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

CU's Phishing Awareness Program [1]

July 16, 2020 by Janet Bravo, OIS [2]

Phishing scams are one of the leading online threats to people at work and at home. According to a 2020 report by Verizon, phishing scams continue to be the top cause of incidents and breaches in the education sector. Motivated by financial gains, cybercriminals primarily targeted personal information and account credentials. Cybercriminals use the phishing technique because, unfortunately, it's easy to do and often effective.

The University of Colorado implemented a phishing awareness program many years ago in an effort to help you be successful in recognizing phishing tactics and red flags when receiving a suspicious email. Over three years ago, phishing simulation was added to the suite of awareness and training tools to help you identify legitimate emails. In that time, technology has become more advanced, and so have the cybercriminals' tactics. Because of this, we are ramping up our awareness efforts.

Beginning this month, the Office of Information Security will send a simulated phishing email to all employees each month. The simulated phish may appear to come from an IT department, Microsoft Teams or Zoom, or vendors we use for services or supplies. Those who inadvertently respond to a simulated phish will receive an immediate response in the form of an educational page that highlights the red flags in that specific phish example.

The goal of the phishing simulation is educational and protective, not punitive. The results are confidential. CU's information security team, and no one else, will have access to the details regarding which employees responded to the messages. This information may be used to better target which emails are sent and which training materials are presented. The information security team may also reach out directly to individuals for follow-up.

Keep an eye out for new awareness and training opportunities from the Office of Information Security that will be made available in the coming months.

Learn more about phishing simulation [3] at CU.

As a reminder, if you receive a suspicious email:

- Don't trust the display name - A favorite phishing tactic among cybercriminals is to fake the display name of an email.
- Check the links - Hover your mouse over any links in the body of the email. If the link address has numbers or special characters don't click on it. Check for spelling mistakes - Companies are pretty serious about email. Legitimate messages from companies usually do not have major spelling mistakes or poor grammar.
- Beware of urgent or threatening language in the subject line - Invoking a sense of urgency or fear is a common phishing tactic. Beware of subject lines that claim your

"account has been suspended" or your account had an "unauthorized login attempt."
- Don't click on attachments - Including attachments that contain viruses and malicious software (malware) is a common phishing tactic. Malware can damage files on your computer, steal your passwords or spy on you without your knowledge. Don't open any email attachments you weren't expecting.

Report Suspicious Email

The university relies on you to report suspicious email that you receive at work. This allow us to investigate its legitimacy, and if necessary, block other attempts from reaching more email boxes.

If you receive or inadvertently respond to a suspicious email, report it to your campus contact listed below:

- System Administration: security@cu.edu [4]
- CU Boulder: phish@colorado.edu [5]
- CU Denver and Anschutz Medical Center: phishing.samples@ucdenver.edu [6]
- UCCS: helpdesk@uccs.ed [7]

Display Title:
CU's Phishing Awareness Program
Send email when Published:
No

Links
[1] https://www.cu.edu/blog/ois-blog/cus-phishing-awareness-program [2] https://www.cu.edu/blog/ois-blog/author/28163 [3] https://www.cu.edu/security/cu-phishing-simulation [4] mailto:security@cu.edu [5] mailto:phish@colorado.edu [6] mailto:phishing.samples@ucdenver.edu [7] mailto:helpdesk@uccs.ed