LAVC Cybersecurity Event Frequently Asked Questions

LATEST UPDATE (January 6, 2017):

Did LAVC pay the ransom?
In consultation with district and college leadership, outside cybersecurity experts and law enforcement, a payment was made by the District. It was the assessment of our outside cybersecurity experts that making a payment would offer an extremely high probability of restoring access to the affected systems, while failure to pay would virtually guarantee that data would be lost.

Did it work?
After payment was made, a 'key' was delivered to open access to our computer systems. The process to 'unlock' hundreds of thousands files will be a lengthy one, but so far, the key has worked in every attempt that has been made.

How did we pay for it?
The District has a cybersecurity insurance policy to address these specific types of cyber intrusions and it was activated during this incident. While much time will pass before this matter is resolved, we have already availed ourselves of the resources provided by the policy, including assistance of cybersecurity experts.

Was student and employee information taken before we paid the ransom?
To reiterate, our top priority is the integrity of student, faculty and employee data. At this early stage of this complex investigation, no data breach has been identified; however, we will continue to communicate with the LAVC community and the public as the investigation proceeds.

How soon can I connect with LAVC departments, faculty and staff by email and/or leave a voicemail message?
The college's information technology department has a plan in place to bring back servers in a logical manner that prioritize key college services that impact communications with students, faculty and staff. There currently isn't a set time table for when all communication services are restored.

January 4, 2017

What happened?

Los Angeles Community College District (LACCD) is investigating malicious cyber activity targeting Los Angeles Valley College (LAVC). The malicious activity has disrupted many computer, online, email, and voice mail systems.

The college's winter session classes began on Tuesday, January 3, and classes continue to be held normally, including distance education courses. There is no indication that this activity goes beyond LAVC. Out of an abundance of caution, computer experts are analyzing the computer systems at other

LACCD colleges.

LACCD and LAVC staff, outside cybersecurity experts and law enforcement have determined that many of the college's computer servers have been infected with a ransomware virus. Ransomware viruses block access to computer systems until a payment is made. At this early stage in the investigation, it appears LAVC was randomly targeted.

When did this happen?

The district has a cybersecurity protocol in place; it was activated on December 30, within hours of staff detecting a virus within LAVC's computer system. That protocol includes district and college staff, outside experts and law enforcement, and all are involved in investigating and resolving this incident.

Was employee or student personal information compromised?

At this point, no data breach has been identified; however, this complex investigation is in its early stages.

LACCD and LAVC information technology staff, outside cybersecurity experts and law enforcement are working together to determine the specific nature and impact of this incident. Our top priority is the integrity of student, faculty and employee data, and we will continue to communicate with the LAVC community and the public as the investigation proceeds.

What communication tools have been impacted?

The malicious activity has disrupted many computer, online, email, and voice mail systems. Student email is still operational. Distance education classes are accessible through Canvas at https://ilearn.laccd.edu/login/canvas. Phone lines are operational; however, callers will be unable to leave voicemail messages.

We do not have a time frame to restore communication services, but we are working diligently to resolve these problems.

Now what?

We are at the early stage in the investigation. We will continue to communicate with the LAVC community and the public as the investigation proceeds.