**Abstract**

In many organizations, security awareness is generally mandatory training for every individual in the organization. Security or training personnel typically assign training annually and to ensure that every individual completes the required training.

Although many engaging and effective security awareness programs exist, it is still a challenge to persuade an individual to engage with their security awareness course, retain the knowledge and implement these secure behaviors that assist the organization to avoid security threats. Gamified security awareness and training takes these challenges and allows employees to play through various cybersecurity scenarios, make choices and see the successes or consequences of their decisions. This not only makes security awareness entertaining and engaging, but it prepares employees for a real security threat in the future. Gamification gives individuals an additional reason to complete tasks that they otherwise feel difficult, uninteresting, or unimportant to the individual. For one, games are pleasurable. Turning a mandatory task into an enjoyable game transforms completing a task into an enjoyable or easy activity.

1. Introduction
   1. Details about fake news/social engineering
   2. Impact of fake news/social engineering
   3. Topic of system
   4. Problem that system solves
      * 1. Increase awareness of social engineering and how it relates to cyber security.
        2. Determine what types of social engineering tactics are most/more effective.
        3. Collect data on how people identify and react to social engineering situations.
        4. Determine if there is a certain group of people that is more susceptible to social engineering attempts.
        5. Determine if individuals can correctly identify social engineering
   5. What is presented in the paper?
2. Background
   1. About fake news/social engineering
   2. Fake news/social engineering reporting levels
   3. Impact of fake news/social engineering
   4. Estimate of fake news/social engineering reporting
   5. Societal impact of fake news/social engineering reporting
   6. Issues with fake news/social engineering
3. Proposed system
   1. System needs and requirements
   2. System design
   3. System operations
4. Evaluation of the proposed system
   1. Experimental methodology
   2. Data and analysis
   3. System evaluation
5. Conclusions and future work
   1. Importance of the system
   2. What has been presented in the paper
   3. System evaluation conclusions
   4. System immediate next steps
   5. Future work

Acknowledgements

* Funding sources, if applicable
* Resources used, if applicable
* Those who helped (who are not co-authors), if applicable
* Other required acknowledgements

Disclosures (if required by publication venue or necessitated by ethical or other considerations) References Appendixes (if applicable and allowed by publication venue)