

# TIPS FOR DEALING WITH 'GIFT CARDS,' FAKE BILLS, & SIMILAR FINANCIAL SCAMS



---

*If you have been a victim of a scam, report it to [cybersecurity@ucdavis.edu](mailto:cybersecurity@ucdavis.edu) ASAP*

---

Cyber criminals use sophisticated methods to steal money and data. A typical scam tries to trick you into sending money. It might direct you to a fake vendor website, or say your supervisor wants you to buy gift cards. Scammers use email, phone calls, texts, social media ... whatever they think will work.

## General advice

- **Most scams try to prey on a sense of urgency and anxiety. Resist it.**  
Examples: A fake email from your boss demands that funds be sent to some account ASAP; or a fake email for a vendor states it never received a payment and will contact a lawyer if payment is not received ASAP. Feeling anxious? That's the scammer's goal.
- **Fraudulent messages don't always have bad grammar.**  
Yes, countless scams use awkward language. Others look valid. Maybe they claim to come from your boss, finance person or a dean, and ask for a payment that sounds legitimate.
- **Don't be rushed into financial decisions.**  
Have a standard process for procurement that includes a standard intake process, and has checks and balances to ensure a transaction is legitimate. If you need to deviate from this process, call a known contact and ask why there is a deviation.

*Continued...*

(TIPS FOR DEALING WITH ‘GIFT CARDS,’ FAKE BILLS, & SIMILAR FINANCIAL SCAMS, cont.)

**Here are common attacks, what to watch for, and what to do.**

| <b>Scam</b>                          | <b>What to watch for</b>  | <b>What to do</b>  |
|--------------------------------------|---|--|
| <b>Apple (or any) gift card scam</b> | An email impersonating your supervisor or other high-level individual asks you to purchase gift cards ASAP, and to reply to the email with the codes. | Have a standard process for purchasing anything, including gift cards. If a request is urgent, call your supervisor and double-check.  |
| <b>Vendor imposter fraud</b>         | A change, or an unexpected invoice, arrives from a known vendor.  | Always call your known vendor contact if you receive altered or unexpected invoices.   |
| <b>Wire transfer fraud</b>           | An email asks you to wire funds, for any reason.  | Stop, and review the request with your supervisor or accounting department to ensure the payment is appropriate. Call a known number; ask the purported requester to verify the request for the payment. |
| <b>Check fraud</b>                   | An unexpected check arrives, with a request to wire some or all of the amount back to the sender  | Check with your accounting department, and perhaps with the bank, to verify the check.   |

Questions? Inquire with Your Local IT Support or Call the IT Express Service Desk at 530-754-HELP (4357)

**For more information:**

- [“April 2019: Whaling, SMiShing, and Vishing...Oh My!”](#)
- [“Boss on vacation this month? Beware the employer imposter scam”](#)