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

Cybercriminals Like to Phish - Don't Take the Bait [1]

Phishing – when a cybercriminal poses as a legitimate party in hopes of getting individuals to engage with malicious content or links – remains one of the most popular tactics among cybercriminals today. According to Spanning, 80% of cybersecurity incidents stem from a phishing attempt. However, even though phishing has gotten more sophisticated, keeping an eye out for typos, poor graphics, and other suspicious characteristics can be telltale signs that the content is potentially coming from a phish.

Signs can be subtle

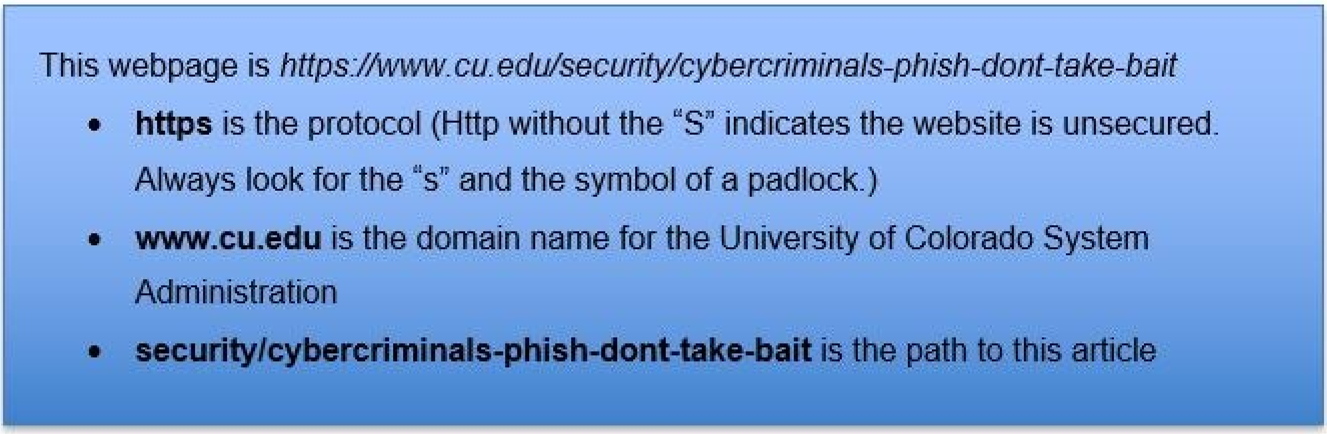
Recognizing the signs of a phishing attempt can help you avoid falling for it. Before clicking any links or downloading attachments, take a few seconds and determine if the email is legitimate. Here are some quick tips on how to spot a phishing email:

- Does it contain an offer that’s too good to be true?
- Does it include language that’s urgent, alarming, or threatening?
- Is it poorly crafted writing riddled with misspellings and bad grammar?
- Is the greeting ambiguous or very generic?
- Does it include requests to send personal information?
- Does it stress an urgency to click on unfamiliar links or attachments?
- Is it a strange or abrupt business request?
- Does the sender’s e-mail address match the company it’s coming from? Look for little misspellings like pavpal.com or anazon.com.
- Does it contain links? If so, does the link's URL match what you expect to see?

More about URLs

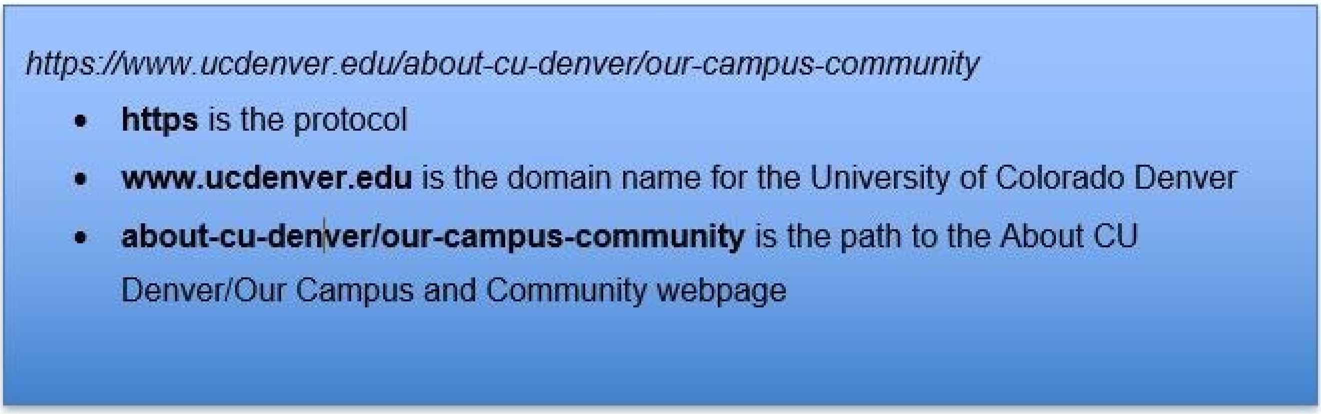
A URL (Uniform Resource Locator) is the electronic address for a unique resource on the web. Reading URLs can be helpful in identifying a phish. Check out this brief video, Understanding URLs [2], and then view the CU examples below.

Here are two URLs at the University of Colorado.



This webpage is *https://www.cu.edu/security/cybercriminals-phish-dont-take-bait*

- **https** is the protocol (Http without the “S” indicates the website is unsecured. Always look for the “s” and the symbol of a padlock.)
- **www.cu.edu** is the domain name for the University of Colorado System Administration
- **security/cybercriminals-phish-dont-take-bait** is the path to this article

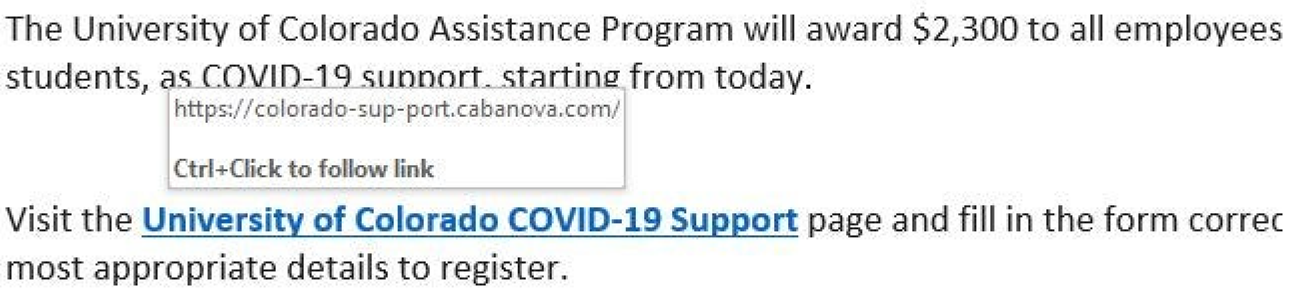


https://www.ucdenver.edu/about-cu-denver/our-campus-community

- **https** is the protocol
- **www.ucdenver.edu** is the domain name for the University of Colorado Denver
- **about-cu-denver/our-campus-community** is the path to the About CU Denver/Our Campus and Community webpage

To see the URL, hover your cursor over the link - the tooltip box will appear - and verify that the URL leads to a site you recognize. This methods works for email attachments, too. (How to verify links on mobiles devices will depend on the device.)

Here are examples of URLs contained in phishing emails:

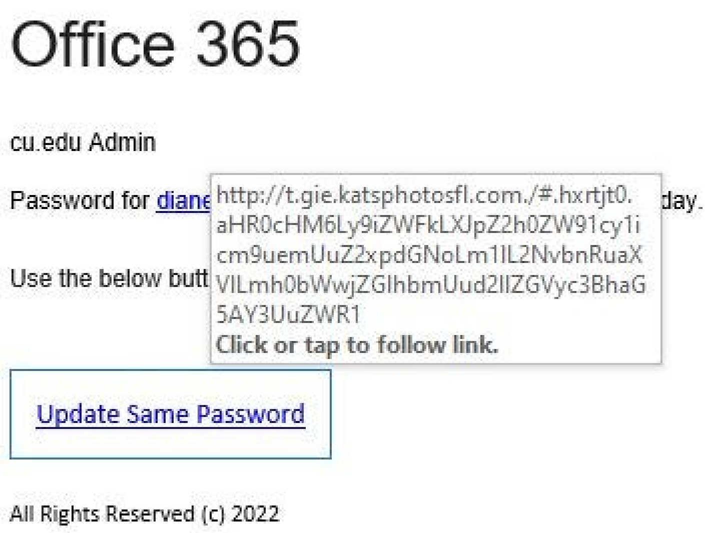


The University of Colorado Assistance Program will award $2,300 to all employees students, as COVID-19 support, starting from today.

https://colorado-sup-port.cabanova.com/

Ctrl+Click to follow link

Visit the University of Colorado COVID-19 Support page and fill in the form correc most appropriate details to register.



Office 365

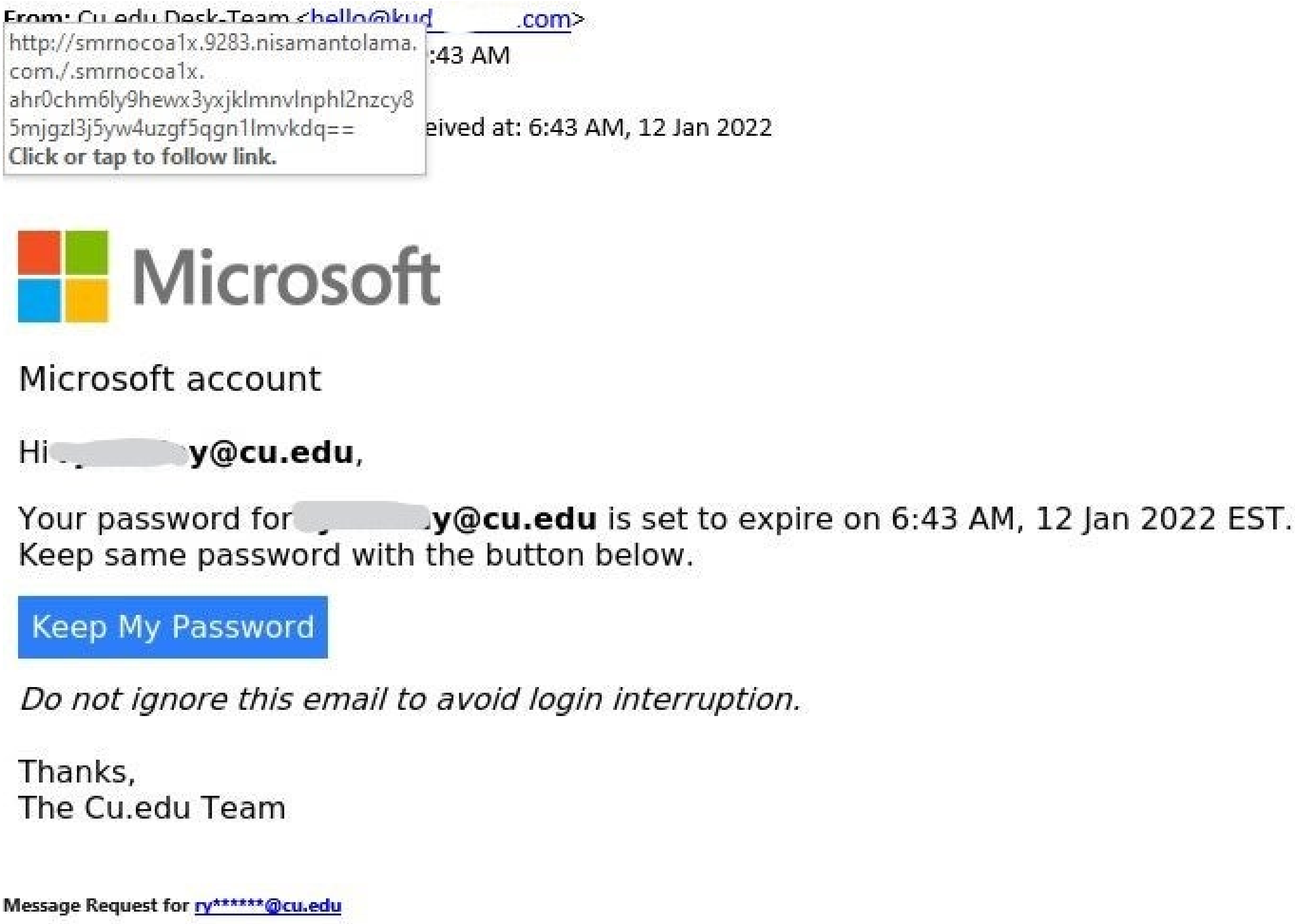
cu.edu Admin

Password for diane day.

Use the below butt

http://t.gie.katsphotosfl.com./#.hxrtjt0.
aHR0cHM6Ly9iZWFkLXJpZ2h0ZW91cy1i
cm9uemUuZ2xpdGNoLm1lL2NvbnRuaX
VlLmh0bWwjZGlhbmUud2llZGVyc3BhaG
5AY3UuZWR1
Click or tap to follow link.

All Rights Reserved (c) 2022



From: Cu.edu Desk-Team <hello@kud .com>

http://smrnocoa1x.9283.nisamantolama.com./.smrnocoa1x.ahr0chm6ly9hewx3yxjklmnvlnphl2nzcy85mjgzl3j5yw4uzgf5qgn1lmvkdq==
Click or tap to follow link.

:43 AM

eived at: 6:43 AM, 12 Jan 2022

Microsoft account

Hi [redacted]**y@cu.edu**,

Your password for [redacted]**y@cu.edu** is set to expire on 6:43 AM, 12 Jan 2022 EST.
Keep same password with the button below.

Keep My Password

Do not ignore this email to avoid login interruption.

Thanks,
The Cu.edu Team

Message Request for ry******@cu.edu

Remember...

When in doubt, throw it out: links in emails, social media posts, and online advertising are often how cybercriminals try to steal your personal information. Even if you know the source, if something looks suspicious, delete it.

Learn more

- Phishing Scams FAQs [3]

Groups audience:
Office of Information Security

Source URL:https://www.cu.edu/security/cybercriminals-phish-dont-take-bait

Links
[1] https://www.cu.edu/security/cybercriminals-phish-dont-take-bait
[2] https://training.knowbe4.com/modstore/view/9e96a153-a5a0-428c-abe1-d24cbe71386d
[3] https://www.cu.edu/security/awareness/phishing-scams-faqs