SOCIAL ENGINEERING: TOWARDS A USER INTROSPECTIVE COUNTERMEASURE APPROACH

University of the Cumberlands

Miguel Buleje, Ph.D.

Ulrich Vouama, Ph.D.

Agenda

- Intro & Fundamentals of Social Engineering
- Social Engineering Taxonomy & Human Factors
- Implications of Human Personality & Persuasion Strategies
- User Introspective Countermeasure Approach (UIAC)
- Defense Recommendations

Fundaments of Social Engineering

Attack Classification & Types

- Multiple Classifications and Categories presented in the literature
- Social, Technical, and Physical-based attacks, Salahdine & Kaabouch (2019)
- Human-based or Computer-based Classes, Peltier (2006).

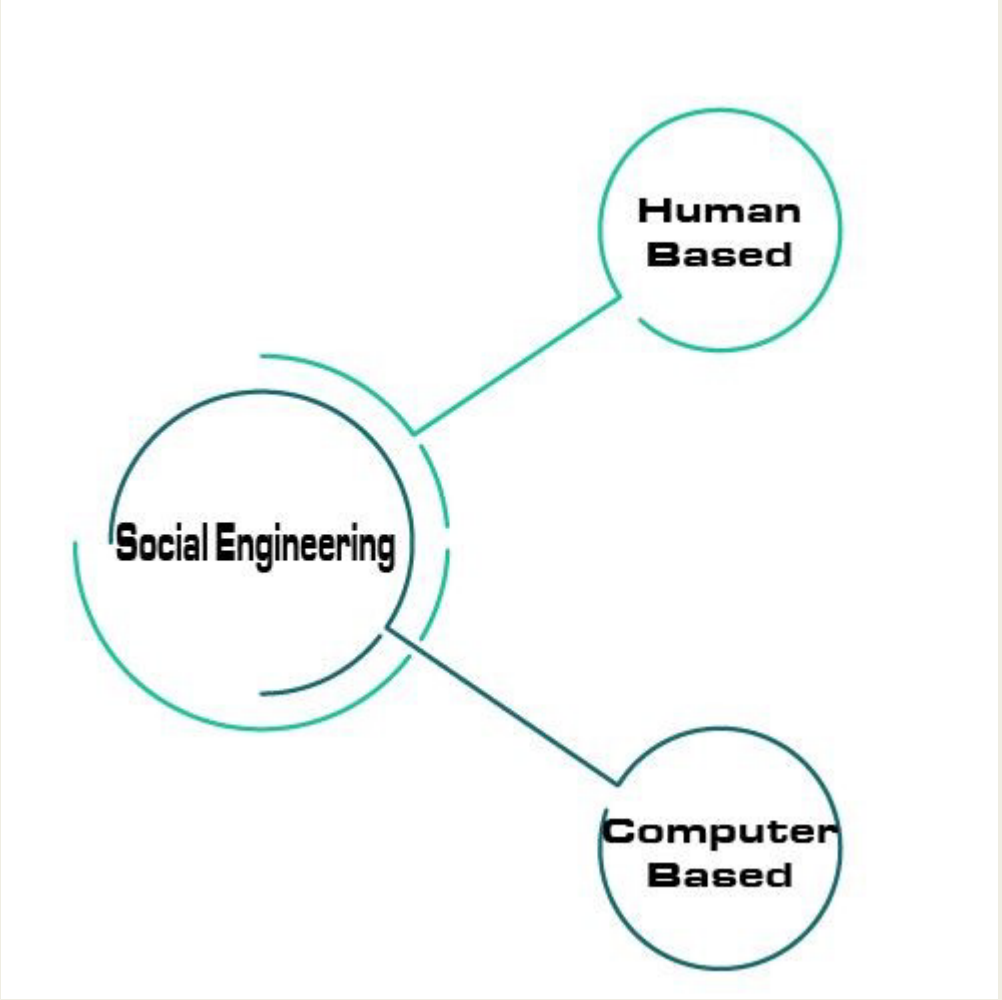


Figure 1: Type of Social Engineering Attacks, adapted from Peltier (2006).

Lifecycle of Social Engineering

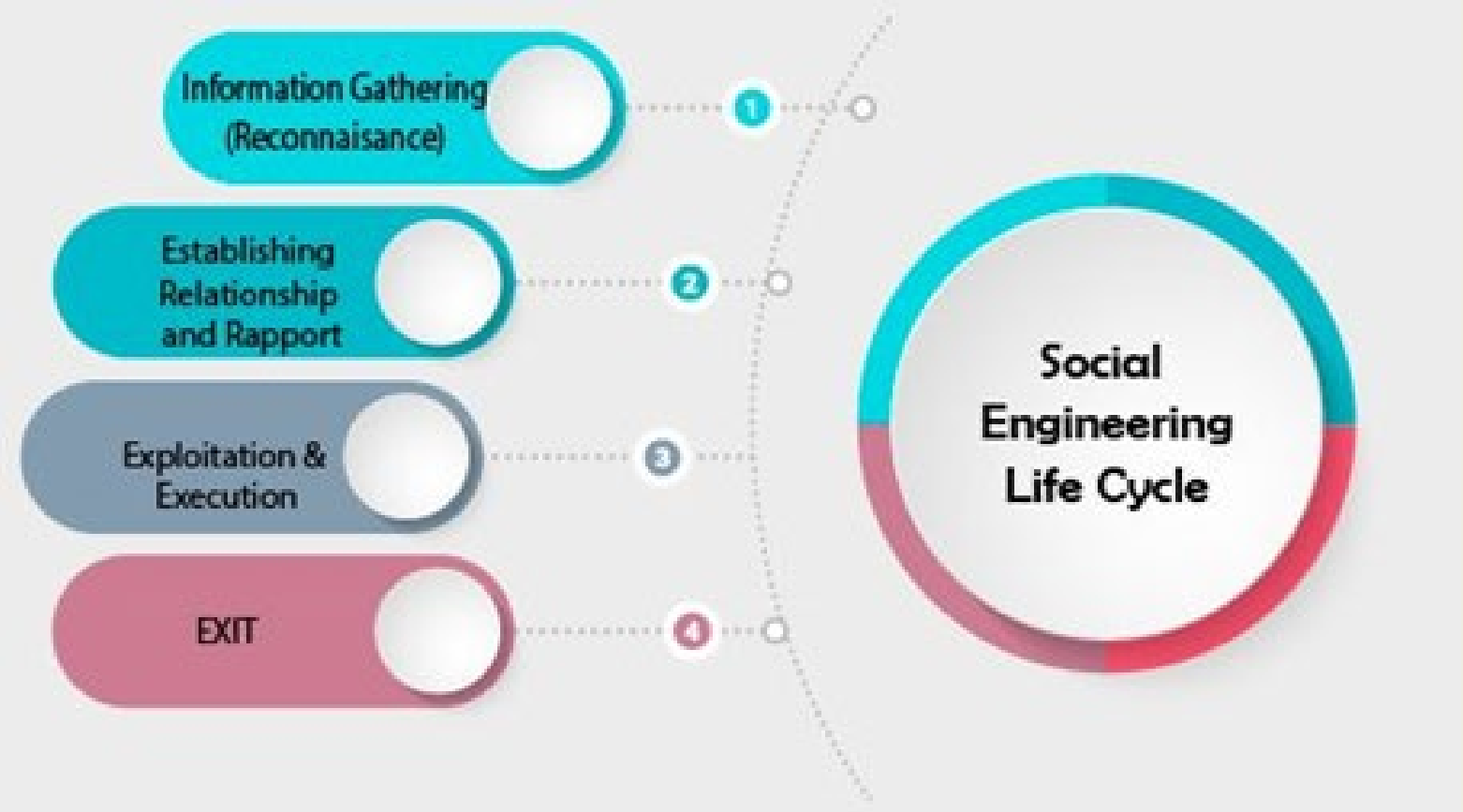


Figure 2: Social Engineering Attack Stages. Adapted from Salahdine and Kaabouch (2019).

Classification of Vectors

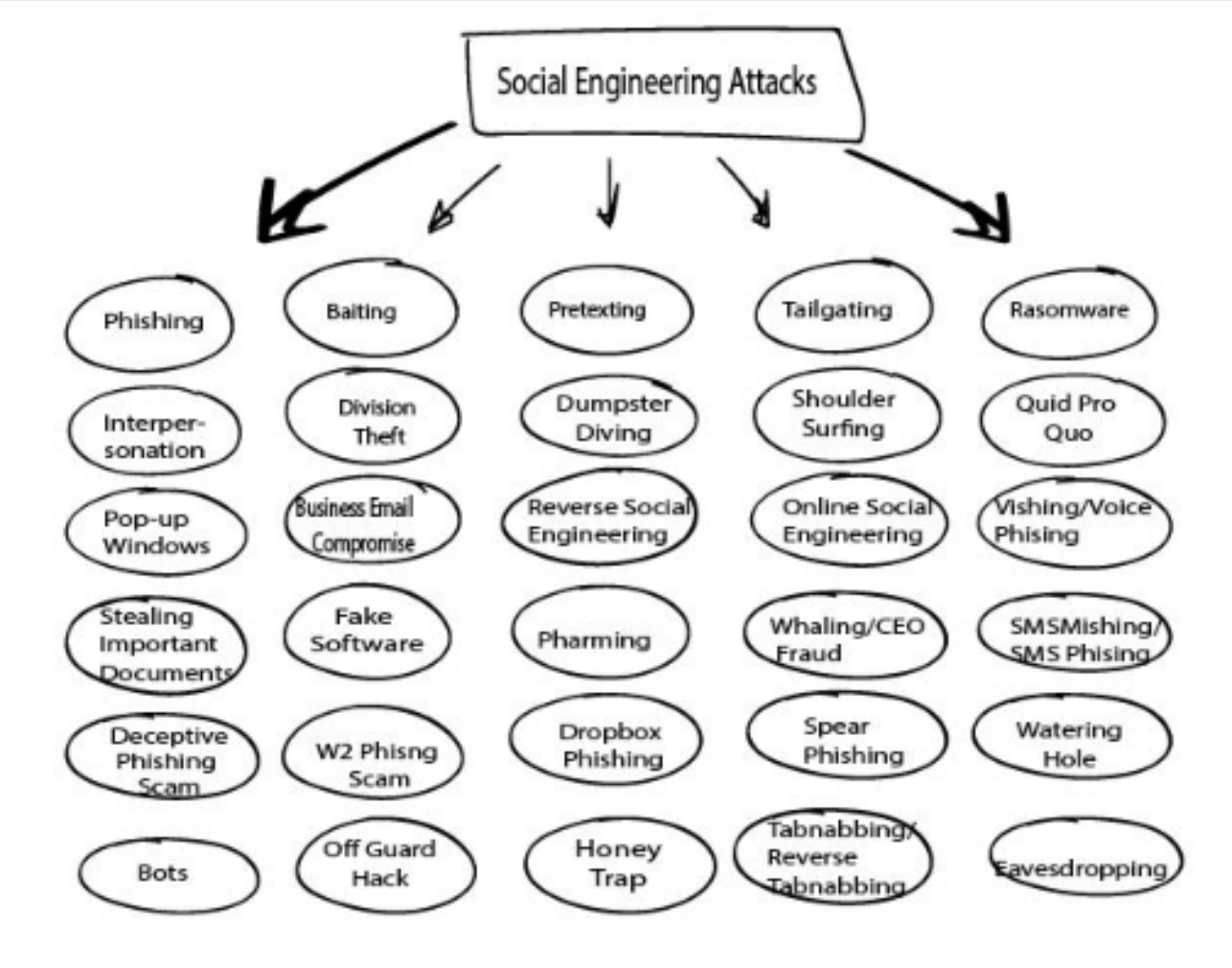


Figure 3: Classification of Vectors

Social Engineering Taxonomy: Human Factors

Mitnick (2011)	• Proposed the Social Engineering Attack Cycle (SEAC)
Nohberg & Kawalski (2008)	• Descriptive Model, depicts “Deceptive" crimes in SE.
Mouton et al. (2014)	• Introduced the “Ontological Model" for SE attacks
Harley (1998)	• One of the first Taxonomies in the SE Space
Laribee (2006)	• “Trust Model" and an “Attack Model."

Human Persuasion Strategies

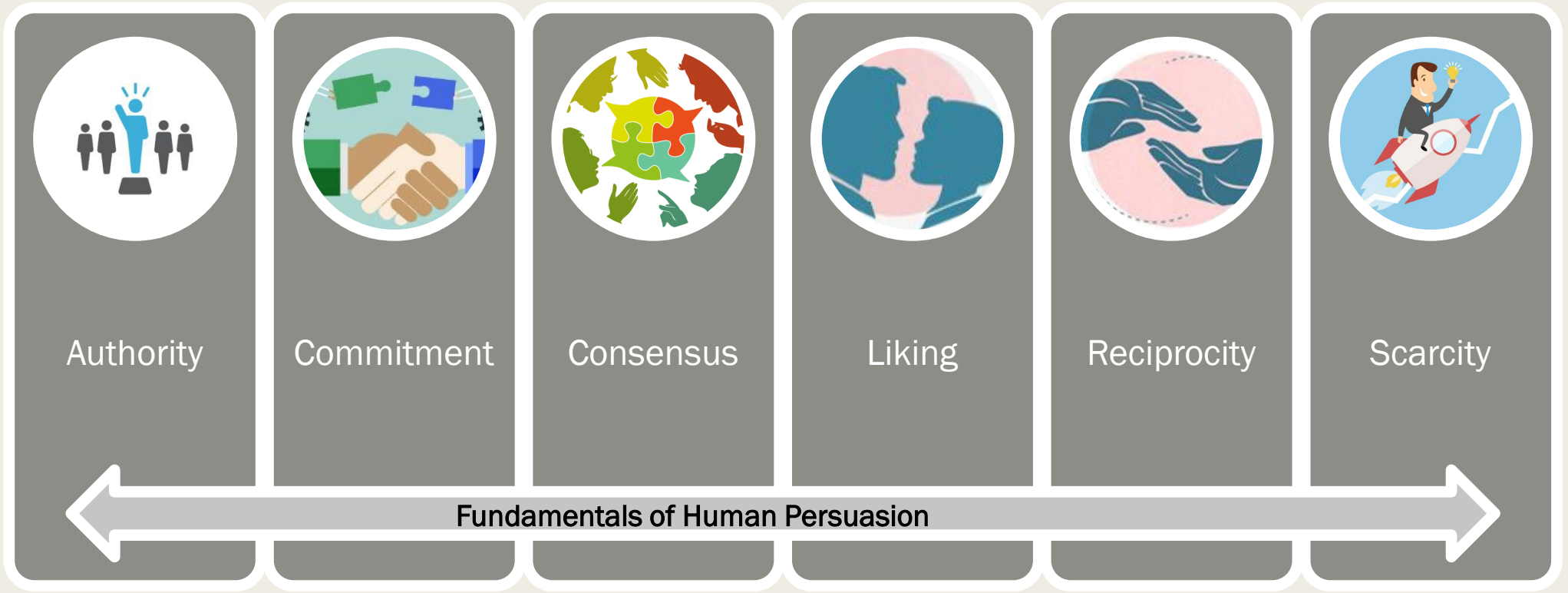


Figure 4: Six Fundamental Persuasion Principles for Human Behavior. Adapted from Cialdini (2001).

Human Five Factor Model of Personality

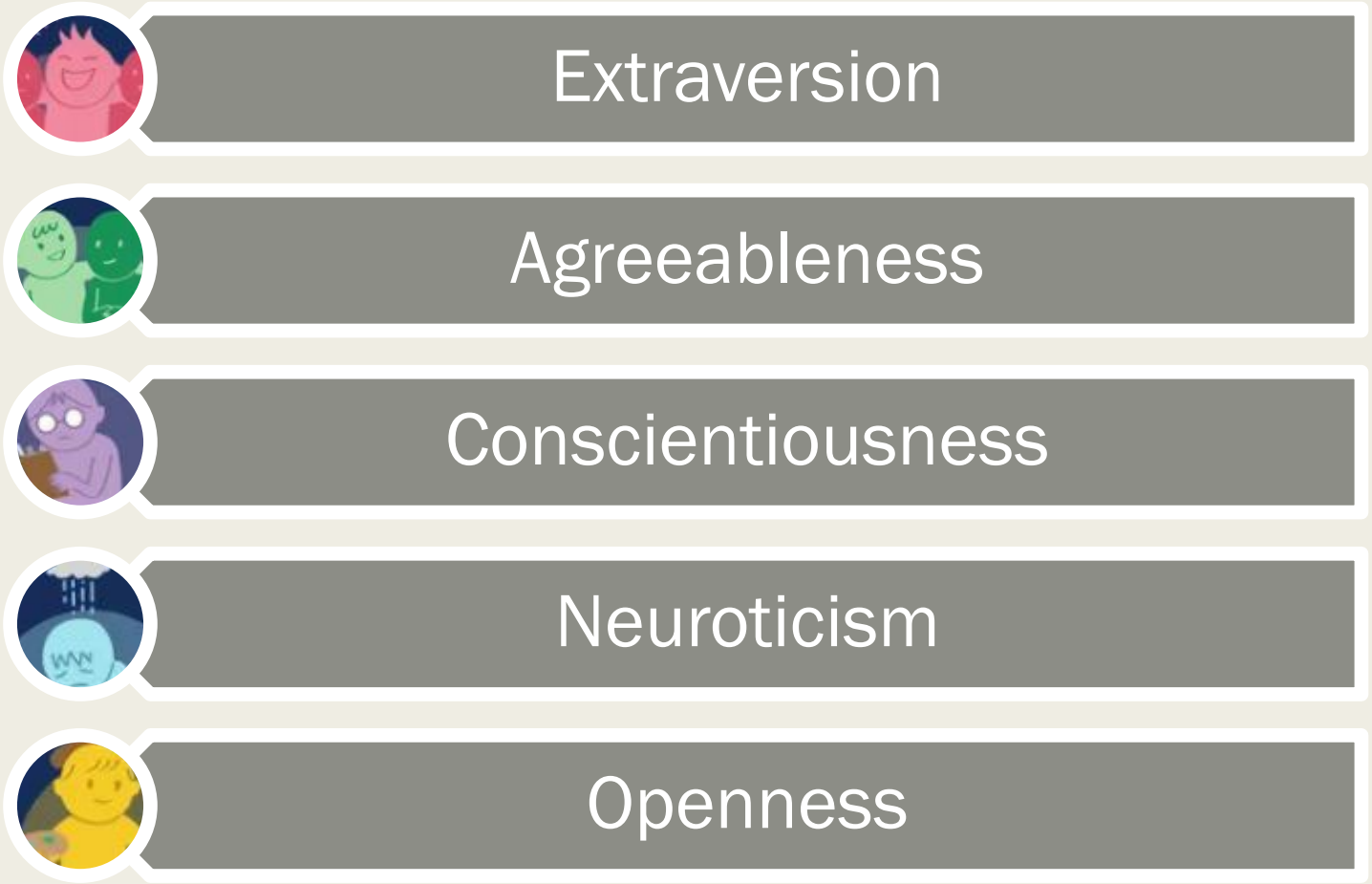


Figure 5: Five Factor Model of Personality. Adapted from McCrae an Oliver (1992).

Introspective Countermeasure Approach (UICA)

Table 1: Introspective Countermeasure Approach (UICA)

SE Attack Vectors	Personality Categories					Persuation Principles					
	Extraverstion	Agreeableness	Counscientiousness	Neurotocism	Openness	Authority	Commitment	Consensus	Liking	Reciprocity	Scarcity
Computer-based											
Phishing		X			X	X			X		
Pop-Up Windows				X	X						X
SMSMishing/ SMS Phishing		X		X	X	X			X		X
Ransomeware		X		X	X	X					X
Deceptive Phising/Scam		X	X	X	X	X			X		X
W2 Phishing scam		X	X			X	X		X		
Dropbox Phishing		X	X			X			X		
Spear Phishing		X	X	X	X	X	X		X		

SE Attack Vectors	Personality Categories					Persuation Principles					
	Extraverstion	Agreeableness	Counscientiousness	Neurotocism	Openness	Authority	Commitment	Consensus	Liking	Reciprocity	Scarcity
Human-based											
Baiting		X			X					X	X
Pretexting		X			X	X			X		
Interpesonation	X	X		X	X	X			X		X
Dumpster Diving				X							X
Tailgating	X	X		X	X	X		X	X		
Shoulder Surfing	X	X							X		X
Eavesdropping	X	X			X						X
Division Theft	X	X		X	X			X	X	X	X
Reverse Social Engineering (RSE)	X	X		X	X	X			X	X	X
Off-Guard Hack	X	X		X	X	X			X	X	X
Honey Trap	X	X		X	X				X		X
Stealing Important Documents		X									X

Introspective Countermeasure Approach (UICA)

SE Attack Vectors	Personality Categories					Persuation Principles					
	Extraverstion	Agreeableness	Counscientiousness	Neurotocism	Openness	Authority	Commitment	Consensus	Liking	Reciprocity	Scarcity
Hybrid-based											
Reverse Social Engineering (RSE)	X	X		X	X	X			X	X	X
Watering hole		X		X	X						X
Online Social ENgineering	X	X		X	X				X		

Defense Recommendations

Social Engineering Map:

- Leverage UICA to assess “Individual Strength”
  - *Assess Personality Types*
  - *Assess Strength by each individual as a dimension of Personality and Persuasion*
- Assess Systemic Strength
  - *Define Data & Information Threats*
  - *Classify multiple security mechanism*
- Map the system as presented in the Figure
- Testing, recommended to validate information presented
- Develop implementation plan to address vulnerabilities by system and individuals.

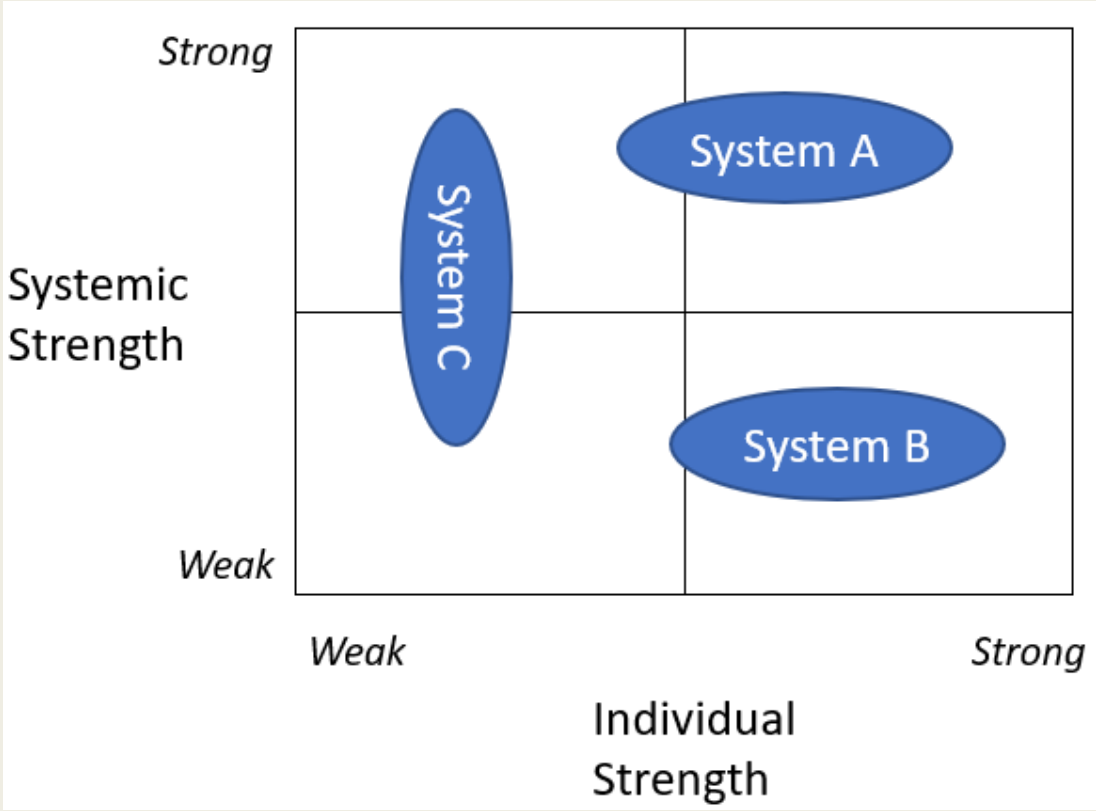
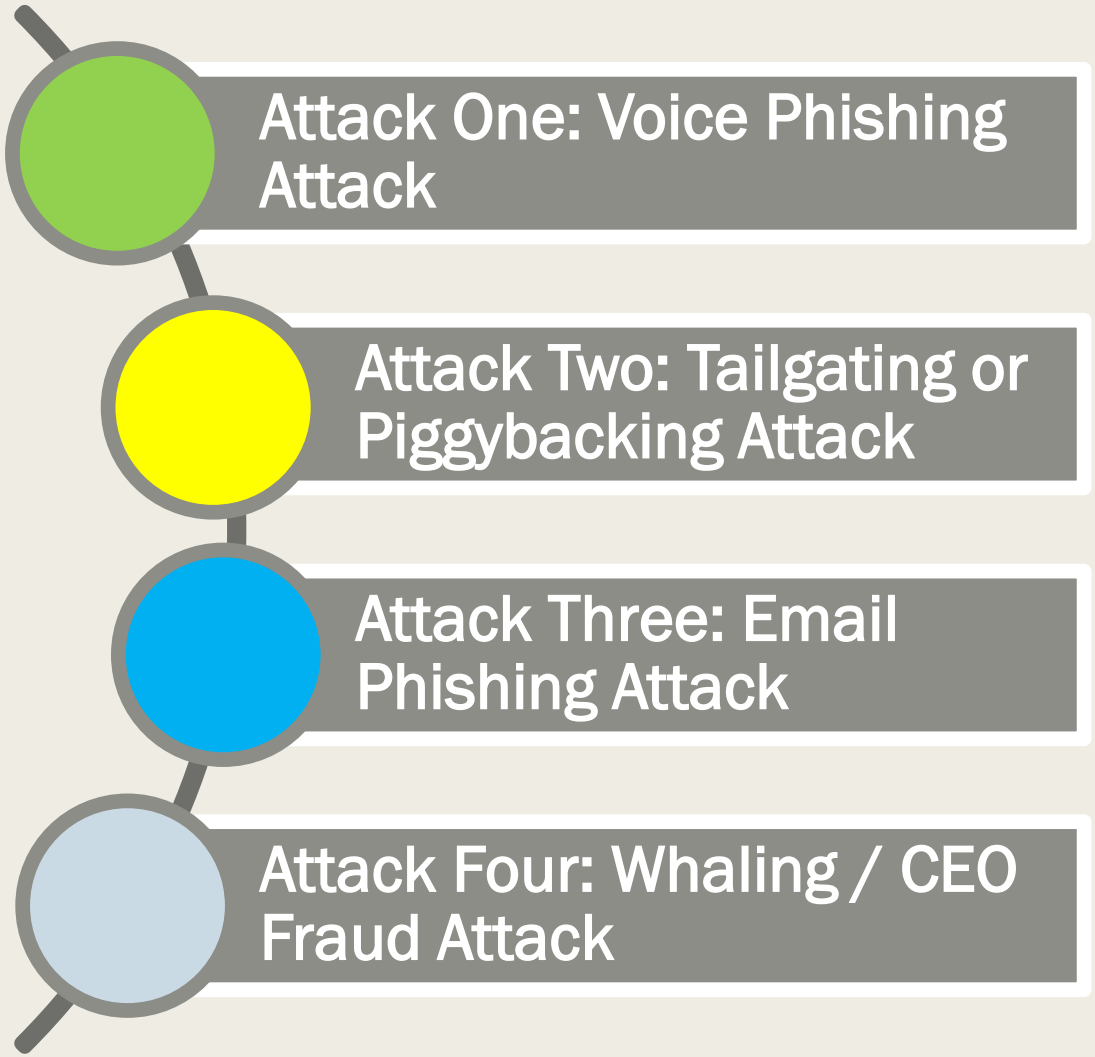


Figure 6: Social Engineering Map

Defense Recommendations



Conclusion & Future Research

References

- Airehrour, D., Nair, N. V., & Madanian, S. (2018). Social Engineering Attacks and Countermeasures in the New Zealand Banking System: Advancing a User-Reflective Mitigation Model. *Information*, 9(5), 110. doi:10.3390/info9050110
- AP NEWS (2021, April 3). Facebook Data on More than 500M Accounts Found Online. AP NEWS.https://apnews.com/article/business-media-social-media-fce118b1adfef8f6c51518f71465dd4b
- Bajak, F. (2019, December 20). Data on 267 million Facebook users exposed. *AP NEWS*.
- https://apnews.com/article/technology-us-news-business-bdf02dbe7bf266b025b6f1b0ae5860fd
- Cialdini, R.., Rhoads, K. (2001). Human Behavior and the Marketplace. *Marketing Research. 13*, 8–13 (2001)
- Francois Mouton, Louise Leenen, and H.S. Venter (2014). Social Engineering Attack Examples, Templates, and Scenarios. *Computers & Security, 59*:186 – 209
- Greitzer, F., Strozer, J., Cohen, S., Moore, A., Mundie, D., Cowley, J. (2014). Analysis of Unintentional Insider Threats Deriving from Social Engineering Exploits. *2014 IEEE Security and Privacy Workshops*, pp. 236-250, doi: 10.1109/SPW.2014.39.
- Harley, H. (1998). Re-Floating the Titanic: Dealing with Social Engineering Attacks. *EICAR*, London. p. 13.
- John, O. P., & Srivastava, S. (1999). The Big Five trait taxonomy: History, measurement, and theoretical perspectives. *Handbook of Personality: Theory and Research, 2*, 102–138.
- Mitnick, K., and Simon, W. (2011). *The Art of Deception: Controlling the Human Element of Security*. John Wiley & Sons.
- Krombholz, K., Hobel, H., Huber, M., and Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and Applications, 22*(C):113–122, June 2015.
- Nohlberg M., Kowalski, S. (2008). The Cycle of Deception – A Model of Social Engineering Attacks, Defenses and Victims. *Proceedings of the Second International Symposium on Human Aspects of Information Security & Assurance* (HAISA 2008). Page 1- 11.
- Nyirak, A. (2017). The Social Engineering Framework. Security Through Education.
- https://www.social-engineer.org/framework/attack-vectors/attack-cycle/
- Laribee, L. (2006). Development of Methodical Social Engineering Taxonomy Project. *Msc, Naval Postgraduate School, Monterey* (California. June 2006).
- Love, T. (2014). Oxytocin, Motivation and the Role of Dopamine. Pharmacology. *Biochemistry, and Behavior, 119*, 49–60. https://doi.org/10.1016/j.pbb.2013.06.011
- Mann, I. (2008). *Hacking the Human. Social Engineering Techniques and Security Countermeasures*. Gover Publishing Limited. Burlington, VT. USA.
- Mathews, a.m (1990). Why worry? The Cognitive Function of Anxiety. *Behavior Research and Therapy, 28*(6):455 – 468, 1990.
- McCrae, R.R., John, O.P. (1992). An introduction to the five-factor model and its applications. *Journal of Personality, Vol. 60*, No. 2, 1992, str. 175-215.
- McLaughlin, M. (2012). Using Open Source Intelligence for Cybersecurity Intelligence.
- Computer Weekly. https://web.archive.org/web/20180629155103/https://www.computerweekly.com/tip/Using-open-source-intelligence-software-for-cybersecurity-intelligence
- Peltier, T. (2006). Social Engineering: Concepts and Solutions. *Information Systems Security 15*, 5: 13-21.
- Ryan Heartfield and George Loukas. A Taxonomy of Attacks and a Survey of Defense Mechanisms for Semantic Social Engineering Attacks. *ACM Computing Surveys., 48*(3):37:1–37:39, December 2015.
- Salahdine, F., Kaabouch, N. (2019). Social Engineering Attacks: A Survey. *Future Internet, 11*(4):89. https://doi.org/10.3390/fi11040089
- Shropshire, J., Warkentin, M., & Sharma, S. (2015). Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *Computers and Security, 49*, 177–191.
- Uebelacker, S., & Quiel, S. (2014). The Social Engineering Personality Framework. *2014 Workshop on Socio-Technical Aspects in Security and Trust*, 2014, pp. 24-30, doi: 10.1109/STAST.2014.12.