From: LC Network Notice
<lc-bulletin@lclark.edu>
Date: March 8, 2023

(3/8/23) Urgent Network Outage Update

Dear LC Community,

Work has continued today on rebuilding our IT infrastructure so that we can restore our IT systems and make them available to the campus. The infrastructure needs to be rebuilt in a careful and methodical manner before end-users will see much tangible progress, but please know that significant progress is being made through round-the-clock effort. We have been able to provide access to some of our externally hosted systems, such as Slate, Box, Panapto, Parchment, Salesforce, and StarRez, to a fair number of campus users. And a delivery of wifi hotspots will arrive tomorrow and be deployed strategically on campus to improve wifi service.

However, access to systems that require authentication through the Lewis & Clark single sign-on system remains unavailable for most users. **It is likely that these systems will remain down for the remainder of the week,** but we are optimistic that significant advances in access will occur next week.

The Pionet-Guest wifi network was down for a portion of today, and there have been reports of phones not ringing as they would normally. This is simply the result of operating with significantly diminished IT capacity. As progress is made to complete the build-out of the IT infrastructure, these systems will stabilize.

We know that many of you have questions about data integrity and whether any of your files or personal information may have been compromised. At this point, the forensic analysis of the cyberattack is not yet complete. This work is complex and time consuming. We are committed to sharing information with the campus community once we have reliable information to share, and we will do so as soon as we can.

We do not know whether or not the persons responsible for the attack are contemplating further hostile actions against institutional systems. **Please be vigilant for suspicious activity**. If you receive any email, text or phone call from a person claiming to have your personal information, immediately report the threat to IT at security@lcark.edu and do not respond.

When you receive any email, 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 a pay bonus, bank account issues, and such. No reputable organization, including LC, will ever ask you to email sensitive information such as a tax return, direct deposit bank account numbers, W2, or SSN.
- Use apps that you know and trust. Download software only 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 an order, claim a prize, or change your payment method.
- Pause before you open an email. Ask yourself if you were expecting an offer or a notice of a 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.
- Use official apps from FedEx, USPS, and UPS rather than clicking on links claiming a package is delayed or canceled, particularly if you don't remember ordering something to be delivered.

If you receive a suspicious message, 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 LC—identify the offending message for quarantine.
- Always exercise extreme caution when clicking on links that are hidden in email text. Try to hover over the text and if the full URL is not available, go directly to the website yourself and navigate to where the message is trying to take you.
- **DO NOT give passwords to anyone!** IT will *never* request this information, nor will the government or any reputable organization, whether it is your bank or your ISP.

Please continue to direct questions to your dean’s office or supervisor. IT staff are hard at work on restoring operations. We have established a webpage with current information on available systems and FAQs and will keep it up-to-date as new information becomes available.

Thank you to the IT team, and to all of you for your patience and support.

The Executive Council.