College of the Desert's Information Technology team would like to remind you about best email practices from a security standpoint.

- Do not open attachments or click on links in emails that you are not expecting. This is true even if the sender appears to be from within COD. Hover over the link to ensure legitimacy before clicking. Any email that is suspicious, please delete.
- Check the URL by hovering over the sender's address to ensure legitimacy. If not legitimate, please delete.
- If you respond to a suspicious email in error, please change your password immediately.
- Use strong passwords. Strong passwords include upper and lower case, numbers, and special characters. Think in terms of phrases as opposed to one word.
- Do not send personal information via email or in attachments. This includes social security numbers and birthdates.

For additional information about email red flags, click here.