Panel Hacking

Jon Puleston
Private & Confidential
How do fraudsters hack the system?

1. **Fake panellists:** Respondents who are not who they say they to join panels e.g. someone from China pretending to be from USA

2. **Ghost respondents:** Hackers over-riding the transfer link process

3. **Screener hackers:**
   - **Professional respondents:** Skilled at getting through screeners
   - **Chatroom hackers:** “this is how you get through the screener”

4. **Multi-completers:** People completing surveys multiple times on multiple devices (this could be individuals or a more organised process)

5. **Bots:** Automated survey completion processes
Dealing with fake panellists: how we weed them out

Email address validation procedures:
- Verity (US) = score 1-5
- Global Z (global) = Groups A-J

IP proxy testing:
- MaxMind (used to detect credit card fraud)

Same device activity:
- Kantar Digital Fingerprint testing

Machine learning:
- Patterns of behaviour across devices, browser types, operating systems and IP addresses e.g. identified certain older operating systems more likely to be fraudulent
Ghost respondents

Much bigger industry-wide challenge right now
Ghost respondents

Survey server → Respondent does survey → Complete forwarding link → Panel company giving reward
Problem: we can only spot ghosts when we tally up completes between systems...

- Much more rife with sample only projects where it's not so easy to cross compare
- Requires an industry co-ordinated initiative to solve

Right now panel companies are taking the hit: But these costs are getting indirectly passed back to clients
Ghost respondents: solutions?

Server to server dual validation

Survey server → Respondent does survey → Complete forwarding link → Panel company giving reward

Encryption
Moving battle: Shoals of ghost respondents moving from one country to the next, one survey system to the next
Screener hacking

Amateurs → Pro

Has anyone one else dedicated browser for just surveys. I primarily use Firefox and Chrome on a Mac. I do this to manage tracking, cookies and browser history.

I don’t typically wait for an email notification to visit a panel, I cycle through my bookmarks on both phones and mobile device.

I have a dedicated mailbox where all survey notices are directed and I check that daily. I also have a mailbox for survey panels I’m deciding to drop but I have contest and sweepstakes entries I want to wait for a drawing before I nix the account. I also move all canceled survey panels email in the junk panel mailbox, you never know when you’ll need to reference it.

I also maintain an extensive list of bookmarks to Survey panels I’ve canceled, so I don’t accidentally sign back up.

I also use two browsers simultaneously because some panels are notoriously slow or invalidate a survey because you were too quick. I command-tab (control-tab on windowe) constantly through out the day.
How to spot a screener hack…

Numer of items purchased in last 6 months

- UK
- China

Profiles Division
Kantar Honesty detection

Ask a series of low incidence rate questions

Q1 = 1
Q2 = 0
Q3 = 1
Q4 = 0
Q5 = 1
Q6 = 0
Q7 = 1
Q8 = 0
Q9 = 1
Q10 = 0

If sum Q1-Q10 > X

Potential Hacker

The trouble is hackers are getting wise to this…
Another ways – looking for formula answers

Q1 = 1  
Q2 = 0  
Q3 = 1  
Q4 = 6  
Q5 = 1  
Q6 = 0  

Covert to number  
1010610 = 2+  
Potential hack
Random Individuals

Chatroom hack:
Don’t score 9 for 3rd option

<table>
<thead>
<tr>
<th>China Suspicious answer patterns</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>989399999999999999</td>
<td>99</td>
</tr>
<tr>
<td>999999999999999999</td>
<td>91</td>
</tr>
<tr>
<td>776777777777777777</td>
<td>80</td>
</tr>
<tr>
<td>7767777777777777</td>
<td>69</td>
</tr>
<tr>
<td>8868888888888888</td>
<td>66</td>
</tr>
<tr>
<td>8878888888888888</td>
<td>40</td>
</tr>
<tr>
<td>7757777777777777</td>
<td>28</td>
</tr>
<tr>
<td>8888888888888888</td>
<td>19</td>
</tr>
<tr>
<td>7777777777777777</td>
<td>19</td>
</tr>
<tr>
<td>6666666666666666</td>
<td>9</td>
</tr>
<tr>
<td>6656666666666666</td>
<td>7</td>
</tr>
<tr>
<td>7777777777777777</td>
<td>6</td>
</tr>
<tr>
<td>1111111111198999</td>
<td>5</td>
</tr>
<tr>
<td>1111111111198899</td>
<td>5</td>
</tr>
<tr>
<td>9899999999999999</td>
<td>4</td>
</tr>
<tr>
<td>7767777777777777</td>
<td>4</td>
</tr>
<tr>
<td>9899999999999999</td>
<td>3</td>
</tr>
<tr>
<td>9999999999999999</td>
<td>3</td>
</tr>
<tr>
<td>9999999999999999</td>
<td>3</td>
</tr>
<tr>
<td>9877779999999999</td>
<td>3</td>
</tr>
<tr>
<td>9878888999999999</td>
<td>3</td>
</tr>
<tr>
<td>9878888888888888</td>
<td>3</td>
</tr>
<tr>
<td>8878888888999999</td>
<td>3</td>
</tr>
<tr>
<td>8879999999999999</td>
<td>3</td>
</tr>
<tr>
<td>8878888778888886</td>
<td>3</td>
</tr>
<tr>
<td>7768888778888877</td>
<td>3</td>
</tr>
<tr>
<td>9998888888888899</td>
<td>2</td>
</tr>
<tr>
<td>9899999999999999</td>
<td>2</td>
</tr>
<tr>
<td>9899999999999999</td>
<td>2</td>
</tr>
<tr>
<td>9899999999999999</td>
<td>2</td>
</tr>
<tr>
<td>9899999999999999</td>
<td>2</td>
</tr>
<tr>
<td>9899999999999999</td>
<td>2</td>
</tr>
<tr>
<td>9899999999999999</td>
<td>2</td>
</tr>
<tr>
<td>9899999999999999</td>
<td>2</td>
</tr>
<tr>
<td>9899999999999999</td>
<td>2</td>
</tr>
<tr>
<td>9899999999999999</td>
<td>2</td>
</tr>
</tbody>
</table>

Difficult to write code to dynamically spot this activity in a live survey
Multi-completion processes:

Double registrations → Click farms
Traditional methods of spotting

IP + computer fingerprint matching → a room full of devices each with unique id

Screening out speeder → now looking for the opposite – regular longer gaps between answering questions an indicator
New methods

1. **Looking for cluster of similar answers**: within the same time frame respondents giving similar (not identical) answers

2. **Analysing open ended answers**: looking for similar answers with the same time frame

3. **Consistent answer time gaps**: the time it takes to answer each question across a survey

4. **Long, short, short, short patterns**: the time it takes to answer each question across a survey

Exploring machine learning techniques to spot these types of patterns
Bots and automated responses
The future…

**Algorithmic consistency checks**: bespoke designed or powered by machine learning

**More sophisticated answer time based algorithms**: time gap analysis

**Using verbatim question analysis**: One of the easiest way to spot hacking activity

**Fraud screening moving to the end of the survey**: to make it less clear where it has been spotted making it much harder to hack the process

**Honest respondent validation**: hard to spot a hacker, easy to pick out real & honest respondents
Differentiating between fraud & satisficing

**What gets commonly overclaimed**
Purchase activity - ownership of prestige consumer items
Education levels
Car ownership
Baby related questions
Premium media consumption activity e.g. newspaper readership

**What gets commonly under claimed**
Smoking
Finance related stuff
Medical related
Any activity that is not socially desirable
Watching reality TV
Fraud or bored?
Differentiating between fraud; satisficing, bored respondents, and simply badly asked questions delivering odd results
China study data: 10,000 responses

34% purchase questions correlate above 0.6

299 pairs of twins
High proportion of overclaiming

Items purchased in last 6 months in China
“Real Lives” honesty priming

但在本次调研中，我们关注的是人们的真实生活。
Done recently: China

- Unprimed 2019
- Honesty primed 2019
Panel hacking

Mostly our problem right now – but we are all paying for it one way or another

New procedures needed to spot hackers

Co-ordinated response needed

Right now if you can’t spot a fraudulent respondent in your data more fool you

Honesty priming can help to significantly reduce the overall scale of overclaim making it easier to identify and deal with real fraudulent behaviour
Questions for you…

1. What can we do to tackle ghosting more effectively?

2. Does any one have any smart ideas on how to better pick up on fraudulent activity on the fly in live survey?

3. How to we square of the fact that in doing this we reduce panel supply and so it will push up cost for those that implement it?