Faculty, Staff, and Auxiliaries on October 28, 2020. Why? Ninety-one percent of security breaches are caused by phishing messages. This campaign contained an attachment to educate the campus about real phishing scams that contain malicious payloads that can launch when opening attachments. Malicious payloads can include viruses, malware, or ransomware. The phishing simulation message and the education page that accompanied it are part of a comprehensive anti-phishing program 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 students, faculty, staff, and auxiliaries. The graphic contains call-outs to the items that help identify a phishing message. The results of the campaign follow.



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 contained an attachment which can contain a malicious payload.
3. The message greeting is not personalized for Sacramento State.
4. The message does not include specific information about which account was affected; instead, it directs you to open an attachment.
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.

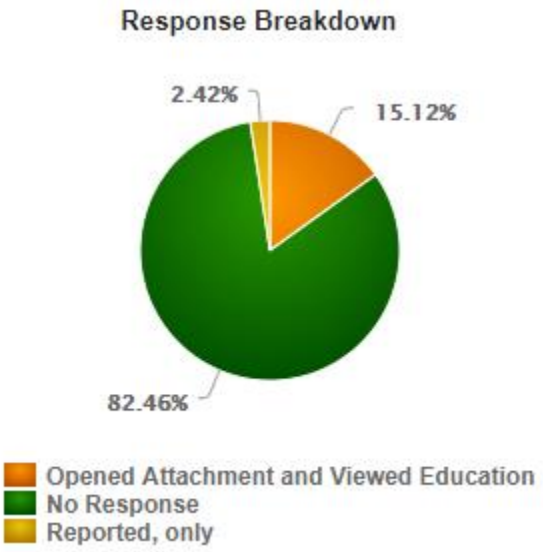
Student results of the October 2020 Phishing Simulation

Of 41,950 recipients, 6,340 (15.12%) clicked the link in the phishing simulation email. 1,016 (2.42%) used the Report Phishing tool to report the phishing simulation.

6,340 of 41,950 Students Found Susceptible to Phishing

Unique Recipients:	41,950
Opened attachment	6,340
Reported via Cofense Reporter & Did Not Click:	1,016

October 2020 Phishing Simulation Response Breakdown for Students



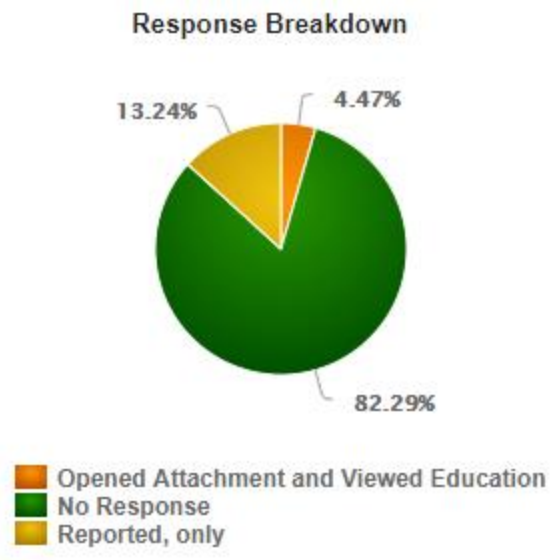
Faculty, Staff, and Auxiliary results of the October 2020 Phishing Simulation

Of 4,995 recipients, 223 (4.47%) clicked the link in the phishing simulation email. 661 (13.24%) used the Report Phishing tool to report the phishing simulation.

223 of 4,995 Faculty, Staff, and Auxiliaries Found Susceptible to Phishing

Unique Recipients:	4,995
Opened attachment	223
Reported via Cofense Reporter & did not click link:	661

October 2020 Phishing Simulation Response Breakdown for Faculty, Staff, and Auxiliaries



What is Phishing?

Phishing emails are designed to steal your identity or money, damage your computer or your organization's network with viruses, or encrypt files and hold them 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.

Why PhishMe Training?

1. PhishMe training is designed to help protect and educate, not to trick you. Not to worry, results of this training are used for educational purposes only.
2. Knowledge is power. The simulated emails provide hands-on experience in what a phishing email looks like. If you had opened the attachment on the simulated phishing message, you'd 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 at servicedesk@csus.edu, (916) 278-7337, or drop by at AIRC 2005.

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