1. Falling for phishing attempts: An investigation of individual differences that are associated with behavior in a naturalistic phishing simulation (2024)
   Citation -
   Beu, N., Jayatilaka, A., Zahedi, M., Babar, M. A., Hartley, L., Lewinsmith, W., & Baetu, I. (2023). Falling for phishing attempts: An investigation of individual differences that are associated with behavior in a naturalistic phishing simulation. *Computers & Security, 131*, 103313. https://doi.org/10.1016/j.cose.2023.103313

   This study shows the personal characteristics that make employees more likely to fall for phishing attacks. This study was performed in a real organization and it uses a phishing simulator followed by a survey to identify predictors and behaviors. Results show that low employee satisfaction, newer employees, and weak organizational loyalty leads to higher vulnerability. This directly shows that good employers that create a likeable work environment are more likely to keep up with security policies. This study makes since and is peer reviewed making it credible and a good source. Its findings contribute to the overall understanding of how phishing attacks are stopped and how they are so effective. For a project focused on social engineering this article adds real value about human behavior and shows that technical solutions are usually not the answer to some of the hardest questions. Technical solutions especially don't work in the dysfunctional work environments that some companies have.

2. The health belief model and phishing: Determinants of preventative security behaviors (2023)
   Citation -
   Du, J., Kalafut, A., & Schymik, G. (2024). The health belief model and phishing: Determinants of preventative security behaviors. *Journal of Cybersecurity, 10*(1), tyae012. https://doi.org/10.1093/cybsec/tyae012

   This article utilizes the Health Belief Model (HBM) to examine what motivates individuals to engage in phishing prevention behaviors. The authors studied that perceived threat severity, susceptibility, and self-efficacy play big roles in influencing security conscious behaviors. This study is peer-reviewed and is theoretically and statistically sound making it a good academic resource for the effects of social engineering. It directly supports the psychological theories that impact real world cybersecurity prevention and would be a good resource for awareness training.

3. A comprehensive survey on social engineering attacks, countermeasures, case study, and research challenges (2025)
   Citation -
   Rathod, T., Jadav, N. K., Tanwar, S., Alabdulatif, A., Garg, D., & Singh, A. (2025). A comprehensive survey on social engineering attacks, countermeasures, case study, and research challenges. *Information Processing & Management, 62*(1), 103928. https://doi.org/10.1016/j.ipm.2024.103928

This article shows a thorough review of social engineering attack types, including phishing, baiting, and pretexting; it also outlines defence strategies. The authors present a case study that uses artificial intelligence and blockchain to detect malicious URLs on social media platforms. The case study combines academic literature, technical experimentation, and real world data to show the practical solutions as well as the theoretical predictions. This article is peer reviewed and would be a great resource for overall social engineering papers that study the prevention and response to attacks. This would also be a good resource to make predictions about things like oversharing on social media leading to easier attack vectors.

4. Development of a new 'human cyber-resilience scale'
   Citation -
   Joinson, A. N., Dixon, M., Coventry, L., & Briggs, P. (2023). Development of a new ‘human cyber-resilience scale’. *Journal of Cybersecurity, 9*(1), tyad007. https://doi.org/10.1093/cybsec/tyad007

   This article introduces a measurement tool called the Human Cyber-Resilience Scale, which assesses people's ability to recover or cope with cyber threats. This scale is based on psychological concepts like emotional regulation, confidence and social support. The study uses survey data and statistical analysis to validate the tool and is a credible piece of research in a respected journal. This source is a good tool to determine people's response to social engineering attacks and how those responses could impact or contribute to subsequent attacks.