

Methodological Innovation is Causing New Problems for Researchers Here's how to play it safe...

Co-authored by: Ken Zeldis, Partner & Kristina Witzling, Sr. Research Director
Zeldis Research Associates, Inc. 800 Denow Road, Pennington, NJ 08534.

The Problem

Because of the cost and time savings offered by online research, Internet-based methodologies are becoming the standard in market research. However, online research data is at risk from hackers and cheaters. These individuals and groups are working to beat panels' security measures and complete surveys multiple times, either by hand or by machine. They may have a number of motives for breaching panel security – trying to obtain multiple incentive awards or points, or simply for fun or to prove that they can.

Most large panel companies are aware of this problem. Multiple completes from the same IP are difficult to definitively explain: it is not known exactly what is going on or how many respondents are responsible for the behavior. These results could all be from the same person or an affiliated group of persons – or they could be a mix of legitimate and bogus completes.

It is difficult to discuss any security breach that revolves around IP addresses as they are easily spoofed by those who seek to cheat any system. It can happen that several groups of Internet users share identical IP addresses due to common ISPs, geographic areas, proxy servers, and the like.

What Panel Companies Are Doing

Panel companies are working to develop and test enhanced security measures, such as those utilizing flash, java and iframe technologies. These technologies help ensure that a single computer is associated with a single record. This makes creating multiple profiles or spoofing IP addresses a waste of time for cheaters. These technological enhancements are continually being tested and implemented as tests are complete.

Duplicate IPs are removed from the panel and those IPs have been flagged in the system and will be blocked from further access. In addition, cases of fraudulent data coming from non-duplicate IP addresses are being addressed, with perpetrators removed and blocked as well.

What Researchers Can Do

Beyond the technological innovations that panel companies are testing, researchers can take steps to make sure that data are accurate. Technology can only go so far: researchers will need to be vigilant in spotting potential signs of fraud.

Below are a few “red flags” to check for before moving forward with data processing.

Interview Length Review: Most researchers routinely review interview length to eliminate “speeders,” or those who quickly complete an interview, either by hand or through an automated system. One rule of thumb is to investigate any interview with a completion time of 30% or less of the average.

Not everyone meeting this criterion must be removed. Sometimes, skip patterns allow respondents to complete a very short interview. However, short interviews should be reviewed for other signs of fraud: poor verbatims, patterns of similar responses, non-sensical or non-logical responses.

In addition, programs can incorporate “speed traps,” especially in long attribute series. These are questions that ask respondents to check a particular box, and are typically used to make sure respondents are paying full attention to the task at hand.

Straight-lining Review: Responses should be reviewed to make sure they are not “straight-lined,” in which one or two response codes are used for the entire questionnaire. Questionable cases should be removed from the data.

IP Address Review: Although panels should screen out duplicate IP addresses, data files should be reviewed for duplicates. In addition, multiple cases in a row that come from a similar IP address should be reviewed for any of the fraud signs listed above (speeding, verbatim quality, response patterns, etc.)

Consecutive Time Review: In most online studies, interviews come in very quickly. Therefore, interview times should overlap. One warning sign for fraudulent data is a series of interviews that take place consecutively (for example: 1:10 to 1:20, 1:21 to 1:30, etc.) This may indicate that one individual has managed to access the survey multiple times, even if the IP addresses are different. These cases should be investigated for other signs of fraud.

Data Review: Research vendors are trained to check data mid-field to look for programming problems, illogical data, etc. However, particularly in business-to-business studies, it’s often a good idea for the client to review the data with the research vendor, to potentially identify any data that does not correspond with internal data or findings from previous studies. This informal review can be done with topline data from a small sample of respondents.

If fraudulent data is suspected (even a few speeders), it’s important to report this to the panel company immediately. Researchers need to partner with panels to keep data secure, and often the only way a panel company can learn about a potential problem is through researchers.

Finally, trust your instincts! If something seems “off,” it just may be. Following up on your intuition can save a lot of trouble later on.

For more information regarding this methodology and/or Zeldis Research Associates, Inc. please look for us online at www.zeldisresearch.com or call us at 609-737-7223.