iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** IV **Month of publication:** April 2024

DOI: https://doi.org/10.22214/ijraset.2024.61106

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue IV Apr 2024- Available at www.ijraset.com

Exploring Phishing Awareness and User Behavior: A Survey-based Investigation

Mahesh Kudalkar[1], Janhavi Singh[2], ShanuKumar Singh[3]
[1]*Assistant Professor,* [2,3]*UG-DS, Thakur College of science and commerce, Maharashtra, India*

Abstract: ***Phishing attacks remain a significant threat to internet users, exploiting vulnerabilities in human behaviour to deceive individuals into divulging sensitive information. Understanding user awareness of these attacks and their responses is crucial for developing an effective environment. This paper presents findings from a survey-based study aimed at assessing public awareness of phishing attacks and evaluating user responses. The survey explored participants' familiarity with phishing, knowledge levels, encounter frequencies, security practices, and responses to suspicious emails. Additionally, participants were queried about their experiences with phishing awareness training and their interest in receiving further education on the topic. The results provide insights into the current landscape of phishing awareness among internet users, highlighting areas of strength and vulnerability. These findings contribute to the ongoing efforts to enhance internet security and mitigate the risks posed by phishing attacks. The implications of the study's findings for cybersecurity education, awareness campaigns, and the development of anti-phishing tools are discussed.***

I. INTRODUCTION

In today's digital age, the internet has become an indispensable tool, permeating almost every aspect of our daily lives. From communication and commerce to entertainment and education, the internet empowers individuals worldwide with unprecedented access to information and opportunities. However, amid its vast benefits lies a darker underbelly of cyber threats, chief among them being phishing attacks.

Despite its myriad benefits, the internet also exposes users to various risks, including cybercrime and data breaches. Among these threats, phishing attacks represent a pervasive and insidious menace, exploiting human psychology and technological vulnerabilities to deceive unsuspecting individuals. Phishing attacks typically involve fraudulent emails, messages, or websites designed to trick users into disclosing sensitive information such as login credentials, financial details, or personal data.

The working of phishing attacks often relies on social engineering tactics, preying on human trust and curiosity to manipulate recipients into taking harmful actions. For instance, attackers may masquerade as legitimate entities, such as banks, government agencies, or reputable companies, and craft deceptive communications that mimic official correspondence. These emails or messages may contain urgent requests, enticing offers, or alarming warnings, designed to prompt recipients to divulge confidential information or unwittingly download malware.

The consequences of falling victim to phishing attacks can be severe, ranging from financial loss and identity theft to reputational damage and compromised cybersecurity. Moreover, phishing attacks pose significant challenges for individuals, businesses, and society at large, eroding trust in online communications, undermining cybersecurity measures, and perpetuating a cycle of cybercrime.

Despite the prevalence and risks of phishing attacks, public awareness and preparedness remain variable, with many individuals lacking the knowledge or resources to effectively recognize and mitigate these threats. Consequently, there is a pressing need to enhance education, awareness, and preventive measures to empower users in safeguarding against phishing attacks and preserving the integrity of online interactions.

This research paper aims to explore the landscape of phishing awareness among internet users, examine common behaviours and responses to phishing attempts, and evaluate the effectiveness of existing awareness initiatives and countermeasures. By shedding light on these issues, this study seeks to inform strategies for enhancing internet security, bolstering user resilience against phishing attacks, and fostering a safer online environment for all.

II. ORIGIN

The execution of this included a multifaceted approach, comprising writing survey, study plan, information collection, and investigation.

Drawing upon existing investigation and writing on phishing attacks, cybercrime, and web security, we synthesised bits of knowledge into the different measurements of phishing attacks, counting their verifiable advancement, predominant strategies, and advancing patterns. Also, we conducted a comprehensive overview to survey open mindfulness of phishing attacks, assess user behaviours and reactions, and recognize ranges for intercession and change.

Phishing attacks can be executed through a bunch of channels and procedures, each exploiting diverse vulnerabilities and mental triggers.

Phishing attacks originated in the early 1990s, emerging from the term "phreaking," which referred to hacking phone systems. The term "phishing" is a play on "fishing," reflecting the deceptive practice of luring victims by baiting them with fraudulent communications. Initially, phishing attacks targeted AOL users, exploiting their trust in unsolicited emails to steal login credentials. Over time, phishing evolved to include a variety of tactics, such as social engineering and malware distribution, targeting individuals, businesses, and organisations worldwide. The term has since become synonymous with online fraud and cybercrime, highlighting the persistent threat posed by deceptive tactics in the digital landscape.

Common strategies utilised by cybercriminals incorporate:

1) *Email Phishing*[5]*:* This strategy includes sending false emails disguised as authentic communications from trusted substances, such as banks, government offices, or trustworthy companies. These emails frequently contain misleading substance, such as pressing demands for individual data or luring offers, planned to draw beneficiaries into uncovering touchy information or clicking on noxious joins.
2) *Skewer Phishing*[(5)]*:* Skewer phishing targets particular people or organisations, fitting the substance of phishing emails to misuse individual data or organisational connections. By leveraging social building strategies and surveillance, cybercriminals make exceedingly personalised messages to extend the probability of victory.
3) *Phishing Websites*[(5)]*:* Cybercriminals make fake websites that mirror genuine platforms, such as managing account entrances, e-commerce sites, or social media platforms. These phishing websites are outlined to trick users into entering their login credentials or financial data, which is at that point collected by the attackers for evil purposes.
4) *Smishing and Vishing*[(5)]*:* Smishing (SMS phishing) and vishing (voice phishing) include utilising content messages or phone calls, separately, to misdirect people into disclosing delicate data or performing specific activities.

By looking at the major ways in which phishing attacks are executed, we aim to illustrate the complexity and seriousness of the risk scene and emphasise the significance of proactive measures and user education in combating cybercrime. Through observational investigation and investigation, this paper looks to contribute to the continuous efforts to improve internet security, raise awareness of phishing attacks, and empower users with the information and assets to ensure themselves in a progressively digitised world.

III. CURRENT STATUS

The current status of this research paper is educated by a comprehensive survey of past phishing attack occurrences, which serve as case ponders highlighting the differing strategies and repercussions of such cyber threats. Later a long time have seen an expansion of phishing focusing on people, businesses, and organisations over different divisions, underscoring the unavoidable and determined nature of this risk.

A few notable past phishing attack incidents:

1) *The Google Docs Phishing Scam (2017)*[(1)]*:* In April 2017, a broad phishing attack focused on Google users with a misleading mail invitation to collaborate on a Google Docs document. The e-mail showed genuine and incited clients to press on a connection, which coordinated them to a phishing site asking to get to their Google accounts. This advanced attack exploited the belief associated with Google's services and highlighted the vulnerability of email-based confirmation mechanisms.
2) *The WannaCry Ransomware Attack (2017)*[(2)]*:* Whereas not a traditional phishing attack, the WannaCry ransomware outbreak in May 2017 demonstrated the devastating impact of malicious programs engendered through phishing emails and vulnerable frameworks. WannaCry exploited a Windows vulnerability to infect thousands of computers around the world, encrypting records and demanding ransom payments in Bitcoin. The attack underscored the interconnecting of cybersecurity threats and the significance of timely software updates and security patches.
3) *The SolarWinds Supply Chain Attack (2020)*[(3)]*:* In December 2020, it was uncovered that the SolarWinds Orion software had been compromised in an advanced supply chain attack, influencing various government offices and enterprises around the world.

The attack included the addition of malicious code into program updates distributed by SolarWinds, allowing risk performing artists to penetrate targeted systems and exfiltrate delicate information. Whereas not a traditional phishing attack, this incident underscored the need for increased watchfulness and supply chain security measures.

4) *SlashNext State of Phishing Report for (2022)(4):* This indicates a significant rise in phishing attacks, with a 61% increase from the previous year, totaling over 255 million attacks. Traditional security solutions like email gateways and firewalls are becoming less effective against these attacks, especially as they are increasingly launched from trusted servers and through popular messaging apps. The report highlights a 50% surge in attacks on mobile devices, with scams and credential theft being the primary concerns. Notably, there's been an 80% increase in threats emanating from reputable services such as Microsoft and Google. The report suggests that 54% of all detected threats were zero-hour, indicating that attackers are rapidly adapting their tactics. It also states that 76% of threats were targeted spear-phishing attacks aimed at harvesting credentials. The healthcare, professional services, and IT sectors were the most targeted.

These past phishing attack episodes outline the advancing strategies and procedures utilised by cybercriminals to misuse vulnerabilities in innovation and human behaviour. Additionally, they emphasise the far-reaching results of cyber dangers, counting budgetary misfortune, reputational harm, and national security suggestions.

In light of these improvements, this term paper looks to supply an opportune and comprehensive investigation of phishing assaults, enveloping their beginnings, techniques, and effect on web security. By looking at past incidents and current patterns, this paper points to recognizing designs, vulnerabilities, and best homes for moderating the dangers posed by phishing attacks and defending against future threats.

As the investigation advances, continuous investigation of later phishing attack episodes and their suggestions will be joined to guarantee the significance and money of the discoveries. Through observational inquiry about and data-driven examination, this paper endeavours to contribute to the collective understanding of phishing attacks and educate procedures for upgrading web security and flexibility within the confrontation of advancing cyber dangers.

IV. FINDINGS AND ANALYSIS

This study gives important insights into the mindfulness, behaviours, and demeanors of web users with respect to phishing attacks. Information for this investigation was collected through a comprehensive online study conveyed to a differing test of members. The overview enveloped different statistical bunches and web usage patterns, with questions covering a wide extent of topics related to phishing mindfulness, encounters, and preventive measures. Members were questioned about their nature with phishing, information levels, experience frequencies of suspicious emails,activities taken when getting suspicious emails, and intrigued in phishing mindfulness preparation. Moreover, respondents were inquired about their utilisation of anti-phishing devices, encounters with phishing mindfulness preparing in a working environment or instructive settings, and nature with common phishing strategies. The study got an overpowering reaction, with an add up of 1028 members giving important experiences into the predominance and discernments of phishing attacks among web clients. Through thorough investigation of the collected information, this considers points to explain key patterns, designs, and relationships to advise techniques for improving web security and relieving the dangers posed by phishing attacks.

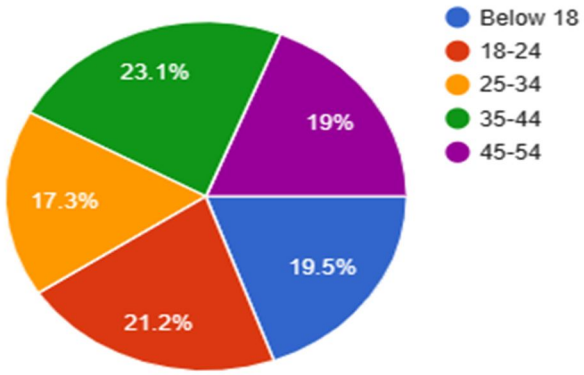


Figure -1: Victims over age group

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue IV Apr 2024- Available at www.ijraset.com

It outlines the distribution of phishing attack casualties over diverse age bunches. Among the age categories overviewed, people aged 45-54 speak to the most elevated extent of casualties at 23.1%, followed closely by those aged 25-34 at 21.2%. Members aged 18-24 and 35-44 contain 19.5% and 17.3% of casualties, separately. This chart highlights a striking variety in victimisation rates over age socioeconomics, with middle-aged people showing the next vulnerability to phishing attacks. Understanding these age-specific patterns is pivotal for fitting focused on mindfulness and anticipation techniques to relieve the effect of phishing attacks on diverse age groups.

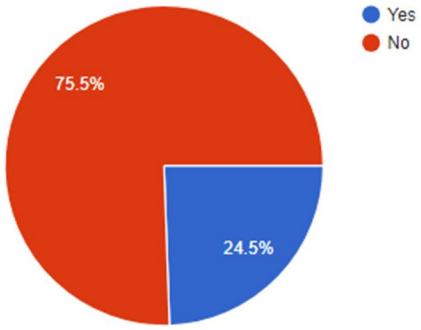


Figure-2: People who received hacking awareness at workplace

It outlines the proportion of respondents who got hacking awareness training at their work environment. The information uncovers that a larger part of members, accounting for 75.6%, did not get any frame of hacking awareness preparing in their working environment. On the other hand, 25.5% of respondents detailed accepting such preparation. This chart underscores a concerning gap in cybersecurity instruction inside organisational settings, with a significant portion of workers missing the essential information and abilities to recognize and relieve hacking dangers. Addressing this difference through comprehensive preparing programs is basic for supporting organisational strength against cyber dangers and shielding delicate information and resources.

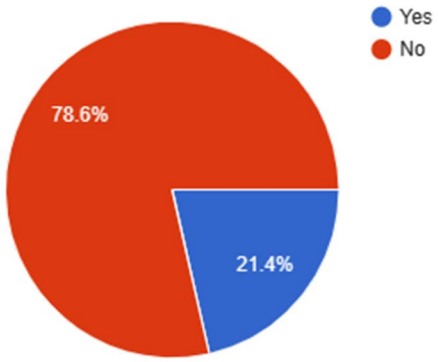


Figure-3: People who report to IT authorities

This chart portrays the rate of respondents who report phishing endeavours to IT specialists inside their organisations. The information shows that a lion's share of members, comprising 78.6%, don't report phishing endeavours to IT specialists. Then again, 21.4% of respondents detailed that they do advise IT specialists about such occurrences. This chart underscores a notable inconsistency within the detailing of phishing assaults inside organisational settings, with a noteworthy parcel of representatives electing not to raise potential dangers to IT divisions. Upgrading awareness and empowering proactive announcing components can reinforce organisational guards and encourage reactions to phishing occurrences, in this manner moderating potential dangers and minimising the effect of cyber threats.

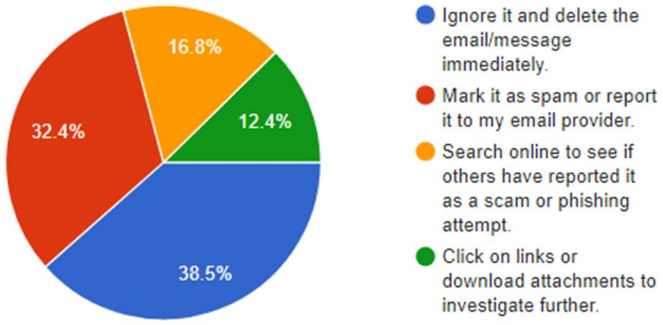


Figure-4: People's action on suspicious email or messages

It presents the actions taken by respondents upon receiving suspicious emails or messages. The data reveals that the majority of participants, accounting for 38.5%, opt to ignore and delete the email or message immediately. Additionally, 32.4% of respondents choose to mark such communications as spam or report them to their email provider. A smaller proportion, comprising 16.8%, indicates that they search online to ascertain if others have reported the email as a scam or phishing attempt. Furthermore, 12.4% of participants admit to clicking on links or downloading attachments to investigate further. This graph underscores the diverse responses to suspicious communications and highlights the importance of fostering informed decision-making and proactive cybersecurity practices among internet users.

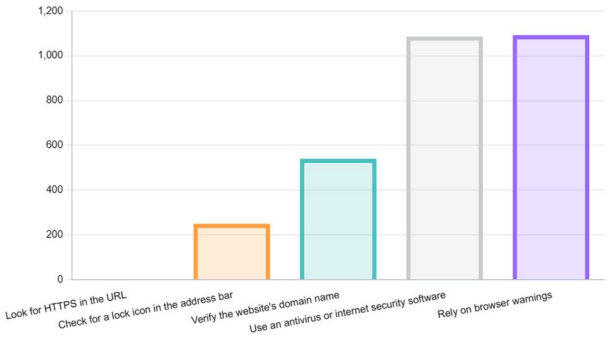


Figure-5: Methods people follow for web safety

Figure illustrates the methods employed by respondents to ensure web safety while browsing. Interestingly, 0% of participants reported looking for "HTTPS" in the URL as a safety measure. Instead, 22.8% indicated that they check for a lock icon in the address bar, while nearly half of the respondents (49.5%) stated that they verify the website's domain name. Moreover, an overwhelming majority, comprising 99.5% of participants, reported using antivirus or internet security software to enhance web safety. Notably, all respondents rely on browser warnings as a key strategy for identifying potentially unsafe websites. This graph underscores the reliance on a combination of visual cues and security tools to mitigate the risks associated with browsing the internet and underscores the importance of browser-based security features in maintaining online safety.

V. CONCLUSION

In conclusion, this research paper has provided valuable insights into the awareness, behaviours, and attitudes of internet users regarding phishing attacks and internet security. Through a comprehensive survey analysis, we have identified key trends, patterns, and areas for improvement in combating the pervasive threat of phishing attacks.

Our findings reveal a concerning gap in phishing awareness and preventive measures, with a significant proportion of respondents lacking familiarity with phishing tactics and exhibiting suboptimal cybersecurity practices.

Despite the prevalence of phishing attacks and the potential risks they pose, a considerable number of individuals do not receive hacking awareness training in their workplaces and fail to report phishing attempts to IT authorities.

Moreover, our analysis highlights the diversity of responses to suspicious emails or messages, with varied levels of caution and proactive measures taken by respondents. While some users adopt precautionary actions such as marking emails as spam or relying on browser warnings, others exhibit riskier behaviours, such as clicking on suspicious links or downloading attachments without verification.

Furthermore, our research underscores the importance of education, awareness, and proactive measures in mitigating the risks posed by phishing attacks. By enhancing phishing awareness training programs in workplaces and educational institutions and promoting proactive reporting mechanisms, organisations can bolster their defences against cyber threats and empower users to identify and mitigate phishing attempts effectively.

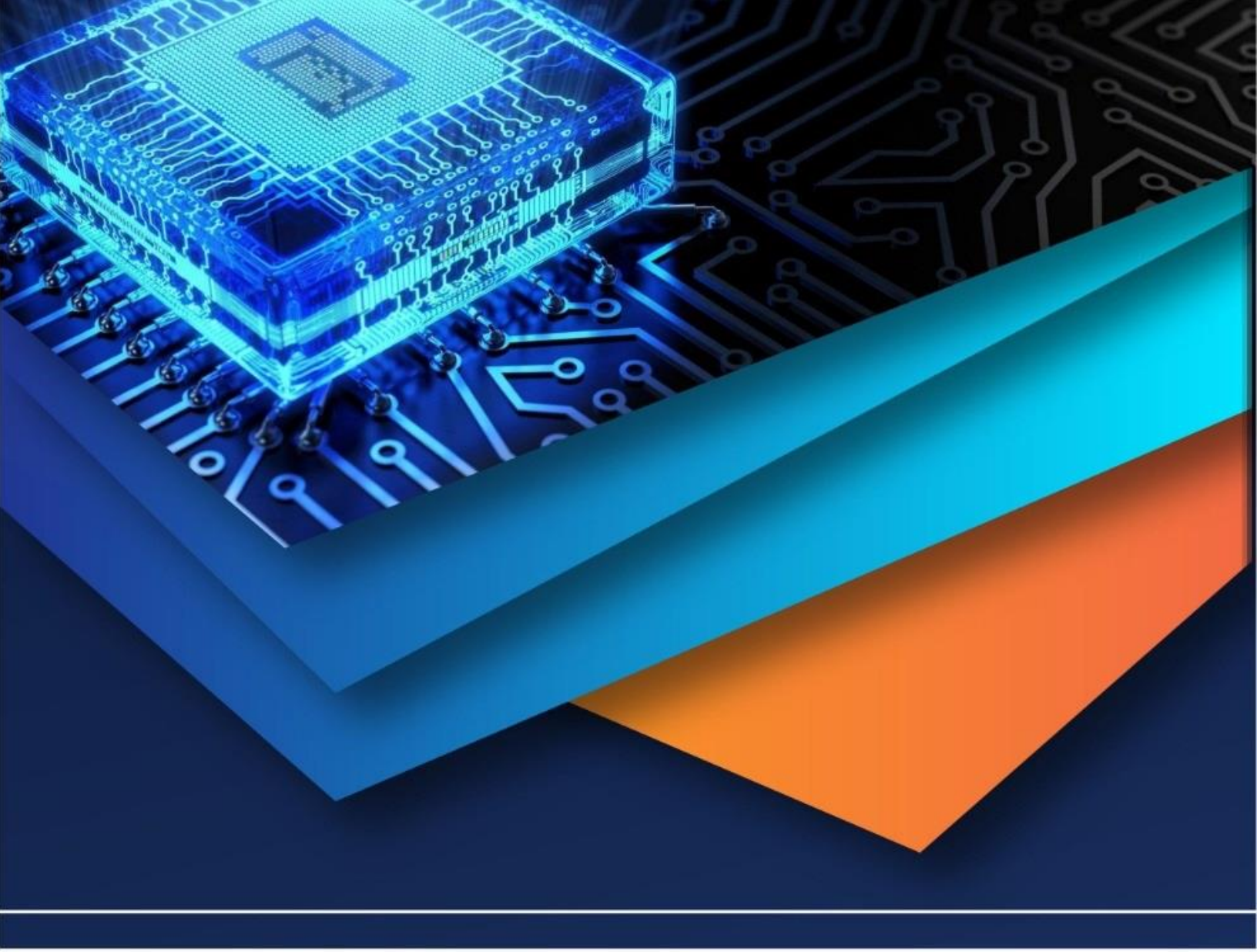
Additionally, our findings emphasise the critical role of technological safeguards, such as antivirus software and browser warnings, in enhancing web safety and protecting against malicious activities online. By leveraging a combination of user education, awareness campaigns, and technological solutions, stakeholders can collectively work towards creating a safer and more secure online environment for all.

VI. RECOMMENDATIONS

1) Be cautious of unexpected emails or messages requesting personal information – verify the sender's identity before responding.
2) Avoid clicking on suspicious links or downloading attachments from unknown sources to prevent malware infections.
3) Double-check website URLs for accuracy and look for HTTPS encryption to ensure secure browsing.
4) Enable two-factor authentication for added security when accessing online accounts.
5) Keep software and security applications up-to-date to protect against known vulnerabilities.
6) Educate yourself about common phishing tactics and stay informed about emerging threats to enhance your awareness.
7) Trust your instincts – if something seems too good to be true or feels suspicious, it's best to err on the side of caution.
8) Integrate interactive phishing response tools into email clients or organisational intranets, allowing users to report suspicious emails with a single click.
9) Foster collaboration and information sharing among organisations, industries, and cybersecurity communities to exchange real-time phishing threat intelligence.
10) Assess the security practices of third-party vendors and partners who have access to your systems or data to ensure they meet your security standards.
11) When accessing the internet, especially on public Wi-Fi networks, use a VPN to encrypt your connection and protect your data from potential eavesdropping.
12) Be cautious about sharing personal information on social media and regularly review privacy settings.
13) Refrain from using public charging stations or USB ports to prevent potential malware installation.
14) Promote cybersecurity awareness, training, and recognition within your organisation.

REFERENCES

[1] Jakobsson, M., & Myers, S. (2007). “Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft”. Wiley-Interscience
[2] https://www.theguardian.com/technology/2017/may/03/google-docs-phishing-attack-malware
[3] https://en.wikipedia.org/wiki/WannaCry_ransomware_attack
[4] Akerlof, G. A., & Shiller, R. J. (2015). “Phishing for Phools: The Economics of Manipulation and Deception”. Princeton University Press.
[5] https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know
[6] https://www.securitymagazine.com/articles/98536-over-255m-phishing-attacks-in-2022-so-far
[7] https://www.fortinet.com/resources/cyberglossary/types-of-phishing-attacks
[8] James, L. (2006). “Phishing Exposed: An In-depth Examination of Phishing Techniques”. Syngress.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY