Phishing Awareness [1]

What is Phishing?

Phishing scams are crude social engineering tools designed to induce panic in the reader. These scams attempt to trick recipients into responding or clicking immediately, by claiming they will lose something (e.g., email, bank account). Such a claim is always indicative of a phishing scam, as responsible companies and organizations will never take these types of actions via email.

Phishing scams are typically fraudulent email messages appearing to come from legitimate enterprises (e.g., your university, your Internet service provider, your bank). These messages usually direct you to a spoofed web site or otherwise get you to divulge private information (e.g., passphrase, credit card, or other account updates). The perpetrators then use this private information to commit identity theft.

The University of Colorado and other reputable organizations will never use email to request that you reply with your passphrase, Social Security number, or confidential personal information. Be suspicious of any email message that asks you to enter or verify personal information, through a web site or by replying to the message itself. Never reply to or click the links in a message. If you think the message may be legitimate, go directly to the company's web site (e.g., type the real URL into your browser) or contact the company through a known communication channel to see if you really do need to take the action described in the email message.

What is Phishing Simulation?

Phishing simulation involves periodically sending “phishing” emails to employees and students. If individuals respond to the messages, we recommend that they take one minute to review the very brief educational material that is presented afterward. The intent of this program is to improve awareness and help us understand how to better address phishing.

These simulated scams are completely safe and there are no negative consequences if you mistakenly reply to a simulated phishing message. The Office of Information Security will not share responses from individual employees or students with anyone else. The focus of the output is on aggregated statistics about response rates and no further information will be shared.

The Office of Information Security currently sends approximately 20,000 simulated phishing emails to employees on a quarterly basis. Users who click these emails receive additional training to increase their awareness about ways to better detect and avoid phishing emails in the future.
Here are some frequently asked questions that should help explain how the program works:

Q: How do I know that emails are legitimate and not a simulation or a real phish?
A: Your training starts now!

- 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.
- You have to read all URLs carefully. To check the link in an email, hover your mouse over the URL to verify that it leads to a site you recognize. The real link will be displayed either in a pop-up or in the lower part of your email program's window.
- Don’t reveal personal or financial information in an email, and do not respond to email solicitations for this information. This includes following links sent in email.
- 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.

Q: Is there anything you can provide me so that I can find out more about CU's process for handling phishing emails?
A: Yes! You can review your campus' phishing educational materials:

- UCCS [2]
- CU Boulder [3]
- CU Denver | Anschutz Medical Center [4]
- CU System Office [5]

Q: What is the educational portion of the phishing simulation program?
A: If a user takes action on a simulated phishing email they will be directed to educational materials or a video. There will be an "Acknowledge" button on each training to report that the training has been completed. On average, most users complete it in 60 seconds.

Q: How does this benefit me?
A: This training will help you secure University of Colorado data as well as your personal accounts, computers, and mobile phones. Every phishing simulation will help you to become a "smart skeptic" to avoid malicious phishing emails.

Q: Will my manager be told if I click on a simulated phishing message link?
A: No. The goal of the phishing simulation process is educational and not punitive. As such, the results are confidential and only information security staff will have access to the details regarding which users responded to the messages. This information may be used to better target which emails are sent and which training materials are presented, as well as the potential for information security staff to reach out directly to individuals for follow-up.

Q: How will the information collected in this program be used?
A: The information security staff will provide summary information of the results to a variety of oversight and governance groups. These summaries will include information like response rates for different user populations (a campus, school, department, etc.) to help inform
decisions on training and awareness as well as demonstrate improvements over time. In addition, customized reports are available for departments that would like to view overall statistics about how well they are doing.

Q: I'm a manager/leader at CU and I'd like more information on how my department reacts to simulations. How do I get more information and what can you tell me?
A: To learn more about your department’s handling of the simulated phishing, please contact security@cu.edu [6]. Those in leadership roles may request a summarized report for their area. The Office of Information Security will not provide departments with information on specific individuals. To preserve confidentiality, we will not provide data for departments that are so small that a summary might provide insight into individual responses. Check out Phishing Education and Awareness Tool [7] for additional service offerings available through OIS!

Q: Why do you need our help? Don’t we have security?
A: The security systems we have in place have made attackers shift their sights from our servers and firewalls to our employees. Everyone in an organization is a target. The attacker’s goal is to break into your computer or mobile phone that has access to our network.

Q: What recent phishing emails have been reported?
A: The University of Colorado has a diverse landscape and, as such, each campus has their preferred method of displaying recent phishing activities that have been reported. To see what phishing messages your campus recently reported, please click on your campus link below.

CU Boulder [3]
CU Denver | Anschutz Medical Center [8]

Q: Does this really help??
A: Yes. Many other universities, including the Boulder campus, have seen a reduction in the number of individuals who fall victim to phishing.

Q: How can I report phishing emails to external entities?
You can report a phishing scam attempt directly to the company that is being impersonated. You can also send reports to the Federal Trade Commission (FTC) [9]. Depending on where you live, some local authorities also accept phishing scam reports. Details can be sent to the Anti-Phishing Working Group [10], which is building a database of common scams to which people can refer.

Groups audience:
Office of Information Security

Source URL: https://www.cu.edu/ois/tools-and-services/phishing-awareness

Links
[5] https://www.cu.edu/ois/so-youve-been-phished-what-now
[6] mailto:security@cu.edu
[8] https://www1.ucdenver.edu/offices/office-of-information-technology/software/secure-campus