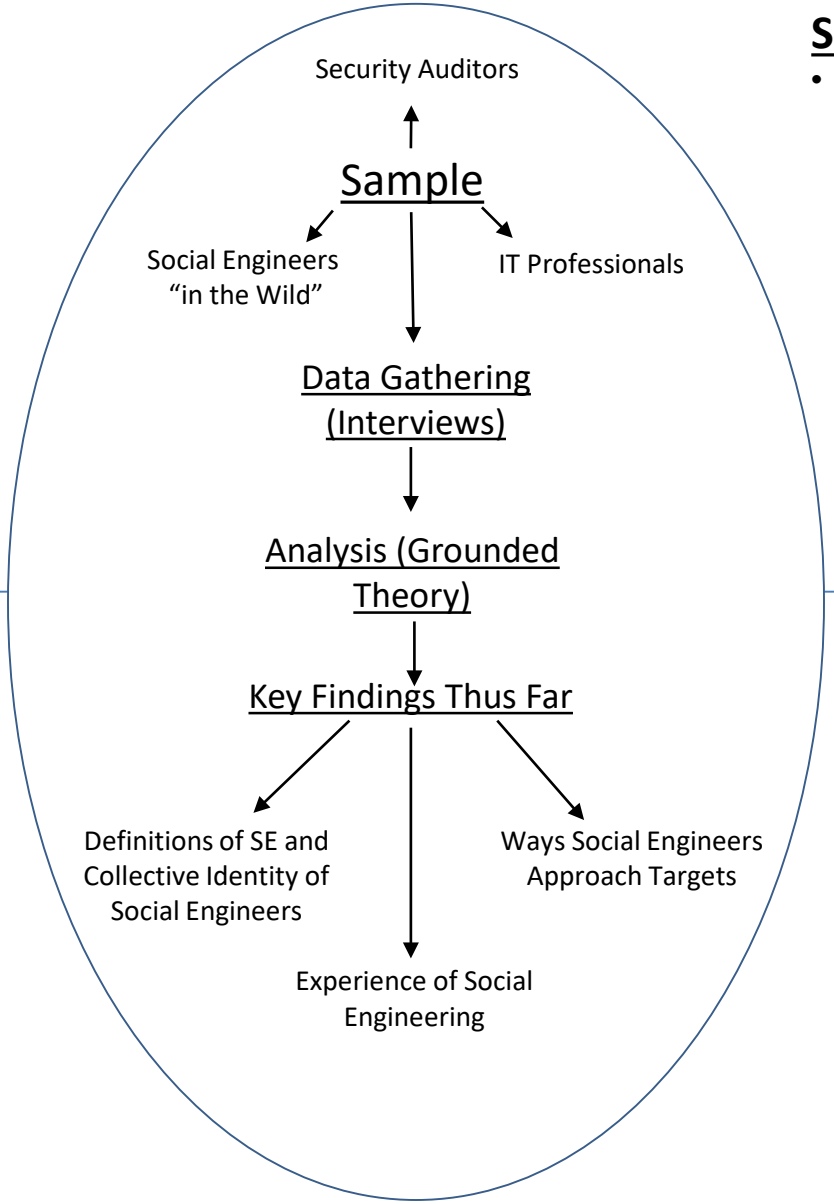
SBE: Small: Technological Con-Artistry: An Analysis of Social Engineering

Challenge:

- The current project studies "social engineering" or the manipulation of the human element of information security for the purposes of gaining access to sensitive information or computer networks.
- This research is largely exploratory and involves qualitative, semi-structured interviews with social engineers "in the wild," security auditors who make use of social engineering techniques, and IT professionals tasked with protecting organizations from social engineering threats.
- Upon completion of the research, our goal is to provide a sociologically and criminologically grounded understanding of social engineering. In addition, we plan to provide insights and recommendations concerning information security awareness and best practices.



Scientific Impact:

- Contribute to knowledge base about social engineering from criminological and sociological perspectives.
  - Tactics taken by social engineers.
  - Formation of collective worldview or identity.
  - Experience of social engineering.
  - Learning of social engineering tactics.
  - Etc.

Solution:

- Key results thus far include:
  - Worldview of social engineers tends to frame human interaction in computational terms.
  - Experiences of social engineering mirror of types of crime in that fraudsters not only pursue instrumental ends (i.e. money) but also experiential ones as well (thills, fun, etc.).
  - Strategies taken by social engineering

Broader Impact:

- Generate policy suggestions for fraud prevention at both the individual and organizational levels.
- Suggestions for refining security awareness training programs.
- Educational and training opportunities for undergraduate and graduate students.
- Results shared at academic conferences and publication outlets.

Project #: NS9664
Kevin F. Steinmetz, kfsteinmetz@ksu.edu
W. Richard Goe, goe@ksu.edu
Kansas State University