Phishing

- What is the "Are you there?" credit card scam?
- What to do when you receive spam or phishing emails?

What is the "Are you there?" credit card scam?

Patterns

The typical gift card scam follows this pattern:

1. The scammer will send out an e-mail, impersonating an important faculty member and/or department chair. Sometimes the scammer will use the exact name and e-mail signature to match the faculty member. However, often the e-mail address the scammer uses is not a legitimate ucdavis.edu e-mail account.
2. The content of the e-mail will typically start with an urgent request such as "are you available?" or the request will indicate a fake job offering.
3. If the victim responds, the scammer will eventually ask the victim to purchase gift cards of various amounts and to send over the codes associated with the cards or the scammer will send a fake check asking that the victim deposit it and then send the attacker legitimate funds once the check "clears" the bank. It can take a few days for this process and the fake checks do clear the bank sometimes before they are noticed as a fraudulent check.
4. The scammer will often ask for the phone number or personal e-mail of the victim to continue the conversation so that the communication is no longer over the university communication methods.

More Information

Please see the following for more information:

- https://www.consumer.ftc.gov/articles/paying-scammers-gift-cards
- https://support.apple.com/gift-card-scams

- https://www.consumer.ftc.gov/articles/what-do-if-you-were-scammed

What To Do

We will investigate the impact of the message you submitted to us, but for now, please simply delete the email message. If you happened to provide any account credentials, please change any associated passphrase's immediately.

If you have any other questions or concerns, please let us know.

What to do when you receive spam or phishing emails?

Thank you for being aware of potential malicious activity. Please do not click any of the links within the email.

To report a phishing attempt, please mark the suspicious message as phishing within your mailbox by clicking on **"more" (three dots)** > **Report Phishing**.
We also recommend blocking the suspicious email address.

If you downloaded any attachments or clicked any of the provided links, we recommend performing a malware scan on your device as soon as possible.
If you were prompted to enter any account information and provided credentials, please reset any relevant account passwords immediately.

For additional information regarding phishing attacks and how to remove malware, please visit the following knowledge base articles:

Phishing information

https://kb.ucdavis.edu/?id=0220

Removing malware

https://kb.ucdavis.edu/?id=0302

If you have any other questions, please let us know