International Journal of Engineering Inventions
e-ISSN: 2278-7461, p-ISSN: 2319-6491
Volume 12, Issue 4 [April. 2023] PP: 245-253

The Impact of the Covid-19 Pandemic on The spread of phishing on the Internet

Dr. Najah Al-shanableh
Computer Science Department
Al al-Bayt University
Mafraq, Jordan

KholudM.shawaqfeh
Computer Science Department
Al al-Bayt University
Mafraq, Jordan

Dr. Mazen Alzyoud
Computer Science Department
Al al-Bayt University
Mafraq, Jordan

ABSTRACT
Phishing is a cyberattack designed to steal confidential data from internet users. Since phishing scams are typically sent via email, they can be thwarted by practicing good email security habits, such as checking the sender's domain and paying attention to the URL when clicking on links.
The COVID-19 pandemic has led to a significant increase in the use of digital technologies and the Internet, which has created new opportunities for phishing attackers. In this paper, we examine the spread of phishing during the COVID-19 pandemic, including the motivations of phishing attackers, the methods they use to carry out attacks, and the impact of the pandemic on individuals and organizations. We also discuss the challenges and opportunities for defending against phishing in the current context and provide recommendations for individuals and organizations to protect themselves from phishing attacks better.
This paper is structured as a review paper for most of the research dealing with phishing. Since the time sequence is different since the emergence of the problem and how it spread more widely in the world at the time of the epidemic, we included in this paper most of the mechanisms for dealing with the problem, the way to solve it, and how to increase the awareness of users in dealing with it, based on the available technology.
Keywords: *Phishing, cyberattack risk awareness, security management, disaster prevention, and mitigation.*

Date of Submission: 08-04-2023 Date of acceptance: 21-04-2023

I. INTRODUCTION

Cyber threat

Cyber threats increase as the environment is well suited for cybercriminals to strike. Such pandemics can cause the stock markets to collapse, which may bring down the economies of infected countries. Cybercriminals around the world will undoubtedly take advantage of this crisis [1].

Cyber threats are malicious attacks on computer systems, networks, and data. There are many different types of cyber threats, including [2]:

1. Malware: Malware is a type of software that is designed to harm computer systems. It can include viruses, worms, trojans, and other malicious programs.

2. Ransomware: Ransomware is a type of malware that encrypts a victim's files and demands payment in exchange for the decryption key.

3. Phishing: Phishing is a type of attack that uses social engineering techniques to trick victims into revealing sensitive information, such as passwords or financial details.

4. Distributed Denial of Service (DDoS) Attacks: DDoS attacks involve overwhelming a website or network with traffic to make it unavailable to users.

5. Advanced Persistent Threats (APTs): APTs are long-term, targeted attacks that are designed to steal sensitive information from a specific organization.

6. Spyware: Spyware is a type of malware that is designed to gather information about a victim's computer usage and internet habits.

7. Adware: Adware is a type of malware that displays unwanted advertisements on a victim's computer.

8. Rootkits: Rootkits are a type of malware that are designed to hide the presence of other malicious software on a computer system.

9. Botnets: Botnets are networks of infected computers that can be used to carry out DDoS attacks and other malicious activities.

It is important for individuals and organizations to be aware of these different types of cyber threats and to take steps to protect their computer systems and data. This may include using anti-virus software, regularly applying security patches, and being cautious when opening emails and clicking on links.

Phishing

Phishing is a type of cyber attack that uses social engineering tactics to trick individuals into revealing sensitive information, such as passwords, financial details, and other confidential information. The goal of phishing is to trick the victim into providing personal information or clicking on a malicious link [3].

Phishing attacks are typically carried out through emails, text messages, or websites that are designed to look like legitimate sources, such as banks, government agencies, or well-known companies. For example, a phishing email might appear to be from a bank and ask the recipient to click on a link to update their account information. If the victim clicks on the link, they may be taken to a fake website that looks like the real thing, and asked to enter their login credentials and other sensitive information [1].

Phishing attacks can have serious consequences, as the attackers can use the information they collect to steal money, commit identity theft, or carry out other malicious activities. It is important for individuals and organizations to be vigilant and to educate themselves about how to recognize and avoid phishing scams. This may include being cautious when opening emails and clicking on links, verifying the authenticity of emails and websites, and using anti-virus software and security updates [4].

To protect against phishing, individuals and organizations should follow these best practices:

- Be wary of unsolicited emails or text messages, especially those that ask for sensitive information.
- Verify the sender of an email before clicking on any links or opening any attachments.
- Use anti-virus software and keep it up-to-date.
- Keep software and operating systems updated with the latest security patches.
- Use multi-factor authentication where available.
- Be cautious of emails that contain spelling or grammar errors, or that seem to be written in a way that is out of character for the sender.
- Use strong, unique passwords for all of your accounts, and change them regularly.
- Don't reuse the same password for multiple accounts.

By being vigilant and taking steps to protect themselves, individuals and organizations can reduce the risk of falling victim to phishing attacks and protect their sensitive information from being compromised.

Background

The following is a brief history review of phishing based on several academic studies organized by the time of development of the concept of phishing and how to deal with it.

In 2005, Jason Military published "Technical Trends in Phishing Attacks."
Phishing is a vastly profitable exercise for culprits. Over the last two decades, there has been an increase in the technology, diversity, and complexity of these attacks. Users have become more apprehensive about phishing crimes and how to identify simpleminded phishing spots.
The malwareprovides the means for culprits to produce further effective phishing attacks that can simultaneously target multiple businesses. Botnets are used to send phishing emails and host phishing sites; specialized malware can be used to target sensitive information with an increased potential to cause damage figure 1 shows how the malware message is sent from the attacker to the victim [1].

As previously stated, after introducing our concept and being familiar with and why The reasons for the interest in this concept are emerging, and the response to it is due to its economic impact.
In 2011, BITS, A DIVISION OF THE FINANCIAL SERVICES ROUNDTABLE, published the paper "Malware RISKS AND MITIGATION REPORT."
Malware is both insidious and pervasive. The financial services business is the best choice. Financial institutions should recognize the increasing threat from both external and internal sources. Financial institutions should take practical measures to detect and defend against potential internal malware interference with business processes. Financial institutions should evaluate their vulnerability to the malware described and implement appropriate safeguards to minimize any potential for damaging impact. This should include measures to detect malware and a plan to respond once it is seen. The program should be exercised periodically, as is done for business continuity and disaster recovery planning. [2]
As explained in the introduction, it is clear that phishing significantly impacts the emergence of some criminal acts.In 2013, the thesis was published at Florida Gulf Coast University under the title "
"How the Internet Has Changed the Face of Crime"Law enforcement and the judicial system have struggled to keep up with the Internet. Millions of people are now affected by illegal online actions. Criminals will continue to exploit the Internet for all aspects of their operations. There is widespread agreement that action is needed to counter this growing threat.

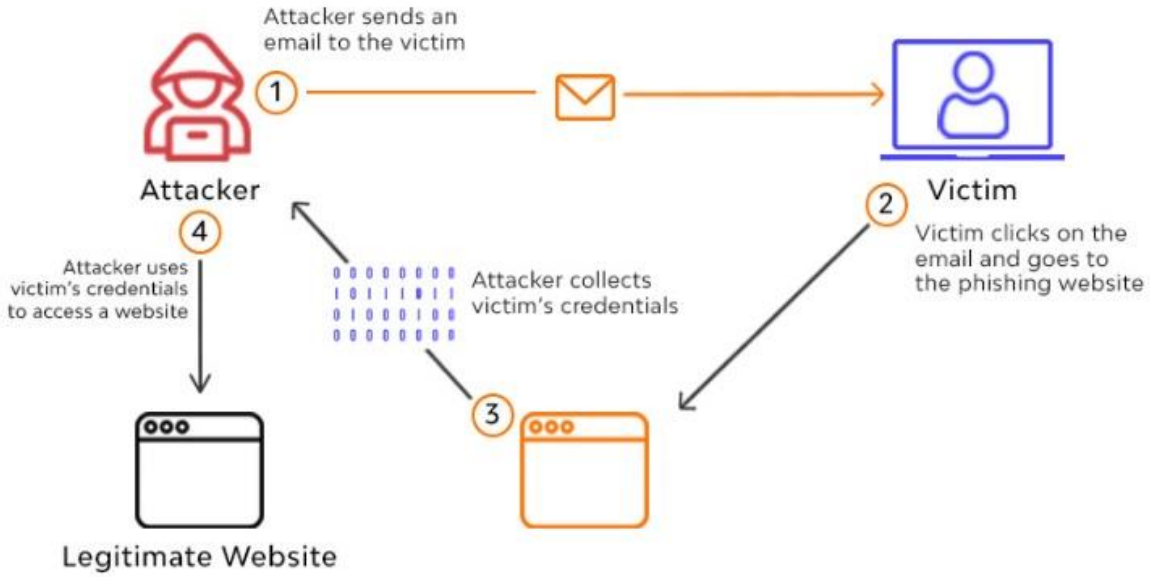

Figure 1 Phishing Attack

However, it would be nearly impossible to eliminate cybercrime. Therefore, steps must be taken to mitigate the threat. Casualties of cybercrime need to be apprehensive about how to cover and help with similar acts. Training for law enforcement and other professionals needs to address the evidential issues relating to child pornography.

Legislation should be passed to mandate the reporting of child pornography. Protocols should be established about countries that continue to facilitate the production and spread of images depicting the sexual offenses of children. Strict global penalties must be enacted for those who continue to produce, distribute, and view child porn. Existing international conventions are not effective in prosecuting and combating cyber terrorism. Governments, especially countries with minimal cybercrime laws, must ensure that their rules apply to cybercrimes. Even after an international legal framework is established, the most significant challenges will lie in policing and detection.

Most organizations and individuals adopt a reactive rather than a proactive approach to information security. There is an urgent need for information security, ethical education, and awareness programs. Enforcement agencies must increase and improve their understanding of available technology. Children must be taught how to use the Internet safely and responsibly. The Internet has brought issues with transnational crime and the ability to prosecute these crimes. Cyberspace is not the first or only domain that lies beyond the control

of any single nation. Professionals must understand the impact of technology rather than just focusing on the technology itself. There is a need to understand and measure the positive, not just the negative, aspects of online communication with peers, family, and friends. Research on cybercrime data is minimal in comparison to traditional crime. Standardizing data and reporting measures will increase the available information about cybercrime.

There is a clear need for further in-depth research to understand and address the multiple issues and consequences of cybercrime nationally and globally. Cybercrime and victimization will continue to be growing areas of research and policy influence as the world increasingly relies on cyber technologies and the Internet. [3]

The following part describes the policy of countries dealing with cybersecurity and its importance in greater detail.

In 2015, it was published on DCAF HORIZON, a WORKING PAPER No. 7 by F. Schreier under "On Cyberwarfare,"

which dealt with the new concept of Cyberwarfare. Cyberwar has become the barrage of the day as nations-countries are arming themselves for the cyber battlespace. Attacks can quickly go global as covertly acquired or manipulated computers and servers worldwidehave demurred into service. Numerous prominent authors see a war being waged in cyberspace today.

This contribution examines what cyberwar means, what it entails, and whether threats can discourage it or defense can alleviate its effects. Its focus is on cyberwarfare conditioning patronized by nation countries. Other cyber-attacks occur regularly, which is more frequent than state-sponsored activities.

Cyber vandalism is "cyber hacktivism," a common term for hackers who use illegal digital tools. Cybercrime provides a terrain in which attack ways can be meliorated. The global cost of cybercrime is estimated to be in the range of US $1 trillion annually.

Cyber espionage collects information on an opponent's secrets, intentions, and capabilities. Cyber spying can be as important or more pervasive than acts of cyberwarfare. The return on investment for targeting sensitive information can be extremely high compared to the chops required to penetrate systems.

Cyberspace is the 5th space of warfare after land, sea, air, and freedom. It comprises the two billion computers currently in existence, plus servers, routers, switches, fiber-optic cables, and wireless communications. Cyberspace defies measurement in any physical dimension or time-space continuum. For the US Department of Defense, "cyberspace is a sphere characterized by the use of computers and other electronic bias to store, modify, and change data." Defining the term may be one of the difficulties in creating any joint agreement among states. New functionalities such as "Network Centric Warfare" would be impossible without cyber-based systems and capabilities. The ability to reprogram targeting data within an armament on its way to the target and calculate real-time updates from a GPS satellite to precisely strike that target is possible only through cyberspace.

It has to be successful all the time. Third, the range is no longer an issue in cyberspace since attacks can be launched worldwide. Fourth, the criterion of attacks is particularly delicate, complicating possible responses. And fifth, ultramodern society's inviting reliance on cyberspace furnishes any bushwhacker with a target-rich terrain, putting tremendous strain on the protector to defend the sphere successfully. Many consider cyberspace the newest and most important addition to the global commons. Cyberspace can also be seen as the "terrace" of technology-mediated communication. More than a quarter of the world's population uses it daily, which continues to expand. Cyberspace is qualitatively different from the ocean, air, and space disciplines, yet it both overlaps and continuously operates within all of them. It's the only sphere in which all instruments of public power—political, instructional, military, and profitable—can be coincidently exercised.

Cyber power is the capability to control IT systems and networks in and through cyberspace. Transforming the goods of cyber power into policy objects is the art and science of strategy. Cyber power is shaped by multiple factors, from technology to organizational priorities to national borders.

In the 21st century, cyber power is transforming how power is wielded and how is wielded. Cyberwarfare is usingthe cyber ability to inflict or threaten punishment against an adversary. Malware is malicious software that interferes with standard computer and Internet-grounded operation functions. It can also achieve political objectives through force without the opponent's consent.

Cyber power is complementary to land, sea, air, and space power in that it generates strategic effects in all domains but is less coercive than these instruments. The coercive capability of cyber management is still limited, but this may change in the future as coercion must first be proven.

Cyberwarfare refers to a primarily coordinated digital assault on a government by another or large groups of citizens. It's the action by a nation-state to access another nation's computers and networks. There's no widely accepted definition of cyber warfare. A computer network attack is "operations to disrupt or destroy information resident in computers." Cyberwarfare is the employment of computers or digital expedients by an administration against another state. The Washington Post's Julian Zelizer writes that a successful cyberwar depends on means and vulnerability.

The possibility of cyberwar causing significant damage to the public and profitable security of the state exists. Conducting an "information operation" of strategic significance would not be easy, but it is insolvable. Still, cyber alone is a doubtful way to win wars. No one knows how destructive a strategic cyber-attack in a conflict conducted in the virtual realm would be—it may well be less decisive. Operational cyberwar may have the potential to contribute to warfare. How much is unknown and, to a large extent, still unknowable?

Operational cyberwarfare operations may rarely harm individuals directly, nor do they, with some exceptions, destroy equipment. Such operations are more likely to confuse and frustrate operators of military systems. Cyberwar at the operational level may well only be a support function for other elements of warfare. The vast majority of attacks about which concern has been expressed apply only to Internet-connected computers. Many civilian systems are victims of cyber security lapses and cyber-attacks. The fortified forces must think hard as they draft their cyber defense pretensions, programs, strategies, and operations. [4]

As was mentioned previously, all the dangers of phishing. Let us now turn to defend our system.

In 2018, Springer Nature published the paper "Defending against Phishing Attacks: Taxonomy of Methods, Current Issues, and Future Directions."
They classified social engineering phishing as relying on spoofed email attacks and fake websites. They've also classified different results in spoofed email filtering or artificial page finding. They further categorize these results based on some standard parcels that they share. These groups are grounded on block lists, networks, heuristics, some points, and other properties. After the classification,they also described various issues and challenges with current results to understand future study ideas to help humanity by defending against phishing attacks [5]

Types of phishing attacks
There are several types of phishing attacks that cyber criminals use to steal sensitive information and compromise individuals and organizations as figure 2 shows. Some of the most common types of phishing attacks include [10]:

- Email phishing: This is the most common type of phishing attack, and involves sending an email that appears to be from a trusted source, but actually contains a malicious link or attachment. The goal is to trick the recipient into clicking on the link or attachment and revealing sensitive information, such as login credentials, financial information, or personal data.

- Spear phishing: This type of phishing attack targets specific individuals or organizations, using personalized messages and information gathered from social media and other sources. The goal is to trick the recipient into revealing sensitive information, such as login credentials, financial information, or personal data.

- Whaling: This type of phishing attack targets high-level executives and executives, using messages that appear to be from a trusted source. The goal is to trick the executive into revealing sensitive information, such as login credentials, financial information, or personal data.

- Smishing: This type of phishing attack involves sending a text message that appears to be from a trusted source, but actually contains a malicious link or attachment. The goal is to trick the recipient into clicking on the link or attachment and revealing sensitive information, such as login credentials, financial information, or personal data.

- Vishing: This type of phishing attack involves making a phone call that appears to be from a trusted source, such as a bank or government agency. The goal is to trick the recipient into revealing sensitive information, such as login credentials, financial information, or personal data.

- Clone phishing: This type of phishing attack involves creating a duplicate of a legitimate email and sending it to the recipient, with a malicious link or attachment. The goal is to trick the recipient into clicking on the link or attachment and revealing sensitive information, such as login credentials, financial information, or personal data.

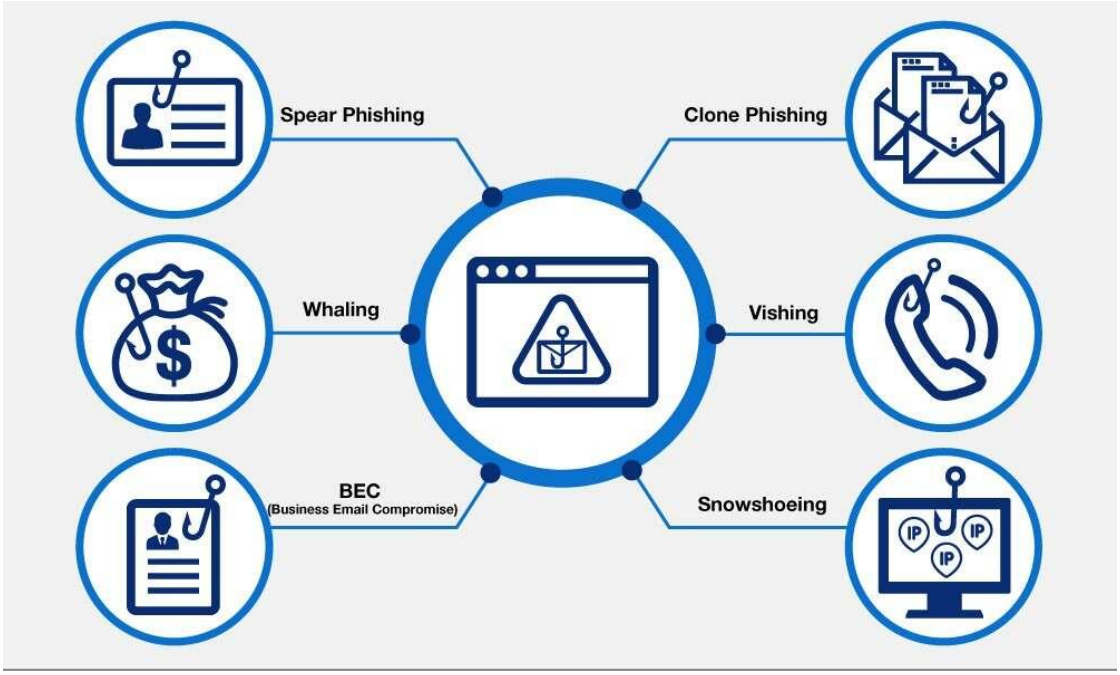

Figure 2 Types of Phishing Attacks

COVID-19 Pandemic and Phishing

The COVID-19 pandemic has had a significant impact on cybercrime, as more people have shifted to remote work and increased their use of digital devices and online services. This has created new opportunities for cyber criminals to exploit vulnerabilities and target individuals and organizations with a range of cyber threats, including phishing, malware, and ransomware attacks [16,17,18,19].

- Increased phishing attacks: The COVID-19 pandemic has been a prime target for phishing attacks, as cyber criminals use the pandemic as a way to trick individuals into revealing sensitive information. For example, phishing emails may claim to be from the World Health Organization (WHO) or other organizations and offer information about the pandemic, but actually contain links to malicious websites or attachments [16].

- Rise in malware attacks: The shift to remote work has also led to an increase in malware attacks, as cyber criminals take advantage of the increased use of personal devices and the absence of IT support to spread malware. For example, cyber criminals may send phishing messages that appear to be from remote work tools or instant messaging platforms, but actually contain links to malicious websites or attachments [18].

- Increased ransomware attacks: The COVID-19 pandemic has also seen a rise in ransomware attacks, as cyber criminals target organizations that are struggling to maintain their operations in the face of the pandemic. For example, cyber criminals may use ransomware to encrypt an organization's data and demand a ransom in exchange for the decryption key [17].

- Supply chain attacks: The COVID-19 pandemic has also created new opportunities for cyber criminals to launch supply chain attacks, by compromising the networks and systems of organizations' suppliers.

- Financial fraud: The COVID-19 pandemic has also seen an increase in financial fraud, as cyber criminals target individuals and organizations that are looking for information about financial assistance and stimulus packages. For example, phishing emails may claim to be from the Internal Revenue Service (IRS) and offer information about financial assistance, but actually contain links to malicious websites or attachments.

The COVID-19 pandemic has had a significant impact on the spread of phishing attacks. With more people working from home and relying on digital tools and online platforms, cyber criminals have taken advantage of the increased exposure to launch more phishing attacks [20].
One of the ways that phishing attacks have increased during the pandemic is through the use of COVID-19-related themes. For example, phishing emails may claim to be from the World Health Organization (WHO) or

other organizations and offer information about the pandemic, but actually contain links to malicious websites or attachments.
Another way that the pandemic has contributed to the spread of phishing is through the increased use of remote work and online collaboration tools, such as video conferencing and instant messaging. Cyber criminals have taken advantage of the increased use of these tools by sending phishing messages and setting up fake websites that appear to be legitimate remote work tools.
In addition to these types of attacks, phishing scams related to financial relief and stimulus packages have also increased during the pandemic. For example, phishing emails may claim to be from the Internal Revenue Service (IRS) and offer information about financial assistance, but actually contain links to malicious websites or attachments.

In 2021, the Advanced Transportation Journal published a review paper titled "Cybersecurity and Countermeasures at the Time of Pandemic."
Cybersecurity attacks during the pandemic were classified into four different types. Episodes include flow control, injection, information leakage, denial of service (DoS), and sabotage. The paper goes beyond traditional cybersecurity to study newly developed attacks such as phishing and work from home. [6]

In 2021, the Egyptian Informatics Journal published the paper "Detecting COVID-19 chaos-driven phishing/malicious URL attacks by a fuzzy logic and data mining based intelligence system."
A paper highlights the effect of the COVID-19 pandemic on cyber security's spending, priorities, and aspects. A first-of-its-kind fuzzy logic and data mining-based intelligence system was designed to identify all the launched attacks with an accuracy of 98.19%. [7]

In 2022, WIT Transactions on The Built Environment published "Role of awareness to prevent personal disaster: reducing the risks of falling victim to phishing by strengthening user awareness."
Phishing is a tremendous hazard and will remain one. Phishing allows attackers to target the user as the potentially weakest link in the chain. Technical solutions are increasingly available to mitigate the risk of phishing. Organizations should not entirely rely on user awareness since there is an indication of the partial ineffectiveness of training. Information sharing is one measure to increase the recognition of phishing emails and raise awareness among users.

Information sharing can be done differently to address the various target groups. Other measures such as regular training, including active feedback or phishing test campaigns, are reflected as more efficient. Despite several years of anti-phishing solutions, a continuous threat still requires ongoing initiatives to reduce the risk. Research shows that a bundle of measures ranging from technical arrangements to awareness measures is most promising to fight against phishing threats successfully [8, 19,20,21].

There have been several studies conducted to understand the impact of the COVID-19 pandemic on the spread of phishing on the internet. These studies have found that the pandemic has significantly contributed to the increase in phishing attacks, as cyber criminals take advantage of the increased use of digital devices and online services during the pandemic [22].

- A study by Check Point Software Technologies found that the number of phishing websites increased by 667% between February and March 2020, as the COVID-19 pandemic spread around the world. The study also found that phishing attacks targeting remote workers and healthcare organizations increased significantly during this period.

- A study by Kaspersky Lab found that phishing attacks related to the COVID-19 pandemic increased by 600% in March 2020, compared to the same period in 2019. The study also found that the number of phishing emails increased dramatically, with messages related to the pandemic accounting for almost 10% of all phishing emails.

- A study by Google found that phishing attacks related to the COVID-19 pandemic increased by 250% between January and March 2020, compared to the same period in 2019. The study also found that the number of phishing emails targeting remote workers increased significantly during this period.

- A study by Proofpoint found that phishing attacks related to the COVID-19 pandemic increased by 667% in the first quarter of 2020, compared to the same period in 2019. The study also found that phishing attacks targeting remote workers and healthcare organizations increased significantly during this period.

These studies suggest that the COVID-19 pandemic has had a significant impact on the spread of phishing on the internet. By taking advantage of the increased use of digital devices and online services during the pandemic, cyber criminals have been able to target individuals and organizations with a range of phishing attacks, compromising sensitive information and causing significant damage [16,23].
During the COVID-19 pandemic, there have been several types of phishing attacks that have emerged:

- COVID-19 themed phishing attacks: These attacks use the pandemic as a way to trick individuals into revealing sensitive information. For example, phishing emails may claim to be from the World Health Organization (WHO) or other organizations and offer information about the pandemic, but actually contain links to malicious websites or attachments [17,24,25].

- Remote work and online collaboration tool phishing attacks: These attacks target individuals and organizations that are working remotely and using online tools and platforms to collaborate. For example, cyber criminals may send phishing messages that appear to be from remote work tools or instant messaging platforms, but actually contain links to malicious websites or attachments [16,17,19].

- Financial relief and stimulus package phishing attacks: These attacks target individuals and organizations that are looking for information about financial assistance and stimulus packages. For example, phishing emails may claim to be from the Internal Revenue Service (IRS) and offer information about financial assistance, but actually contain links to malicious websites or attachments [22,23,24,25].

- Supply chain attacks: These attacks target organizations by compromising their suppliers and using that access to launch phishing attacks. For example, a cyber criminal may compromise a supplier's email account and use it to send phishing messages to the supplier's customers [25].

- SMS phishing attacks: These attacks use text messages to trick individuals into revealing sensitive information. For example, phishing text messages may claim to be from a bank or other financial institution and ask the recipient to click on a link to update their account information [25].

It is important for individuals and organizations to be aware of these types of phishing attacks and to take steps to protect themselves. This may include being cautious when opening emails and clicking on links, verifying the authenticity of emails and websites, and using anti-virus software and security updates. By being vigilant and taking steps to protect themselves, individuals and organizations can reduce the risk of falling victim to phishing attacks and protect their sensitive information from being compromised [23,26].

II. Conclusion And Recommendation

The joy has shifted from our transition from the concept of a single computer and an information exchange network to the adoption of many notions and problems resulting from criminal ideas that destroyed people or countries. Phishing transcends only stealing personal information from a person or taking a picture and accessing it and the secrets of this person or even accessing his knowledge through the bank.

It transcends it to more complex and political concepts and a war tactic that countries wage against each other to gather information and sabotage. Because it is the simplest and cheapest form of technical attack because it only depends on the ignorance of the user, Thus, we moved to the concept of cyber security, whose nature and importance must be established for users, whether governments or individuals, because legislation and penalties have been developed after falling victims to these attacks.

And because the therapeutic reactions are not commensurate with the rapid development of technology and the attackers' adoption of new methods of attack, especially in periods of epidemics in which a person is more sensitive to existence and coexistence against a disease or war, the messages that are saturated with emotional provocation come to invite the user to open these messages and know the content. Unfortunately, we fall into the trap of the attacker.

It is a practical solution to train users and publish brochures and awareness advertisements, not to deal with messages that carry this deceptive nature.

As a more radical and feasible solution, this technology must be fought with more robust technology, and we must be one step ahead of the attackers.

The idea of phishing is generally based on the botnet. So we should watch the information flow for messages so that it is possible to customize a counter in the header of the message. To calculate the extent of circulation of this message so that the number is ascertained if it is more than the reasonable number in the

circulation of the news. It is ensured that there are no reports on it and deleted immediately so that it is confirmed in the firewall of the network or the individual computer. It is forbidden to enter the user's.

In conclusion, the COVID-19 pandemic has created a perfect storm for the spread of phishing on the internet. The shift to remote work, increased internet usage, and heightened fear and uncertainty has all contributed to the growth of phishing attacks. It is crucial for individuals and organizations to be vigilant and to educate themselves about how to recognize and avoid phishing scams.

References

[1]. Milletary, J., & Center, C. C. (2005). Technical trends in phishing attacks. Retrieved December 1(2007), 33.
[2]. Risks, M. Mitigation Report. BITS-The financial services roundtable (2011).
[3]. Norden, S. (2013). How the internet has changed the face of crime.
[4]. Schreier, F. (2015). On cyber warfare. Geneva Centre for the Democratic Control of Armed Forces.
[5]. Gupta, B. B., Arachchilage, N. A., &Psannis, K. E. (2018). Defending against phishing attacks:
[6]. Taxonomy of methods, current issues, and future directions. Telecommunication Systems, 67(2), 247-267.
[7]. Ramadan, R. A., Aboshosha, B. W., Alshudukhi, J. S., Alzahrani, A. J., El-Sayed, A., &Dessouky, M. M. (2021). Cybersecurity and Countermeasures at the Time of Pandemic. Journal of Advanced Transportation, 2021.
[8]. Zahra, S. R., Chishti, M. A., Baba, A. I., & Wu, F. (2021). Detecting Covid-19 chaos-driven phishing/malicious URL attacks by a fuzzy logic and data mining-based intelligence system. Egyptian Informatics Journal.
[9]. ISER, B., & BRANDTWEINER, R. (2022). ROLE OF AWARENESS TO PREVENT PERSONAL DISASTERS: REDUCING THE RISKS OF FALLING FOR PHISHING BY STRENGTHENING USER AWARENESS. WIT Transactions on The Built Environment, 207, 79-88.
[10]. D.W.B. Li and S. K. Das, "The Anatomy of Phishing Attacks," IEEE Transactions on Dependable and Secure Computing, vol. 3, no. 4, 2006, pp. 308-322.
[11]. J. R. Crandall and S. J. Stolfo, "An Empirical Study of the Role of Social Engineering in Phishing Attacks," Journal of Computer Security, vol. 19, no. 2, 2011, pp. 191-214.
[12]. M. K. H. Au and M. Li, "Countermeasures against Phishing Attacks: A Survey," IEEE Communications Surveys and Tutorials, vol. 13, no. 4, 2011, pp. 542-560.
[13]. S. K. Das and D. W. B. Li, "Phishing Detection and Defense: A Review," IEEE Communications Surveys and Tutorials, vol. 16, no. 1, 2014, pp. 49-63.
[14]. A. B. Jain and M. Ross, "Phishing Detection and Prevention: A Machine Learning Approach," Journal of Computer Security, vol. 23, no. 2, 2015, pp. 167-184.
[15]. S. K. Das and D. W. B. Li, "Phishing Attack and Defense: A Machine Learning Approach," IEEE Transactions on Information Forensics and Security, vol. 11, no. 7, 2016, pp. 1575-1586.
[16]. Check Point Software Technologies, "COVID-19 Cyber Threat Intelligence Report," 2020.
[17]. Kaspersky Lab, "Phishing attacks related to the COVID-19 pandemic increased 600% in March 2020," 2020.
[18]. Google, "The Impact of the COVID-19 Pandemic on Phishing Attacks," 2020.
[19]. Proofpoint, "COVID-19 Phishing Attacks: An Update," 2020.
[20]. S. DeFino, "The COVID-19 Pandemic and the Rise of Cybercrime," Journal of Cybersecurity, vol. 6, no. 2, 2020, pp. 113-120.
[21]. D. Wall, "COVID-19 and Cybercrime: Understanding the Threat Landscape," Journal of Information Security and Cybercrime, vol. 2, no. 2, 2021, pp
[22]. K. Shetty, "The Impact of COVID-19 on Cybersecurity Threats and Trends," McAfee, 2020.
[23]. J. Kim, "Phishing and the COVID-19 Pandemic: A Rising Threat," Trend Micro, 2020.
[24]. S. Hershey, "The COVID-19 Pandemic and the Rise of Cybercrime," Journal of Cybersecurity, vol. 6, no. 2, 2020, pp. 123-129.
[25]. R. A. VanDyke, "The COVID-19 Pandemic and the Growth of Phishing Scams," Symantec, 2020.
[26]. M. Smith, "COVID-19 and the Rise of Remote Work: Implications for Cybersecurity and Privacy," Information Security Journal, vol. 29, no. 3, 2020, pp. 107-112.
[27]. S. K. Das, "The COVID-19 Pandemic and the Future of Cybersecurity," Journal of Cybersecurity, vol. 6, no. 4, 2020, pp. 251-256.