IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 5, June 2023

Artificial Intelligence's Advantages and Disadvantages in Terms of Cybersecurity and Phishing Attacks

Vaibhav Chandrasen Vaidya and Payal Tekchand Rewatkar
Students, Master of Computer Application
Late BhausahebHiray S.S Trust's Hiray Institute of Computer Application, Mumbai, India

Abstract: *As artificial intelligence continues to develop and expand, there is a growing need for protection and security. While there are positive applications of AI, there are also negative ones. Analogous to phishing attacks that are getting progressively complex and delicate to descry. presently, AI helps us sludge incoming emails effectively and safely. Still, this composition aims to raise public awareness about implicit new and more sophisticated risks, as well as easier methods for detecting implicit risks in cyberspace. Attackers who use AI can exploit audio and visual information to deceive stoners and gain access to requested information or data.*

Keywords: artificial intelligence, phishing attacks, cyberspace, social engineering.

I. INTRODUCTION

The rise of technology and computer networks has led to an increase in cybercrime. Lawbreakers have shifted their focus from the physical expressways to the virtual world. With the advancement of software results, communication bias, smartphones, and laptops, cybercrime has become more prevalent. Artificial intelligence is also expanding and being integrated into all aspects of society. Still, there is a concern that cybercriminals will use this technology to achieve their pretensions. Artificial intelligence has been developing for some time and has been primarily associated with specific business forms analogous as e- government, and e-banking. Some believe that artificial intelligence will eventually take over all business processes, but this would require significant resources. One area where artificial intelligence is being used by cybercriminals is in phishing attacks. These attacks are getting more sophisticated and challenging to decry. Artificial intelligence enables attackers to produce and execute attacks quickly, making it a significant problem for associations and individuals.

II. THE CONCEPT OF ARTIFICIAL INTELLIGENCE (AI)

Artificial intelligence (AI) became popular through shows and films depicting the conflict between humans and robots. Still, AI has been present in our lives for some time, particularly in e-commerce, and e-government. AI assists stoners in searches, behavior

Analysis, and emphasis suggestions. With the emergence of Chat GPT and the expansion of AI, enterprises' concerns about security, integrity, rights, power, and operation have arisen. This paper aims to examine how AI affects phishing attacks in cyberspace. Phishing attacks were chosen because AI can pretend to mimic the behavior of a user who wants to gain important information from another person. The Turing test is used to describe AI, which aims to mimic mortal behavior to make opinions, estimate, suggest, and communicate. Cybersecurity experts are interested in this because it's easy to manipulate stoners and gain information that can be abused. AI can also be used to decry attacks and alert stoners to vicious software or algorithms.

III. AI AND CYBER ATTACKS

Artificial intelligence can be employed for vicious purposes in various cyberattacks, including phishing attacks. Phishing attacks are a common form of cybercrime that involves tricking individuals into discovering sensitive information such as watchwords, credit card numbers, and social security numbers. With the help of artificial

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 5, June 2023

intelligence, cybercriminals can produce more sophisticated and satisfying phishing emails that are harder to descry. This can lead to ruinous consequences for individuals and businesses alike, making it vital to stay vigilant and take the necessary precautions to protect against analogous attacks.

A. Phishing Attacks

Phishing attacks have been a problem since the early days of the Internet. These attacks use social engineering to trick druggies into sharing their particular information with the bushwhacker. The bushwhacker may use the name of an estimable company or an existing one to gain the user's trust. There are several types of phishing attacks, but the most well-known is

- Email phishing attacks,
- HTTPS phishing attacks,
- Whaling attacks,
- Vishing,
- Smishing
- Pharming [l].

1) Email Phishing Attacks

Phishing attacks are a common threat that organizations and individuals face daily. These attacks are carefully planned and require the attacker to gather enough information to make their approach convincing. Attackers often use false identities and information obtained from the internet to increase their chances of success. The phishing email usually contains urgent information about a problem that needs to be solved. These attacks are successful because they rely on social engineering tactics to trick the victim into taking action [9].

2) HTTPS Phishing Attacks

One common type of attack involves sending an email with a link that the recipient is supposed to click on. This link may lead to a website with compromised content or prompt the user to download malicious software. Attackers often use tools to shorten the link or make it appear secure. However, users can check the link's legitimacy by hovering their mouse over it and looking for suspicious content such as strange letters, characters, or symbols. These types of attacks are widespread, but there are tools available to help users protect themselves from them. [9].

3) Spear Phishing Attacks

Sophisticated spear attacks require more effort from the attacker and are carefully planned. The attacker gathers information from social networks, the internet, presentations, and seminars to select a target. They then falsely present themselves and request a service from the victim using information such as phone numbers, emails, or pictures. These attacks are aimed at individuals or small groups, making it easy for them to go unnoticed if not reported. [9].

4) Whaling Attacks or CEO Fraud

A type of attack that uses publicly available information to target organizations or individuals is known as a spear phishing attack. In this type of attack, the attacker pretends to be the CEO of the organization and sends an email to the finance department, asking them to transfer money to another account. The email is designed to look like it came from the real CEO and may include real information about the victim's job position, travel, and location. The attacker creates a sense of urgency and asks the victim to take immediate action without verifying the information provided. This type of attack relies on the victim's trust and can be very effective. [9].

Hi Raj, I'm in a meeting right now, but we have to do a wire transfer urgently to complete a payment that Madhu wants us to finish today. Can you take care of it this morning? If so, please let me know, and I'll provide you with the necessary information. Thank you.

5) Vishing Attacks

Vishing attacks are a type of scam where the attacker uses voice manipulation to make their request seem more important and urgent. They will call someone and ask for information or actions based on publicly available

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 5, June 2023

information, like a phone number. It's important to be aware of these attacks and take steps to prevent them. There are now artificial intelligence tools that can replicate someone's voice and create new content based on audio information. This means that vishing attacks could become more targeted and realistic. Attackers might even use the voice of a company's director, for example, if they have spoken publicly before. [9].

6) Smishing Attacks Smishing and Vishing attacks are types of cyberattacks that use information that is publicly available about individuals, groups, and organizations. These attacks are carried out through SMS [9] messages. The attackers often use prize games, discounts, and other enticing offers to trick their victims into providing personal information or performing certain actions. Several types of Smishing attacks are currently popular in cyberspace.
The following are common tactics used by attackers to trick people into giving away their personal information: - Pretending to be a postal or package delivery service and asking for confirmation of an order by filling out a form with confidential information. - Posing as a bank and sending an SMS message to inform the user of changes to their account, then requesting data entry to complete or stop an action on their bank account. - Sending an SMS message to the victim claiming they have won a prize in a sweepstake and asking them to confirm their identity as the winner. - Informing the victim that their email, social media, or website account has been maliciously taken over and asking them to enter a two-factor authentication code. After gathering information about the victim, the attacker executes the forgot password action and then asks the victim to send them their authentication code for account recovery. It's important to be cautious and verify the legitimacy of any requests for personal information before providing it. [6].

7) Pharming
Sophisticated attacks go beyond social engineering and require technical knowledge. These attacks involve taking control of DNS servers to redirect requests to malicious websites. The attacker may make subtle changes to the website, such as hiding grammatical errors or using different fonts or photos, to make it appear legitimate. Once the user enters their login information or grants management rights, the attacker has achieved their goal

IV. ANALYSIS OF THE CYBER SPACE

This section provides an evaluation of the present condition of cyberspace. It includes details about the benefits and drawbacks of artificial intelligence in the ongoing conflict between cyber attackers and experts. [2].
According to INTERPOL's 2022 report, cybercrime through phishing attacks is a major problem on all continents, in addition to other criminal activities [2]. The goal of these attacks is to gather information about the victim and gain access to their financial resources, either directly or indirectly. Phishing attacks have become more prevalent during the COVID-19 pandemic, as more people have moved their activities online. Attackers have taken advantage of this shift to create more sophisticated and disguised attacks, resulting in increased attacks on organizations and negative consequences such as financial losses, data misuse, and data leakage.

A. Risks of AI in Cyber Security and Phishing Attacks

The Guardian reports that identifying phishing emails has become more challenging because attackers can now use popular chatbots to create emails and avoid detection by filters on SMTP servers. Previously, it was possible to spot malicious phishing emails if they contained spelling or grammatical errors. However, with chatbots, attackers can generate emails with all the necessary information and no grammatical errors in the specified language. Cybersecurity experts used to analyze emails based on these parameters to determine if they were spam, but it is now difficult to identify them due to the email's content [8]...
Artificial intelligence can be used by attackers to create convincing content and make victims believe that they are knowledgeable about a particular topic. This content is mostly created by artificial intelligence, making it easier and faster for attackers to create successful phishing emails using chatbots. This could lead to an increase in email phishing attacks that bypass mail server controls. To combat this, cyber security experts should analyze the organizations they work with and limit communication to reliable partners or clients. Another challenge that experts will face is voice cloning using artificial intelligence. Attackers can use this to prepare and execute an attack quickly by using the voice of someone close to the victim and demanding payment or data using phishing methods. Artificial intelligence can

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 5, June 2023

mimic the thinking, habits, vocabulary, and approach to information of the person it clones, making these attacks more difficult to carry out. However, attackers need a certain database of information about the victim or someone close to them to be successful. Victims who are constantly exposed in public or have a large amount of video and audio content available online are at higher risk. As these problems become increasingly difficult to solve in traditional ways, additional surveillance of systems, information, and material that can be compromised is necessary.

B. Advantages Of Artificial Intelligence In Cyber security And Phishing Attacks

Artificial intelligence has an advantage in protecting digital systems because it can connect events and detect malicious software or spam emails. Currently, unwanted messages are detected by implementing a filter that sends emails containing defined keywords or from marked unwanted addresses to spam. However, artificial intelligence can connect similar words or expressions that are related to the keywords and inform the user that it may be spam. Phishing attacks are more dangerous and complex, but artificial intelligence has been used to detect them for some time. With further development, artificial intelligence can provide deeper analysis by linking brands or persons with real ones, checking codes, and other email features. Artificial intelligence can also detect other attacks by learning from the large amount of data that passes through mail servers every day. Therefore, email should make rapid progress in machine learning and recognizing unwanted emails. [4].

V. CONCLUSION

The field of artificial intelligence is expected to expand in the coming years, with its development and application increasingly permeating all aspects of modern human life. Failure to adapt to these new circumstances could lead to significant problems, such as changes in the economy, marketing, growing social inequality, and other negative aspects of technological development. In the future, AI will create increasingly persuasive messages and more complex algorithms in conversations with humans. The advantage of AI over humans lies in its ability to process a large amount of high-quality data quickly and adapt easily to changes and new information. However, this also means that AI can be used to develop effective manipulation algorithms to obtain desired information from users, leading to personalized attacks and the automatization of attacks. To protect users, individuals, and organizations must invest significant effort and knowledge in security technologies, focusing on social engineering and developing mechanisms for recognizing malicious emails. Checking web addresses should become a new reality, as attackers often clone addresses of popular brands to obtain personal information from victims. Research in this field will be highly interesting in the future, and it is crucial to conduct a comprehensive review of existing security systems and prepare users for potential new trends. The development of new methodologies is necessary to enhance existing knowledge and safeguard against future threats. Security will become the most valuable resource in the future, and every individual should focus on personal growth and the establishment of ethical and responsible standards to effectively and positively utilize the advantages brought by artificial intelligence..

REFERENCES

[l] Duplico.io. Phishing napadi: kojesvevrstepostojeikakoihprepoznati? .https://duplico .io/phishing-napadi-koj e-sve-vrste¬ postoje-i-kako-ih-prepoznati/ . 2021.
[2] INTERPOL. 2022 INTERPOL global crime trend summary re¬ port. https://www.interpol.int/content/download / 18212/304202/ file/2022_Interpol_ Global_ Crime_ Trends_ Summa1y_Report. pdf 2022
[3] J. T.Minkus and N. Memon. Leveraging Personalization to Facilitate Privacy .https://papers. ssm.com/ sol3/papers.cfm ?ab¬ stract id244802. 2014.
[4] The Guardian. AI chatbots making it harder to spot phishing emails, say experts. https://www.theguardian.com /technolo gy/2023/mar/29/ai-chatbots-making-it-harder-to-spot-phishing¬ emails-say-experts. 2023.
[5] Help net Security. Sophistication of phishing emails. https:// www.helpnetsecurity.com /2023/03/ 08/ sophistication-of-phish¬ ing-emails/. 2023.
[6] Terranova, M. Smishing Examples: What They Are and How to Stay Safe. Te1rnNova Security. https://terranovasecurity.com / smishing-example s/ . 2022.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 5, June 2023

[7] F. Enos, S. Benus, R. L. Cautin, M. Graciarena, J. Hirschberg , and E. Shriberg. Personality Factors in Human Deception De¬ tection: Comparing Human to Machine Performance. INTER¬ SPEECH - ISLP, 2006.
[8] EUROPOL. Digital skimming. https://www.europol.europa.eu / crime-areas-and-statistics/crime-areas/cybercrime. 2019.
[9] IT Governance. The 5 most common types of phishing attack. https:// www.itgovernance.eu / blog/ en/ the-5-most-common¬ types-of-phishing-attack # : :text Smishing%20and%20vish¬ ing&text One%20of"/o20the%20most%20common ,link%20 to%20prevent%20further%20damage. 2019.