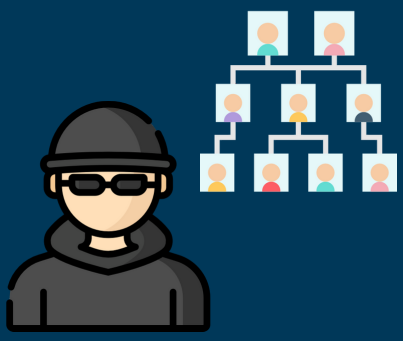
"Are you available?" Gift Card Scam

If a supervisor or co-worker emails and asks you to buy gift cards, chances are good that it's a fake message from a cybercriminal. Know the signs and what to do.



Initial Email

Thief checks org chart to find people you know

To: You
From: Your Boss (or Coworker)
Subject: Urgent Request

Are you available?

Request

To buy, scratch and send gift card numbers

To: You
From: Your Boss (or Coworker)
Subject: Urgent Request

Can you go get some gift cards? I will reimburse later.

Repeat

Sometimes they do it again!

To: You
From: Your Boss (or Coworker)
Subject: Urgent Request

Can you go get some *more* gift cards?

What to 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 UW address may be used. Contact them 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 *security@uw.edu*
- Send other types of phishing messages as attachments to *help@uw.edu*
- Pass this information along to colleagues and friends.
- More information: *https://www.consumer.ftc.gov/blog/2018/05/asked-pay-gift-card-dont*
- More on UW Scams: *https://ciso.uw.edu/education/scams/*

OFFICE OF THE CISO
UNIVERSITY of WASHINGTON