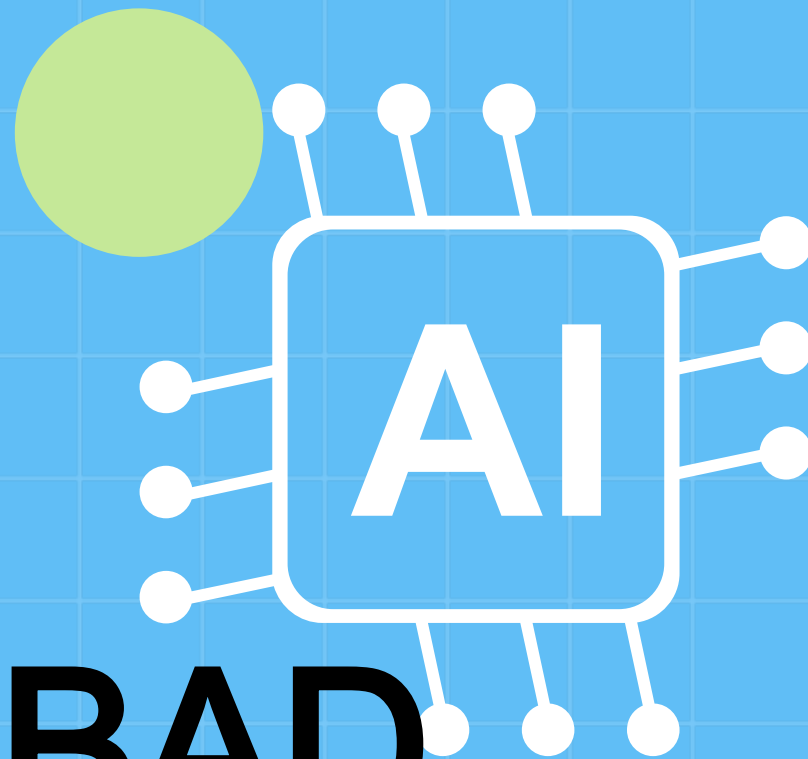
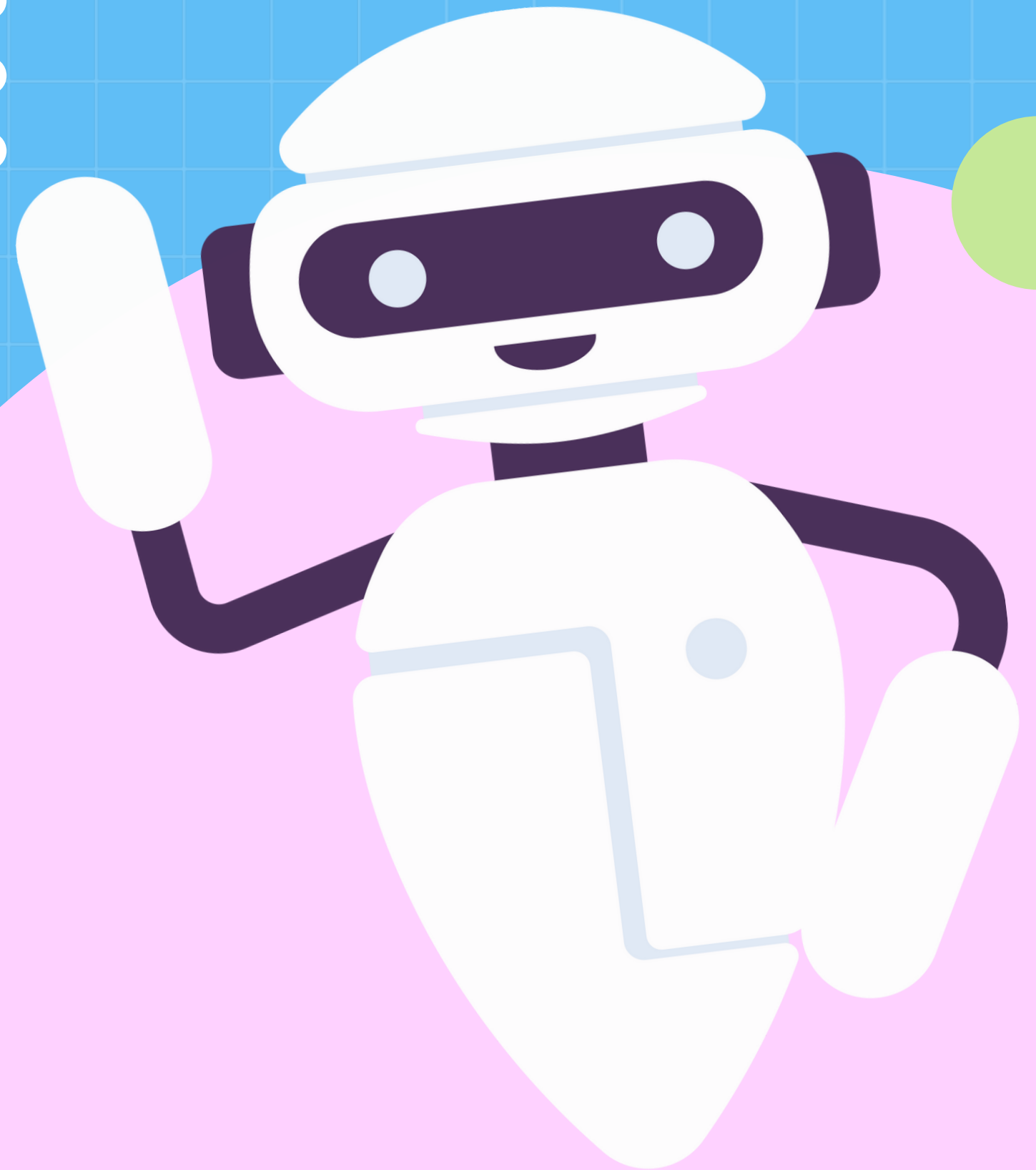




BOTS AND BAD ACTORS

*Strategies for Preventing and
Detecting Fraudulent
Responses in Online Survey
Research*



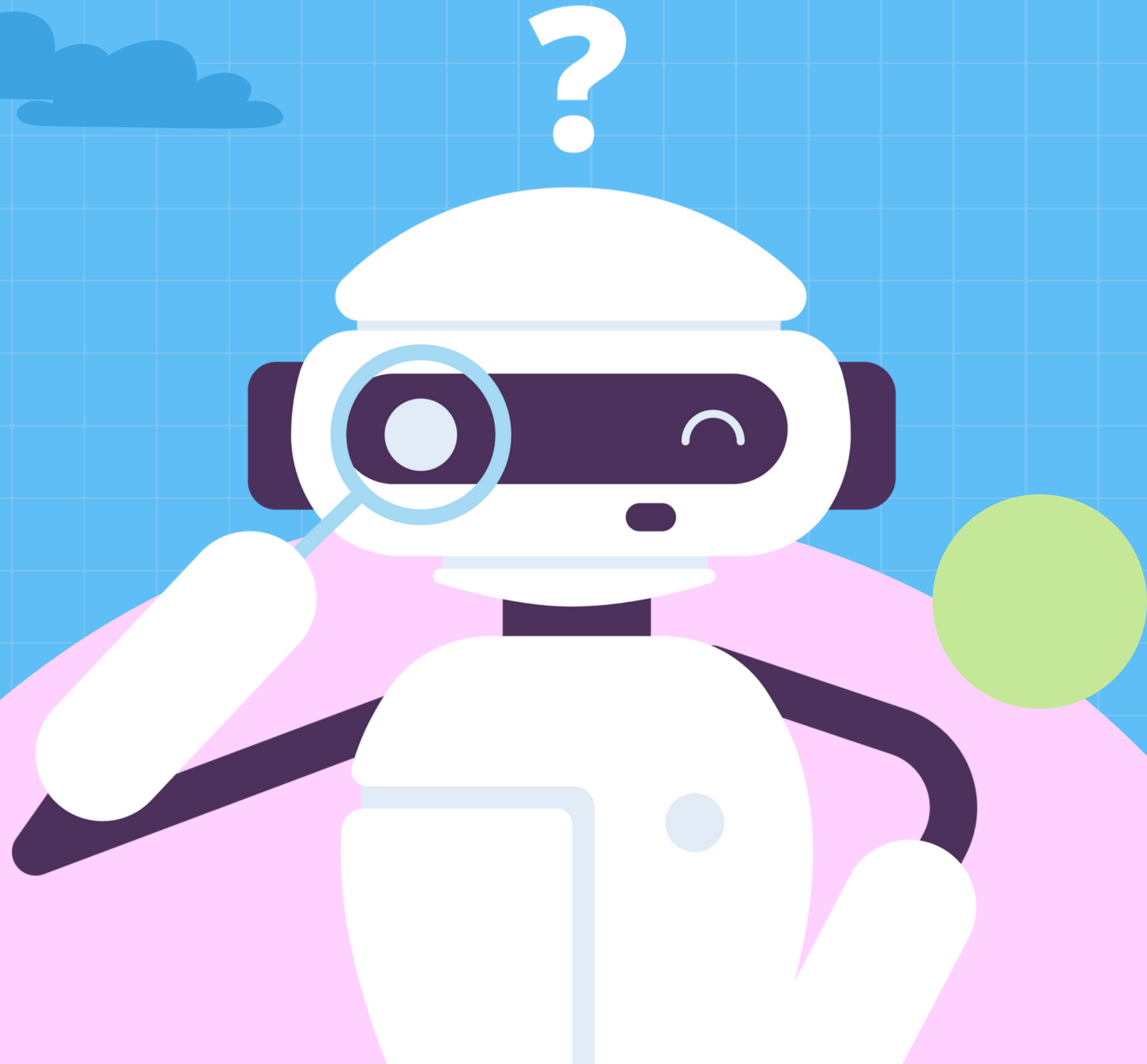
OVERVIEW

What are Bots and how do bad actors utilize them to target research studies?

- Threats to Research
 - What threats do Bots pose to researchers and their data?
- Survey Fraud
 - How prevalent is fraud and how can researchers detect fraud?
- Survey Design Safeguards
 - What survey design measures can be implemented to protect research from falling victim to bad actors and fraud?

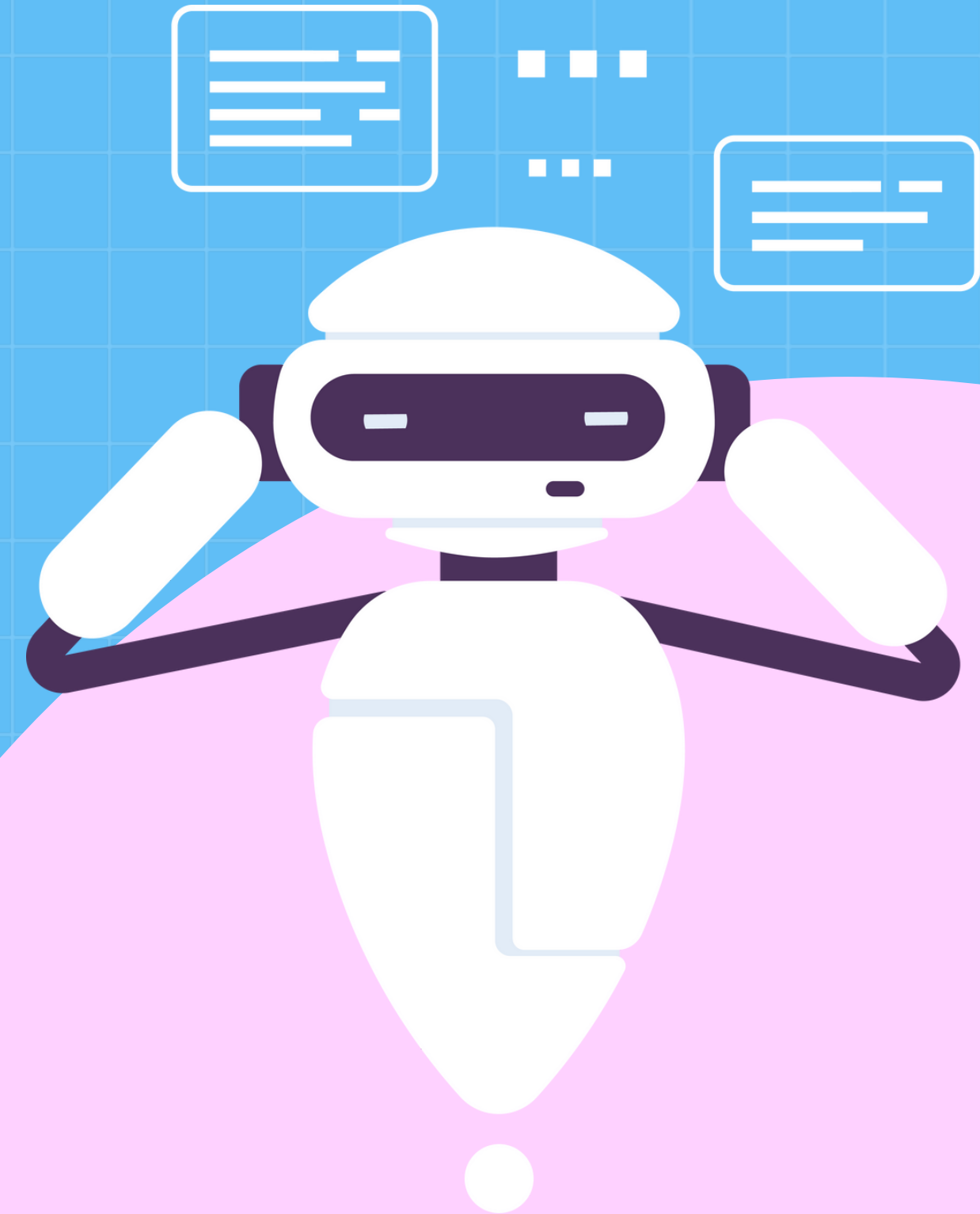
WHAT ARE BOTS?

- A bot, short for 'robot', is an automated software program or script that can perform repetitive or complex tasks.
- Bots are designed to mimic human behavior.
- They are increasingly used in survey research with the intent to receive compensation or disrupt research efforts by providing fake data.
- Bad actors also misrepresent themselves, and safeguarding online research involves preventing both bots and dishonest individuals.



SIGNIFICANT THREATS POSED BY BOTS

- **Data Contamination/Fraudulent Responses** : Bots can be programmed to complete surveys, generating fraudulent or inconsistent data. If undetected, this fraudulent data can skew or bias research results.
- **Drain on Resources** : Survey research offering payment for participation is susceptible to bots and bad actors. Researchers may unknowingly compensate bots, which can deplete funding if proper safeguards are not in place.
- **Impact on Research Validity** : Untrustworthy data prevents accurate assessment of research questions, especially critical for underrepresented and diverse populations where data integrity is paramount for addressing health disparities.



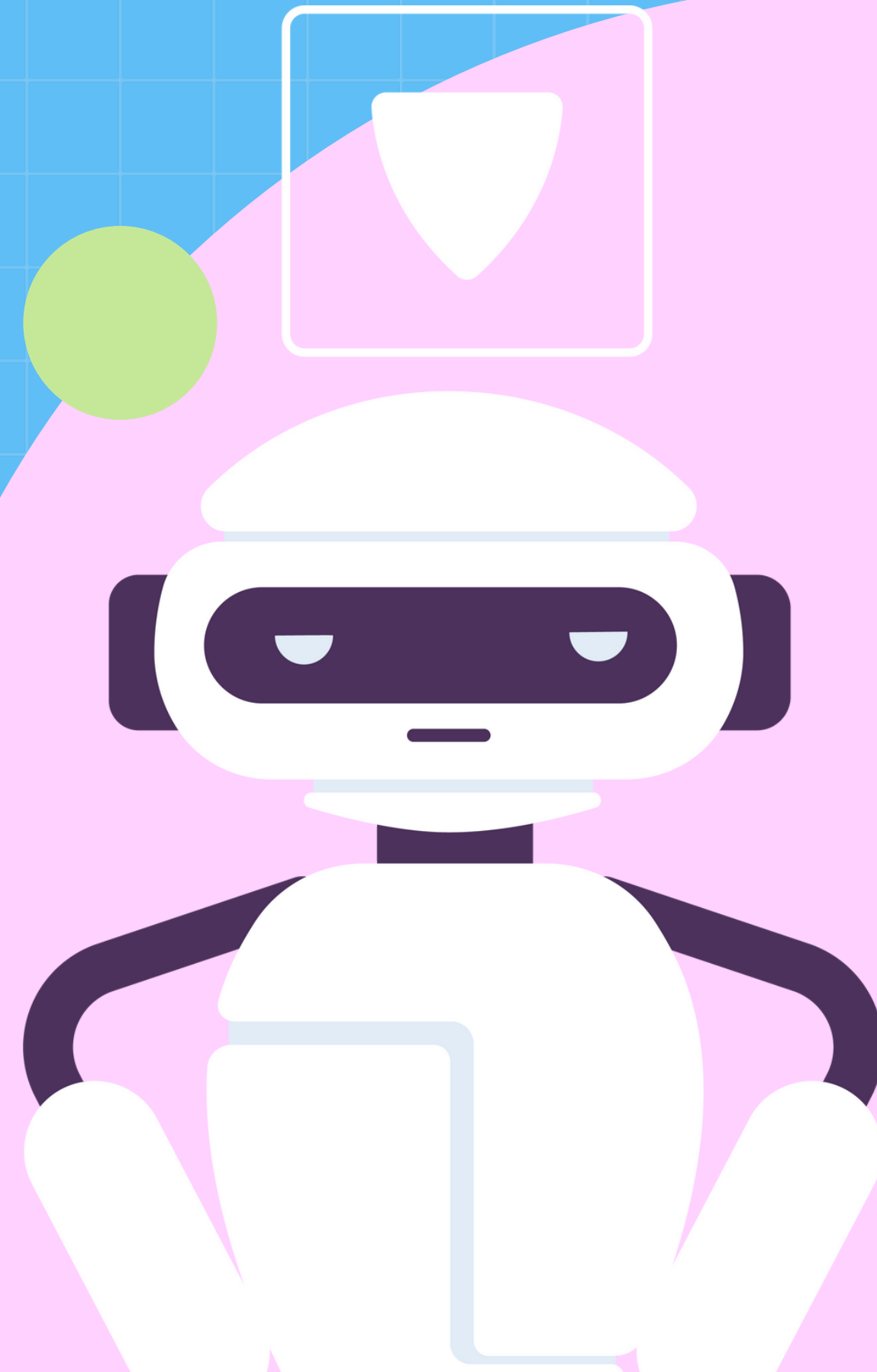
THE ALARMING PREVALENCE OF SURVEY FRAUD

- Online survey questionnaire fraud is a well-known phenomenon, particularly when incentives are offered.
- A study on families' experiences with COVID-19 found that over 70% of responses were flagged as fraudulent.
- Even among responses initially considered "non-fraudulent," further analysis revealed significant inconsistencies (e.g., only 33% consistent information in a follow-up).
- This suggests that fraud can be extremely prevalent and often operates on a continuum, posing distinct challenges.



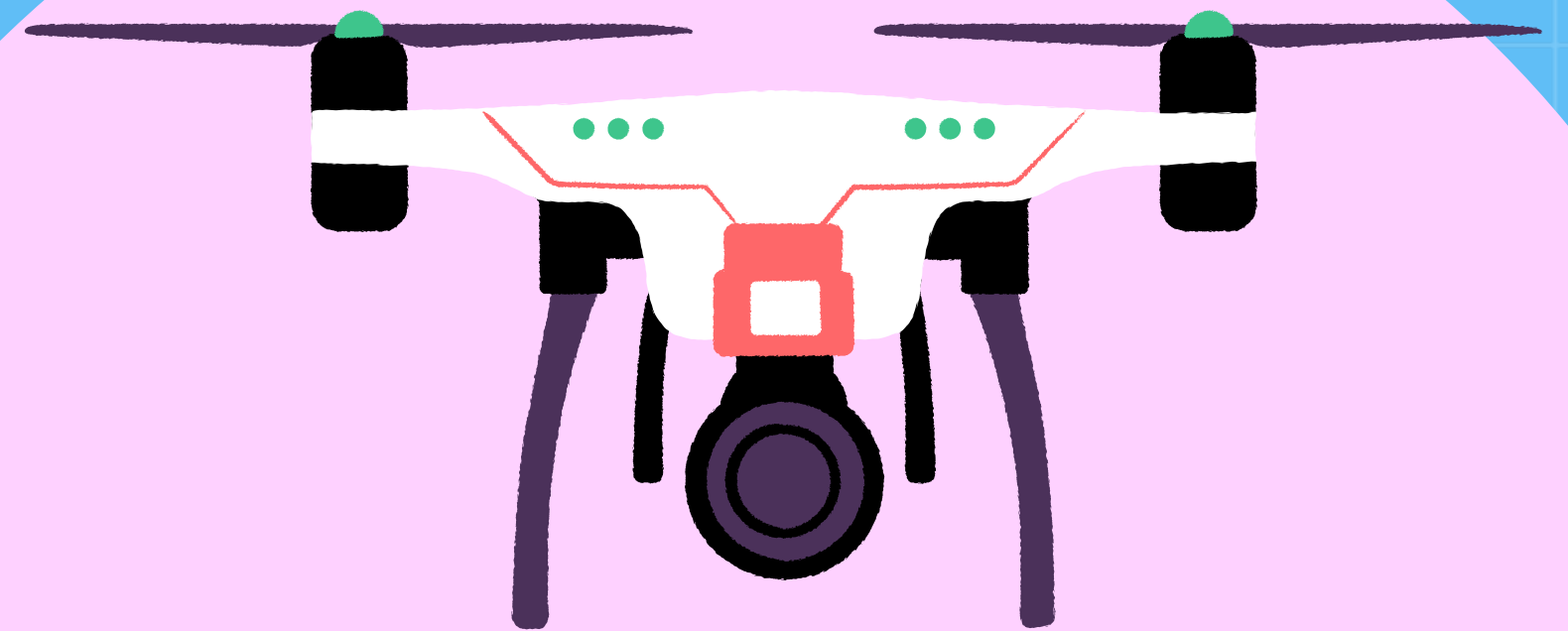
DETECTING PATTERNS OF FRAUD: TECHNICAL CLUES & METADATA

- **Duplicate IP Addresses** : A common indicator of fraud, especially when multiple submissions come from the same IP address. This often co-occurs with inconsistent answers, suggesting human-like manual completion multiple times.
- **Concurrent Start/End Times** : Responses that start and end within a minute of another respondent on the same day are a strong indicator of bot-like activity, particularly when coupled with short survey completion times. This was the most common fraud measure in one study.
- **Duplicate Module Time** : Consistent quick completion across specific sections of a survey.
- **Unique Survey Links** : Creating unique links accessible only through study sites and usable only once per participant can limit multiple submissions.
- **Collecting IP Addresses** : Utilize survey methods that allow for IP address collection to screen for multiple submissions.



SURVEY DESIGN SAFEGUARDS: ATTENTION CHECKS

- **Purpose :** Attention checks are questions designed to ensure participants are reading questions carefully and not just clicking random responses to quickly complete the survey.
- **Implementation :**
 - Researchers can design surveys so that attention checks must be answered correctly for participants to receive compensation.
 - They are also used to gauge the validity of data.
- **Examples :**
 - "Which of the following is a living creature? A boat / A balloon / A cat / A diamond ring".
 - "What is your favorite color? Regardless of the actual answer, select green. Blue / Green / Yellow / Black / Purple".
- Failing attention checks can be a reason to deny compensation.



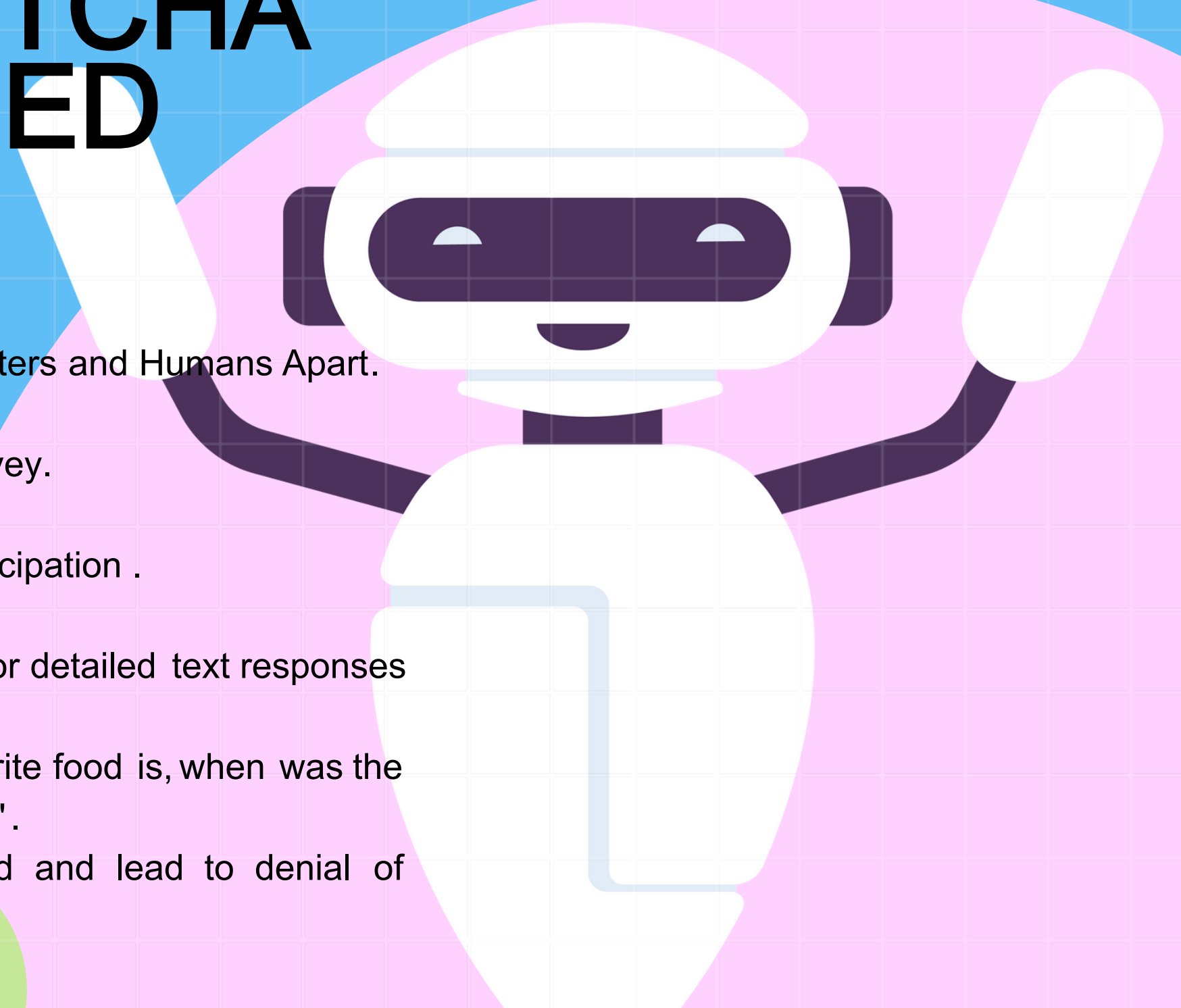
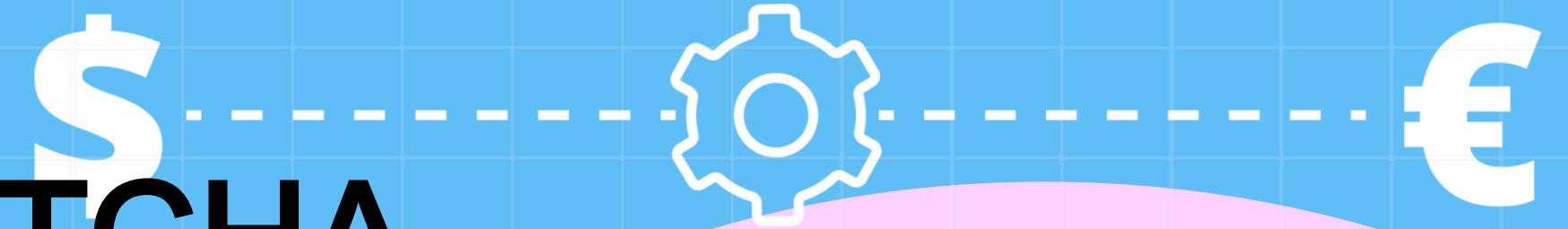
SURVEY DESIGN SAFEGUARDS: CAPTCHA TESTS & OPEN ENDED QUESTIONS

- **CAPTCHA Tests:**

- Stands for: Completely Automated Public Turing Test to tell Computers and Humans Apart.
- Purpose: Used to differentiate between human users and bots.
- Placement: Often used to screen out bots at the beginning of a survey.
- Format: These can be image- or text-based tests.
- Effectiveness: Implementing CAPTCHA can reduce fraudulent participation .

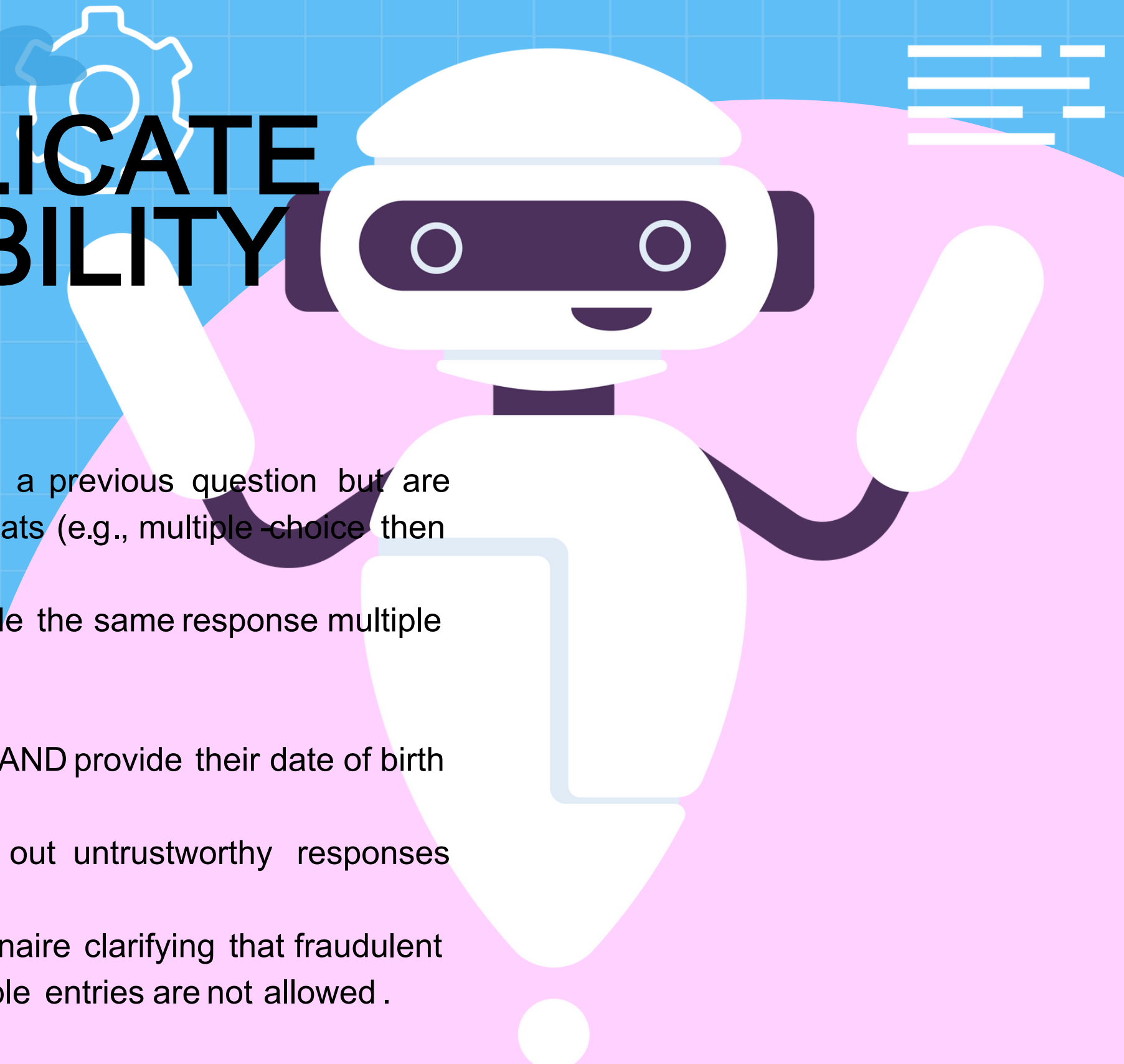
- **Paragraph -Type/Open -Ended Questions :**

- Purpose: These questions require participants to provide specific or detailed text responses to prompts, which are harder for bots to generate meaningfully .
- Example: "Within a few sentences, please describe what your favorite food is, when was the last time you had your favorite food, and why it is your favorite food".
- Detection: Nonsensical or unrelated answers can indicate fraud and lead to denial of compensation .



SURVEY DESIGN SAFEGUARDS: DUPLICATE QUESTIONS & ELIGIBILITY CHECKS

- **Duplicate Questions :**
 - Purpose: These questions require the same answer/response from a previous question but are placed in different parts of the survey or presented in different formats (e.g., multiple-choice then open-ended).
 - Benefit: Bots have a harder time realizing they are supposed to provide the same response multiple times for different questions.
- **Enhanced Eligibility Questionnaires :**
 - Verifiable Information : Ask participants to enter their age in a text box AND provide their date of birth to cross-verify.
 - "Trap" Questions: Include questions with untrue options to screen out untrustworthy responses (e.g., asking how they heard about the study with incorrect choices).
 - Warning Statement: Add a statement at the beginning of the questionnaire clarifying that fraudulent behavior or falsifying information will not be compensated, and multiple entries are not allowed .



COMPENSATION PROCEDURES & PARTICIPANT VALIDATION

- **Compensation Safeguards :**
 - Procedures can be designed to deny compensation upon receipt of fraudulent responses or require member checks prior to payment.
 - These procedures must be detailed in the IRB protocol and disclosed to participants in the informed consent form.
- **Scenarios for Denying Compensation :**
 - Surveys completed too quickly (e.g., 10 minutes for a 30-minute survey).
 - Failure to correctly answer attention checks.
 - Nonsensical/unrelated answers for open-ended questions.
 - Straight-lining (selecting the same option for most questions).
- **Member Checks (Participant Validation) :**
 - Purpose: Researchers review participant data with the participant to ensure accuracy.
 - When necessary: If answers appear to be AI-generated or responses contradict each other.
 - Disclosure: The consent form should describe when and how researchers would contact subjects for these checks, and participants should be informed that payment may not be immediate.
 - Contact information (email/phone) should be collected for this purpose.

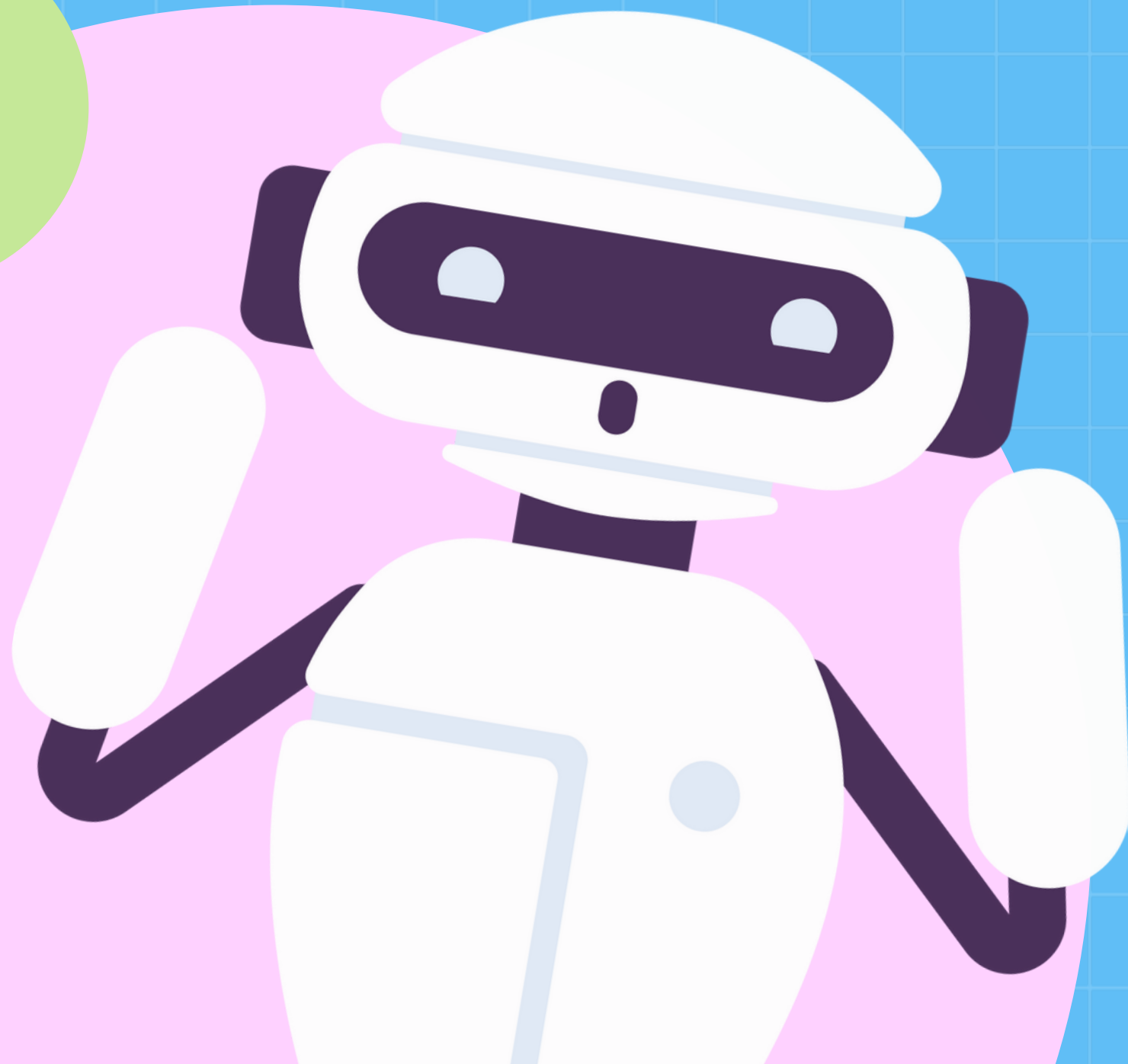




OTHER CONSIDERATIONS

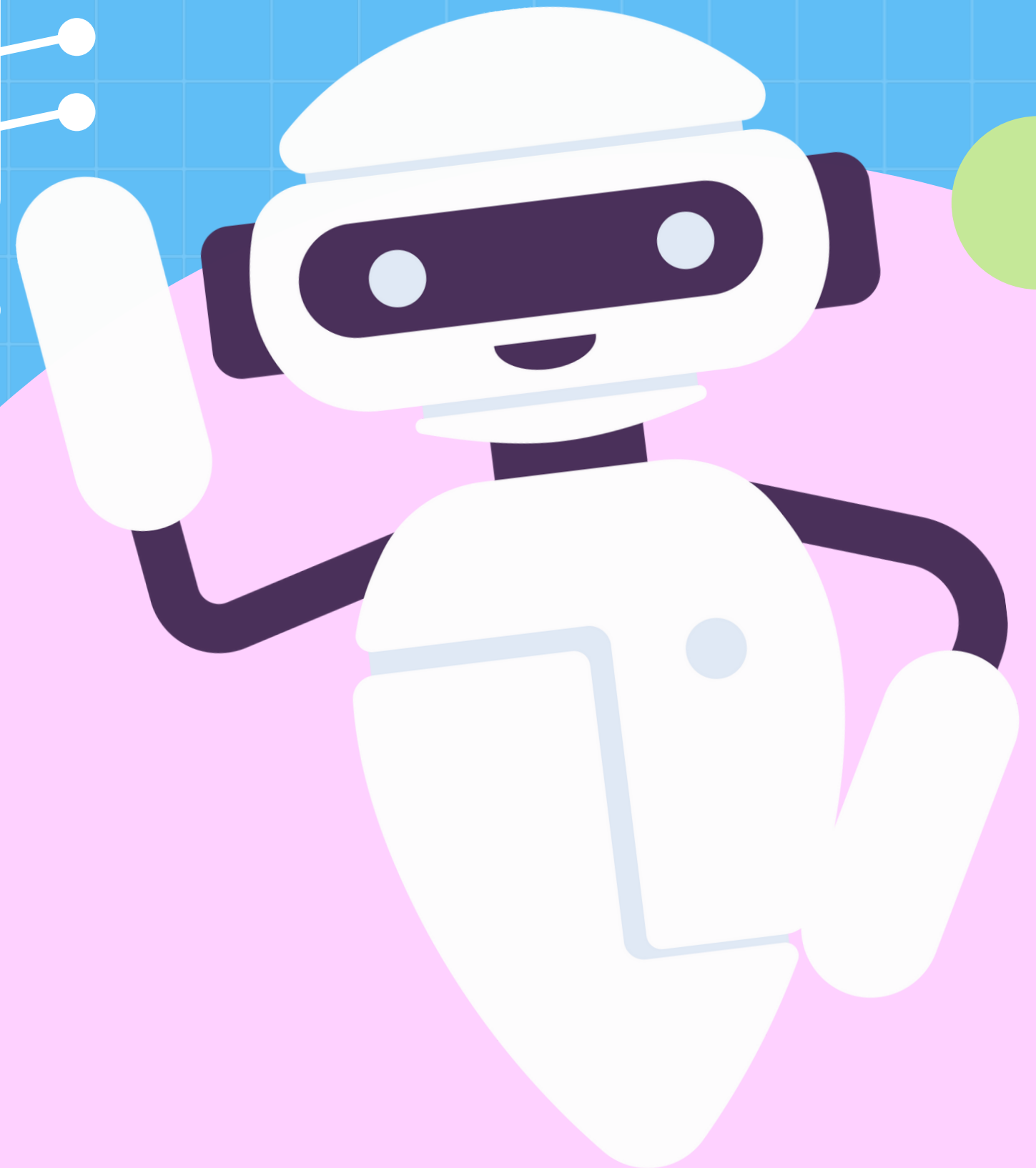
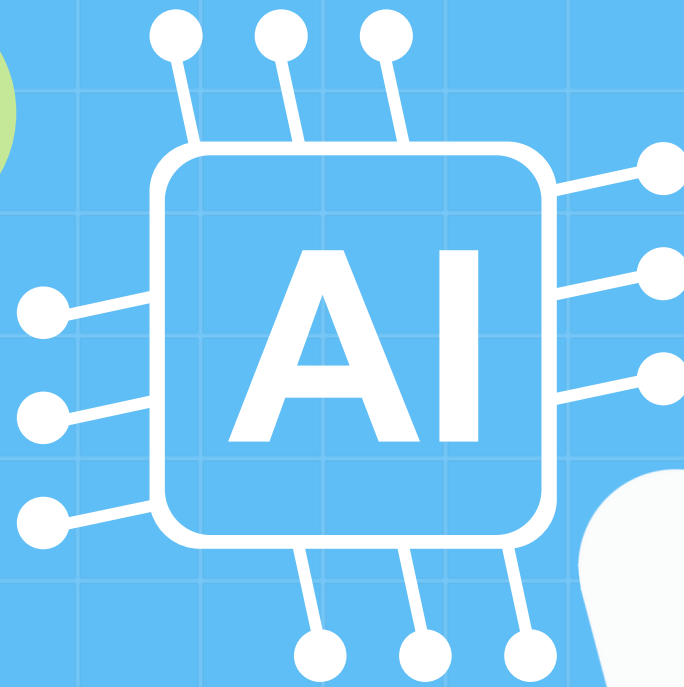
Consider how and where you recruit:

- Not mentioning potential compensation (or the specific amount) within advertisements placed on social media/internet can deter bad actors. Please note, the full compensation amount must be listed in the consent form. Additionally, it should be specified in the Kuali protocol why the compensation amount is omitted from recruitment materials.
- Create unique survey links that are only accessible through study sites and can only be accessed once per participant .
- Be careful where you post recruitment messages. Posting on social media can be beneficial due to the potential number of people who may see your posting ; however, it also opens the door for bad actors to see your post.
- Consider utilizing Qualtrics as the survey platform, as they have fraud and bot detection capabilities that can be enabled into your survey settings with the appropriate license:
<https://www.qualtrics.com/support/survey-platform/survey-module/survey-checker/fraud-detection/>



CONCLUSION: THE IMPORTANCE OF A MULTI-PRONGED APPROACH

- **No Single Solution** : Single fraud checks, like duplicate IP or email addresses, are not sufficient to protect against the diverse types of invalid responses.
- **Proactive and Reactive Measures** : Researchers should consider the possibility of untrustworthy responses during the study design phase and integrate preventative strategies from the outset. Be prepared to implement additional strategies reactively if suspicious patterns emerge.
- **Continuous Evolution** : Just as new algorithms are developed to detect bots, the scientific community must report concerns and develop amelioration strategies to address the constant evolution of these threats.



THANK YOU

