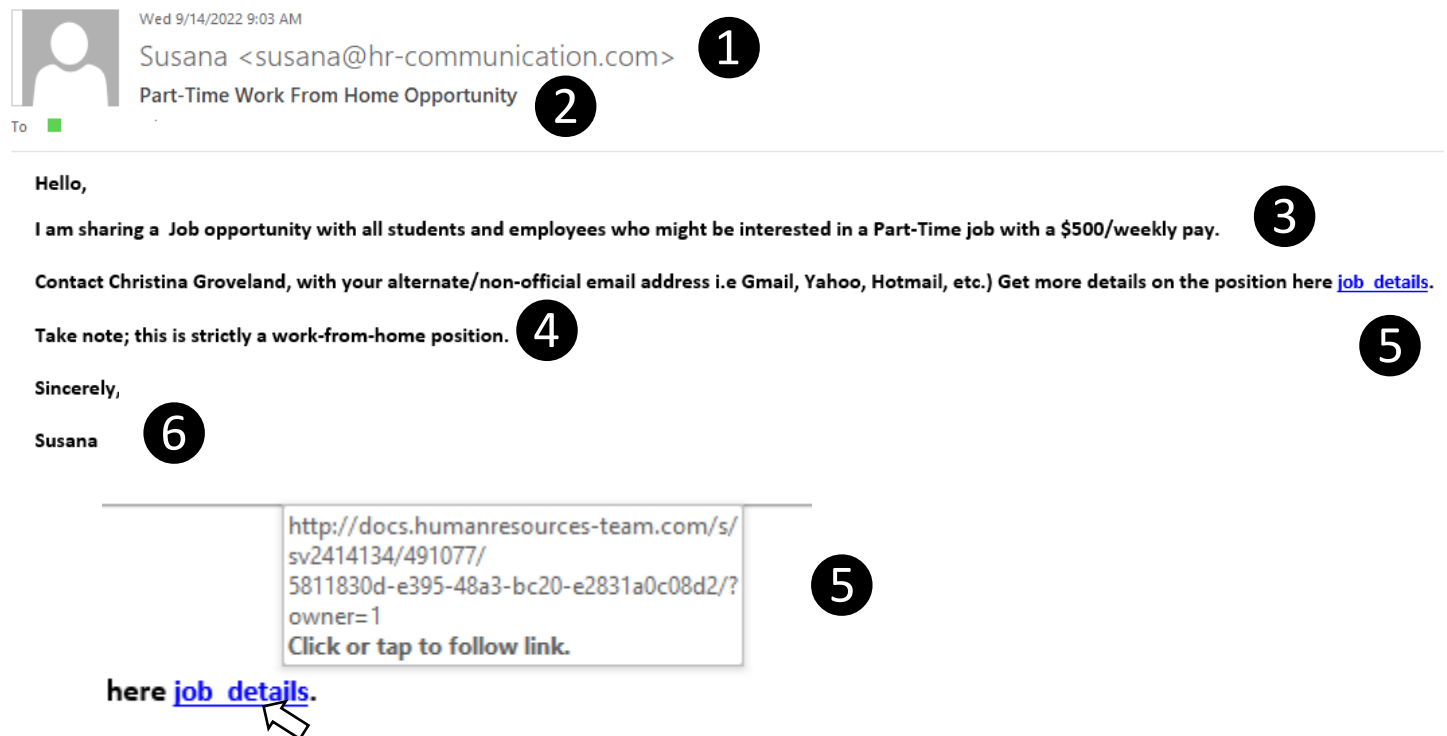


On September 14, 2022 the IRT Information Security Office sent Cofense PhishMe phishing simulation email messages to all faculty, staff, and students. Why? Phishing messages account for the over 90% of security breaches. Many cyber security agencies such as the FBI and the Cybersecurity & Infrastructure 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 separate campaigns to students than to faculty and staff to provide awareness pertinent to those groups.

Student Campaign

Below is a graphic of the simulated phishing email sent to all students. 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 with the following content and call-outs:

- 1**: Sender email address: `<susana@hr-communication.com>`
- 2**: Subject line: `Part-Time Work From Home Opportunity`
- 3**: Body text: `I am sharing a Job opportunity with all students and employees who might be interested in a Part-Time job with a $500/weekly pay.`
- 4**: Body text: `Take note; this is strictly a work-from-home position.`
- 5**: A call-out box highlights a URL: `http://docs.humanresources-team.com/s/sv2414134/491077/5811830d-e395-48a3-bc20-e2831a0c08d2/?owner=1` with the instruction `Click or tap to follow link.`
- 6**: Sign-off: `Sincerely, Susana`

Additional text in the email includes: `Hello,` and `Contact Christina Groveland, with your alternate/non-official email address i.e Gmail, Yahoo, Hotmail, etc.) Get more details on the position here job details.`

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. Part-time job scams are very common and they often target students. Be very cautious of unsolicited job offers and notifications.
3. Part-time job scams often sound very appealing by offering fantastic flexibility or high pay for the short hours.
4. Be very suspicious when they ask you to contact them with a different email address. They are trying to evade campus security. Also be suspicious when they ask you to respond to a different email address than the address it was sent. When they use a compromised account, they want you to contact them and not the account they compromised.

5. Hover over the link to see where it will go. This one points to a suspicious site.
6. Check the signature line in messages. Does this come from a person with a position you can verify by doing a web search? Does it match the email address the web search identified?

Faculty and Staff Campaign

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.

Wed 9/14/2022 9:34 AM

Invoice <drive-shares-noreply@edoctransfer.com> **1**

Status of invoice A2170180-43 **2**

To ■

20080920_181657.doc **3**
10 KB

Hello,

Could you please let me know the status of the attached invoice? I appreciate your help! **4**

Best regards,

Ruthie Boutflower **5**

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. Phishing scammers try to establish legitimacy by adding numbers and codes. Check to see if the coding is consistent with what your department usually receives and is consistent with the sender's organization.
3. Beware of attachments. Do not open an attachment unless you are sure it is from a legitimate source and is safe to open.
4. The message does not contain any context to let you know why it was sent to you. If the message is vague and everything else in the message looks legitimate, contact the sender to get more information. Contacting the sender by phone instead of email is best if you have that contact information.
5. Check the signature line in messages. Do you know the sender? Were you expecting a message from the sender?

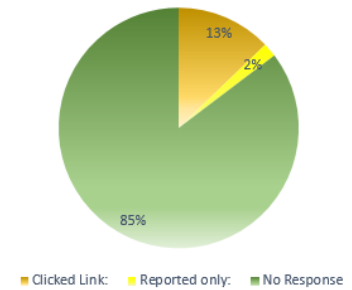
Results of the September 2022 Phishing Simulation

Results of the September 2022 Student Phishing Simulation

Of the 42,209 recipients, 5,414 (12.8%) clicked the link in the phishing simulation email. 788 (1.8%) used the Report Phishing Button to report the message.

5,414 Found Susceptible to Phishing

Unique Recipients:	42,209
Clicked Link:	5,414
Reported only:	788

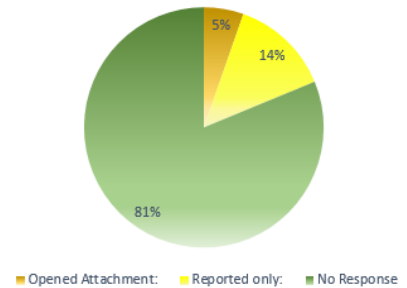


Results of the September 2022 Faculty and Staff Phishing Simulation

Of the 5,487 recipients, 294 (5.3%) opened the attachment in the phishing simulation email. 737 (13.4%) used the Report Phishing button to report the message.

294 Found Susceptible to Phishing

Unique Recipients:	5,487
Opened Attachment:	294
Reported only:	737



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.

