Abstract

Events and circumstances that accompany crises such as losses of loved ones, losses of material resources, dislocation, or physical harm, have an overall negative impact on people's mental health. It is this impaired state of man which makes him vulnerable to manipulation of social engineers who wants to take advantage of him in order to enrich themselves. This was also the case of the COVID-19 pandemic, the unprecedented crisis in modern history, during which phishing and fraud campaigns rapidly increased as people have been forced to stay safe at home and spent most of a day online. This work analyzes the psychological strategies of cybercriminals on a sample of more than 200 phishing e-mails in order to understand how the situation was abused and what can be learnt to prevent it in the future. It also provides theoretical and research frameworks for researchers who can apply it also on other types of crises. The results contribute to the fields of psychology, cybercrime as well as crisis management.

Keywords

COVID-19, phishing, social engineering, psychology, persuasion, crises, pandemic, impersonation, pretexting