Lewis & Clark

615 S. Palatine Hill Road
Portland, Oregon 97219
Phone 503-768-7000
lclark.edu

LC Network Notice **lc-bulletin@lclark.edu**
Phishing Scheme Targeting LC Students **11.17.22**

Dear Students,

It has come to our attention that some of you have been targeted in an email phishing scheme made to appear as though you were being offered employment in an academic research project. This scheme involved sophisticated social engineering where a scammer presented as a known LC professor. The emails were so convincing that at least one student had several interactions with the scammer before handing over valuable information, reminding us that as scammers become more sophisticated we must become more diligent in ensuring we know who we are communicating with before giving out personal information.

Based upon our review of available data we have learned that the phishing emails did not originate from any LC email account. The emails were "spoofed," meaning they were deliberately made to appear as though they were from a sender that they were not. All reports of spoofed emails received by LC students were sent to personal email accounts. Spoofed emails sent to LC email accounts were caught by our email filters and quarantined before they were seen by the intended recipients. We have found no evidence of a data breach or account compromise.

This incident is an unfortunate reminder that cybercrime has become incredibly common. We all play a part in data security. Please play an active role in keeping your data secure by ***Stopping, Looking, and Thinking***: ***Stop*** and resist immediate action when receiving an email; ***Look*** for anything unusual in the message or of the sender; and ***Think***, does something seem "phishy"?

When contacting you about financial or other sensitive information, Lewis & Clark will never:

- ask you to email sensitive personally identifiable information such as a tax return, W-2, or Social Security Number (whole or partial).
- charge a fee to process a financial aid application (this is a common scam).
- process payments related to tuition, payroll, or expense reimbursements via cash transfer apps such as Venmo or Zelle.
- request your password.

Be aware of these warning signs of phishing:

- The message may have an unusual "From" address or an unusual "Reply-To" address rather than a recognizable "@lclark.edu" address. An example is fao.lclark.edu@gmail.com
- Phishing messages are often delivered outside normal delivery schedules such as emails normally delivered during business hours but instead at 3 a.m., or a monthly bill delivered midcycle.
- The subject line of the email is irrelevant or does not match the message content.
- The email is about something you never requested or a receipt for something you never purchased.
- The message is not personalized. Valid messages from banks and other legitimate sources usually refer to you by name.
- There are grammar or spelling errors.
- The email is asking you to look at compromising or embarrassing pictures of yourself or someone you know.
- The email requests payment to people or organizations via services such as Venmo or Zelle.
- You have an uncomfortable feeling, or it just seems odd or illogical.

What to do with phishing messages:

- If you suspect the message is phishing but want to be sure, reach out directly to the person or organization using saved contact information or information found on a trusted website.
- If using Gmail in your browser, click on the kebab menu (three vertical dots menu in the upper right corner) and select “Report Phishing”. This will help Google—and therefore L&C—identify the offending message for quarantine.

Together we can protect our data, systems, and user community.

Adam Buchwald

Associate Vice President & Chief Information Officer