Modeling Deception for Identifying and Protecting against Advanced Email Phishing

Abdullah Almoqbil[a], Brian O'Connor[a], Rich Anderson[c], Patrick McLeod[c], Jibril Shittu[a], and Bader Alshemaimri[f],

[a]University of North Texas, United States of America

[c]UNT SYSTEM

[f]University of Texas Arlington, United States of America

AbdullahAlmoqbil@my.unt.edu, brian.oconnor@unt.edu, rich.anderson@untsystem.edu, patrick.mcleod@untsystem.edu, JibrilShittu@my.unt.edu, and bader.alshemaimri@mavs.uta.edu

ABSTRACT

Cheating, beguiling, and misleading information exist all around us; understanding deception and its consequences is crucial in our information environment. This study investigates deception in phishing emails that successfully bypassed Microsoft 365 filtering system. We devised a model that explains why some people are deceived and how the target individuals and organizations can understand the motivation behind deception and how to prevent or counter attacks. The theoretical framework used in this study was Anderson's Functional Ontology Construction (FOC). The methodology of the study involves quantitative and qualitative descriptive design, where the data source for this study is the phishing emails archived from an educational organization. We looked for term frequency-inverse document frequency (Tf-idf) and the distribution of words over documents (topic modeling) and found the subjects of phishing emails that targeted educational organizations are related to banks, jobs, and technologies. Also, our analysis shows the phishing emails in the dataset come under six categories; reward, urgency, curiosity, fear, job, and entertainment. Results indicate that staff and students were primarily targeted, and a list of the most used verbs for deception was compiled. We uncovered the stimuli being used by scammers and types of reinforcements used to misinform the target to ensure successful trapping via phishing emails. We identified how scammers pick their targets and how they tailor and systematically orchestrate individual attack on targets. The limitations of this study pertain to the sample size and the collection method. Future work will focus on implementing the derived model into building a software that can perform deception identification, target alerting and protection against advanced email phishing.

ALISE RESEARCH TAXONOMY TOPICS

information security; data visualization; ontologies; sociology of information

AUTHOR KEYWORDS

information security; deception; phishing emails; functional ontology construction; reinforcement