Assessing contributor features to phishing susceptibility amongst students of petroleum resources varsity in Nigeria

Rume Elizabeth Yoro[1], Fidelis Obukohwo Aghware[2], Bridget Ogheneovo Malasowe[2], Obinna Nwankwo[3], Arnold Adimabua Ojugo[4]
[1]Department of Computer Science, Dennis Osadebey University Asaba, Asaba, Nigeria
[2]Department of Computer Science, University of Delta, Agbor, Nigeria
[4]Department of Computer Science, Novena University Ogume, Delta State, Nigeria
[5]Department of Computer Science, Federal University of Petroleum Resources Effurun, Effurun, Nigeria

Article Info

Article history:

Received Jul 13, 2021
Revised Oct 7, 2022
Accepted Nov 1, 2022

Keywords:

Federal University of Petroleum Resources Effurun's
Online presence
Personality traits
Phishing vulnerability
Social media contents
Socially-engineered attacks

ABSTRACT

In this observational quasi-experimental study, we recruited 200 participants during the Federal University of Petroleum Resources Effurun's (FUPRE) orientation, who were exposed to socially engineered (phishing) attacks over nine months. Attacks sought to extract participants' data and/or entice them to click (compromised) links. The study aims to determine phishing exposure and risks among undergraduates in FUPRE (Nigeria) by observing their responses to socially-engineered attacks and exploring their attitudes to cybercrime risks before and after phishing attacks. The study primed all students in place of cybercrime awareness to remain vigilant to scams and explored the various scam types with their influence on gender, age, status, and their perceived safety on susceptibility to scams. Results show that contrary to public beliefs, these factors have all been found to be associated with scam susceptibility and vulnerability of the participants.

Corresponding Author:

Arnold Adimabua Ojugo
Department of Computer Science, Federal University of Petroleum Resources Effurun
Delta State, Nigeria
Email: ojugo.arnold@fupre.edu.ng

1. INTRODUCTION

The internet's birth also witnessed the ever-increasing need for its users to stay connected via enabling support devices. However, such a need to stay connected and share data with other users within and outside of the user's locality has continued to open up many such users on a larger scale, to avenues of exploitation that can be harnessed by adversaries via threats and cyber attacks [1], [2]. This consequently has birthed the social media websites that have today, continued to gain great and significant popularity over the years, with over a 3.484 billion users worldwide reported in 2019 [3]. As users connect and perform many other feats over such media, they become more prone to threats and attacks of various forms. These attacks (many of which, socially-engineered today) reveal how vulnerable and susceptible a connected user is over the network-as the attacks are designed to exploit system errors and behavioral traits resulting from relations and operations between users. An adversary seeks to exploit an unsuspecting user as its victim and weakest link within the network. These amongst others are the reason(s) for which socially engineered attacks will continue to rise [4], [5].

Adversaries seek to compromise a potential victim and often succeed based on the target's (potential victim's) judgment rather than considering the security measure in place on the victim's network [4], [6]. The first quarter of 2018 witnessed a launch of fake Facebook pages with 60% of phishing attacks on social media networks and later on, in 2019, phishing on both Instagram and Facebook among others saw a 74.7%