GIFT CARD SCAMS

If a dean, supervisor, coworker or fellow student emails and asks you to buy gift cards, chances are, it's a fake message from a cybercriminal. Here's a common pattern:

1. Reach out

It starts when you receive an unexpected message. Thieves can pretend to be peers or authorities by researching your organization and creating a fake email address.

From: Your boss or coworker
To: You
Subject: Urgent request

Hey, are you available?

2. Request

The thief may ask you to buy, scratch, and send gift card numbers.

Could you go purchase 20 gift cards? I'd do it myself, but I'm in a meeting. I'll reimburse you later.

3. Repeat

They might try to pull the wool twice.

Thanks so much! Before you get back- I was just talking with Adam, and we actually need 20 more. Could you...?

WHAT CAN YOU DO?

- Be suspicious of any email that makes unusual requests.
- Examine the sender's email and look for unusual variations of their usual address. Sometimes a letter or number is added, or a spoofed university address may be used.
- Contact the sender with a trusted email address or by phone to verify unusual requests.
- If you receive a gift card message, send the email as an attachment to abuse@byu.edu
- Pass this information along to colleagues and friends

Church Educational System
Security Operations Center