A socio-technical approach to misplaced digital trust judgements

Rob Huw Peace - rhp34@bath.ac.uk
Dr. Laura G.E. Smith - L.G.E.Smith@bath.ac.uk
Prof. Adam Joinson - A.Joinson@bath.ac.uk

UNIVERSITY OF BATH

The challenge:

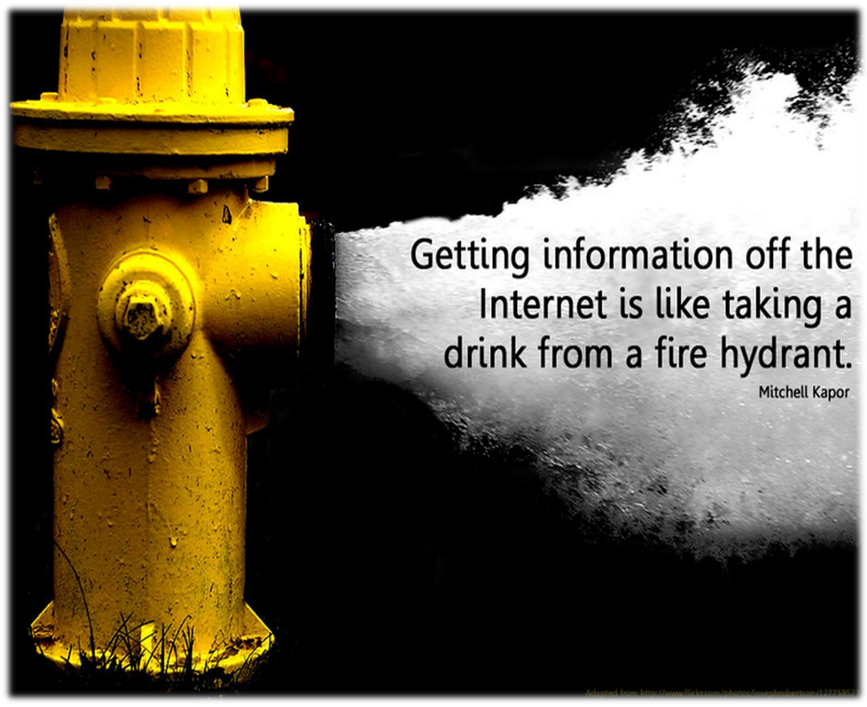
Today's hyperconnected digital world has allowed for a huge increase in the amount of information with which individuals interact.

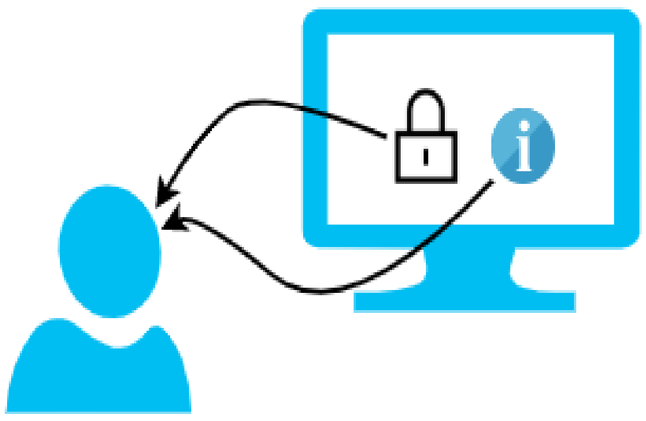
However, the veracity of digital information is not always clear

Inaccurate or malicious information such as mis- or disinformation has the potential to cause harms to individuals and societies (Hansen, Köhntopp, & Pfitzmann, 2002; Amazeen & Bucy, 2019)

.

This raises the question of how and why users trust both trustworthy and untrustworthy information?





Phase 1 – identifying digital trust signals and symbols

Phase 1 has identified an evidence base for digital trust signals and symbols that trustees convey to influence the trustor's perception of trustworthiness.

Research undertaken:

Identifying digital trust signals and symbols: A systematic review

Identifying digital trust signals and symbols in an open-source software library: A think aloud study

...

Phase 2 – Experimental phase

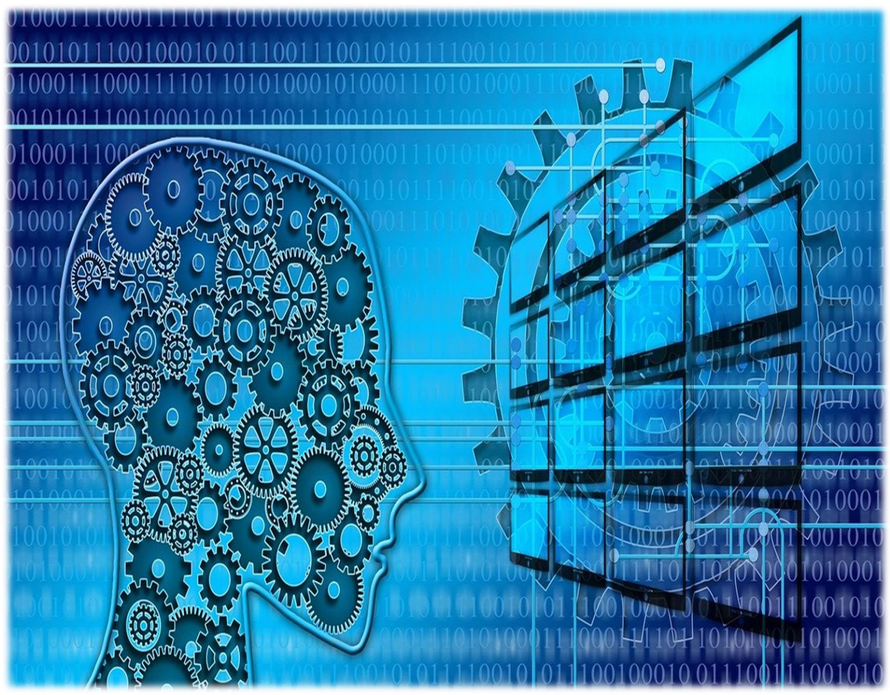
The focus of the research will shift from conveying trust through signals/symbols (Riegelsberger, Sasse, & McCarthy, 2005) to understanding how users make decisions about the trustworthiness of digital information

Potential research:

Manipulating specific trust signals/symbols within OSS libraries

Exploring moderating effects such as social identity theory (Tajfel, 1974)

How users process trust signals/symbols for digital information (automatic vs deeper thought)



Phase 3 – Intervention and ethics

The final phase of the research focuses on the creation of an intervention to support users to correctly evaluate the trustworthiness of digital information

However, the nature of the research means strong ethical considerations are needed

Planned research:
Combining the results from the first two phases to create an intervention

Focus groups with industry and academia experts to explore how the research in digital trust can be ethically guided

Industry applications:

Attacks on physical infrastructure – 5G towers have been damaged because of malicious information.

Trust evaluations in OSS libraries - help users make better evaluations of the trustworthiness of code in OSS libraries.
Help guide security policy for users.

Correctly evaluating the trustworthiness of digital health information – A huge amount of mis and disinformation exists about COVID-19

References:
Amazeen, M. A., & Bucy, E. P. (2019). Conferring resistance to digital disinformation: The inoculating influence of procedural news knowledge. *Journal of Broadcasting & Electronic Media, 63*(3), 415-432.
Hansen, M., Köhntopp, K., & Pfitzmann, A. (2002). The Open Source approach—opportunities and limitations with respect to security and privacy. *Computers & Security, 21*(5), 461-471.
Riegelsberger, J., Sasse, M. A., & McCarthy, J. D. (2005). The mechanics of trust: A framework for research and design. *International Journal of Human-Computer Studies, 62*(3), 381-422.
Tajfel, H. (1974). Social identity and intergroup behaviour. *Social science information, 13*(2), 65-93.