Instructure.

CANVAS BY INSTRUCTURE

INCIDENT FACT SHEET

We're Instructure, the company behind Canvas, Mastery, Parchment, and other learning solutions. We built these tools because we believe in the power of education. When something disrupts that mission, as it did over the past few days, we owe you a full explanation.

Many of you experienced real disruption to your learning environment. We want to be transparent about what happened, the immediate actions we've taken and our ongoing efforts to prevent this from happening again.

True to our roots as educators, we believe in learning together. Here are the facts we know so far, along with steps you can take to stay informed and protected.

What happened to Canvas by Instructure?

On April 29, we detected unauthorized activity in Canvas by Instructure. This activity was carried out by a cybercriminal organization known for large-scale attacks across multiple sectors, including technology and education. In response, we promptly revoked the unauthorized party's access, started an investigation, and engaged outside forensic experts.

Before we revoked their access, we know the actors responsible for this incident took data from the Canvas platform. We believe the information involved included information like usernames, email addresses, course names, enrollment information and messages. To date, our investigation has not identified core learning data (course content, submissions, credentials) as involved. None of the data fields we understand to be impacted are intended to include information like passwords, dates of birth, healthcare information, social security numbers, financial information, student grades or disciplinary records.

On May 7, 2026, the same threat actor gained additional access through a second Canvas vulnerability. The unauthorized actor made changes to the pages that appeared when some students and teachers were logged in through Canvas. Due to monitoring implemented after the first attack, Instructure detected and disabled the second attack approximately 10 minutes after it began. No additional data was accessed or exfiltrated in this second attack, but we chose to put Canvas into maintenance mode until we could verify both the scope of the attack and that the attackers' access was fully closed.

As of May 9, 2026, Canvas is fully back online and available for use. We have since confirmed that the unauthorized actor carried out this activity in both instances using one of our Free-For-Teacher accounts. We temporarily disabled Free for Teacher while we complete a full security review. We know that many educators rely on Free-For-Teacher, and so we are working on solutions that will allow us to bring it back online without exposing the rest of the Canvas community to undue risk.

We're still validating all findings, but we want to be clear about what we understand was and wasn't affected.

What are you doing now?

We've been working around the clock to make this right. Here's some insight into our actions thus far:

- **Keeping you informed.** We've launched a dedicated Incident Update page, a single place containing what we know, what we're doing, and what's next. The many schools, families and students that we support can find further guidance and resources on this page.

- **Canvas operations restored.** Canvas by Instructure is fully operational and remains safe to use. The core learning information used for coursework is not compromised.
- **Listening and responding.** Our Customer Success and community teams are hearing your concerns and using your feedback to shape how we support you through this.
- **Bringing in the experts.** We are working with a best-in-class forensic firm, CrowdStrike, to support our team's forensic analysis of this incident, as well as recommendations to further harden our environment.
    - **Taking action to protect your data.** We reached an agreement with the unauthorized actor involved to have the data involved returned and deleted. While there is never complete certainty when dealing with cyber criminals, we took every step within our control to give our community additional peace of mind, to the extent possible.

Your organization is your first point of contact. They'll share information specific to your situation as we provide it. However, you can continue to reference https://www.instructure.com/incident_update for the latest information from us.

What actions can I take?

While we don't expect the information involved to be made public, we feel it is important to share helpful reminders around recognizing scams and common practices to remain vigilant. Let's start with the basics.

What do common scams look like?

EMAIL / TEXT

Phishing / Smishing

Attackers impersonate trusted senders (a bank, school, or familiar organization) to trick you into clicking a link or handing over personal information.

PHONE

Vishing

Callers pretend to be tech support, an acquaintance, or school representative to pressure you into giving sensitive information verbally.

Red Flags to Watch For

- ⚠ Urgent or threatening language ("Act now or lose access")
- ⚠ Unexpected requests for sensitive information like passwords, Social Security numbers, or payment info
- ⚠ Mismatched sender email -- always check the actual address, not just the display name
- ⚠ Links that look almost right -- "paypa1.com" instead of "paypal.com"
- ⚠ Generic greetings like "Dear Customer" from places that know your name
- ⚠ Unexpected attachments -- especially .exe, .zip files
- ⚠ Requests to bypass normal security steps "just this once"

How do I protect myself?

1. Stop and verify before clicking

Hover over links to preview the real destination URL. When in doubt, go directly to the website by typing it in your browser rather than clicking any link.

2. Use strong, unique passwords

Never reuse passwords across accounts. Use a reputable password manager. Enable two-factor authentication (2FA) on every account that offers it — especially email and school accounts.

3. Verify unexpected requests

If someone from your school or organization asks for sensitive information unexpectedly, hang up or close the message and call them back using an official number you look up yourself.

5. Think before you share online

The less personal information that is publicly visible on social media, the harder it is for attackers to craft convincing, personalized messages.

6. Trust your instincts

If something feels off, it probably is. You are never obligated to respond immediately to a message or call. If you think your account has been compromised or you engaged with suspicious activity, reach out to your organization's IT team.

Where can I learn more?

We are committed to keeping you updated. This incident hub (https://www.instructure.com/incident_update) will serve as the central source for the latest updates and FAQs about this incident. This incident update page also includes a feed from status.instructure.com to provide you with the latest on service availability and operational updates.

###