Online Teaching and Learning Committee

How to Spot Bots in your Online Class

Over the past few years, community colleges have seen an increase in fraudulent applications and enrollments. Although SMC has implemented additional security measures, some fraudulent enrollments still occasionally slip through, particularly in online courses.

Faculty observations can help identify suspicious activity early, and addressing these cases does not have to be a major drain on your time. This guide highlights a few quick ways to spot potential “bot students” so you can focus your energy where it belongs—on your real students!

The sections below outline a streamlined approach to identifying and reporting bots.

Possible Red Flags

Keep an eye out for these patterns during the first week of the term:

Enrollment & Add Requests

- **Sequential IDs.** Student ID numbers that follow a strict numerical order (e.g., 1234567, 1234568).
- **Duplicate Messaging.** Multiple add requests that use identical wording or arrive in a rapid-fire sequence.

Classroom Behavior

- **The "Mismatched" Student.** A student logs very little time in Canvas but submits highly detailed, complex work.
- **Generic Responses.** Submissions or communications are vague, off-topic, or sound automated.
- **Carbon Copies.** Assignments from different students are identical or suspiciously similar.
- **Bulk Submissions.** Large groups of students submit work at the exact same moment.

Practical Strategies for Faculty

You can integrate these verification steps into your existing workflow to catch bots early:

- **Roster Screen.** Quickly scan your **mProfessor** roster for sequential ID numbers.

- **The "Reply Test."** If you receive a suspicious add request, ask the student to confirm their SMC ID using their official SMC email address.
- **Authentic Check-ins.** Create a simple first-week assignment or extra credit, such as asking students to upload a profile picture or a short video introducing themselves.
- **Syllabus Update.** Add a note to your syllabus stating that 1:1 Zoom sessions may be requested.
- **Identify and Drop Inactive Students.** Consistently reach out to non-participating students; faculty are required to drop these students by the census date.

A Note on AI Detection: While you can use AI detection tools, use them with extreme caution. They are currently not reliable enough to be the sole basis to determine fraud.

Reporting Suspected Fraud

If you notice multiple concerning patterns, invite the student to a brief virtual meeting. If communication remains unsuccessful or concerns persist, follow up with Admissions for guidance at enrollment@smc.edu.

Please include the following details in your email:

- Student Name and ID number.
- Class and section number.
- A brief summary of the red flags you observed.

Sources and Further Reading

- California Community Colleges Chancellor's Office. (2024). *Fraud prevention and detection in CCCApply*.
- Chow, K., & Curry, S. (2021). *How student engagement can mitigate enrollment fraud*. Academic Senate for California Community Colleges.
- Hall, E. (2023). *Meet the cybersecurity threat haunting community colleges: "Ghost students."* The Chronicle of Higher Education.
- Tovar, E. (2021, September). *Email to faculty regarding fraudulent admissions applications and enrollments.* Enrollment Services.