e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:05/May-2024 Impact Factor- 7.868 www.irjmets.com

EVOLUTION OF ONLINE SCAMS

Deepesh Baid*1, Dr. Febin Prakash*2

*1MCA Department School of Computer Science and IT, Jain (Deemed to be University), Banglore-560069, India.

*2Professor MCA Department School of Computer Science and IT, Jain (Deemed to be University), Banglore-560069, India.

DOI : https://www.doi.org/10.56726/IRJMETS58476

ABSTRACT

A new age of online frauds has been brought about by the development of the internet and digital technologies, which pose serious risks to people, companies, and society at large. This study investigates the development of internet frauds, following their beginnings and analyzing how sophisticated and widespread they have become in today's digital environment. It explores the range of strategies used by cybercriminals to take advantage of weaknesses and trick gullible people, including phishing, virus distribution, identity theft, and social engineering techniques. The study delves deeper into the factors that contribute to the spread of online scams, such as the anonymity that the internet provides, the worldwide reach of frauds, and the financial rewards that scammers receive. It looks at the social and psychological elements that help these frauds succeed by taking advantage of human weaknesses including trust, greed, and fear. Additionally, the study examines how internet scams change over time, examining how they adjust to new developments in technology, new laws, and greater public awareness. It draws attention to new developments like deepfakes, the use of artificial intelligence, and the abuse of new platforms and technology. Lastly, the study offers suggestions for successful countermeasures and promotes a multi-stakeholder strategy including law enforcement, IT firms, and public education campaigns. In order to tackle the ever-evolving menace of online frauds, it highlights the significance of proactive methods, such as cybersecurity measures, legislative frameworks, and international collaboration.

Keywords: Online scams, Tech support scams, Online Frauds, Ransomware attacks, Phishing.

I. INTRODUCTION

The internet has completely changed the way we interact, transact business, and obtain information while providing hitherto unseen benefits. Online scams are a new type of criminal activity that have emerged as a result of this digital world. These dishonest methods have spread quickly, taking advantage of the internet's inherent anonymity, worldwide access, and technological flaws. Online scams were very simple in the early days of the internet, mostly depending on email-based phishing operations and crude social engineering techniques. Cybercriminals, however, modified their tactics as technology developed and internet usage expanded, creating ever intricate and dishonest plans to attack people, companies, and even governmental organizations. These days, identity theft, money fraud, virus dissemination, and data breaches are just a few of the many actions that fall under the umbrella of internet scams. Sophisticated tactics like spear phishing, ransomware, and advanced persistent threats (APTs) are frequently used by these scammers to penetrate targets' networks and get private data or demand money. The widespread prevalence of online scams may be ascribed to several causes, such as the worldwide reach of the internet, the anonymity it affords, and the substantial cash rewards available to those who engage in them. Furthermore, as digital technologies become more widely used and people depend more on online services, new attack routes and vulnerabilities are being generated, which cybercriminals are happy to take advantage of. As online scams continue to evolve, they pose significant threats to individuals, businesses, and national security. [8]

These harmful behaviors have several implications, including financial losses, data breaches, and a decline in public faith in digital systems. A multidisciplinary strategy incorporating law enforcement, cybersecurity experts, legislators, and public awareness campaigns is needed to address this situation. The purpose of this research paper is to present a thorough examination of the development of internet scams, looking at their causes, methods, strategies, and social effects. We may create strong tactics and efficient countermeasures to deal with this ubiquitous menace in the digital era by comprehending the characteristics and dynamics of these frauds.[1].

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:05/May-2024 Impact Factor- 7.868 www.irjmets.com

II. EVOLUTION OF ONLINE SCAMS

Online scams have been well researched and reported, providing insight into the changing strategies used by cybercriminals as well as their effects on people, companies, and society as a whole. This examination of the literature looks at how internet scams have changed over time, comparing and contrasting the techniques and patterns seen in the years between 2018 and 2020 with the state of the industry in 2023 and 2024.

From 2018 to 2020, the main emphasis of internet scams was taking use of tried-and-true methods like virus distribution and phishing. The Anti-Phishing Working Group (APWG) reported that in 2019 there were 65% more phishing assaults than the year before (APWG, 2020). With the intention of stealing login credentials, these assaults frequently targeted social networking, e-commerce, and financial organizations. [3]

During this time, exploit kits, hacked websites, and email attachments were the main ways that malware was distributed (Symantec, 2019). According to Bert (2017), ransomware is a kind of virus that encrypts files and demands money in exchange for a key. Notoriety has increased due to assaults like WannaCry and Not Petya, which have caused extensive disruption and monetary losses.

The frequency of impersonation schemes, in which hackers impersonate as government institutions, tech support firms, or romantic interests to swindle victims, was highlighted by research undertaken by the Federal Trade Commission (FTC) in 2019 (FTC, 2020). These frauds frequently used social engineering techniques including instilling a feeling of urgency and preying on trust. The environment of online frauds has changed significantly in 2023 and 2024 due to the advent of new threats and a shift in strategies. As per research published by Cisco in 2023, hackers are progressively utilizing cutting-edge technology, such deepfakes and artificial intelligence (AI), to augment the complexity of their assaults.

In impersonation frauds, hackers have begun exploiting deepfakes—the artificial intelligence-driven alteration of audio and video content—to create incredibly lifelike fake recordings or movies that fool victims (Chesney & Citron, 2022). This method has proven especially useful in business email compromise (BEC) schemes, in which thieves pose as CEOs or other high-ranking authorities in order to start financial transactions under false pretences. The spread of messaging apps and social media has also given rise to new online fraud attack avenues. According to University of Cambridge research from 2023, romance scams are becoming more common on social media and dating apps. Cybercriminals fabricate accounts in these situations in order to build emotional ties with their victims and ultimately rob them.[7]

Furthermore, the COVID-19 epidemic has created an ideal environment for internet frauds, as hackers take advantage of people's worries and anxieties around the health emergency. The World Health Organization (WHO, 2023) reported an increase in fraudulent schemes involving COVID-19 relief funding, phishing attempts, and phony internet storefronts offering false medical supplies. It is anticipated that as technology develops, internet frauds will get increasingly complex and challenging to identify. MIT researchers (2024) have issued a warning about the possible abuse of cutting-edge technology by hackers to avoid detection and enable illegal activity, including blockchain and quantum computing. A multi-stakeholder strategy including law enforcement agencies, technological corporations, academics, and public awareness campaigns is essential to combating the constantly changing danger posed by internet frauds. Staying ahead of the curve and shielding people and organizations from the malicious actions of cybercriminals requires ongoing study, the creation of sophisticated detection and prevention measures, and international collaboration.[4]

III. TYPE SQUATTING DOMAINS

Typo squatting is one of the social engineering attacks where owners of certain domains purposefully spelled them wrongly. Hackers and even sophisticated groups such as those backed by some states are developing typo squatting domains from frequently visited sites for jobs. These domains appear almost similar to the legitimate websites but they contain small differences such as use of wrong spelling or wrong domain extension. The goal of these domains is to make the target individuals believe they are applying for a specific employment through a genuine website, while actually sharing their personal data with the criminals. We have also observed that there is a growing trend of registration of new typo-squatted domains especially those related to job or employment search such as LinkedIn, indeed among others.[2]

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:05/May-2024 Impact Factor- 7.868 www.irjmets.com

IV. MEASURES TO AVOID ONLINE SCAMS

Verify the source: In case one is curious to follow a link or provide some personal information, ensure that the link and the website or the link-source is reliable. Look for official websites with secure URLs and telephone numbers This means that the survey was carried out on a few respondents and those who responded did not provide their e-mail addresses.[6]

Be cautious with emails: Nowadays, you should never reply to e-mails from unfamiliar senders, especially those, which require to reveal personal information including your monetary affluence. The typical online phishing scam is an email alert that says it is urgent, has grammatical mistakes, sends from an unrecognized address. Successful avoidance of spam requires you to use email filters. Use strong, unique passwords: Choose unique passwords for all your social networking accounts and avoid recycling previous passwords. For example, you may need to create and remember complicated passwords in this case, you may consider using the special characters.

[4] Update security software: Utilize the antivirus and anti-malware programs are installed and up to date to prevent latest infected programs. Keep your O/S and browsers and applications up to date because there is always a new version with security fixes coming out. Educate yourself: It is important to read about the most frequently used scams and fraud schemes and stay constantly updated for any change in them. Studying the current scams and understanding how to differentiate between them is one informative activity. On its part, government website, social media and consumer protection agencies offer some of the most comprehensive information about commonly encountered scams.[5]

V. CONCLUSION

Due to hackers' ongoing adaptation of strategies to take advantage of new technology and human weaknesses, online frauds have developed quickly. The threat environment is always changing, ranging from straightforward phishing emails to intricate deepfakes and AI-powered assaults. A multi-stakeholder strategy comprising law enforcement, internet firms, researchers, and public awareness campaigns is needed to combat these frauds. It takes constant watchfulness, flexibility, and cross-border cooperation to keep one step ahead of cybercriminals and safeguard people and companies. In order to combat the ongoing threat of online frauds in the digital era, pre-emptive tactics, strong cybersecurity measures, and public education on digital safety will be essential as technology develops. We can protect the integrity and trust that underpin our online interactions and lessen the dangers presented by these constantly changing cyber threats by working together to create resilience.

VI. REFERENCES

[1] Tuli, K., & Juneja, N. (2015). Evolution of identity thefts and online frauds on internet. International Journal of Advanced Research in Engineering and Applied Sciences, 4(10), 10-21
[2] Tuli, K., & Juneja, N. (2015). Evolution of identity thefts and online frauds on internet. International Journal of Advanced Research in Engineering and Applied Sciences, 4(10), 10-21
[3] Nagpal, R. (2008). Evolution of cyber Crimes. Asian School of Cyber laws, 2Tambe Ebot, A. C., Siponen, M., & Topalli, V. (2023). Towards a cybercontextual transmission model for online scamming. European Journal of Information Systems, 1-26
[4] Berzins, M. (2010). Online scams: case studies from Australia. In Handbook of Research on Social Interaction Technologies and Collaboration Software: Concepts and Trends (pp. 561-573). IGI Global
[5] Malav, D., & Chawla, S. (2022). ONLINE SCAMS–A CRISIS IN ONLINE WORLD
[6] Ansari, S. (2020). From the Scammer Perspective: Predispositions Towards Online Fraud Motivation and Rationalization (Doctoral dissertation, Purdue University)
[7] Chen, H., Beaudoin, C. E., & Hong, T. (2017). Securing online privacy: An empirical test on Internet scam victimization, online privacy concerns, and privacy protection behaviors. Computers in human behavior, 70, 291-302