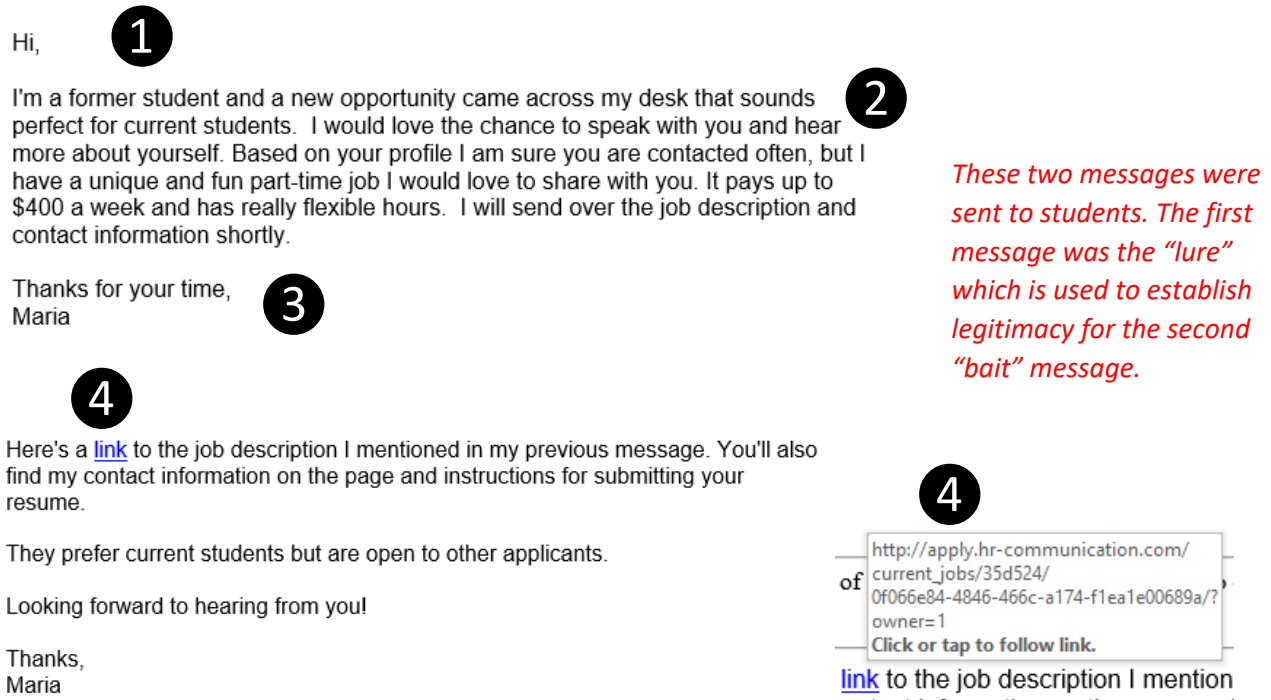


On July 30, 2019, IRT sent out a Cofense PhishMe training email to all student, faculty, and staff. Why? During the Spring 2019 semester, many students were affected by a large phishing run where scammers reached out with false job opportunities, leading to potential advance check fraud.

What Makes This a Phish?

Below is a graphic of the simulated phishing email sent to students, faculty, staff, and auxiliaries. The call-outs identify signs that can help you recognize a real phishing email. Scroll down for the full results.



Hi, **1**

I'm a former student and a new opportunity came across my desk that sounds perfect for current students. I would love the chance to speak with you and hear more about yourself. Based on your profile I am sure you are contacted often, but I have a unique and fun part-time job I would love to share with you. It pays up to \$400 a week and has really flexible hours. I will send over the job description and contact information shortly. **2**

Thanks for your time,
Maria **3**

4

Here's a [link](#) to the job description I mentioned in my previous message. You'll also find my contact information on the page and instructions for submitting your resume.

They prefer current students but are open to other applicants.

Looking forward to hearing from you!

Thanks,
Maria

These two messages were sent to students. The first message was the "lure" which is used to establish legitimacy for the second "bait" message.

4

http://apply.hr-communication.com/current_jobs/35d524/0f066e84-4846-466c-a174-f1ea1e00689a/?owner=1
Click or tap to follow link.

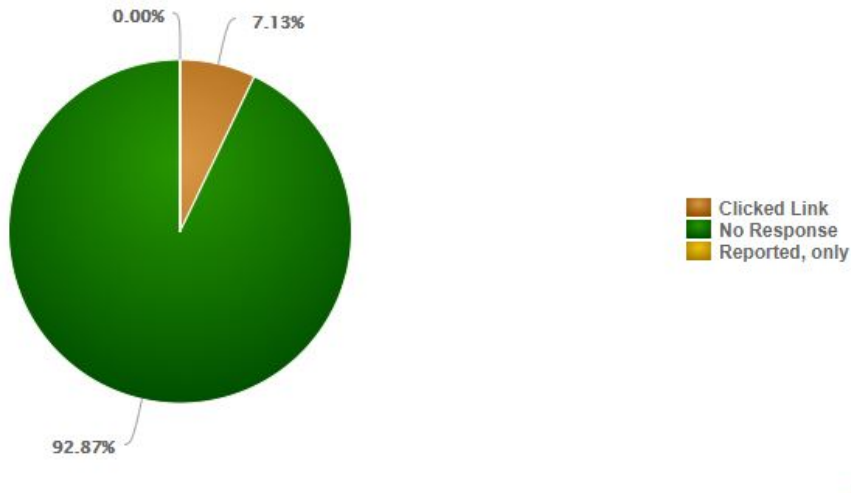
[link](#) to the job description I mention

1. Indirect and unprofessional greeting. A general greeting like this is an indicator of a mass email.
2. No details regarding the actual job are provided, except for the salary which quickly catches the reader's eye.
3. No information regarding the individual or the company is provided in the signature which is unusual for recruiters.
4. The "hover test" shows where the link directs to once clicked. "apply.hr-communication.com" does not indicate a legitimate company's career page and should not be trusted.

Results of the Phishing Simulation

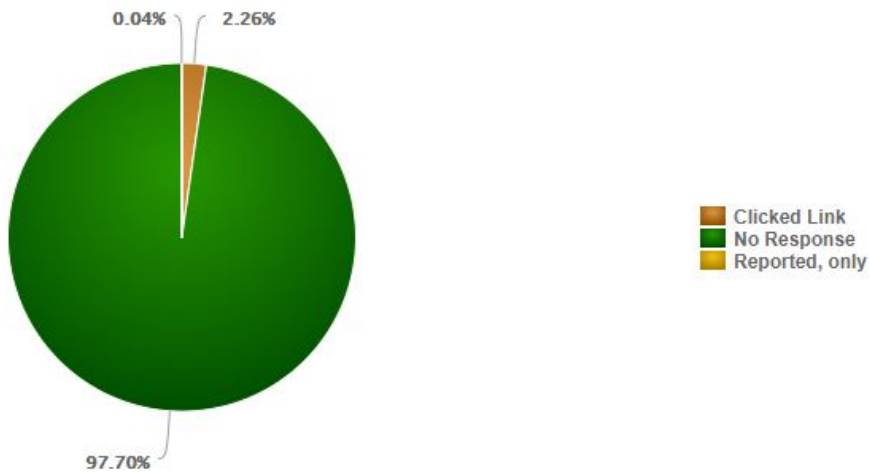
Of the 41,849 recipients, 2,984 (7.13%) students clicked the link in the simulated phishing email.

Student Results



Faculty/Staff Results

Of the 4,717 recipients, 106 (2.26%) faculty, staff, and auxiliaries clicked the link in the simulated phishing email.



What is Phishing?

Phishing emails are designed to steal your identity. They can look very official, with familiar logos or messages, 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 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 simulations, you'll instantly see that it was a training exercise. Educational materials will help improve your "phish finding" abilities.

Suspect A Phishing Attack?

1. Don't panic or click on anything until you can verify it's legitimate.
2. Check for red flags like strange email addresses, bad grammar, or typos.
3. Forward the email as an attachment to abuse@csus.edu.
4. If you clicked on anything and submitted your information, reset your password immediately, and then contact the IRT Service Desk Team at 916-278-7337 or servicedesk@csus.edu.

Future Campaigns

We hope these campaigns help to educate and 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.

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