

The Challenge of Scripts and Bots

Addressing automated cheating in education

With the rise of generative AI, schools and educational technology companies face sophisticated external tools designed to bypass academic integrity policies. *Userscripts* and *bots* can complete some or all of a student's coursework undetected, presenting a unique academic integrity challenge, especially in remote learning environments.

- A *userscript* is a bit of code that makes interacting with a website more efficient, allowing for automation of many tasks
- A *bot*, short for *robot*, is an automated software program that performs repetitive tasks to imitate human behavior

Understanding the Threat

Userscripts and bots can complete assignments for students without detection, severely compromising academic integrity. These tools can play videos, automatically answer questions, and generate essays, making it essential for schools to take proactive measures to safeguard against their use.

PREVENTATIVE MEASURES

- **Block installations:** IT staff should prevent students from installing scripts and extensions on district-managed devices
- **Monitor activities:** Regularly review data logs to detect unusual student behavior
- **Update policies:** Include generative AI and other current methods of possible cheating in academic policies

Imagine Learning's Commitment

Imagine Edgenuity® and Imagine EdgeEX are equipped to detect and block some scripts, giving students a zero score when a script is detected and recording this action in the **Recent Actions** report. However, combating these tools on student-owned devices remains a challenge.



Empowering Educators and Students

Tools and strategies for schools

Schools can adopt several strategies to both reduce the temptation for students to use cheating tools and to detect their use. Consider these steps to address academic integrity:

- 1 Communicate academic integrity expectations:** Proactively communicate academic integrity expectations to students, teachers, and families to create a culture of honesty and trust.
- 2 Update academic policies:** Include current technologies and methods for cheating such as generative AI, scripts, bots, online answer sites, and using social media to find people to do online coursework for a fee.
- 3 Block malicious software:** IT staff should block students from installing userscripts and malicious extensions on district-owned devices.
- 4 Leverage available tools:** Utilize available tools within educational technology products to enhance security. That includes these tools in Imagine Edgenuity and Imagine EdgeEX:
 - **IP Registry** to manage access outside of the school network
 - **SecureLock Browser Experience** to prevent students from accessing other websites and applications while logged into Edgenuity
 - **Teacher Review** to require teachers to unlock assessments before students can begin
- 5 Proctored assessments:** Require students to take assessments in an onsite, proctored environment. For hybrid learning, require onsite testing for exams and consider weighting these assessments to form the majority of the course grade.
- 6 Monitor student behavior:** Regularly review data to detect unusual patterns of behavior. Use tools like attendance logs, session logs, course reports, and student gradebooks in Imagine Edgenuity and Imagine EdgeEX to monitor activities and the speed of work completion.

Proctorio Lockdown Browser

The Proctorio Lockdown Browser is a browser extension that allows districts to block scripts and bots on Edgenuity and EdgeEX assessments. Proctorio works on both district-managed and student-owned devices and is an essential tool in ensuring academic integrity.

For more information, visit the Proctorio section of the Imagine Edgenuity Help Center.

