Journal of Nonlinear Modeling and Analysis
Volume 7, Number 1, February 2025, 91–110
https://journal.global-sci.org/jnma
DOI:10.12150/jnma.2025.91

Mathematical Model Dynamics of Cyber Accounts for Vices, Recovery and Relapse

Oluwatayo Michael Ogunmiloro[1,†] and Samuel Olukayode Ayinde[1]

Abstract In this study, we develop a mathematical model through a system of first-order nonlinear ordinary differential equations. This model covers the dynamics between vulnerable cyber accounts and those implicated in cyber vices such as bullying, scams, spreading of misinformation, and the creation of harmful digital footprints. It further explores the mechanisms of recovery and relapse among these accounts. Through some mathematical analysis, we apply relevant theorems to affirm the model's fundamental properties, which includes its existence, uniqueness, positivity, and boundedness. We also determine the model's cyber vice-free and endemic equilibrium states, analyzing their local and global asymptotic stability based on when the basic reproduction number R_{cb} is greater or less than one. Simulation exercises are conducted to substantiate our theoretical findings and demonstrate the model's behavior in relation to R_{cb}. The simulation outcomes reveal an escalating trend in cyber vices, showing the necessity for targeted interventions that promote a more secure online environment for users and the broader cyber space.

Keywords Local stability, global stability, positivity and boundedness, basic reproduction number R_{cb}

MSC(2010) 92B05, 92B20.

1. Introduction

Cyber vices, including cyberbullying, scams, fraud, fake news, and digital footprints, have emerged as formidable challenges in the digital era. Understanding their dynamics and developing effective strategies to combat them is crucial for ensuring online safety and security. The advent of the digital age has revolutionized the way we communicate, work, and interact with each other [23]. The internet and social media platforms have brought numerous opportunities for connectivity and information sharing. However, along with these advancements, there has also been a rise in online cyber vices, posing significant challenges for individuals, organizations, and societies as a whole [22]. Cyberbullying, scams, fraud, fake news, and the creation of digital footprints are just a few examples of the detrimental activities that can occur in the online realm [19–21]. Understanding the dynamics of online cyber vices and developing effective strategies to combat them is of utmost importance in today's interconnected world. Mathematical modeling provides a powerful tool for gaining understanding into the mechanisms driving these vices and can aid

†the corresponding author.
Email address:oluwatayo.ogunmiloro@eksu.edu.ng(O.M.Ogunmiloro), olukayode.ayinde@eksu.edu.ng(S.O. Ayinde)
[1]Department of Mathematics, Ekiti State University, Ado-Ekiti, Nigeria

in the development of proactive measures to mitigate their impact. By constructing mathematical models, interactions between different entities involved in cyber vices and recovery dynamics can be studied [11–15]. Additionally, mathematical models enable us to study the effectiveness of various intervention strategies and assess their potential outcomes before implementation. In recent years, there has been a significant research focus on studying the effects of cyber defense and attacks using mathematical models, with notable contributions from Alexopoulous and Daras [1], Emmanuello and Ridley [2], Gencoglu [3], and Guilan, Del-Rey, and Cassado [4]. Furthermore, several researchers [9, 10] and [16–18], have developed mathematical models to address security threats and issues in the cyber space. Additionally, the cyber analysis of smart power and grid processes has been explored through mathematical modeling by researchers such as [5–8]. Despite these advancements, to the best of our understanding, we have identified a crucial gap regarding the understanding of how cyber accounts/sites are created and utilized to perpetrate vices such as scams, frauds, bullying, and leaving digital footprints. Moreover, the potential mitigation of these cyber activities using mathematical modeling has yet to be comprehensively discussed. To address this gap, our study seeks to investigate and analyze cyber accounts and their role in fostering various vices. We propose a robust mathematical model to shed light on this important aspect of cyber behavior. In Section 2, we provide a detailed formulation of the mathematical model, aiming to capture the cyber activities. Subsequently, in Section 3, we present the mathematical analysis of the existence and uniqueness, positivity, boundedness, and stability properties of the model. To gain understanding and verify the model's performance, we perform numerical simulations in Section 4. Finally, in Section 5, we conclude our study, summarizing the key findings and proposing potential future directions for the work.

2. Mathematical model formulation

The model assumes a deterministic system, where the future behavior of the system is entirely determined by its initial conditions and parameter values. This assumption disregards any random or stochastic elements that may exist in the real-world dynamics of cyber vices and recovery. The following system of equations describes the dynamics of various online vices, including cyber bullying, scams, fake news, and digital footprints, as well as the recovery process of affected online accounts. The total number of online cyber accounts ($N_{cb}(t)$) is divided into compartments such that $N_{cb}(t) = V_a(t) + C_b(t) + S_c(t) + F_n(t) + D_f(t) + R_s(t)$, where the rate of change of vulnerable cyber accounts (V_a) is given by

$$\frac{dV_a}{dt} = \Phi - (\beta_1 C_b + \beta_2 S_c + \beta_3 F_n + \beta_4 D_f)V_a - \delta V_a. \tag{2.1}$$

The rate of change of cyber account dedicated to cyber bullying (C_b) is

$$\frac{dC_b}{dt} = \beta_1 C_b V_a - (\delta + \psi_1)C_b + \varsigma_1 C_b. \tag{2.2}$$

The rate of change of cyber account involved in scams (S_c) is

$$\frac{dS_c}{dt} = \beta_2 S_c V_a - (\delta + \psi_2 S_c + \varsigma_2 C_b. \tag{2.3}$$