Nov. 9: Active Cybersecurity Incident Updates

7:15 p.m.

To the Vanderbilt community:

Thank you for your patience as we continue managing the cybersecurity incident affecting university devices, systems and cloud-based services. Campus Wi-Fi is now available, but access to most Vanderbilt systems and applications remains restricted. We know this has disrupted important work and caused frustration across the university. Vanderbilt Information Technology is working with government agencies and other partners to manage this situation.

On Tuesday, Nov. 10, Vanderbilt University will operate on a normal schedule.

Students: Classes will proceed on a normal schedule. Please contact your course instructors for any additional guidance, including flexibility on course work deadlines. Student services will also operate normally, and Student Care Network offices are open and hosting appointments.

Faculty: Please plan to teach classes as scheduled. If you have grant submissions due this week, contact Vice Provost for Research and Innovation Susan Marguiles, whose team can provide focused support to ensure timely submission.

Staff: Please report to work as scheduled. We will share additional guidance as needed.

We will provide the next update by 9 a.m. Tuesday, including the status of systems and applications.

1 p.m.

VANDERBILT CLASSES ON NORMAL SCHEDULE: Vanderbilt University classes are proceeding as scheduled. Please refer to your course instructor for any additional guidance. If you do not hear from your instructor, proceed to class as planned.

10:45 a.m.

We are currently responding to an active cybersecurity incident that may impact university devices, systems, and cloud-based services. Our Information Technology team is actively investigating and working to contain the situation.

We are asking all members of the university community to shut down university devices, disconnect from university WiFi, and remain extremely vigilant. Take immediate action if you notice any unusual or suspicious activity on your devices.

Examples of suspicious activity include, but are not limited to:

- Unexpected pop-ups, warnings, or security notifications.
- Unusual changes to files, folders, or permissions in OneDrive, Box, or other cloud storage platforms.
- Files that have been unexpectedly moved, deleted, renamed, or modified.
- Unfamiliar applications, messages, or prompts appearing on your device.
- Unexpected requests to enter passwords, approve authentication requests, or provide login credentials.
- Any other unexpected or unusual behavior on your device.

IMMEDIATE ACTION REQUIRED

If you experience ANY unusual or suspicious activity, please take the following steps immediately:

1. DO NOT CLICK on any links, pop-ups, attachments, or unfamiliar prompts.
2. DO NOT attempt to investigate, troubleshoot, or resolve the issue yourself.
3. SHUT DOWN YOUR DEVICE IMMEDIATELY to help prevent potential further security risks.
4. CONTACT THE IT SERVICE DESK IMMEDIATELY using a separate device or telephone to report the incident.

Nov 9, 2026, 11:19 AM

Share

Media Inquiries

615-322-6397

Latest Stories

Nov. 9: Active Cybersecurity Incident Updates

Vanderbilt to establish unified organization for enterprise and research computing

Celebrating learning with Teaching@Vanderbilt

Share this Story