12-12-2022

Gullible by cuelessness: Operationalizing deception in information systems communication

Dejan Tatić
University of Economy Vienna, dejan.tatic@wu.ac.at

Margeret Hall
Wirtschaftsuniversität Wien, margeret.hall@wu.ac.at

TREO
Technology, Research, Education, Opinion

Gullible by cuelessness

Operationalizing deception in information systems communication

Dejan Tatić, dejan.tatic@wu.ac.at, Margeret Hall, margeret.hall@wu.ac.at

Gullible behavior in digital environments generates pervasive security risks, extensive financial damage and, in case of misinformation campaigns on Computer Mediated Communication (CMC) platforms, pose exceptional threats to whole democratic systems. Gullibility has been defined as behavior manifesting in deception blindness and propensity to accept false premises in the presence of untrustworthiness cues (Teunisse et al., 2020). This definition introduces untrustworthiness cues as operationalizable units of scientific research into manipulation via false premises in CMC. This provides us with the possibility for theoretical modelling to identify and distinguish specific indicators of harmful intent and covert messages in predatory internet content. Moreover, literature on gullibility suggests that there could be at least three different explanatory models including social skill deficiency, cognitive errors, or psychometrically inter-individual processing differences.

However, research has not yet adequately addressed the potential to operationalize the threats of false-premise manipulative messages in Information Systems (IS) by utilizing the cues of untrustworthiness. This research gap leaves us blind to urgently needed solutions to identify, and make salient, signals of dangerous or predatory content exploiting the gullibility of IS users at the scale of the internet. We can bridge this gap by researching the underlying mechanisms of untrustworthiness cues and the distinct ways gullibility does or doesn't override them. Therefore, defining and taxonomizing digital aspects of gullibility and its differing modes will be part of the endeavor to make the internet safer. The research challenge is intersecting different explanatory models with distinct untrustworthiness cues across use cases like Phishing, E-Commerce Fraud, Man-in-the-Middle-Attacks, or Misinformation Campaigns as each use case both merits and requires its own operationalization. For example, a phishing email and a social post with misinformation intent may contain distinct cues of untrustworthiness in their propagation format, source salience, or message content. While phishing may contain cues of invoked urgency, misspelling and links to unfamiliar websites misinformation campaigns are more likely to have emotionally tainted, or dogmatic and un-factual content. Systematic identification via mapping and taxonomizing the mechanisms and use of untrustworthiness cues in digital content will provide a stronger understanding for the drivers of gullibility, which supports the design and development of resilient IS.

References

Teunisse, A. K., Case, T. I., Fitness, J., & Sweller, N. (2020). I Should Have Known Better: Development of a Self-Report Measure of Gullibility. *Personality and Social Psychology Bulletin*, *46*(3), 408–423. https://doi.org/10.1177/0146167219858641