



From: LC Network Notice
<lc-bulletin@lclark.edu>
Date: March 31, 2023
Update on Cyberattack

Dear LC Community,

As you are aware, we experienced a cyberattack beginning on March 3 which significantly impacted almost all IT systems on campus. We are now at a point in our response in which we are able to share more information about the nature of the incident.

It is common in such an instance for the attackers to use ransomware, which is a type of malicious software, or malware, to prevent the victim from accessing their computer files, systems, and networks until a ransom is paid. We now know that the attack was perpetrated by a group known for similar attacks against educational institutions.

Following the advice of law enforcement and our external experts, the college has chosen not to pay ransom. Instead, we have worked nonstop to rebuild our IT systems from backups which are regularly retained by the college. At the same time, we have been working with a cybersecurity forensic firm to assess whether and to what extent there has been any compromise of protected or otherwise sensitive data as a result of this incident.

The cybercriminals responsible for the incident now claim to have published a limited amount of Lewis & Clark data on a "dark web" website maintained by the threat actors. Our external cyber forensic firm is helping us to investigate this claim. We are currently working to retrieve the information, at which time we will conduct a thorough review. When cybercriminals publish data of this nature, they do so on portions of the internet that are unindexed, not easily searchable, and only accessible by means of special software, which means that it may take a while to investigate the scope and nature of this claim.

Given that we do not have reliable information about the scope or content of the allegedly published data, there is no action for you to take at this time. In the event we determine that the incident resulted in unauthorized access or acquisition of protected information related to students, faculty, staff, parents, or other friends of the college, we will provide notification to impacted individuals in accordance with state and federal regulations.

To date, we do not have evidence that the information involved in this incident has been used for identity theft or financial fraud. We are taking this very seriously and using all resources available to conduct a thorough and diligent review of the impacted data.

As a reminder, if you receive communications from persons claiming to have your personal information, or which are otherwise suspicious, please do not respond, and immediately report the incident to security@lclark.edu.

Once again, we appreciate your patience during our continued response to the incident.

Sincerely,

The Executive Council