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

Stay vigilant against phishing attempts [1]

October 14, 2024 by ES and UIS Communications [2]

The University of Colorado is a proud champion of Cybersecurity Awareness Month, a global effort to promote cybersecurity best practices and increase awareness of security threats among organizations and individuals.

Visit CU's Cybersecurity Awareness Month web page [3] for more information and to learn how to get involved.

Phishing remains the top threat to cybersecurity today, with new methods for breaching institutions and companies frequently reported. Staying vigilant against these threats is vital to maintaining CU's cybersecurity.

What is a phishing attempt?

A phishing attempt is an email crafted by a cybercriminal posing as a legitimate or commonly known entity, sent to individuals within an organization in hopes of getting someone to engage with malicious attachments or links.

Potential signs of a phishing attempt

Phishing attempts come in a variety of different formats, posing as anything from a colleague to a popular retailer or even your bank.

Indicators that an email might be a phishing attempt:

- A sense of urgency, pushing you to act on fear
- Spelling and grammatical errors.
- References to services or orders you didn't request.
- Suspicious links (see below).
- Misspelled or masked email addresses that don't match the expected sender's name or address.
- Offers of employment or services that are too good to be true.
- Ambiguous or generic greetings.
- Claims to be public figures and company or institution executives, especially from well-known companies.
- Threatening or alarming language.

Identify phishing attempts by URLs

The phishing attempt's goal is to gain access to personal or institutional data or systems by

retrieving legitimate login details from an individual.

Hyperlinks can be easily manipulated to lead to a URL that does not match the organization they are posing as. To see if a hyperlink is pointing to a malicious link, hover your cursor over the link until the preview box appears.

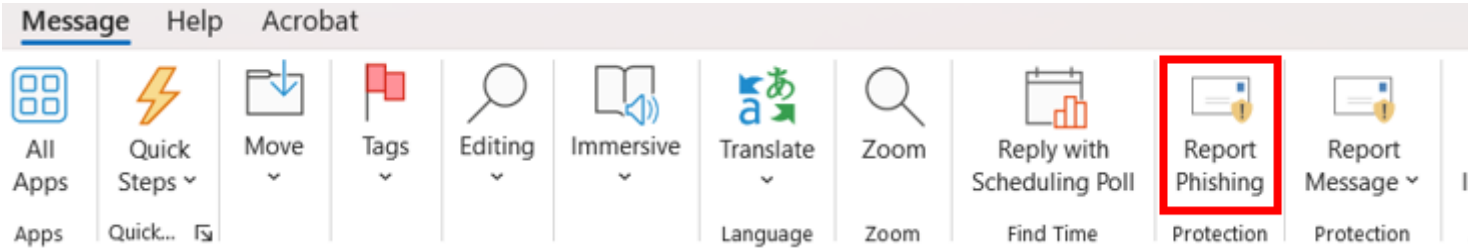
Once the preview box appears, scrutinize the URL for indicators of a malicious or unusual link, as in the example below.

In this case, the URL 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. Thus, this is a phishing attempt.

It is always safest to log into a website from your browser rather than from an email link.

Reporting a phishing attempt

When encountering a suspected phishing attempt, do not click on any links or attachments. Instead, report the email using the **Report phishing** function in Outlook. Click on **Message** in the taskbar, then click **Report phishing**.



Outlook will screen the suspected phish and forward it to OIT and OIS for further review, if needed.

Oh no, I opened a suspicious link or attachment! Now what?

Immediately report it as a possible incident. Reporting it immediately allows the information security team to act quickly, determine the level of impact and contain the incident. Visit the Report an Incident [4] web page to learn more.

Information security incidents can happen to anyone. No retaliation will be taken against anyone who, in good faith, reports a possible information security incident.

To learn more about phishing emails and cybersecurity, visit the Office of Information Security [5].

cybersecurity [6], Outlook email [7]

Display Title:

Stay vigilant against phishing attempts

Send email when Published:

No

Links

[1] https://www.cu.edu/blog/tech-tips/stay-vigilant-against-phishing-attempts [2] https://www.cu.edu/blog/tech-tips/author/110439 [3] https://www.cu.edu/security/cybersecurity-awareness-month [4] https://www.cu.edu/security/reporting-incident [5] https://www.cu.edu/security [6] https://www.cu.edu/blog/tech-tips/tag/cybersecurity [7] https://www.cu.edu/blog/tech-tips/tag/outlook-email