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

Spot and stop phishing scams [1]

October 6, 2025 by ES and UIS Communications [2]

Phishing is a type of online scam where cybercriminals pose as trusted individuals or organizations to steal sensitive information, such as passwords, financial data or university login credentials.

Phishing scams often use urgency or fear to trick you into taking quick action without thinking. These scams are becoming more sophisticated, with some messages now free of obvious spelling errors and even crafted using AI tools.

Common signs of phishing

Look for these red flags when reviewing your emails, texts or messages:

- **Suspicious sender:** Appears to be from someone you know or a trusted organization but comes from an unexpected or suspicious email address.
- **Generic greeting:** "*Dear user*," "*Dear customer*," or no greeting at all.
- **Urgent or threatening language:** The sender pressures you to act quickly, like *"Your account will be disabled unless you click this link now."*
- **Unexpected links or attachments:** Especially files that ask you to "enable content" or links that don't match the stated destination.
- **Unusual requests:** For money, gift cards, passwords or other sensitive info.
- **Poor grammar or spelling mistakes:** While still common, phishing emails are becoming increasingly error-free, so this is not the only indicator.
- **Spear phishing:** Targeted, personalized phishing scams may refer to or appear to come from your department, coworkers or university affiliates.

Phishing attempts may also use **texts**, **phone calls** or **collaboration tools like Teams [3].**

Check URLs before you click

- Hover over links before clicking to see where they really go. On mobile devices, long-press a link to preview its destination.
- Look carefully at URLs:
    - Secure sites may display a security information icon in your browser's address bar.
    - Watch for look-alike domains, like "**micros0ft.com**" or "**cuboulder.securelogin.net.**" Small changes in spelling, extra words or unusual punctuation are red flags.
    - Be cautious even with .edu addresses — cybercriminals can sometimes compromise legitimate accounts.
- If you receive a message from someone you know but something feels "off," **verify using a different channel**

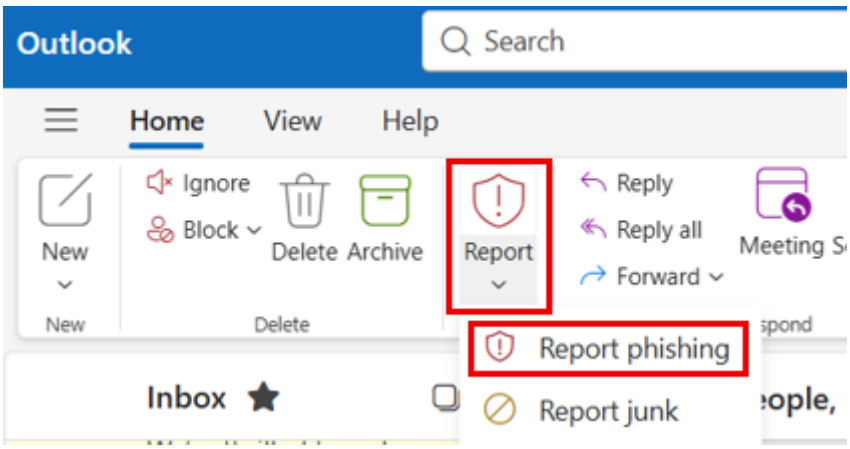
, like calling or texting them directly.

For example, the URL in the image below points to a link that is entirely dissimilar from a normal University of Colorado webpage. Links associated with the university always end with .edu. Also, the “-sup-port-cabanova” wording is not associated with any university service or found in any university URLs. This is clearly a phishing attempt.

If you suspect phishing

1. Don't click any links or open attachments.
2. Use the **Report phishing** function in Outlook to send it to the security team.
   a. In Outlook, click the **Message** tab, then select **Report phishing**.

Depending on which version of Outlook you are using, you may need to click **Report** and select **Report phishing** from the drop-down menu.



3. If you already clicked a link or entered your credentials:

a. Immediately report it to CU as a possible incident. Visit the Report an Incident [4] and OIS webpage [5] to learn more and find the correct incident report contact.

b. Change your password.

c. Contact the UIS Service Desk [6] for urgent support and guidance.

4. Reporting immediately [7] helps stop cybercriminals, protect others and contain the possible incident. CU does not penalize employees or students for reporting suspicious messages in good faith.

Protect yourself long term

- Enable multifactor authentication (MFA) [8] for all university and personal accounts.
- Keep your device [9], browser and applications up to date.
- **Think before you click:** if an email seems urgent, unusual or too good to be true, it probably is. Pause and verify first before proceeding.
- Regularly review CU's Information Security policies [10] and cybersecurity trainings [11], available on Skillsoft Percipio [12].

Quick reference checklist

Before acting on a suspicious message, ask yourself:

- Do I know the sender and expect this message?
- Does the link or attachment make sense?
- Is there urgency or a request for sensitive info or money?
- Have I verified through another method (phone call, text message, etc.)?

cybersecurity [13], Outlook email [14]
Display Title:
Spot and stop phishing scams
Send email when Published:
No

Links
[1] https://www.cu.edu/blog/tech-tips/spot-and-stop-phishing-scams [2] https://www.cu.edu/blog/tech-tips/author/166688 [3] https://support.microsoft.com/en-us/office/prevent-spam-or-phishing-attempts-from-external-chats-in-microsoft-teams-c81de898-5845-4c52-9375-33f148f987d7
[4] https://www.cu.edu/security/reporting-incident [5] https://www.cu.edu/security
[6] https://www.cu.edu/service-desk/about#contact [7] https://www.cu.edu/blog/tech-tips/reporting-cybersecurity-incident [8] https://www.cu.edu/blog/tech-tips/using-multifactor-authentication-mfa-stay-safe-online [9] https://www.cu.edu/blog/tech-tips/avoid-fake-browser-update-scams
[10] https://www.cu.edu/security/policies [11] https://www.cu.edu/security/services/awareness-and-training
[12] https://share.percipio.com/cd/v7cCUzgDF

[13] https://www.cu.edu/blog/tech-tips/tag/cybersecurity [14] https://www.cu.edu/blog/tech-tips/tag/outlook-email