# Pandemic Exploitation: Systemizing Social Engineering-Based Cyber Threats During the COVID-19 Pandemic

Anik Chowdhury
ID - 40275019

Pushpeswaree Degamber
ID - 40296526

***Abstract*—Recent global crises, such as the COVID-19 pandemic, have presented unique opportunities for cybercriminals to exploit vulnerabilities through social engineering tactics. This paper systematizes knowledge on the nature and evolution of social engineering-based cyber threats during the pandemic, focusing on common attack vectors, targeted sectors, and the socio-economic impacts of these attacks. Our findings show a significant increase in phishing, vishing, and ransomware attacks, with healthcare, government, and financial sectors being the most affected. The paper highlights the critical need for robust cybersecurity frameworks, international collaboration, and public awareness to mitigate these threats in future crises. We conclude with recommendations for improving defenses against evolving social engineering tactics.**

## I. Introduction

Pandemics have historically occurred three to four times per century, though their timing is unpredictable [1]. These crises create opportunities for cybercriminals to exploit vulnerabilities through social engineering by using fear, urgency, and false information to carry out targeted attacks. During the COVID-19 pandemic, there was a sharp rise in phishing scams, fake health updates, and fraudulent financial aid schemes, as criminals took advantage of the global shift to remote work and online communication. The FBI's Internet Crime Complaint Center (IC3) received 791,790 reports of suspected internet crimes in 2020, representing a 69% increase from 2019 [2]. This paper seeks to organize and analyze existing knowledge on social engineering threats during the pandemic, addressing gaps and offering insights to improve defenses against such attacks in the future.

This paper is structured as follows: The introduction outlines the motivation, and objectives of the study. The methodology section details the approach employed in this Systematization of Knowledge (SoK) project to evaluate the existing body of research. The literature review provides a comprehensive overview of prior studies in the field. The analysis section presents key findings, highlights limitations, and discusses their implications. Finally, the paper concludes with a summary of the findings and recommendations for future research directions.

## II. Methodology

### A. Research Questions

The COVID-19 pandemic has posed significant cybersecurity challenges, marked by a surge in social engineering-based attacks. However, limited understanding exists regarding how these threats evolved and their broader impacts. This study aims to address these gaps by answering key questions to systematize knowledge in this area.

- What were the most common social engineering tactics used during the COVID-19 pandemic?
- What specific methods did attackers use to exploit fear and urgency during the pandemic, and which vectors were most frequently used?
- Which sectors were most appealing to cyber attackers during the COVID-19 pandemic?
- What were the socio-economic impacts of pandemic-themed social engineering attacks?

### B. Search Strategy

The search string was constructed by identifying keywords and their corresponding alternatives from social engineering research. These keywords and alternatives were then combined using the Boolean operators "AND" and "OR" to formulate the search string.

### C. Inclusion & Exclusion Criteria

The study must be published in a reputable journal, address at least two of the identified research questions, and have a significant number of citations unless it is a relatively recent publication. Studies will be excluded if they are not published by a reputable publisher, have a low number of citations, do not address the identified research questions, or are not journal articles or conference papers.

## III. Literature Review

The COVID-19 pandemic has significantly reshaped the global cybersecurity landscape, with cybercriminals exploiting the unprecedented reliance on digital platforms. Multiple studies have observed a surge in COVID-19-themed cyberattacks, ranging from phishing campaigns and ransomware to cryptocurrency scams and insider threats. Phishing attacks witnessed a staggering increase during the pandemic, with a 667% spike reported as attackers leveraged pandemic-related themes

to deceive users, often impersonating trusted organizations such as the World Health Organization (WHO) to gain access to sensitive information ( [3], [4])). Similarly, cryptocurrency scams, including fake donation campaigns and fraudulent tokens, collectively caused significant financial losses, with Xia et al. (2020) identifying 195 scams that led to $330,000 in reported damages ( [5]).

Social engineering emerged as a prominent tactic, capitalizing on human vulnerabilities such as fear and urgency. Cybercriminals exploited these emotions to manipulate individuals into clicking on malicious links, sharing sensitive data, or downloading harmful software ( [6], [7]). Alzahrani (2020) highlighted the widespread use of phishing, vishing, and smishing techniques, where attackers tailored their schemes to mimic trusted entities or offer critical pandemic-related information ( [6]). Furthermore, attackers employed impersonation and fake urgency in their messages to amplify the success rate of their campaigns, as demonstrated in a study that analyzed scam patterns and emotional triggers used during the pandemic ( [4]).

The transition to remote work exacerbated cybersecurity risks by introducing new vulnerabilities. The shift necessitated rapid adoption of digital tools, often without adequate security measures. Employees working from home on personal devices or unsecured networks created fertile ground for attackers to exploit ( [8], [9]). Insider threats also increased, with employees' negligence or malicious intent leading to data breaches and security lapses ( [10], [7]). Video conferencing platforms, essential for maintaining business operations, became frequent targets, with "Zoombombing" and unauthorized meeting access highlighting the risks of inadequate platform security ( [10]).

Healthcare systems, as critical infrastructure during the pandemic, faced targeted ransomware attacks that disrupted operations and endangered lives. Attackers capitalized on the essential nature of healthcare services, often demanding exorbitant ransoms to restore access to compromised systems ( [11], [5]). Wiggen (2020) noted that the healthcare sector's dependence on technology made it particularly vulnerable, further emphasizing the need for robust cybersecurity measures ( [11]).

The pandemic also highlighted broader challenges related to cybersecurity policy and resilience. Insights from Gaurav (2022), emphasize the role of international collaboration in combating cyber threats, noting that the rapid proliferation of attacks overwhelmed national frameworks. The study stressed the importance of developing standardized global policies to ensure coordinated responses to large-scale crises like COVID-19 ( [15]). Similarly, Cvitic (2023) explored the evolving nature of cyber threats, focusing on the intersection of misinformation and cybercrime. Attackers leveraged false information to manipulate public perception, which in turn increased susceptibility to phishing campaigns and social engineering ( [17]).

Another significant perspective is provided in Cvitic (2023), which investigates the psychological impacts of sustained cyberattacks on individuals and organizations during the pandemic. The findings suggest that prolonged exposure to these threats not only caused financial damage but also led to stress and decision-making fatigue among victims. The study proposed integrating psychological resilience training into cybersecurity awareness programs as a means to combat these effects ( [17]).

Mitigation strategies discussed in the literature emphasize the importance of proactive and multi-layered approaches to cybersecurity. Okereafor and Adelaiye (2020) proposed the Randomized Cyberattack Simulation Model (RCSM), which provides organizations with a framework to anticipate and mitigate emerging threats through simulation and proactive defense mechanisms ( [9]). Other recommendations included implementing multi-factor authentication, endpoint security solutions, and continuous monitoring of networks ( [7], [12]). Education and awareness programs were identified as critical for empowering individuals and organizations to recognize and respond to social engineering tactics effectively ( [6], [13]).

The pandemic underscored the critical role of cybersecurity resilience in maintaining operational continuity during global crises. The reviewed studies consistently highlighted the importance of integrating technical defenses with behavioral interventions to mitigate evolving cyber threats. These findings provide a foundation for strengthening cybersecurity practices and preparing for future challenges, ensuring that organizations remain adaptable and resilient ( [14], [8]).

## IV. Analysis

***RQ1:*** *What were the most common social engineering tactics used during the COVID-19 pandemic?*

The papers provide a detailed account of various social engineering tactics employed during the COVID-19 pandemic, highlighting how cybercriminals exploited the crisis to target individuals and organizations. Below are their frequency of use across the reviewed documents:

TABLE I
Overview of the Techniques

| Tactics Name | Mentioned Paper |
|---|---|
| Phishing | [4], [6], [3] |
| Vishing and Smishing | [6] |
| Impersonation | [4], [5] |
| Fake Websites | [4], [5] |
| Fear and Urgency Appeals | [6], [7] |
| Fake Donations and Crowdfunding Scams | [5] |
| Fake news and Misinformation | [4], [13] |
| Ransomware and Malware | [4] |
| Business Email Compromise | [7], [10] |

Most Common Tactic: Phishing emerged as the most prevalent tactic across the reviewed papers. It accounted for a significant proportion of reported incidents due to its adaptability and ease of execution. Phishing attacks were particularly successful during the pandemic because they exploited individu-

als' heightened anxiety and reliance on email communications for critical updates.

***RQ2:*** *What specific methods did attackers use to exploit fear and urgency during the pandemic, and which vectors were most frequently used?*

During the COVID-19 pandemic, attackers capitalized on fear and urgency to launch social engineering attacks, exploiting the heightened reliance on digital communication. A prevalent tactic involved impersonating trusted organizations like the World Health Organization (WHO) or government agencies. Phishing emails, often with subject lines such as "Claim Your Financial Aid Now" or "Urgent COVID-19 Update," created a sense of panic or urgency, prompting victims to click on malicious links or download harmful attachments. These emails targeted sensitive information such as login credentials or financial details and often deployed malware or ransomware on victims' devices. Fake websites, mimicking official COVID-19 tracking dashboards or donation pages, further expanded the attackers' arsenal, tricking users into sharing personal data or downloading malicious software ( [6], [4], [5]).

Attackers also utilized SMS phishing (smishing) and voice phishing (vishing), sending fraudulent messages or making calls that urged immediate action. Examples included fake vaccination appointments or account verification requests. Scareware campaigns were another common approach, where attackers warned of dire consequences, such as health risks or financial penalties, if victims failed to comply with instructions. Social media platforms were leveraged to spread misinformation and malicious links, often disguised as trending COVID-19 topics. These tactics took advantage of public anxiety, amplifying their effectiveness during a time of widespread uncertainty ( [4], [7], [5]).

Phishing emails remained the most frequently used vector due to their broad reach and ability to mimic legitimate organizations effectively. However, smishing, fake websites, and scareware also played significant roles, enabling attackers to exploit victims' emotional vulnerabilities and compel quick, uncritical responses. The success of these methods highlights the critical need for public awareness, robust cybersecurity frameworks, and proactive defense mechanisms to mitigate the impact of manipulative strategies. The pandemic underscored the importance of vigilance and preparedness in addressing evolving social engineering threats ( [6], [4], [3]).

***RQ3:*** *Which sectors were most appealing to cyber attackers during the COVID-19 pandemic?*

Several sectors became key targets for cyber attackers during the COVID-19 pandemic due to their vital roles and underlying vulnerabilities, as outlined below.

- ***Healthcare:*** The healthcare sector was the most frequently targeted, as it played a critical role during the pandemic. Attackers exploited the urgency and chaos in healthcare systems by launching ransomware attacks on hospitals, clinics, and research organizations. These attacks disrupted essential services and endangered lives, with attackers often demanding exorbitant ransoms to restore systems. Wiggen (2020) highlighted that healthcare organizations' reliance on technology and their urgency to access patient data made them particularly vulnerable ( [11], [4]).
- ***Government and Public Sector:*** Government agencies managing COVID-19 response and relief programs were also heavily targeted. Attackers impersonated government entities in phishing campaigns to steal sensitive information, disrupt operations, or defraud citizens through fake relief schemes. Fraudulent emails and websites claiming to provide stimulus checks or unemployment benefits were common tactics used against this sector ( [6], [3]).
- ***Financial Sector:*** The financial sector was another key target due to the pandemic's economic impact. Cybercriminals exploited financial anxieties by launching phishing and vishing attacks aimed at accessing bank accounts and financial credentials. Additionally, cryptocurrency scams, including fake token sales and fraudulent donation campaigns, caused significant financial losses ( [5], [12]).
- ***Education:*** The education sector, which rapidly transitioned to remote learning, became a target for cyberattacks, including ransomware and phishing. Attackers disrupted online learning platforms, stole sensitive data, and exploited vulnerabilities in poorly secured video conferencing tools ( [10], [7]).
- ***Private Businesses and Remote Work:*** Businesses across sectors experienced increased threats due to the shift to remote work. Attackers targeted employees working from home, often exploiting unsecured devices and networks. Business Email Compromise (BEC) attacks and malware distribution through fake COVID-19 updates were commonly observed ( [8], [9]).

***RQ4:*** *What were the socio-economic impacts of pandemic-themed social engineering attacks?*

Pandemic-themed social engineering attacks had significant socio-economic impacts. Financially, they caused substantial losses through phishing, ransomware, and fraud, disrupted operations in critical sectors like healthcare and education, and increased cybersecurity costs for organizations ( [11], [5], [9]).

Socially, these attacks eroded public trust in institutions, caused stress and anxiety among victims, and disproportionately targeted vulnerable groups, such as the elderly and economically disadvantaged populations [ [4], [6]].

Broader impacts included strain on critical sectors like healthcare, widening socio-economic inequalities, and disruptions to global supply chains. These effects highlight the need for enhanced cybersecurity awareness and proactive measures to address such threats ( [11], [12], [5]).

### *A. Limitations*

The papers collectively provide valuable insights into the socio-technical landscape of pandemic-themed cyberattacks;

TABLE II
A SNAPSHOT OF THE MOST COMMON OCCURRENCES

| **Tactics** | Phishing |
|---|---|
| **Attack vector** | Email |
| **Vulnerable Sector** | Healthcare |

however, several limitations emerge across the studies:

- **Lack of Real-Time Data:** Many studies relied on data collected early in the pandemic or used historical incidents to model trends. This temporal gap limits the ability to assess ongoing and emerging threats accurately, especially as attackers continually adapted their methods ( [8], [9]).
- **Focus on Specific Sectors:** While some papers provided a broad analysis, others focused narrowly on specific sectors such as healthcare or government. This sectoral focus neglects insights into industries like retail, logistics, and non-critical infrastructure, which were also impacted ( [11], [4]).
- **Quantitative Over Qualitative Analysis:** Several papers emphasized quantitative statistics, such as the number of phishing attacks or financial losses, but offered limited qualitative insights into the psychological or social impacts of these cybercrimes on individuals and organizations ( [6], [7]).
- **Geographic Bias:** A significant portion of the research focused on specific regions, such as North America or Europe, with less attention to cybersecurity challenges faced by developing nations. This creates an incomplete picture of the global impacts ( [12], [10]).
- **Generalization of Attack Techniques:** Some papers generalized social engineering tactics without delving into nuanced differences in how attackers targeted various demographics or technological environments ( [4], [3]).
- **Insufficient Focus on Long-Term Impacts:** Few papers addressed the long-term consequences of pandemic-themed attacks, such as their influence on future cybersecurity policies or the evolution of social engineering techniques ( [11], [13]). Although many papers proposed mitigation measures, few offered actionable frameworks for organizations to adopt. Most recommendations were high-level and lacked details on practical implementation ( [9], [5]).
- **Insufficient Focus on Long-Term Impacts:** Few papers addressed the long-term consequences of pandemic-themed attacks, such as their influence on future cybersecurity policies or the evolution of social engineering techniques ( [11], [13]).

## V. CONCLUSION

The unprecedented global disruption brought on by COVID-19 revealed the severity of social engineering-based cyber threats, as attackers leveraged widespread fear, anxiety, and the rapid digital transformation. Phishing, vishing, impersonation, and ransomware attacks became widespread, severely impacting healthcare, government, and financial sectors. The socio-economic impact of these threats underscores the need for comprehensive cybersecurity strategies that combine technical, educational, and psychological measures. Future preparedness must focus on improving public awareness, promoting multi-layered defense systems, and fostering international cooperation to counteract large-scale social engineering attacks. Addressing the gaps identified in this paper, such as real-time threat monitoring, broader sectoral analysis, and long-term mitigation strategies, is essential to build resilient and adaptable cybersecurity defenses in the face of future global challenges.

## REFERENCES


[1] Canada, P. H. A. of. (2024, May 7). Government of Canada. Canada.ca. https://www.canada.ca/en/public-health/services/diseases/pandemic-flu/health-professionals.html [Last access: Nov 6, 2024]

[2] IC3 2020 internet crime report. (n.d.). https://www.ic3.gov/AnnualReport/Reports/2020_IC3Report.pdf. [Last access: Nov 6, 2024]

[3] Al-Qahtani, A. F., & Cresci, S. (2022). The COVID-19 scamdemic: A survey of phishing attacks and their countermeasures during COVID-19. IET Information Security, 16(5), 324-345.

[4] Naidoo, R. (2020). A multi-level influence model of COVID-19 themed cybercrime. European Journal of Information Systems, 29(3), 306-321.

[5] Xia, P., Wang, H., Luo, X., Wu, L., Zhou, Y., Bai, G., ... & Liu, X. (2020, November). Don't fish in troubled waters! characterizing coronavirus-themed cryptocurrency scams. In 2020 APWG Symposium on Electronic Crime Research (eCrime) (pp. 1-14). IEEE.

[6] Alzahrani, A. (2020). Coronavirus social engineering attacks: Issues and recommendations. International Journal of Advanced Computer Science and Applications, 11(5).

[7] Chapman, P. (2020). Are your IT staff ready for the pandemic-driven insider threat?. Network Security, 2020(4), 8-11.

[8] Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. Computers & security, 105, 102248.

[9] Okereafor, K., & Adelaiye, O. (2020). Randomized cyber attack simulation model: a cybersecurity mitigation proposal for post covid-19 digital era.

[10] Hakak, S., Khan, W. Z., Imran, M., Choo, K. K. R., & Shoaib, M. (2020). Have you been a victim of COVID-19-related cyber incidents? Survey, taxonomy, and mitigation strategies. Ieee Access, 8, 124134-124144.

[11] Wiggen, J. (2020). Impact of COVID-19 on cyber crime and state-sponsored cyber activities (Vol. 391, p. 2). Konrad-Adenauer-Stiftung.

[12] Okereafor, K., & Adebola, O. (2020). Tackling the cybersecurity impacts of the corona virus outbreak as a challenge to internet safety.

[13] Ghann, P., Tetteh, E. D., & Doe, N. (2022). The Impact of Covid-19 on Cybersecurity. International Journal of Recent Contributions from Engineering, Science and IT (iJES), 10(01).

[14] Khan, N. A., Brohi, S. N., & Zaman, N. (2023). Ten deadly cyber security threats amid COVID-19 pandemic. Authorea Preprints.

[15] Gaurav, A., Gupta, B. B., & Panigrahi, P. K. (2022). A novel approach for DDoS attacks detection in COVID-19 scenario for small entrepreneurs. Technological Forecasting and Social Change, 177, 121554.

[16] Cvitić, I., Peraković, D., Periša, M., & Jurcut, A. D. (2023). Methodology for detecting cyber intrusions in e-learning systems during COVID-19 pandemic. Mobile networks and applications, 28(1), 231-242.

[17] Alawida, M., Omolara, A. E., Abiodun, O. I., & Al-Rajab, M. (2022). A deeper look into cybersecurity issues in the wake of Covid-19: A survey. Journal of King Saud University-Computer and Information Sciences, 34(10), 8176-8206.