FLORIDA ATLANTIC UNIVERSITY
DIVISION OF RESEARCH

Bots and Bad Actors: Identify, Prevent, Manage

Research Roundtable

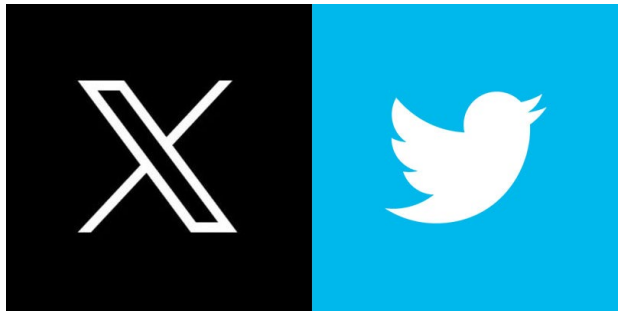
January 2024

Florida Atlantic University

DISCLAIMER

- Information is not from an expert. It was gathered through synthesis of articles on the topic.
- More information available:
  - https://psycnet.apa.org/fulltext/2023-91305-001.html
  - https://lifespan.ku.edu/online-surveys-and-data-collection-tools
  - https://www.research.chop.edu/announcements/survey-bots-and-best-practices-to-avoid-them
  - https://link.springer.com/article/10.1007/s11135-021-01252-1


swagbucks

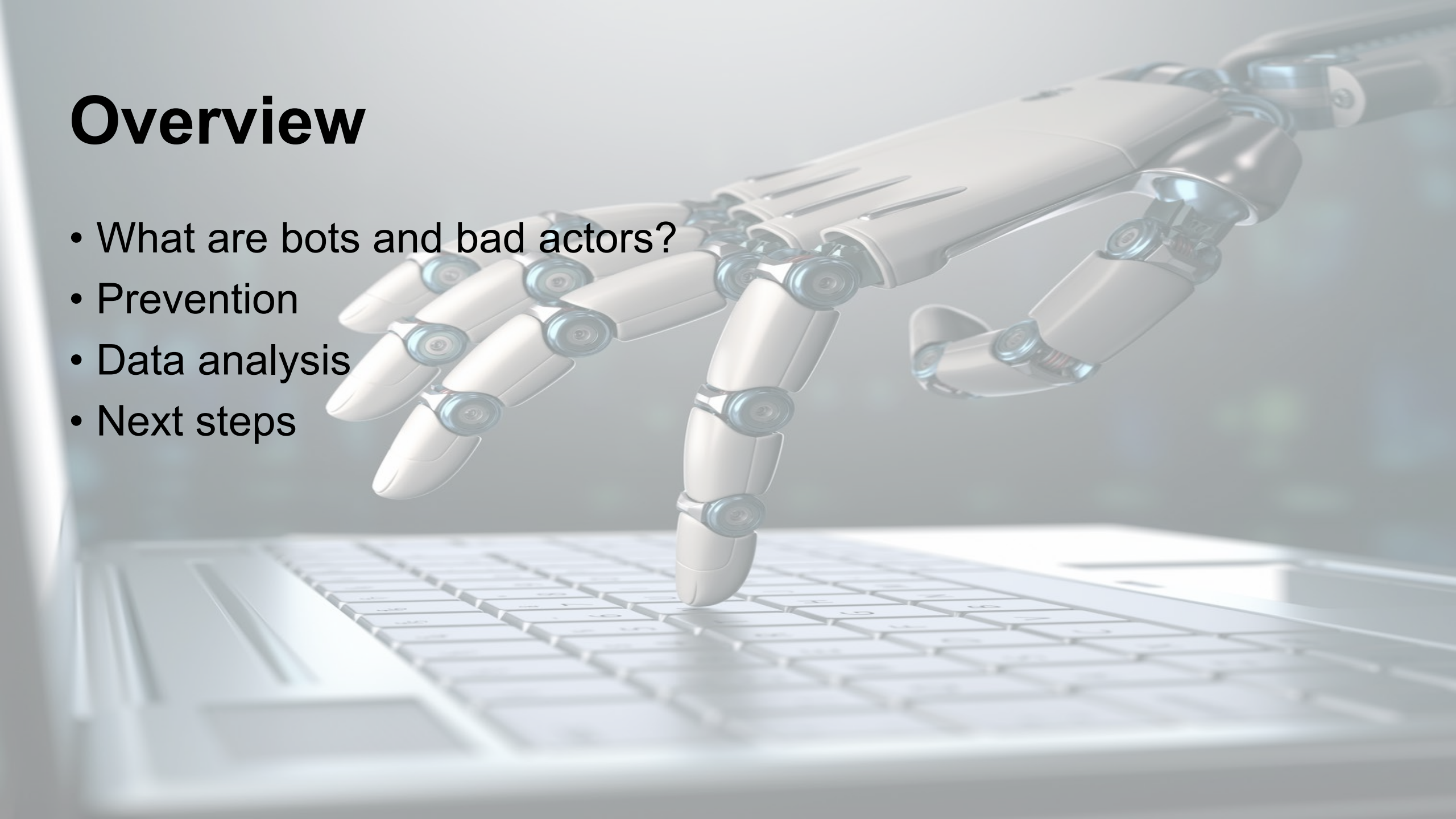



amazon
mechanical turk


kashkick

Overview

- What are bots and bad actors?
- Prevention
- Data analysis
- Next steps

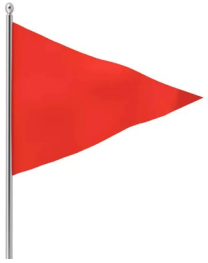


What are Bots and Bad Actors?

The term "bot" in the context of online surveys refers to a script or program that is written to fill in the fields of a survey with fake values and then submit the survey, repeating the process many times, with the goal of receiving the promised compensation, also multiple times. (Hallberg, 2022)

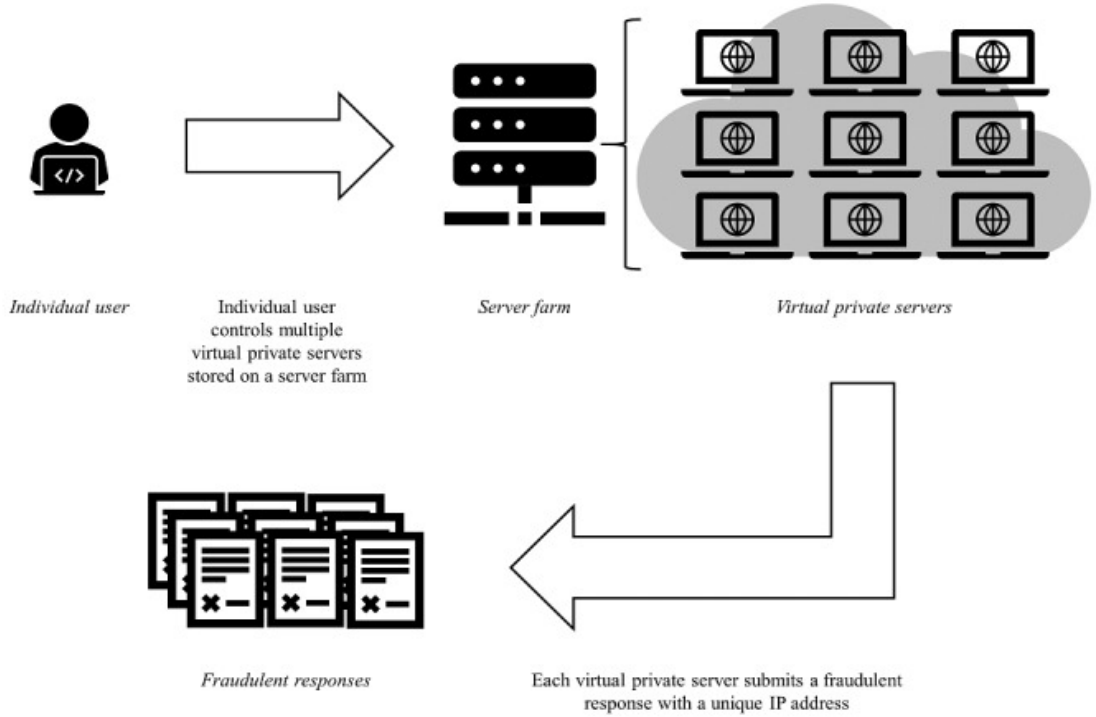
Bad actors, also known as *"mischievous responders" are respondents who mislead researchers by providing extreme and untruthful responses to multiple items*.(Cimpian, Timmer, Birkett, Marro, Turner, and Phillips, 2018).

How to Spot a Bot



- Online survey offering $5 gift card receives over 2,000 responses in less than 24 hours.
- Rapid survey completion time or nonsensical responses.
- Location and completion time zone do not match.
- Reponses provided to hidden items.
- Responses to attention items do not match.

How to Spot a Bot



- Use IP address geolocation to identify source of suspected bots; may come from virtual private servers (VPS).
- Virtual private networks, anonymous proxies, and spoofed IP addresses

Image source: Pozzar R, Hammer MJ, Underhill-Blazey M, Wright AA, Tulsky JA, Hong F, Gundersen DA, Berry DL. Threats of Bots and Other Bad Actors to Data Quality Following Research Participant Recruitment Through Social Media: Cross-Sectional Questionnaire. J Med Internet Res. 2020 Oct 7;22(10)

Prevention Tactics

“Simple Bots”

- Include two or three open-ended questions in the study and require responses to them.
  - Monitor these questions for unusual responses or identical responses across “participants.”
- Track timestamps.
  - Flag impossible dates and times, bundles of participants beginning and completing the survey at the same time, and respondents who completed the survey impossibly fast.
- Use a completely automated, public Turing test to tell computers and humans apart (CAPTCHA).
- Use a data collection platform with fraud prevention and detection features (eg, Qualtrics).
- Do not publicize survey incentives.

Prevention Tactics

“Advanced Bots”

- Include items that require respondents to demonstrate insider knowledge.
- Make it personal.
- Include at least one hidden item in each instrument.
- Add redundancy.
- Include “honeypot” questions.

*Simone, M. (2019). Bots started sabotaging my online research. I fought back. *STAT.* https://www.statnews.com/2019/11/21/bots-started-sabotaging-my-online-research-i-fought-back/

Data Analysis and Integrity

- Develop data integrity protocol.
- Suggestions:
  - Remove responses that do not complete X percentage of survey
  - Remove outlier response times (<5 min or >30 min)
  - Eliminate exact duplicates to open-ended questions
  - Check for conflicting data
  - Remove responses from duplicate email or IP addresses
  - Identify and remove email addresses that are random letters/ numbers

Next Steps


if you
SEE
something
SAY
something


IRB
Sponsor
Report Suspicious Activity
College IT
Platform

FLORIDA ATLANTIC UNIVERSITY
DIVISION OF RESEARCH

Questions and Discussion

FAU Human Research Protection Program
researchintegrity@fau.edu
https://www.fau.edu/research-admin/research-integrity/human-subjects-irb/