

Please check back regularly for the latest updates. New information and announcements will be posted here, with the most recent updates appearing at the top of the page.

CEDAR CREST COLLEGE CYBERSECURITY INCIDENT

Published: July 16, 2026 (9:01 a.m.)

Cedar Crest College recently identified a significant cybersecurity incident affecting portions of the College's technology environment. Upon becoming aware of the incident, the College immediately initiated its emergency response protocols to contain the threat and protect College data. We understand that this situation may cause concern for members of our community, and we are committed to sharing accurate information as it becomes available.

The College is actively investigating the incident, working to secure its systems, and taking steps to restore affected services safely. At this time, we believe that some information may have been accessed or compromised. However, the nature and extent of the affected information have not yet been confirmed.

Our Investigation

The College identified the cybersecurity incident on 7/13/2026 at approximately 7:45 a.m. The incident has affected our FalconLink, FalconApp, and some network and cloud-based file-share systems (e.g., campus-based network drives, OneDrive).

Our investigation remains ongoing. We are working to comprehend the full extent of the breach and systems affected. We do not want to speculate and will provide updates as we learn more, such as what occurred, which systems and information may have been affected, and whether any individuals require direct notification. If we determine that your information has been compromised, we will reach out to you directly.

Because this investigation is in its early stages, we are not currently able to confirm the full scope of the incident or identify all information that may have been involved. We will not speculate while the investigation is underway.

Actions Taken

After identifying the incident, the College took steps to contain the activity and protect its technology environment. Cedar Crest College is working with external cybersecurity experts and law enforcement to investigate the incident and support recovery efforts.

The College is also reviewing its systems, strengthening security measures where appropriate, and restoring services through a careful and controlled process. Because the investigation is still in progress, we cannot yet provide a definitive timetable for the restoration of every affected service.

Where to Get Help

If you are experiencing an account, login, device, email, network, application, or other technology-related problem, contact the Cedar Crest College HelpDesk:

- **HelpDesk website:** [Click Here for IT Support Center](#)
- **Email:** helpdesk@cedarcrest.edu
- **Tech Team Help Channel:** [Click Here for IT MS Teams Help Channel](#)
- **Hours:** Monday-Thursday 8 a.m.-8 p.m.
Friday 8 a.m.-6 p.m.; Saturday-Sunday 9 a.m.-1 p.m.

The HelpDesk should be used for technical support. It is not the correct channel for questions about potentially affected personal information, the scope of the investigation, notifications, or other incident-related concerns.

Do not include passwords, Social Security numbers, financial account information, medical information, identification documents, or other sensitive personal information in an email or general HelpDesk ticket.

Cybersecurity Incident Questions

Questions specifically related to the cybersecurity incident, privacy concerns, or potentially affected information should be directed to the College's dedicated cybersecurity incident-response email:

Incident inquiry email: cybersecurity@cedarcrest.edu

Using this dedicated email will help the College respond to incident-related inquiries while allowing the HelpDesk to focus on technical problems affecting access to College services.

Do not submit sensitive personal information through email. The College will provide secure instructions if additional information is needed to address an inquiry.

How to Protect Your Information

Members of the Cedar Crest College community should remain alert for unexpected emails, text messages, phone calls, or websites that request passwords, payments, personal information, or urgent action.

Please take the following precautions:

- Use unique passwords for College and personal accounts.
- Enable multifactor authentication wherever it is available.
- Do not approve an unexpected multifactor authentication request.
- Verify unusual requests through a known and trusted contact method.
- Avoid clicking links or opening attachments in suspicious messages.
- Rely on the College's official website and established communication channels for updates.

The College will not ask you to provide your password by email, text message, or telephone.

Future Updates

Cedar Crest College will provide additional updates as material information is confirmed and can be shared without compromising the investigation or recovery process. Updates will be posted at cedarcrest.edu/cybersecurityupdate and sent via email.

If the investigation determines that specific individuals were affected and notification is appropriate or required, the College will communicate directly with those individuals.

We recognize the disruption and uncertainty this incident may create. Protecting the information entrusted to Cedar Crest College and securely restoring services remains our highest priority. We appreciate your patience, vigilance, and cooperation during the ongoing investigation.