ACADEMIC PROGRESS REPORT
(For the Academic Year 2024-25)

Dr. RAVIKUMAR. D.B.
Assistant Professor
Saraswathi Law College
Chitradurga.

PAPER PRESENTATION

Sl. No.	National Conference/ Seminar/Symposium	Organised Institution	Topic	Date
01.	Two Day National Conference	Department of Youth Empowerment & Sports, Govt. of Karnataka, K.S.L.U., Hubballi & Saraswathi Law College, Chitradurga	"An Analysis on role of Youth in Eradication of Poverty"	4th & 5th April 2025

PROGRAMME COORDINATOR

SI No	Programme	Place	Date
01	"International Model United Nations Conference" on "The Rule of Youth Involving in the Green Economy, Green Energy, Green Jobs, And Green Transition"	CHITRADURGA	01-02-2025
02	"Right of Persons with Disability to access Knowledge" (International Webinar)	CHITRADURGA	02-11-2025
03	"National Moot Court Competition"	CHITRADURGA	3& 4-11-2025

PARTICIPATION

Sl. No.	Programme	Organised Institution	Concept	Date
01	Data Privacy Day	Manipal Law School, Bangalore	Data Privacy	28-01-2024
02	Faculty Development Programme	JSS Law College, Mysore	Law in the Contemporary World	18-07-2024 to 24-07-2024

ARTICLES PUBLICATION

Sl. No.	National/ International Journals	Title of the Paper	Publication	ISSN/ISBN No.	Year
01	International Journal of Information Movement	"Combatting Phishing in cyberspace: Insights from Indian Law and the Judiciary"	N.K. Publishing	2456-0553	30-09-2024

Principal
Saraswathi Law College
CHITRADURGA

(Dr. D.B. Ravikumar)
Assistant Professor

Department of Youth Empowerment and Sports, Government of Karnataka,
NSS Cell, Karnataka State Law University, Hubballi and
Saraswathi Law College, Chitradurga
Jointly organize

Two-Days National Conference

on

"Relevance of Vivekananda's Views on Youth in the Current Scenario"

CERTIFICATE

This is to certify that Dr. Ravikumar.D.B, Assisstant Professor. of Saraswathi Law College, Chitradurga has participated and presented paper on the topic "An Analysis On Role of Youth in Eradication of Poverty" in the National Conference on "Relevance of Vivekananda's Views on Youth in the Current Scenario" held on 4th & 5th April, 2025 organised by Department of Youth Empowerment and Sports, Government of Karnataka, NSS Cell, Karnataka State Law University, Hubballi and Saraswathi Law College, Chitradurga, Karnataka.

Principal
Saraswathi Law College
CHITRADURGA

Shri. I.B. Biradar	Dr. M.S. Sudhadevi	Prof. (Dr) C. Basavaraj

ISSN:2456-0553

IFSIJ Impact Factor : 5.770
ISSN:2456-0553

NK Publishing

International Journal of Information Movement

A Peer-Reviewed Globally Recognized & Quality Refereed Online Journal of Multidisciplinary Research

Certificate of Publication

This is to certify that paper titled **"COMBATTING PHISHING IN CYBERSPACE: INSIGHTS FROM INDIAN LAW AND THE JUDICIARY "** authored by **DR. D B RAVIKUMAR, SARASWATHI LAW COLLEGE, CHITRADURGA DISTRICT, KARNATAKA STATE, INDIA**; has been published in Volume IX Issue V, September, 2024 of online multidisciplinary International Journal of Information Movement (monthly) which is published by N.K. Publishing.

Date of Issue: 30th September 2024

M.S. Sudhakar
Principal
Saraswathi Law College
CHITRADURGA

Naresh Kumar

Dr. Naresh Kumar
Editor-in-Chief

International Journal of Information Movement *Vol. 9 Issue V* *(September 2024)*
Website: www.ijim.in *ISSN: 2456-0553 (online)* **Pages 21-25**

COMBATTING PHISHING IN CYBERSPACE: INSIGHTS FROM INDIAN LAW AND THE JUDICIARY

Dr. D B Ravikumar
Assistant Professor
Saraswathi Law College, Chitradurga district, Karnataka state, India
Email-id :- dr.ravikumar5066@gmail.com

Abstract: In the age of information technology, the swift increase in internet usage and mobile technology has created new opportunities, not only for innovation and communication but also for criminal activities. One of the most perilous and swiftly changing forms of cybercrime is phishing. Phishing exemplifies social engineering tactics designed to deceive users and takes advantage of the inadequate usability of existing web security technologies. Consequently, a doctrinal study was conducted to examine the rising number of reported phishing incidents. Phishing is not merely a technical concern but also a legal one. In India, various laws and authorities tackle phishing, despite the absence of a singular, dedicated 'anti-phishing' law. It is essential not only to establish suitable legal measures for phishing in cyberspace but also to raise awareness among the public and ensure the effective operation of law enforcement agencies.

Keywords : Anti-phishing, IT, Phishing, Law and Judiciary, cyber space and Law enforcement agencies

1.0 Introduction

Phishing stands out as a top cybercrime in our linked online space. It tricks people into giving away private details like login info or bank numbers. This scam hurts millions each year. In India, the push for more online services makes it riskier. Programs like UPI let users pay with phones in seconds. Digital India aims to connect every village to the web. Aadhaar ties IDs to services with a simple scan. These steps open doors to easy living but also invite attacks. Scammers target them hard. Fraudsters now change their tricks fast. They beat basic defenses and get smarter each time. Early phishing relied on fake emails or sites that fooled users into typing details. People fell for urgent alerts from "banks" or "government offices." But now, crooks avoid waiting for clicks. They know users learn to spot bad links. So, these bad actors send emails packed with hidden threats. Trojans hide inside attachments or downloads. Once opened, they grab passwords without a sound. This hits online bank accounts most. A quick example: An email looks like a UPI alert about a failed payment. It urges you to check a file. That file runs the Trojan and steals your login.

Such attacks spread wide in India. Reports show thousands of cases monthly, with losses in crores. Banks and police see a rise in stolen funds from these schemes. Why does it matter? It shakes trust in digital tools. Folks hesitate to use apps or share data. Yet, the need grows with more e-services. Indian laws fight back. The IT Act covers cyber fraud with fines and jail time. Rules demand banks to spot and stop scams. Police units track these crimes nationwide. Still, the threat shifts quick. Laws update to match, but gaps remain. This piece digs into phishing basics. It looks at harms in India. And it checks how rules try to block these growing dangers.

1.1 Meaning of Phishing: The term "Phishing" is not explicitly defined in Indian Laws. Nevertheless, phishing activities are acknowledged as cybercrimes and are subject to prosecution under different sections of the Information.

2.0 Technology Act 2000

Phishing refers to a form of cyber attack where attackers pose as legitimate individuals or organizations, usually via emails, messaging applications, websites, or phone calls, to deceive victims into disclosing sensitive information, including:

i. Login credentials (e.g., username and password)
ii. Bank account or credit card numbers
iii. Personal identity information (e.g., Aadhaar number, PAN SSN)
iv. One-time passwords (OTPs) or two-factor authentication (2FA) codes.

Phishing is an unlawful act in which sensitive information, such as passwords and credit card details, is fraudulently obtained by an individual or entity misrepresenting themselves as a trustworthy person or business through official electronic communications, like emails or instant messages. Thus, phishing constitutes a criminally fraudulent attempt to obtain sensitive information, including usernames, passwords, and credit card details. These communications, which claim to be from well-known social media platforms, auction sites, online payment processors, or IT administrators, are frequently used to entice unsuspecting individuals. Phishing is usually executed through email or instant messaging and often leads users to input their information on a counterfeit website that closely resembles the legitimate one.

2.1 Example: An SMS purporting to be from your bank states, "your account will be blocked. Click here to verify." The link directs you to a fraudulent page that steals your credentials. Case Study. In 2020, a counterfeit government website promising COVID relief requested users to provide their Aadhaar and bank information. This phishing scheme resulted in significant financial losses for thousands of citizens. The National Association of Software and Service Companies v. Ajay Sood. In 2025, the Indian judiciary system interpreted "phishing" in this case, where the plaintiff filed a suit seeking a permanent injunction to prevent the defendants or anyone acting on their behalf from disseminating fraudulent emails that falsely appear to originate from the plaintiff, using the trademark "NASSCOM" or any similar mark in connection with goods or services. Here, the defendant misappropriated the plaintiff's trademark and sent emails to customers, creating the illusion that the correspondence was from NASSCOM. The court ruled that, "Phishing" constitutes a type of internet fraud. In instances of "phishing," an individual impersonates a legitimate entity, such as a bank or insurance company, to obtain personal information from a user, including access codes and passwords, which are then exploited for personal gain, thereby misrepresenting the identity of the legitimate organization.
Generally, "Phishing" scams consist of individuals who impersonate online banking institutions and steal money from e-banking accounts by deceiving consumers into providing sensitive banking information. The various types of Phishing are as follows:

i. Spear Phishing: A focused assault directed at specific individuals or organizations, frequently utilizing personalized data.
ii. Smishing and Vishing: Phishing efforts executed through SMS (smishing) or phone calls (vishing).
iii. Clone Phishing: Cybercriminals produce a nearly exact copy of a genuine email to deceive users.
iv. Pharming: The act of diverting users from a legitimate site to a fraudulent one without their awareness.
v. Email Phishing: Deceptive emails or websites that imitate authentic sources (such as banks or government sites). This is the most prevalent form, where attackers distribute bulk emails that seem to originate from trustworthy entities.

3.0 The Provisions under the Information Technology Act 2000

Phishing is addressed under the Information Technology Act 2000 as follows:

1. Section 43 of the Information Technology Act outlines penalties for unauthorized downloading, damage, etc.: If an individual accesses, downloads, introduces, disrupts, denies, or assists others without the owner's consent, they may be liable for penalties under this section.
2. Section 66 of the Information Technology Act 2000 pertains to computer-related offenses. If a phisher compromises a victim's accounts and engages in any actions specified in Section 43, they may face imprisonment for a term of up to three years, a fine of up to five lakh rupees, or both.