Phishing Scams FAQs [1]

Important to know

CU or any reputable organization will **never** ask for your passwords in an email or phone call.

Cybercriminals Like to Phish, but Don't Take the Bait

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 a 2021 report by Spanning, 80% of cybersecurity incidents stem from a phishing attempt. However, while phishing has gotten more sophisticated, keeping an eye out for typos, poor graphics and other suspicious characteristics can be a telltale sign that the content is potentially coming from a phish.

What is phishing?

Phishing is a type of electronic scam. Cybercriminals use deceptive tactics to manipulate people into doing what they want with the goal of stealing information and money. They use phishing because, unfortunately, it’s easy to do and often effective.

The tactics used, sometimes called “social engineering,” are the foundation of all phishing scams conducted through emails, text messages, and cell phone calls. As technology becomes more advanced, so do the cybercriminals' tactics.

Make the cybercriminals job harder and ineffective by recognizing the red flags when receiving unusual or unexpected messages.

What are some tactics used in phishing scams?

Tactics often found in phishing scams range from a fake and malicious web link to a directive that appears to come from your supervisor or a university leader.

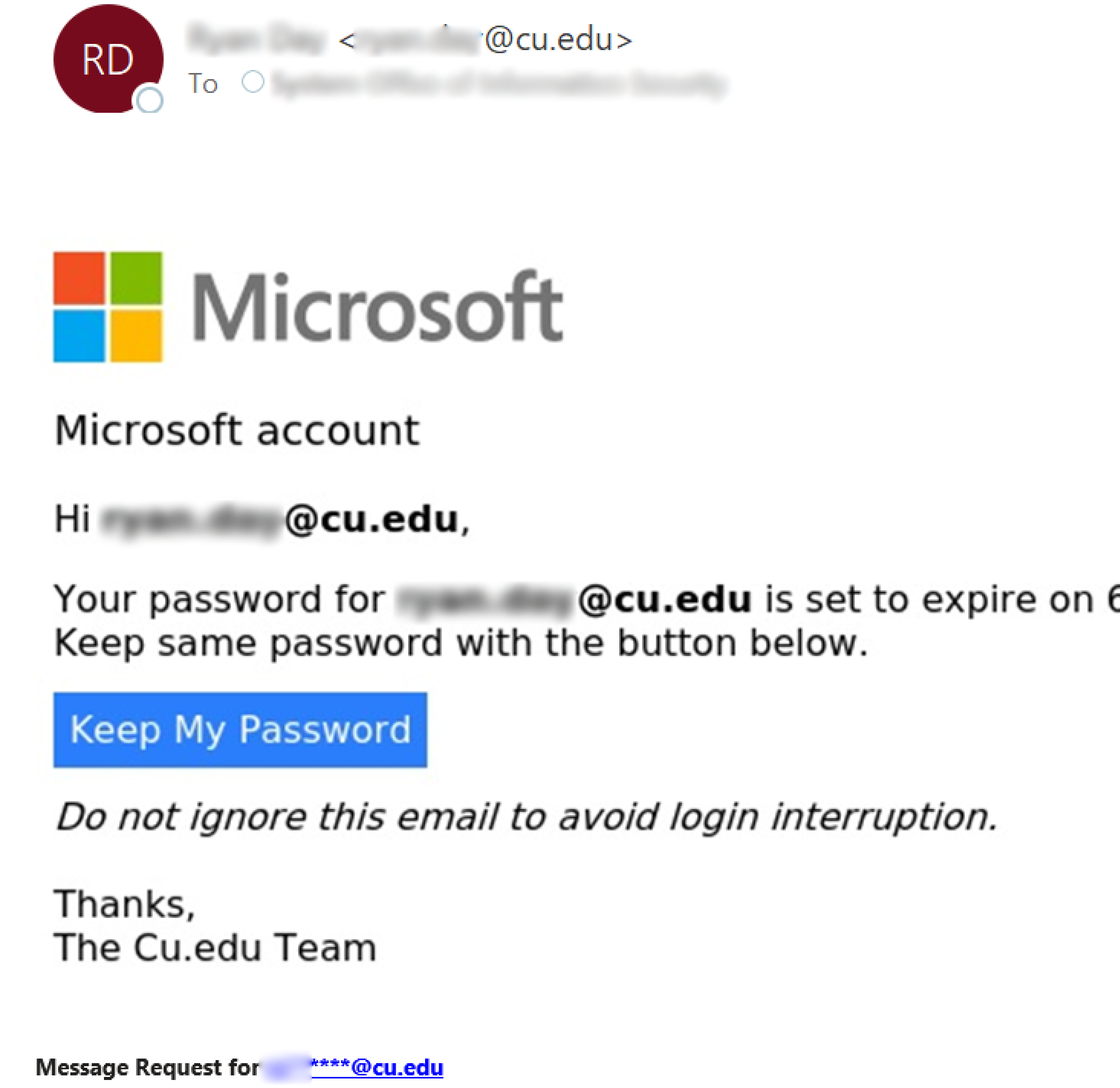
When receiving an unusual or unexpected message, look for these tactics and red flags:

Play on emotions

Phishing messages are often written to generate emotions that will motivate you to take immediately action; fraudsters don't want you to take time to consider the message's legitimacy. The most common emotions include a sense of fear or urgency, or an award of good fortune—something that is too good to be true.

Some real examples:

- Your email account is or will be locked.
- Your computer is infected or compromised.
- You're a cash prize winner for a drawing you never entered. To receive the prize, you are required to prepay the taxes through a wire transfer.
- You're threaten with legal action by a government agency unless payment is promptly made with gift cards.



RD

[redacted] <[redacted]@cu.edu>

To ○ [redacted]

Microsoft

Microsoft account

Hi [redacted]@cu.edu,

Your password for [redacted]@cu.edu is set to expire on 6
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 [redacted]**@cu.edu**

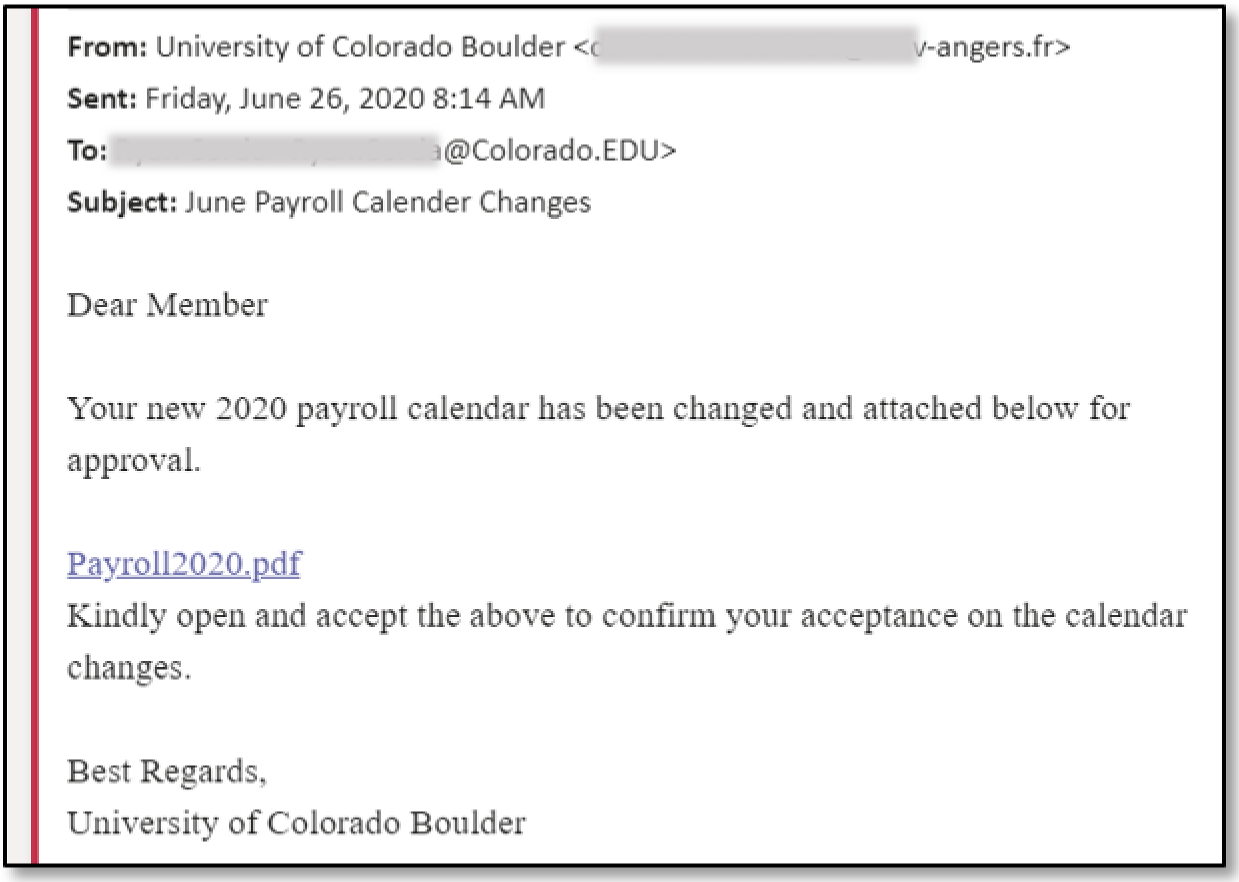
Fake, malicious links and attachments

Cybercriminals can use links and attachments to deliver malware—malicious software—to your computer and possibly gain access to CU networks and sensitive work information. Such access may also allow them to lock your computer for ransom until a payment is received.

Malicious links can be disguised to look like trusted links and take you to fake or infected websites. Attachments can appear to come from a known source, but whose account has been compromised.

Some real examples:

- You receive an email that appears to come from Microsoft stating, “issues with your account” and includes a link titled “Secure Account Here.” By hovering the cursor over the link, you see that the real URL is “microsoft-support.com.” Microsoft has no such link.
- You are urge to open an unexpected attachment from the university. You are asked to review and confirm your acceptance of changes to the payroll calendar.



From: University of Colorado Boulder <[redacted]-angers.fr>
Sent: Friday, June 26, 2020 8:14 AM
To: [redacted]@Colorado.EDU>
Subject: June Payroll Calender Changes

Dear Member

Your new 2020 payroll calendar has been changed and attached below for approval.

Payroll2020.pdf
Kindly open and accept the above to confirm your acceptance on the calendar changes.

Best Regards,
University of Colorado Boulder

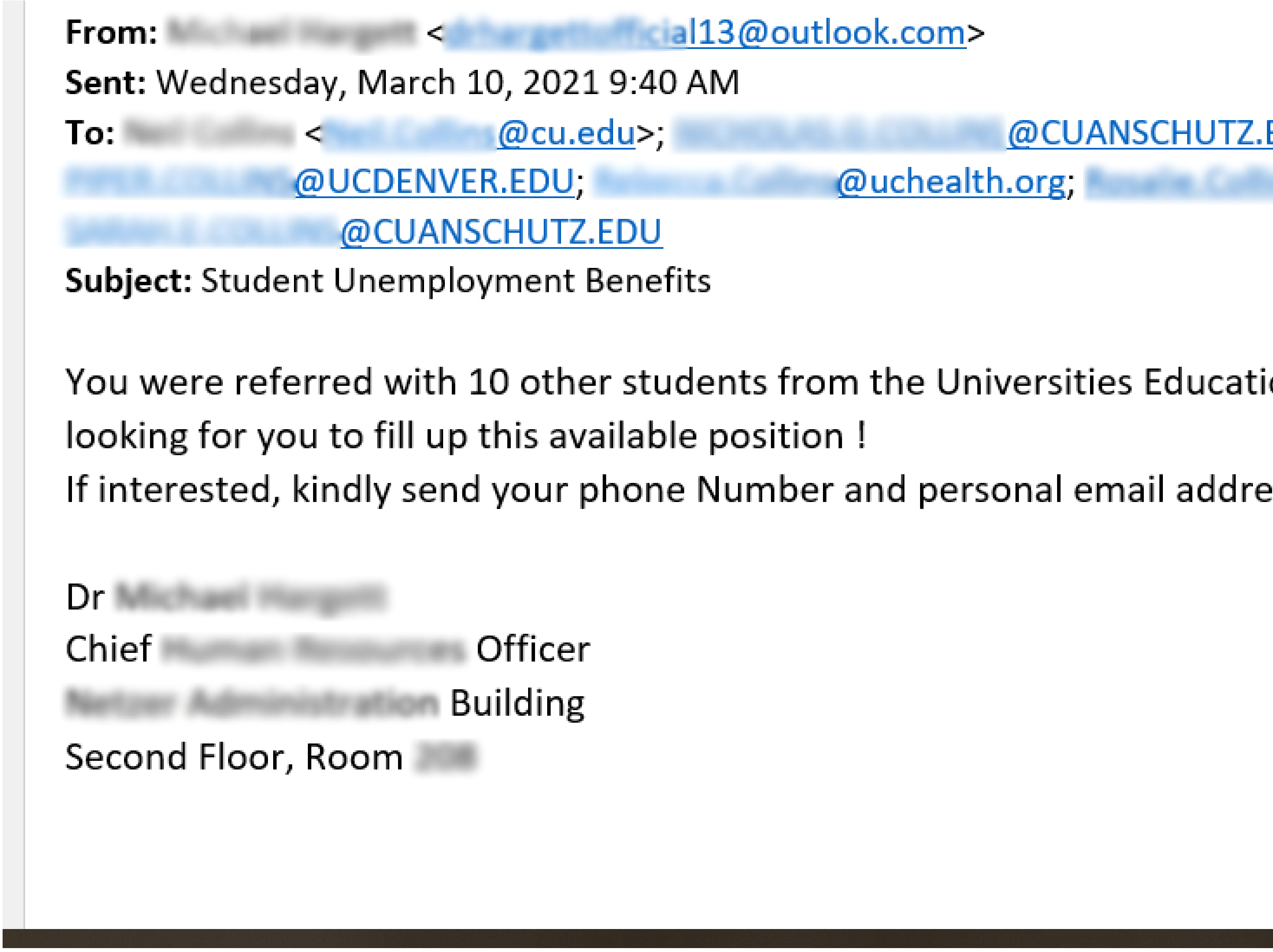
Fraudulent data entry

You’re prompted to fill in sensitive information like user names, passwords, and financial information.

Some real examples:

- Soon after applying for a job, you receive an offer. No interview is necessary; simply complete the attached credit report form and the job is yours.
- You receive an email that appears to come from CU informing you to “upgrade your mail quota.” You are instructed to enter your campus portal password. A legitimate email

from your campus IT department will never direct you to enter confidential information into an email.



From: [redacted] <[redacted]ial13@outlook.com>
Sent: Wednesday, March 10, 2021 9:40 AM
To: [redacted] <[redacted]@cu.edu>; [redacted]@CUANSCHUTZ.E
[redacted]@UCDENVER.EDU; [redacted]@uchealth.org; [redacted]
[redacted]@CUANSCHUTZ.EDU
Subject: Student Unemployment Benefits

You were referred with 10 other students from the Universities Educati
looking for you to fill up this available position !
If interested, kindly send your phone Number and personal email addre

Dr [redacted]
Chief [redacted] Officer
[redacted] Building
Second Floor, Room [redacted]

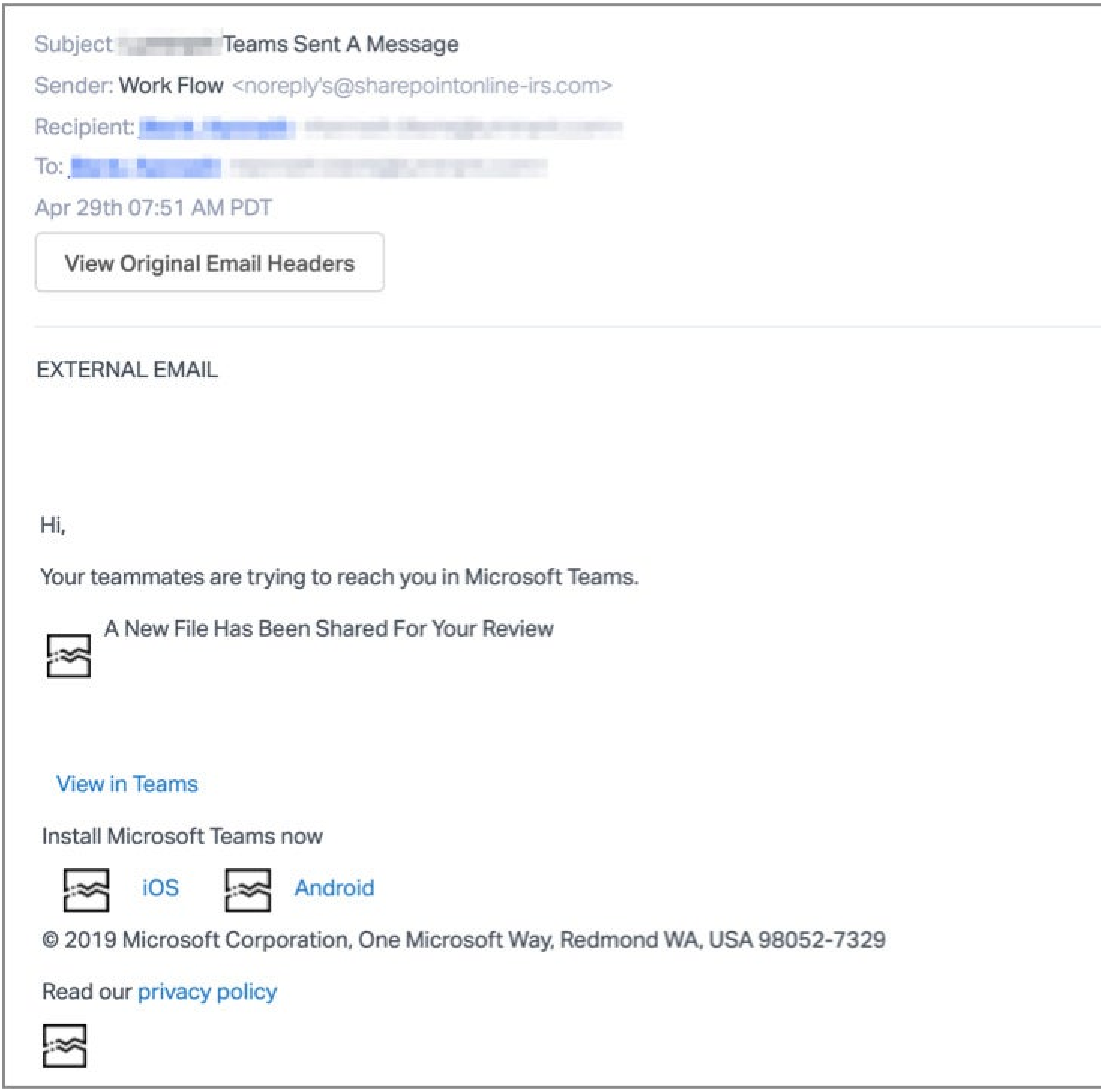
Impersonation of individuals or companies

By impersonating an individual or company or both, cybercriminals can send phish that looks legitimate. They use compromised email accounts and addresses to send the phish. To appear more authentic, business logos are often copied from the Internet and added to the message.

Be aware: cybercriminals may send email that appears to come from a CU address, such as @cu.edu or @colorado.edu. (Think of a return address on a postal letter; someone can list whatever return address they would like, but that doesn't guarantee that is who sent the letter.) The cybercriminal's intention of the email is to get you to click links or open attachments.

Some real examples:

- Staples sends you an email notification that there are delivery issues with your office supply order. You are instructed to click on the link to resolve the issue and schedule another delivery. The logo and formatting look like a Staples email; however, when you hover the cursor over the link, it indicates the URL is "staples-delivery-876976.com," which is not a legitimate address for the site.
- Phishing emails appearing to come from Microsoft Teams have targeted as many as 50,000 Teams users with the goal of obtaining Office 365 logins.



Subject [redacted] Teams Sent A Message

Sender: Work Flow <noreply's@sharepointonline-irs.com>

Recipient: [redacted]

To: [redacted]

Apr 29th 07:51 AM PDT

EXTERNAL EMAIL

Hi,

Your teammates are trying to reach you in Microsoft Teams.

A New File Has Been Shared For Your Review

View in Teams

Install Microsoft Teams now

iOS Android

© 2019 Microsoft Corporation, One Microsoft Way, Redmond WA, USA 98052-7329

Read our privacy policy

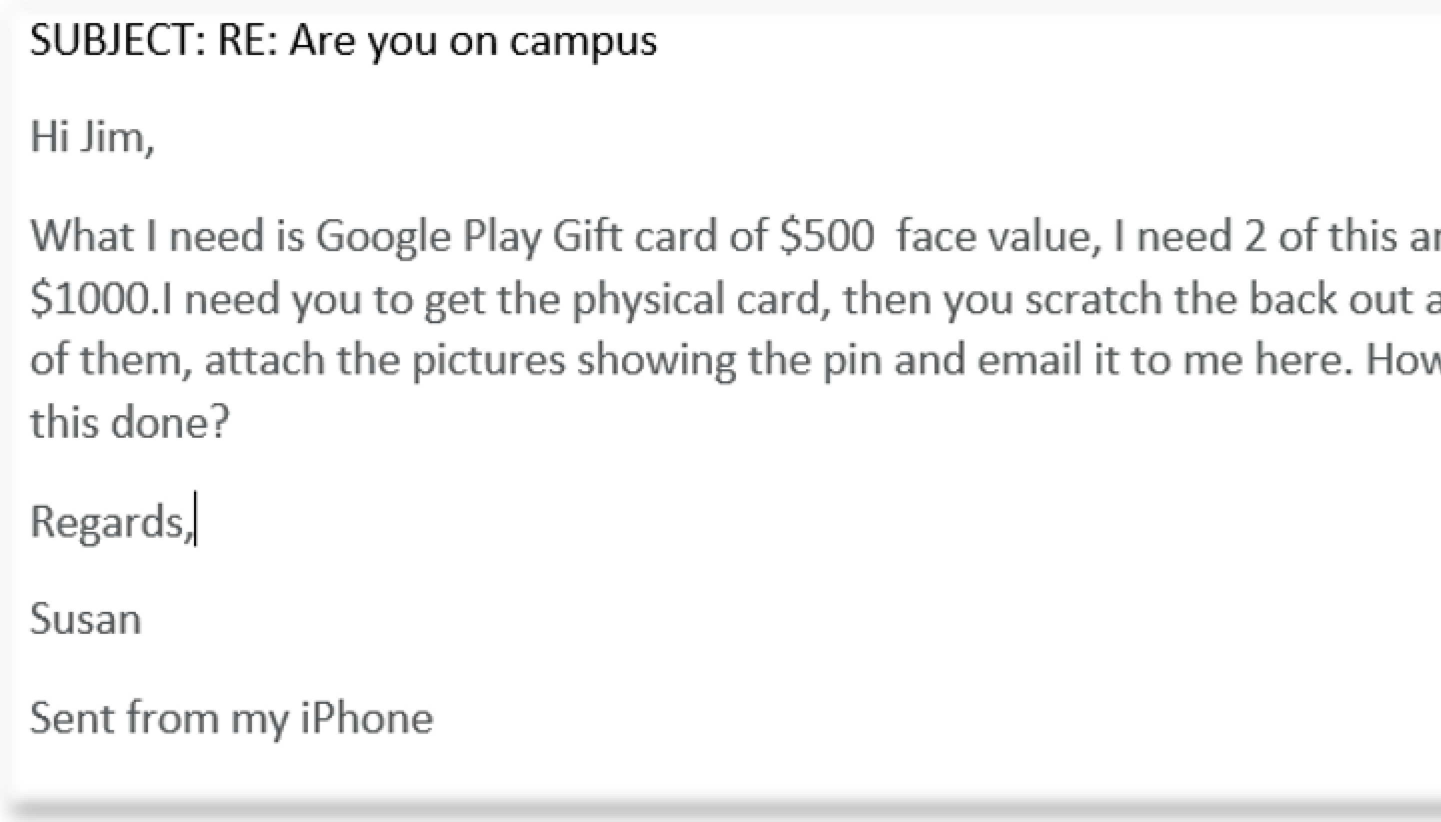
[2]

There's no link, attachment, or data entry request. What’s the catch?

Cybercriminals get more creative, making it more difficult to detect fraud. Recent phishing scams don’t use malicious links or attachments and appear to come from your supervisor, campus leaders, or departments.

Some real examples

- One common phishing email making its way through the university is the gift-card scam. The scam typically starts with a brief email exchange, such as “are you in the office” or “have a special favor to ask.” If you respond, appearing to fall for the impersonation, you will be asked to promptly purchase several gift cards and email the card numbers to them.



SUBJECT: RE: Are you on campus

Hi Jim,

What I need is Google Play Gift card of $500 face value, I need 2 of this ar
$1000.I need you to get the physical card, then you scratch the back out a
of them, attach the pictures showing the pin and email it to me here. How
this done?

Regards,

Susan

Sent from my iPhone

[3]

How can I avoid getting scammed?

- Don't react to tactics aimed to scare you into taking urgent action, including: threats of a lawsuit, a computer full of viruses, locked accounts, or opportunities to earn or save money now.

- Don’t reveal personal or financial information in an email or text messages. (CU will never ask you for your username or password.)

- Don’t open email attachments you are not expecting, even if it appears to come from someone you know. Their account may have been compromised.

- Be cautious of links provided in an email. Hover the cursor over the link to verify that the URL leads to a site you recognize. (How to verify links on mobiles devices will depend on the device.)

- Verify the legitimacy of charities and crowdfunding sites before making donations. Do not provide donations in cash, gift cards, or money wires.

- If you are unsure whether an email request is legitimate, try to verify it by contacting the sender or company directly by an alternate known communication method.

- When in doubt, throw it out. If it looks suspicious, even if you know the source, it’s best to delete or, if appropriate, mark it as junk.

- Think before you respond:

  - Emails from a university leader asking you to make an urgent wire transfer or buy gift cards are likely to be scams.

  - No one from your campus IT department is going to call to inform you about a computer virus and ask for your passwords.

  - Government agencies will not call and threaten you, or make demands for payment in the form of gift cards.

I’m still not sure if it’s a legitimate message or a phish. What should I do?

You don't have to be an expert. If something seems suspicious, it probably is. For university-related messages, forward emails to your campus IT or Information Security office and we’ll look into it for you.

For suspicious messages sent to your personal account, do your research to see if the message if legitimate:

- Contact known persons or companies directly.
- If the sender is unknown, see if the organization actually exists and call them directly.
- Consider ignoring and deleting the message.

What should I do if I opened a suspicious link or attachment or inadvertently shared sensitive information?

Immediately report it as a possible incident. Visit the Report an Incident [4] web page to learn more.

How do I avoid receiving phishing scams in the first place?

The surest way to avoid receiving phishing scams is to live off-the-grid somewhere high in mountains of no-where. For the rest of us, here are some suggestions:

- Be mindful of what you share online. Fraudsters can easily collect email addresses from numerous sources.
- Use email spams filters for your personal devices and accounts.
- Be cautious when joining loyalty or rewards programs. Some companies may unknowingly sell or share your information to deceitful data brokers.

How can I report personal or home phishing scams?

You can report a phishing scam attempt directly to the company that is being impersonated. You can also send reports to the Better Business Bureau at bbb.org [5] and Federal Trade Commission at ftc.gov [6].

Learn more about phishing:

- CU Boulder [7]
- CU Denver / Anschutz Medical Campus [8]
- UCCS [9]

Groups audience:
Office of Information Security
Right Sidebar:

Password Managers

Source URL:https://www.cu.edu/security/awareness/phishing-scams-faqs

Links
[1] https://www.cu.edu/security/awareness/phishing-scams-faqs
[2] https://www.cu.edu/sites/default/files/MS%20Teams%20Phish%201.jpg
[3] https://www.cu.edu/sites/default/files/Gift%20Card%20Email%20Image%202.PNG
[4] https://www.cu.edu/security/reporting-incident [5] https://www.bbb.org/ [6] https://www.ftc.gov/
[7] https://oit.colorado.edu/it-security/phishing-emails/report-suspicious-messages
[8] https://www.cuanschutz.edu/offices/information-security-and-it-compliance/resources/isic-education-and-awareness/phishing [9] https://oit.uccs.edu/phishing-awareness