Published on *University of Colorado* (https://www.cu.edu)

Take a pause: verify unexpected requests through official channels [1]

August 14, 2026 by ES and UIS Communications [2]

Cybercriminals increasingly use tools that can imitate trusted organizations and individuals. For example, you receive an urgent email from someone claiming to be your supervisor urging you to send your Procurement card details for work. The email looks to be official however this seems to be very urgent. Phishing attempts are harder to spot than they used to be, and that’s why it pays to stop and verify before you act on an unexpected request.

How should I handle unexpected requests received outside official university communication channels?

If you receive an unexpected request involving sensitive information, financial transactions, credentials or urgent action, verify it through an established university communication channel before responding; even if it looks like it came from someone you know.

Why official channels matter

They provide better context, recordkeeping and verification than a one-off message. A request that comes through an established UIS or CU channel (such as a university email address, a known ticketing system, an official Teams chat) leaves a trail you can check and reference later.

Unexpected requests delivered through personal accounts, text messages, phone calls or other unofficial channels can be harder to verify. Cybercriminals rely on that difficulty, hoping you'll act quickly before you've had a chance to double-check who's really asking.

When in doubt, verify

If something feels off, such as an urgent ask from your "supervisor" over text, an unfamiliar number claiming to be UIS, or a request to send gift cards or update payment information, don't respond directly. Instead:

1. **Pause before you act.** Urgency is one of the most common tactics used in phishing and social engineering attempts.
2. **Confirm through a known channel.** Reach out to the person or department using a phone number or email address you already know to be correct, not the contact information provided in the suspicious message. In our scenario, you could send a Teams message directly to your supervisor to doublecheck the request directly.
3. **Report it.** Forward suspicious emails to the UIS Service Desk or use Outlook's built-in **Report** button so the university can investigate and warn others if needed.

Phishing button highlighted

Image not found or type unknown

When you're not sure whether a request is legitimate, it's always okay to slow down and confirm through an established CU communication channel first.

cybersecurity [3], UIS Service Desk [4]
Send email when Published:
No

Source URL:https://www.cu.edu/blog/tech-tips/take-pause-verify-unexpected-requests-through-official-channels

Links
[1] https://www.cu.edu/blog/tech-tips/take-pause-verify-unexpected-requests-through-official-channels
[2] https://www.cu.edu/blog/tech-tips/author/249473 [3] https://www.cu.edu/blog/tech-tips/tag/cybersecurity
[4] https://www.cu.edu/blog/tech-tips/tag/uis-service-desk