EXPLOITING URGENCY: ANALYSING PHISHING TACTICS AND USER SUSCEPTIBILITY IN SOCIAL MEDIA STORIES DURING THE COVID-19 PANDEMIC

by

AASHIKA.M

ABSTRACT:

Phishing is an online scam where criminals trick users with various strategies,with the goal of obtaining confidential information or other personal resources.The covid 19 pandemic had a dramatic worldwide impact on all sides of our life. The covid 19 pandemic has increased a surge in phishing attacks especially on social media platforms where the ephemeral nature of stories has been exploited to manipulate user behaviour. Many malicious actors utilized time sensitive messaging to manipulate human emotions and prompt hasty actions from users. This study investigates how phishers leverage urgency in social media stories to extract immediate responses from the users, thereby analysing the specific tactics used by them that enhance user susceptibility. This study aims to fill critical gaps in the understanding of phishing dynamics during the pandemic. The findings inform the development of targeted user education programs, digital literacy, security awareness and platform policies designed to mitigate phishing risks, in turn enhancing online safety in an increasingly urgent digital landscape.

KEYWORDS: Phishing, covid 19 pandemic, urgency in social media stories, phishing dynamics during the pandemic, mitigating phishing risks.

INTRODUCTION:

The COVID-19 pandemic has fundamentally changed how people communicate and share information, making social media a crucial conduit for information and connection. Cybercriminals took advantage of the widespread uncertainty and increased anxiety brought on by the pandemic during this turmoil, utilizing social media platforms as a breeding ground for phishing attempts. During this time, phishing—a type of cyber fraud that tries to trick people into disclosing private information—became much more sophisticated and common. Manipulation of these phishing attempts urgency increased user susceptibility, which resulted in many people unintentionally disclosing personal information or falling for financial frauds. This study is to investigate the elements that contribute to user vulnerability in social media tales and analyze the phishing strategies used during the pandemic. This research will provide insights that can guide future cybersecurity measures and user education campaigns by shedding light on the tactics used by cybercriminals and the responses of users by comprehending the interplay between urgency and vulnerability.

BACKGROUND:

Social media platforms have seen a significant transformation in communication and information sharing due to the COVID-19 epidemic. The environment has become a haven for fraudsters as consumers increasingly rely on these platforms for rapid updates on health, safety, and government announcements. Phishing attempts, which try to trick people into giving up personal information or clicking on harmful links, have become more sophisticated and

common. This is especially the case when social media stories—transient content that vanishes quickly—are used.

Phishers have a significant tool in social media tales because of their unique qualities, which include their transitory nature and the sensation of immediacy they produce. Phishers can take advantage of users' innate need to act quickly by constructing messages that imply urgency, such as alerts regarding vaccine availability, health advisories, or limited-time deals. This allows them to avoid critical thinking and inspection. This kind of persuasion works especially well in times of crisis, when people are frantic to get information and emotions are running high.

Even though these attacks are becoming more common, nothing is known about how urgency is used in social media posts especially, or about the psychological factors that increase user susceptibility to and reaction to these phishing approaches. Prior studies have predominantly concentrated on conventional phishing techniques, resulting in a crucial gap concerning the modification of these strategies inside the framework of swiftly changing social media attributes.

In order to create successful preventive techniques, it is critical to investigate the relationship between urgency, user psychology, and demographic aspects as phishing grows more complex. The goal of this research is to shed light on these processes and offer insights that can help platform regulations and user education programs better prevent phishing attempts during a crisis. It will be essential to comprehend how phishers take use of the distinctive features of social media stories in order to provide users with the information and resources they need to properly traverse this difficult digital terrain.

LITERATURE REVIEW

1. Phishing Tactics in Social Media, Moody et al., 2020

Phishing tactics have evolved to adapt to the characteristics of different platforms. Recent studies have highlighted how phishers utilize social media to create fake accounts, spread malicious links, and disseminate misleading information. Research indicates that social media's informal nature allows for a higher success rate in phishing attacks due to the perceived trustworthiness of peer-to-peer communication.The use of stories as a format has garnered attention for its ability to create a sense of urgency, making users more likely to engage without scrutinizing content.

2. Psychological Triggers and Urgency, Cialdini, 2009

Urgency is a well-documented psychological tactic in phishing schemes. Studies show that when individuals perceive a threat or a time-sensitive opportunity, they are more likely to respond impulsively. The emotional context of the COVID-19 pandemic has heightened feelings of anxiety and fear, which phishers exploit to increase the likelihood of user engagement with phishing messages. This phenomenon, often referred to as "fear-based persuasion," plays a critical role in the success of phishing attacks during crises

3. User Susceptibility and Demographic Factors, Mason et al., 2020

Research has demonstrated that user susceptibility to phishing varies significantly across demographic groups. Factors such as age, digital literacy, and prior experiences with cyber threats influence how individuals respond to phishing attempts. Younger users, who are

generally more active on social media, may exhibit different vulnerabilities compared to older adults, who might be less familiar with the technology but more likely to respond to urgent health-related information. Understanding these differences is crucial for tailoring educational interventions and enhancing cybersecurity measures.

4. Impact of COVID-19 on Phishing Trends, Fang et al., 2020

The COVID-19 pandemic has triggered a notable increase in phishing attacks, particularly those related to health information, government policies, and financial relief efforts. Phishers have exploited the public's heightened concern for health and safety, crafting messages that resonate with their immediate fears and needs .The use of social media stories during this period has amplified these tactics, as users are drawn to rapidly changing information and may overlook potential risks.

PROBLEM STATEMENT:

Despite the insights gained from existing literature, there remains a critical gap in understanding how urgency specifically manifests in social media stories and how this impacts user behavior. research exploring effective countermeasures and user education strategies tailored to the dynamics of social media stories is limited.

This research builds a more resilient framework against phishing in the context of rapidly changing social media dynamics. The phishing tactics exploit urgency in social media stories to influence user susceptibility in Covid- 19.

RESEARCH OBJECTIVES :

This study pinpoints and group the precise methods employed by phishers to instill a sense of urgency in social media reports about the COVID-19 outbreak. This research investigates the psychological triggers (such as health-related fears, fear of missing out) that phishers utilize in urgent communications and evaluate how these affect user susceptibility and engagement and also examins how users' receptivity to phishing efforts is impacted by the urgency of social media stories, with a particular emphasis on the possibility that users will click on links or divulge personal information. And overall create suggestions based on evidence that will improve platform policies, phishing attack defenses that take advantage of urgency, and user education and awareness initiatives.

RESEARCH QUESTIONS

- What specific tactics do phishers use to create a sense of urgency in social media stories during the COVID-19 pandemic?
- How do urgency-based messaging tactics in COVID-19-related social media stories impact user behavior regarding phishing attempts?
- How does this urgency affect user engagement and susceptibility to phishing attacks?
- Which psychological triggers are most effective in persuading users to engage with urgent phishing messages?

- What preventative measures can be implemented on social media platforms to reduce user susceptibility to urgency-based phishing tactics?
- How effective are educational campaigns about phishing in reducing user susceptibility to urgency-based tactics in social media during the COVID-19 crisis?

SCOPE OF THE STUDY:

The research will explore specific phishing techniques that emerged or became more prevalent during the COVID-19 pandemic, particularly those exploiting urgency and fear.The study will analyze how social media platforms (like Facebook, Twitter, and Instagram) were used to disseminate phishing attempts through stories and posts. The research will examine factors influencing user susceptibility, including psychological, social, and contextual elements, particularly in relation to the pandemic's unique challenges.

LIMITATIONS OF THE STUDY:

This study which focuses on access to comprehensive data on phishing incidents and user interactions on social media might be limited, affecting the depth of analysis. However findings may not be universally applicable across all social media platforms or user demographics, as experiences and susceptibility can vary widely.The fast-paced nature of social media and phishing tactics may result in the study quickly becoming outdated as new tactics emerge. While the pandemic context provides a unique angle, it may limit the applicability of findings to non-pandemic situations or other types of crises.

METHODOLOGY:

The study employs a doctrinal research methodology to analyse phishing tactics and user susceptibility in social media stories during covid 19 pandemic.It also uses an analytical approach, which makes it possible to do a thorough investigation of the body of existing literature. The research aims to provide a comprehensive understanding of the phishing landscape during this unique period. The research depends upon pre-existing academic literature for its conclusions rather than obtaining original data from people or organizations.

METHOD

The current study relies on the secondary data collection method, which comprises reading, analyzing and examining over previously published materials,academic Journals and Peer-reviewed articles focusing on cybersecurity, social media behavior, and psychological impacts of crises and Media Articles inclusive of News reports that highlight specific phishing incidents, user experiences, and expert analyses related to COVID-19.

PHISHING TACTICS IN SOCIAL MEDIA:

Phishing attacks are generally the practice of sending fraudulent communications that appear to come from a reputable source where attackers deceive individuals into providing sensitive information, such as usernames, passwords, and credit card numbers. This is often done through emails, messages, or fake websites that look legitimate. Phishing is often considered as a harmful threat thereby causing financial loss, data breaches and reputation damage. Nowadays Phishing on social media has been considerably increased, as attackers leverage these platforms to target users more effectively. Social media has eventually become the fastest growing attack surface. Attacks on social media platforms have increased, and they also

became the attack surface with the quickest rate of growth. Businesses use social media to market their products and services and establish connections with both customers and staff. Workers use social networking sites for both personal and professional purposes for hours on end. Our lives are constantly impacted by social media. Because of its widespread use, scammers are able to obtain personal information about people and use social engineering techniques to target them. Everybody could be a target. Phishing is fundamentally deceit based on impersonation and fakery. Everyone can use social media for free. This implies that creating phony profiles is quite simple. Because social media sites vary differently from one another, attackers have created site-specific specialty strategies to help them avoid discovery. 90% of phishing attacks sent via messaging apps are sent through WhatsApp. The next highest percentage is Telegram, with 5.04%

Phishing tactics employed by phishers are great in number. Some of the ongoing phishing Tactics include

EMAIL NOTIFICATION PHISHING

Social media keeps on revolving around real time information and therefore social platforms need user contributions to keep things interesting. These platforms send email updates to users to communicate what's happening around thereby bringing them back to the platform.Email is often used by social media platforms to alert users of account information or security upgrades. Users are more likely to trust notification emails from reputable social media platforms. It is a typical template that is easily spoofable yet rarely questioned. Individuals who get these emails frequently ignore the rest of the design and click on buttons or links in the message content. Hackers use this behaviour to direct people to phony websites that are hidden behind such buttons. These websites are then used by scammers to steal private data. They could start a virus download or set up a phony password reset scheme. Email phishing attacks always come from bogus email addresses or addresses with incorrect domains. The design, logo position, and language used may be slightly off-brand and can tip you off to a phishing attempt.

TIKTOK PHISHING SCAMS

Tik tok app has 755 billion users worldwide. TikTok scammers use emails and SMS to target users, just as in other phishing scams. Scammers exploit likes, verified account status, and TikTok sponsorships to entice people who value popularity. TikTok coins, which are in-app purchases usually obtained through live streaming, are promised by some. Users visit fraudulent websites that attempt to steal data or take control of their accounts when they click on the links.

One popular app for following influencers and celebrities is TikTok. Imposter accounts are also very common. Many are operated by bots that can have a strikingly realistic appearance. Adoring fans are drawn to fake accounts, and they subsequently make the error of disclosing private information via phony links.

FAKE CUSTOMER SUPPORT

A lot of individuals use social media to contact businesses directly for support. Compared to phone calls, online chats are quicker and more convenient. Younger customers would rather receive text responses than wait on hold. With dedicated support accounts, many businesses are increasing the range of services they offer.
Regretfully, scammers can fool customers with just a stolen logo and business description.

They make phony accounts that look like the business and contact people who are in need of assistance. They steal their targets' login credentials by directing them to phony login pages. Even more egregious scammers trick their victims into paying up front for unfulfilled repair services.

LINKEDIN FAKE JOB SCAM

Employers and employees frequently use social media in a competitive job market to find the next big position or skilled new hire. LinkedIn has simplified the hiring process and facilitated communication between companies and employees. But scammers can also use the site to execute phony employment scams and build false company profiles.

Usually, the fraud begins with a fake job posting. Attackers utilize it to gather applications for jobs or entice candidates with private messaging. The procedure provides private data to cybercriminals for use in subsequent phishing scams.

Some attackers take it a step further. They mail the victim a fake first paycheck after giving them the fictitious job, then fabricate an excuse to ask for a refund of some of the money.Then they abscond with that money.

USING HIJACKED SOCIAL MEDIA ACCOUNTS

By hijacking legitimate accounts, threat actors exploit trust and social connections of individuals or impersonate the target friends or family members. As users are more likely to trust messages or requests from their close ones, phishing attempts are seen more successful. social media hijackers employ methods such as automated tools for guessing passwords, credential stuffing attacks, malware attacks and so on .

PSYCHOLOGICAL MECHANISMS OF URGENCY IN COVID 19:

As noted by United Nations and the world Health Organization, The COVID-19 pandemic was accompanied by an equally-dangerous epidemic of frauds and manipulations. In the fourth edition of the Phishing and Fraud Report, it was discovered that phishing incidents rose 220% during the height of the global pandemic compared to the yearly average. Usually phishers gain attention of the user by way of triggering their fear or desires, by way of compelling the user to respond to the phisher's demands. Several studies have demonstrated the impact of emotions like fear on the effectiveness of phishing schemes and consumers, and consequently, the vulnerability to phishing. The success of a phishing attempt might be influenced by the behavior of users in general.

Since the COVID-19 epidemic accelerated in late 2019, the frequency of phishing attacks has been steadily rising. Using virus-specific information and buzzwords, cybercriminals have used the epidemic to target vulnerable individuals. As the growing health crisis during a pandemic could endanger the lives of the human, users are more likely to be the victims of fraudulent health messages.

Phishers frequently utilize psychological tricks, such as "time pressure," to weaken the user's cognitive abilities. This way, the user is more likely to react fast to the phisher's request rather than paying enough attention to the phishing email's clues to spot the differences in their email.

Emails containing critical and up-to-date information about the coronavirus situation in their area, along with notifications from reputable national or worldwide health organizations about self- or family protection advice, may be sent to users . This raises the question: what is the main motivator for users to open attachments or click on phishing links? Effects of emotions such as anxiety, on the success of phishing scams and users, increase in the susceptibility to phishing. A phisher can draw a user's attention by appealing to their needs or concerns, which will force the user to comply with the phisher's requests .

Stress, worry, and dread of COVID-19 are among the psychological problems that have increased as a result of the pandemic. Phishers exploit this weakness to deceive users into clicking on phishing links or opening harmful attachments by knowing that people are expecting messages, news, warnings, etc. related to the infection. Users therefore got both standard phishing emails (such as those offering a user password reset, a charity donation, better service, etc.) and COVID-19-themed phishing emails (such as those promising quick infection tests, goods to treat or prevent the disease, etc.) during the pandemic. Falling for coronavirus phishing emails rather than regular phishing was linked to fear of COVID-19. This may occur as a result of users' fear of the coronavirus, which leads them to click on the link in an email that appears to be from a reliable health organization such as WHO in order to read the most recent vaccination-related information. Anxiety and terror both serve as warning signs of danger or threat that can cause the right reactions.

IMPACT OF MISINFORMATION RELATED TO COVID 19.:

Social media play an increasingly important role in spreading both accurate information and misinformation. Globally, the coronavirus disease 2019 (COVID-19) pandemic is expanding, and more and more people are getting affected. People want to exchange news about the epidemic and their experiences, therefore it goes without saying that there is a huge demand for information. cammers used misinformation about COVID-19 (e.g., fake cures, misleading health guidelines) to lure victims into clicking malicious links or providing personal information An infodemic is the term used to describe the flood of COVID-19-related content that has resulted from social media's major role in the continuing epidemic. However, inaccurate information about COVID-19 can be harmful because it can encourage people to engage in risky behaviors or perform acts that could spread the illness, diverting them from taking the necessary precautions to safeguard their own and others' health. One of the most well-known examples of misinformation is the potential link of the MMR vaccine with autism and gastroenteritis in children. Because of increased anxiety, uncertainty, and the speed at which information spreads, the proliferation of false information about COVID-19 produced an ideal environment for phishing attempts. Many people were concerned about their health, safety, and financial stability as a result of the pandemic. Phishing schemes took advantage of this anxiety by crafting communications that seemed to provide important information, such as government assistance, vaccine availability, or health updates. False information frequently imitated official communications, making people less vigilant. Phishers took advantage of this by creating emails or messages that appeared to be from government or health institutions, which made it simpler to trick people into divulging personal information. Many people were overwhelmed by the rapid expansion of COVID-19 information and were more prone to believe anything without question. This setting made people more vulnerable to phishing attempts that purported to offer "urgent" resources or upgrades.
Social media made it easy for false information to proliferate, encouraging individuals to click

on links and distribute material without checking its sources. Phishing attempts frequently disseminate malicious links masquerading as reliable content via social media sites. A greater dependence on digital communication resulted from the shift to remote work. Phishing techniques, particularly those claiming to be connected to remote work tools or workplace health protocols, became more successful as employees used personal devices and networks. Some demographics were more susceptible to phishing and false information than others, including the elderly and those with low levels of computer literacy. Scammers adapted their strategies to take advantage of these weaknesses, frequently impersonating organizations that offered help or support. Confusion resulted from conflicting information regarding COVID-19 guidelines, treatments, and vaccines. Phishing attempts exploited this misunderstanding by providing "clarifications" or "new opportunities," which frequently included links to malicious websites.

STATISTICAL REFERENCES:

The earliest cases of COVID-19 were reported in Wuhan, China, in December 2019 . Due to its rapid spread worldwide, the World Health Organization (WHO) declared a pandemic. As of December 20, 2021, there had been 275,007,350 confirmed cases, 5,370,192 reported deaths, and 246,674,846 recovered individuals across the world. Information is the "factual data" that comprises the knowledge that permeates society and directs people's decisions, deeds, and efforts or lack thereof. We get and use information from a wide range of sources, such as radio, television, newspapers, magazines, journals, ads, the internet, professionals, friends, and the constantly growing world of social media. Misinformation makes situational control even more difficult . In the end, it could cause uncertainty that limits the advancement of both public and individual health during emergencies by fostering rumours, stigma, discrimination, and erroneous hypotheses. A recent study from Ofcom research found that since lockdown, 46% of participants had come across inaccurate or misleading coronavirus information. Social media is where most misinformation occurs. Misinformation can result in hate crimes, exploitation, public health risks, and public mistrust. Reports indicated a 400% increase in phishing attempts globally in the early months of the pandemic, with many targeting information about COVID-19 vaccines and government relief funds.

The proportion of COVID-19 misinformation on social media ranged from 0.2% (413/212 846) to 28.8% (194/673) of posts. Studies on social media carried out during previous pandemics also reported a large variation in the proportion of posts identified as misinformation: 4.5% of posts on Twitter about H1N1 influenza, compared with 23.8% of content posted on YouTube about Zika virus disease, and 55.5% of posts on Twitter about Ebola virus disease. According to a recent analysis conducted by Oxford university and Reuters institute of Journalism shows that 225 items of COVID-19 misinformation and found that 88% appeared on social media. Social media content may be broadcast instantly without editorial review or verification, false information can be created quickly and spread widely. Health misinformation negatively affects individuals' decisions, leading to poor outcomes in physical health, mental health, and continued viral spread. The Reuters Institute found that 56% of misinformation around COVID-19 appears to have been based upon true information which has been reconfigured. The Reuters Institute's analysis of COVID-19 misinformation found that 39% of false claims were about the actions of public authorities (such as government, the World Health

Organisation or the United Nations), which was the single largest category of claims within the sample. Official health advice may be contradicted by COVID-19 disinformation that is not backed by medical research and is presented as official guidance. People are therefore more willing to put themselves and other people in danger. There is proof that people who are misinformed may incur more risks, such as sharing meals with sick people and without washing their hands. In certain situations, acting on false information could endanger life.

USER DEMOGRAPHICS AND SUSCEPTIBILITY:

Despite being more tech-savvy overall, young age group people are nevertheless prone to impulsivity and might not assess online conversations critically. Scammers used trendy hooks, such as phony job openings, financial aid, or alluring COVID-19 offers, to target them on social media and messaging apps. Peer pressure and social influence also increased their susceptibility to clicking on dubious links. Personalized phishing emails, frequently with urgent payment requests or security alarms, were prevalent and seemed to originate from colleagues or reputable brands. Because scammers created emails that looked authentic, even knowledgeable people had a hard time spotting the deception.

Economic hardship heightened anxiety and desperation, making low income individuals more likely to respond to offers of financial relief. Phishing schemes often promised government aid or unemployment benefits, playing on urgency and fear.Many scams involved fake websites mimicking government portals, leading to data theft.

Less educated individuals were especially vulnerable due to their lack of knowledge about phishing techniques and internet safety.
To elicit terror and prompt responses, scammers frequently utilized direct and frightening language in their interactions. Victims were enticed to divulge personal information with straightforward, alluring offers.

CHANGES IN USERS SOCIAL MEDIA ENGAGEMENT PATTERNS:

Regular and frequent use of social media can encourage actions that may be carried out with inadequate cognitive ability, like sharing, liking, and clicking links. Cloud services, blogs, relatively simple syndication, wikis, podcasts, social networking sites (SNSs), video conferencing, instant messaging, and blogs are just a few of the new online communication tools brought about by the growth of collaborative web technology. A culture of user-generated content and significantly greater user participation are the outcomes of this change. With an estimated 4.7 billion users worldwide, the proliferation of social networking sites (SNSs) has created a virtual community that encourages its members to exchange information. SNSs, along with its email-like messaging features, have emerged as the main electronic communication tool. Due to the popularity of SNSs and the benefits they have provided for users, this same environment unintentionally fosters certain habits that allow threat agents to target susceptible users. The APWG study states that the third quarter of 2022 was the worst phishing quarter the organization has ever seen, with a record 1270,883 phishing attacks. When creating their communications, phishers take advantage of seasonal occasions, which makes it challenging for unwary consumers. For instance, the security firm Netwrix found that during the first three months of the coronavirus pandemic, almost half (48%) of the firms polled experienced

phishing assaults. Although phishing is typically associated with emails, it can also happen in other contexts, like text messaging and social networking sites. . Users' awareness of phishing on social networking sites is still very low when compared to emails, according to Krombholz, Hobel, Huber, and Weippl. Even people who were aware of and knowledgeable about phishing were vulnerable to it, according to a research by Diaz et al. Although social engineers can take advantage of the technological tools built into SNS platforms, the same characteristics also highlight user behaviors that can be exploited. Because of personal qualities including personality features, messages on social networking sites can effectively evoke strong emotions in some users, causing them to take actions that could expose them to phishing.

How increased online activity led to heightened phishing risks during lockdown:

People resorted to social media for amusement, knowledge, and connection during lockdowns and social distancing measures.User participation on social media sites including Facebook, Instagram, Twitter, and TikTok increased significantly. Facebook, for instance, recorded a rise in video calls and messages of more than 70%.Content about COVID-19, such as pandemic updates, health tips, and community assistance programs, attracted users.Social experiences during lockdowns were reflected in the spike in the sharing of user-generated content, challenges, and memes.Users' need for virtual social connection led to an increase in engagement rates (likes, shares, and comments). Additionally, influencers and brands became more visible, which resulted in a rise in promotional content.A wide range of demographics were drawn to social media, including elderly folks who had not previously used the internet as much. The potential target base for fraudsters grew as a result of this development. As more individuals looked for real-time connections, live streaming became increasingly popular. Virtual meetings, webinars, and events became popular, opening up new channels for interaction.
Users were more vulnerable to phishing efforts that took advantage of their feelings and sense of urgency around the epidemic as they spent more time online.Taking advantage of the increased worry around the issue, scammers created messages pertaining to financial aid, health updates, and vaccine information.

Social engineering techniques, which utilize fear and false information about COVID-19 to fool users into clicking on harmful links or divulging personal information, have been included into phishing methods.Scammers frequently created phony accounts that looked like real health services in order to imitate respectable businesses.Users found it challenging to distinguish between reliable and fraudulent sources due to the widespread dissemination of false information regarding COVID-19 on social media.. As users flocked online for information and interaction, scammers took advantage of the situation, employing sophisticated tactics to exploit emotional responses and misinformation.

KEY FINDINGS:

Phishing tactics generally exploited a sense of urgency, typically associated with financial aid, vaccine information, and health and safety issues. Emotions were skillfully used by scammers to cause panic and compel consumers to behave rashly.

The emotional toll of the epidemic and the quick transition to digital communication increased user susceptibility. Many people unintentionally weakened their defenses against phishing assaults because they were desperate for rapid information and assistance.

Phishers used social media as their main distribution mechanism for malicious content, adjusting their tactics in real time. The strategies used at this time were frequently more advanced and situation-specific, demonstrating a greater comprehension of human psychology.

Although phishing has become more common, many users were not sufficiently aware of how to spot and handle these risks. This disparity emphasizes the necessity of continuing education and awareness initiatives specifically designed for social media users.

CONCLUSION:

A crucial junction between urgency and vulnerability is shown by the examination of phishing strategies and user susceptibility in social media narratives during the COVID-19 epidemic. Fear, false information, and increased internet activity came together in a special way during the pandemic, leaving people more vulnerable to phishing attempts that preyed on these feelings. The pandemic's experiences highlight the need for strong cybersecurity procedures and user education. Social media companies, organizations, and legislators must work together to make the internet a safer place. To reduce the hazards of phishing, it will be essential to implement frequent training, improve reporting procedures, and cultivate a culture of alertness.

In conclusion, understanding how urgency was exploited in phishing tactics during the COVID-19 pandemic provides valuable insights into user behavior and the evolving nature of cyber threats. By learning from these experiences, stakeholders can better prepare for future challenges in the digital landscape, ensuring that users are equipped to recognize and defend against phishing attempts.

PREVENTIVE MEASURES AND FUTURE RECOMMENDATIONS:

Although new phishing attack techniques are constantly being created, they all have certain characteristics that you can spot if you know what to look for. Numerous websites are available to teach you about the most recent phishing assaults and their distinguishing characteristics. Your chances of preventing a possible attack increase with the speed at which you learn about the most recent attack techniques and communicate them to your users through frequent security awareness training. Because phishing assaults cannot be stopped by technical means alone, security awareness training is essential. Employees should be empowered to recognize and report questionable activities as well as learn about the dangers of phishing. Organizations can evaluate their own risk and increase staff resilience by using simulated phishing campaigns to further reinforce the training. When staff members click on phishing-simulation emails, it's critical to remind them of the dangers and how to report any questionable emails. cautious steps must be undertaken when clicking links or opening emails, especially from senders you don't recognize. Downloading attachments should only be done when necessary and from reliable sources. Even if you know the sender, it's usually not a good idea to click on a link in an email or instant message. Hovering over the link to check if the destination is right is the very least you should be doing. Some phishing attacks are quite complex, and the target URL may appear to be an exact replica of the real website, configured to track keystrokes or steal credit card or login credentials. Instead of clicking on the link, you should use your search engine to go directly to the website if that is possible. By serving as a barrier between your computer and

an attacker, firewalls are a useful tool for preventing external attacks. When combined, desktop and network firewalls can strengthen your security and lessen the likelihood that a hacker will enter your system. COVID-19 has affected millions of people around the world, while its long-term impact remains to be seen. However, protecting ourselves against coronavirus-related scams is both a feasible and essential step. On receiving a phishing email, steps can be taken to report it to the IT department by forwarding it as an attachment.and Notifying the organization being spoofed in order to prevent other people from being victimized.

Recommendations for organizations to enhance user awareness and training.

1. Organizing frequent, interesting courses to teach staff members how to spot phishing attempts and cybersecurity best practices thereby assessing employees' replies and giving them quick performance feedback, using simulated phishing campaigns.

2. Making easily readable documentation that describes the company's cybersecurity and phishing rules.

3. Using newsletters or updates to keep employees up to date on the newest phishing techniques and trends.

4. Creating brief, interesting films that illustrate phishing scenarios and defense strategies.

5. Making eye-catching infographics that highlight important phishing warning signs and countermeasures. Providing a simple procedure so that staff members may report suspicious phishing attempts without worrying about the consequences.

6. Encouraging a culture of alertness, think about putting in place a rewards program for staff members who report phishing attempts.
   Keeping staff members educated and alert, provide them with updates on new phishing techniques and risks. Security alerts can be regularly published outlining the latest phishing attacks, their causes, and the lessons discovered.

7. The usage of multi-factor authentication for all organizational accounts can be promoted to increase security.Informing staff members on MFA's operation and significance in preventing unwanted access.

8. Motivating the leadership to give cybersecurity top priority by showcasing its significance in messages and actions.
   Encouraging staff members to be proactive and vigilant by fostering a culture where cybersecurity is everyone's responsibility.
9.
10. Planning phishing awareness events or campaigns and include entertaining activities to keep staff members interested.
    updates of real-world examples, and phishing advice via internal social media platforms can be shared.
11. Providing or suggesting browser extensions that can be used to identify and alert users to dubious websites.
12. Assessing training programs' efficacy on a regular basis via tests or feedback sessions.
13. Making constant improvements to training materials and delivery strategies by utilizing evaluation insights.

LONG-TERM IMPLICATIONS OF PANDEMIC PHISHING TRENDS:

Predictions for the future of phishing tactics post-pandemic:

The future of phishing tactics in social media is likely to be characterized by increased sophistication, personalization, and the exploitation of emerging technologies and trends.

Artificial intelligence may be used by scammers to produce more realistic phishing messages and more accurately mimic authentic accounts, making it more difficult for consumers to spot fraud. Deepfake audio and video will probably become more popular, allowing attackers to create lifelike impersonations of reliable people and further tricking targets. As social media makes more data available, phishing assaults will become more individualized, utilizing personal information about people to craft more convincing and focused frauds. Attackers will increasingly take use of social dynamics, such as using data from a user's social network to create messages that appear credible and relevant. In order to increase the chances of success, attackers would probably use social media, email, and SMS to build multi-channel phishing campaigns that approach victims through several touchpoints. Phishers may utilize compromised accounts to carry out additional network attacks against the victim, utilizing established connections to bolster their legitimacy..

How the experiences from this period may shape user behavior and security practices in social media in the long run:

When there is an enhanced knowledge of cybersecurity dangers,People will probably continue to be more mindful of phishing and other online dangers, which will make them more circumspect when using the internet and scrutinize conversations more

closely.Education regarding cyberthreats will make people look to learn more about how to defend themselves against online scams. By implementing Improved Security Procedures like Multi-Factor Authentication (MFA), people realize how successful MFA is in preventing unwanted access, and there may be a long-lasting movement towards its broad usage on social media accounts. To lower the danger of credential-based assaults, users shall rely more and more on password managers to generate and save complicated passwords. Modifications in Behavior during Online Conversations may enhance users to become more skeptical of the veracity of requests, offers, and sources. Encouraging the practice of Reporting Culture where Users may feel more empowered to report phishing attempts. Bringing new developments in security technology may boost the creation of sophisticated security solutions, such AI-driven threat detection and response systems, will continue to be pushed as phishing methods change. More powerful security features, like improved reporting tools for questionable content and automatic notifications for possible phishing attempts, may be included by social media platforms.

REFERENCES

Facebook phishing is getting cleverer. here's how to protect yourself (no date a) *CNET*. Available at: https://www.cnet.com/tech/services-and-software/these-phishing-tactics-disguised-as-fun-on-social-media-heres-what-to-look-for/ (Accessed: 23 October 2024).

Understanding and dealing with phishing during the COVID-19 pandemic (2021) *ENISA*. Available at: https://www.enisa.europa.eu/news/enisa-news/understanding-and-dealing-with-phishing-during-the-covid-19-pandemic (Accessed: 23 October 2024).

Coifman, K.G. *et al.* (2021) *What drives preventive health behavior during a global pandemic? emotion and worry*, *Annals of behavioral medicine : a publication of the Society of Behavioral Medicine*. Available at: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8344868/ (Accessed: 23 October 2024).

Al-Qahtani, A.F. and Cresci, S. (2022) *The COVID-19 scamdemic: A survey of phishing attacks and their countermeasures during COVID-19, IET information security*. Available at: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9349804/ (Accessed: 23 October 2024).

Countering the 5 most common social media phishing scams (no date) *5 Most Common Social Media Phishing Scam | Terranova Security*. Available at: https://www.terranovasecurity.com/blog/most-common-social-media-phishing-scams (Accessed: 23 October 2024).

Fan, Z. *et al.* (2024) *Investigation of phishing susceptibility with explainable artificial intelligence*, *MDPI*. Available at: https://www.mdpi.com/1999-5903/16/1/31#:~:text=Our%20analysis%20reveals%20that%20psychological,individual's%20susceptibility%20to%20phishing%20attacks (Accessed: 23 October 2024).

The latest phishing statistics (updated June 2024): Aag it support (2024) *AAG IT Services*. Available at: https://aag-it.com/the-latest-phishing-statistics/#:~:text=Millennials%20and%20Gen%2DZ%20internet%20 users%20 (Accessed: 23 October 2024).

Understanding and dealing with phishing during the COVID-19 pandemic (2021) *ENISA*. Available at: https://www.enisa.europa.eu/news/enisa-news/understanding-and-dealing-with-phishing-during-the-covid-19-pandemic (Accessed: 23 October 2024).

Shi, B. *et al.* (2024) *Leveraging social media data for pandemic detection and prediction*, *Nature News*. Available at: https://www.nature.com/articles/s41599-024-03589-y (Accessed: 23 October 2024).

Phin Security (2023) *Future phishing and Social Engineering Trends*, *Phin*. Available at: https://www.phinsec.io/blog/future-phishing-trends (Accessed: 23 October 2024).