Lewis & Clark

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

lc-bulletin@lclark.edu **12.15.22**
Cybersecurity Alert: Holiday Phishing Scams

Faculty, Staff, and Students,

'Tis almost the season for winter break, which means 'tis already the season for phishing scams!

As you shop and book travel and take care of school and work tasks online, please be careful and be safe. This is the time of year when common phishing attacks—those that push you to accept a prize, check on the delivery of a package you are not expecting, provide time-sensitive information to payroll, check your tax status, and more—are at their height.

When you receive such requests, remember to stop, look, and think. ***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"?

Keep the following recommendations in mind as when managing your inbox and spending time online:

- Do not click on links promising information about pay bonus, bank account issues, and such. L&C will never ask you to email sensitive information such as a tax return, direct deposit bank account numbers, W2, or SSN. If you need information about pay, direct deposit, tax forms, etc, go directly to your Workday account.
- Use apps that you know and trust. Download software from verified sources such as the App Store or Google Play.
- Verify that attachments are safe before downloading them. Cybercriminals may ask you to download a virus-containing attachment in order to view an update to your order, claim a prize, or change your payment method.
- Pause before you open an email. Ask yourself if you were expecting that offer or the notice of that prize gift card, or if you have a package scheduled for delivery that may be delayed?
- Verify links before clicking. When online shopping, click only on ads or links from a reputable source such as a retailer's official social media profile.
- Avoid use of public wi-fi networks. Always disable the option to automatically connect to wi-fi networks on your phone, tablet, or computer. Instead, manually choose which network you'd like to join and that you know are safe.
- Use the official apps from FedEx, USPS, and UPS rather than clicking on a text message link claiming your packages are delayed or canceled, particularly if you don't remember ordering something to be delivered.

When you receive suspicious messages, we recommend the following:

- 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.

Enjoy a safe and restful winter break,

Ann Harris
Information Security Officer