

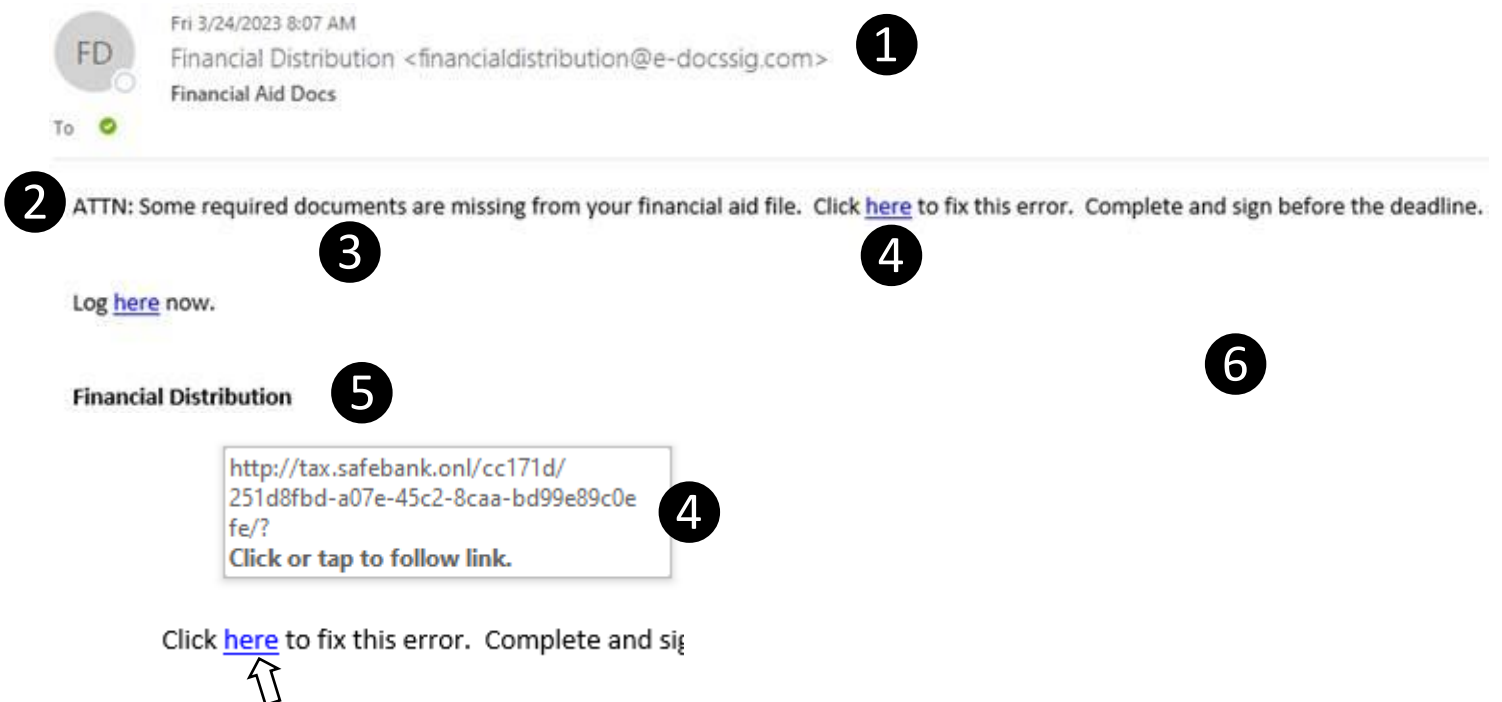
On March 29, 2023, IRT sent Cofense PhishMe phishing simulation email messages to all Faculty, Staff, and Auxiliaries. Why? Ninety-one percent of security breaches are caused by phishing messages.

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

This campaign was Financial Aid themed to bring attention to Financial Aid scams. Below is a graphic of the simulated phishing email sent to all students, 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 screenshot shows an email from 'FD' (Financial Distribution) with the subject 'Financial Aid Docs'. The body text reads: 'ATTN: Some required documents are missing from your financial aid file. Click [here](#) to fix this error. Complete and sign before the deadline. Log [here](#) now.' The signature is 'Financial Distribution'. A link is provided: 'http://tax.safebank.onl/cc171d/251d8fbd-a07e-45c2-8caa-bd99e89c0efe/? Click or tap to follow link.' Callouts 1-6 point to: 1. Sender email address, 2. Greeting, 3. Lack of specific information, 4. Suspicious hyperlink, 5. Non-official signature, and 6. Lack of official branding.

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 does not have any specific information.
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 from 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 | tax.safebank.onl/db8c3b/24b20b53-9797-4a0b-9c97-d1a5f1a7d3d5/?test=1

1

Home

College Account

User Name

Password

Login

Financial Distribution

2

Trouble with login?

Ensure you are using your college account.

New to the site?

Use your college account to access your statement

Privacy Policy | Contact Us | Terms of Use
© 2019 FDA. All Rights Reserved.



Accounts are subject to eligibility and restrictions, including but not limited to restrictions on distributions for qualified school expenses set forth in section 213(d) of the internal Revenue Code. State taxes may apply.

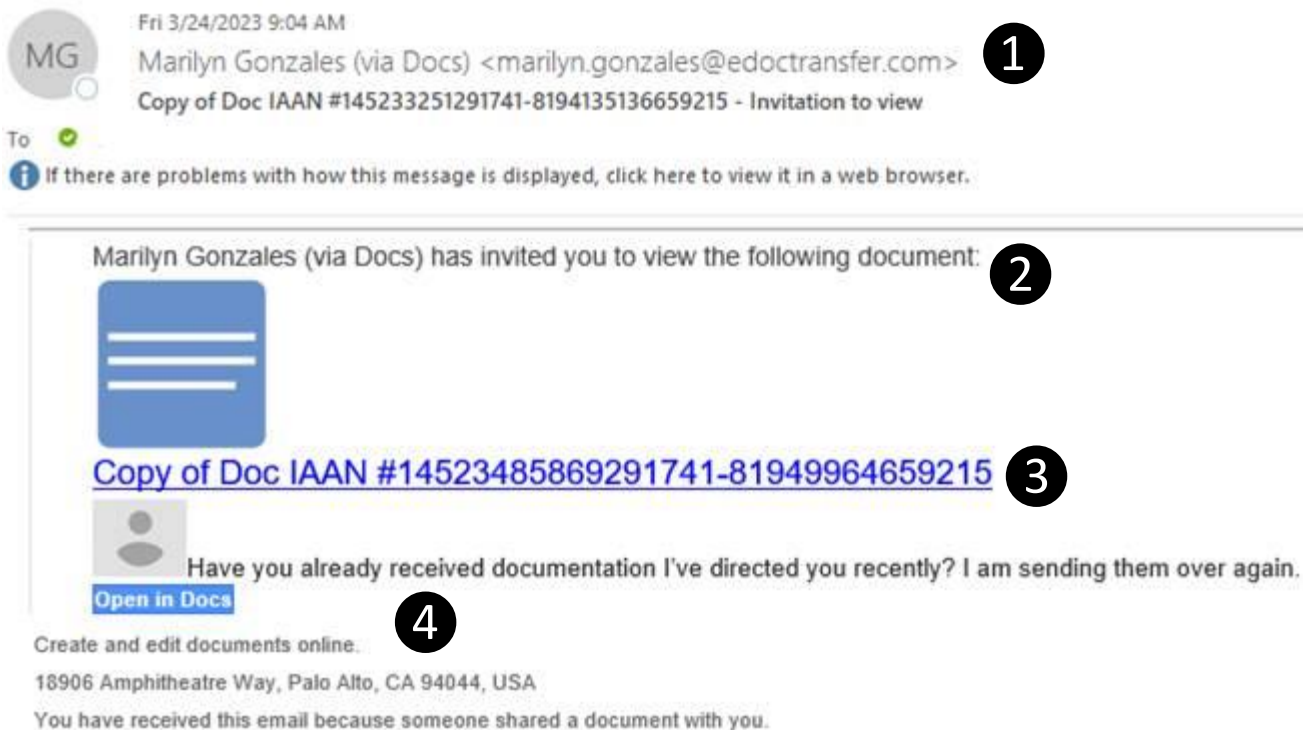
Flexible spending arrangements (FSAs) are subject to eligibility and restrictions.

This communication is not intended as legal or tax advice. Please contact a competent legal or tax professional for personal advice on eligibility, tax treatment, and restrictions. Federal and state laws and regulations are subject to change

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.

Faculty and Staff Campaign

This campaign simulated a known shared document themed phishing scam. 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.



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. Do you know the sender? Were you expecting a document?
3. The document name link is strange and contains many numbers instead of a document title that would give an indication of the contents. When you mouse over the link, it points to a strange web address.
4. The message does not contain any context to let you know why it was sent to you. If the message is vague even though everything else in the message looks legitimate, be suspicious.

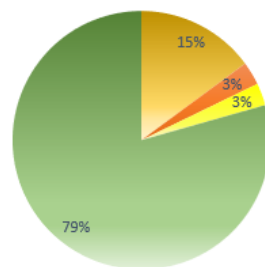
Results of the March 2023 Phishing Simulation

Results of the March 2023 Student Phishing Simulation

Of the 41,353 recipients, 6,345 (15.3%) clicked the link in the phishing simulation email. 1,251 (3%) of these also submitted login data. 1,188 (2.8%) used the Report Phishing Button to report the message.

6,345 Found Susceptible to Phishing

Unique Recipients:	41,353
Clicked Link:	6,345
Clicked and Submitted Data:	1,251
Reported only:	1,188



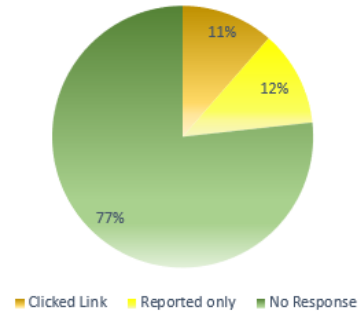
Clicked Link Clicked and Submitted Data Reported only No Response

Results of the March 2023 Faculty and Staff Phishing Simulation

Of the 5,456 recipients, 625 (11.4%) clicked the link in the phishing simulation email. 644 (11.8%) used the Report Phishing button to report the message.

625 Found Susceptible to Phishing

Unique Recipients:	5,456
Clicked Link:	625
Reported only:	644



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.

