


On February 25, 2025 IRT sent phishing simulation email messages to all Students, Faculty, Staff, and Auxiliaries. Why? Ninety-one percent of security breaches are caused by phishing messages.

Many cybersecurity 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.

Student, Faculty, Staff, and Auxiliary Campaign


This campaign mimicked a phishing scam that is currently trending. This campaign was targeted to spread awareness about scams that mimic invoices. Below is a graphic of the simulated phishing email sent to all students, faculty, staff, and auxiliaries. The message contains call-outs to the items that help identify a phishing message. The results of the campaign follow.

Draft Documents

 Rosie Lloyd <rlloyd@financing-banks.com> **1**
To ● G
ⓘ If there are problems with how this message is displayed, click here to view it in a web browser.

Good day **2**

Please find the attached files below . **3**

 Commercial Invoice F4U202502179.pdf **4**
added 02/25/2025

 Commercial Invoice B4U202502170.pdf
added 02/25/2025

 KHD-FRA-05022025.pdf **5**
added 02/25/2025

If you have any questions, please do not hesitate to contact us.

Regards.

1. Do you recognize this sender? 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 greeting is not addressed to a specific individual. It simply says, "Good day." If your name is included, you still have to do additional verification. Not having a name is a tip off that it is an indiscriminate mass mailing.
3. There is no context to the message. It claims to have attached documents, but does not provide information about the purpose of sending the message.

- The message does not contain any branding or company tailored formatting. It does not even have a signature stating who it is from. If branding is used, you still need to use caution because this can be spoofed, but not containing any branding is a tip off. The message also contains punctuation errors.
- The email message looks like it contains attachments, but it is really just images and links to a web page. When you mouse over the link, you see where it is pointing to.



5

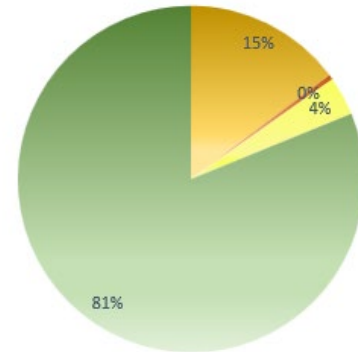
Results of the February 2025 Phishing Simulation

Student Results of the February 2025 Phishing Simulation

Of the 38,213 recipients, 5,819 (15.22%) clicked the link in the phishing simulation email. 1,565 (4%) used the Report Phishing Button to report the message.

5,819 Found Susceptible to Phishing

Unique Recipients:	38,213
Clicked Link Only:	5,633
Clicked Link & Reported:	186
Reported only:	1,379



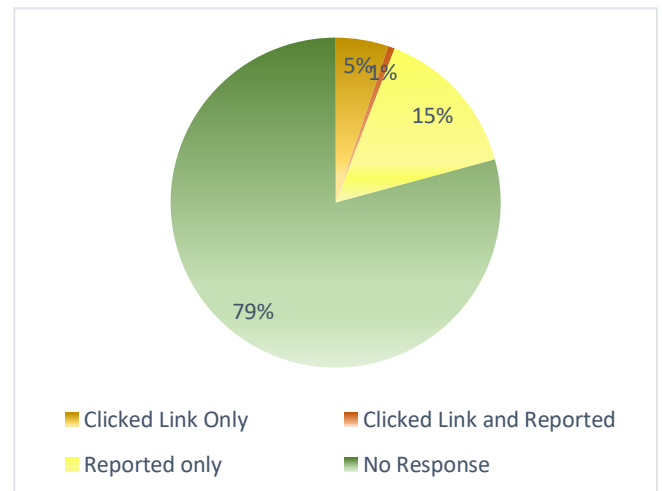
Clicked Link Only Clicked Link and Reported Reported only No Response

Faculty, Staff, and Auxiliary Results of the February 2025 Phishing Simulation

Of the 5,616 recipients, 327 (5.8%) clicked the link in the phishing simulation email. 877 (15.6%) used the Report Phishing button to report the message.

327 Found Susceptible to Phishing

Unique Recipients:	5,616
Clicked Link Only:	290
Clicked Link & Reported:	37
Reported only:	840



Clicked Link Only Clicked Link and Reported Reported only No Response

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 Phishing Training?

1. To protect and educate. Phishing 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. 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.