Mazephishing: The COVID-19 pandemic as credible social context for social engineering attacks

Kristjan Kikerpill[1] and Andra Siibak[2]

[1]University of Tartu
[2]Affiliation not available

May 18, 2021

Abstract

The first months of the COVID-19 pandemic witnessed a surge of social engineering attacks. Although the pandemic is certainly not the first occurrence of socially disruptive circumstances that drive cybercriminals to action, relevant academic scholarship has remained scarce. To fill this gap in literature, and propose the analytical framework of *mazephishing* that places particular emphasis on the importance of credible social context in the functioning of the online scam ecosystem, we carried out a content analysis of (N=563) international news stories reporting on social engineering attacks. Our results indicate that criminals make heavy use of social context and impersonation to make scams seem more credible. Major themes used in the scam messages include health information, personal protective equipment, cures, financial relief and donations. Additionally, scammers diversify their use of mediums depending on the type of scam being perpetrated. Our analysis also shows a significant presence of principles of persuasion in the circulated scam attempts.

Hosted file

`mazephishing manuscript final.docx` available at https://authorea.com/users/718606/articles/703793-mazephishing-the-covid-19-pandemic-as-credible-social-context-for-social-engineering-attacks