Journal of Neonatal Surgery
ISSN(Online): 2226-0439
Vol. 14, Issue 22s (2025)
https://www.jneonatalsurg.com

OPEN ACCESS

A Comprehensive Analysis of Phishing Challenges and Ai Solutions Adopted by it Organizations

Sanjog S. Harihar[1], Dr. Mahesh Potdar[2]

[1]Research Scholar, Teaching Assistant, School of Computer Studies, Sri Balaji University, Pune (SBUP), Survey No. 55/2-7, Tathawade, Off Mumbai-Bangalore Bypass, Pune - 411033, MH, India.

Email ID: [1]Sanjogharihar22@gmail.com

[2]Research Guide, Associate Professor, Institute of Management Studies & Career Development and Research, Ahmednagar, Maharashtra. Savitribai Phule Pune University, India.

Email ID: [2]Maheshpotdar@rediffmail.com

Cite this paper as: Sanjog S. Harihar, Dr. Mahesh Potdar, (2025). A Comprehensive Analysis of Phishing Challenges and Ai Solutions Adopted by it Organizations. *Journal of Neonatal Surgery*, 14 (22s), 17-25.

ABSTRACT

One of the most persistent and dynamic dangers to IT firms globally is still phishing. As cutting-edge technology like artificial intelligence (AI) have become more prevalent, cybersecurity has experienced both advancements and new difficulties. Although AI-powered solutions have improved security, hackers are also using AI to craft extremely dishonest and focused phishing attacks. This study looks at the most recent phishing risks that IT companies must deal with, such as deepfake schemes, Business Email Compromise (BEC), AI-powered attacks, and the abuse of reliable platforms. It also looks at how IT companies are utilizing AI-powered solutions to counter these dangers. This study illustrates how businesses are bolstering their defences by inspecting the efficacy of machine learning, natural language processing, and real-time threat detection. The findings objective is to provide a deeper understanding of the constantly changing phishing landscape and offer strategic insights for building more adaptive, scalable, and proactive cybersecurity frameworks

Keyword: *Quishing, Deepfake, Threat, Phishing, AI, Vishing, Cyber Security, Social Engineering*

1. INTRODUCTION

Phishing assaults are become much more common due to the quick development of digital technology and the growing trend of working remotely. Phishing, one of the most prevalent and destructive types of cybercrime, preys on human weaknesses, takes use of technological flaws, and reveals organizational systemic flaws. Phishing techniques have changed significantly in the last several years as attackers have started using advanced technology, such as artificial intelligence (AI), to carry out extensive, highly customized, and flexible attacks. In order to safeguard their vital assets and preserve stakeholder trust, IT businesses must immediately adopt similarly sophisticated solutions in response to these new threats.

The increased complexity of phishing assaults and the efficiency of AI-driven cybersecurity solutions in thwarting them are two major facets of this expanding problem that are covered in this paper. It specifically looks at contemporary phishing tactics that go over established security measures, like deepfake-assisted fraud, AI-powered email spoofing, and QR-code phishing. The report also looks at how AI tools like machine learning, anomaly detection, and behavioural analytics are being used by IT companies to recognize, categorize, and stop these kinds of risks.

Analysing the changing nature of phishing threats that IT firms encounter and evaluating the potential of artificial intelligence in thwarting these risks are the two main goals of this study. This study attempts to add to the body of knowledge on cybersecurity by combining ideas from case studies, technical assessments, and industry reports. It also hopes to inform future research and real-world security measures.

The paper begins with an introduction, highlighting the growing threat of AI-powered phishing attacks. It then presents a literature review, summarizing key research on phishing detection techniques. The main sections analyse evolving phishing threats, AI tools used in phishing, and AI-driven cybersecurity strategies adopted by IT organizations. The paper concludes with a discussion on AI-powered phishing prevention measures and case studies of organizations using AI for cybersecurity

.

2. LITERATURE REVIEW

[1] The research provides an in-depth analysis of how phishing attacks exploit AI-based techniques to deceive users and steal sensitive data. It explores various phishing methods, including spoofed emails and fake websites, and discusses AI-driven detection mechanisms such as machine learning, deep learning, hybrid learning, and scenario-based techniques. The study equates different AI models for phishing detection, evaluates their effectiveness, and highlights current encounters and future research guidelines in cyber-security.

[2] The review explores various phishing attack techniques, focusing on AI-driven detection methods. It compares traditional phishing detection approaches with ML and DL models, evaluating their effectiveness using datasets and performance metrics. The study reviews over 130 articles from 2020 to 2024, identifying research gaps and challenges in detecting newly emerging phishing threats. By analysing phishing processes, attack types, and preventive measures, the paper provides a roadmap for researchers and cybersecurity experts to enhance phishing detection models and improve online security.

[3] The paper discusses how artificial intelligence (AI) can enhance cybersecurity awareness to mitigate phishing attacks. It highlights that phishing, a prevalent cyber threat, exploits social engineering tactics to trick users into revealing sensitive data. The study emphasizes the importance of AI-driven cybersecurity training programs to educate users on identifying and avoiding phishing attempts. It reviews various phishing techniques, the role of AI in phishing detection, and the benefits of AI-based awareness programs in reducing cyber risks. The paper ultimately advocates for the widespread adoption of AI-powered training to strengthen cybersecurity defences.

[4] The paper explores how Explainable AI (XAI) can improve phishing detection by making machine learning models more transparent and interpretable. It highlights the limitations of traditional phishing detection methods, which often lack clarity in decision-making, and proposes XAI as a solution to provide both accuracy and human-understandable explanations. The study reviews existing phishing detection techniques, emerging trends in XAI-based detection models, and the challenges of balancing accuracy with interpretability. It concludes that integrating XAI into phishing detection systems can enhance cybersecurity by improving trust, accountability, and real-time threat identification.

[5] The paper examines the evolution of phishing attacks, the role of AI in making these attacks more sophisticated and harder to detect. It highlights how AI-powered phishing campaigns exploit human and technical vulnerabilities, leading to financial and data losses. The study reviews various phishing detection methods, including machine learning and behavioural analysis, and identifies gaps in current security measures. It suggests that combining AI-driven threat detection with human oversight and multi-layered security strategies can enhance protection against increasingly complex phishing threats.

[6]The literature review on AI-driven cyberattacks highlights the increasing sophistication of cyber threats as attackers leverage artificial intelligence to enhance their tactics. The study emphasizes that AI is being used to automate cyberattacks, improve penetration strategies, and evade traditional security defences. The review systematically examines AI-driven cyber threats, identifying key attack phases, including reconnaissance, penetration, exploitation, and evasion. Findings indicate that AI-assisted attacks are faster, more unpredictable, and harder to detect, challenging conventional cybersecurity measures. The study concludes that organizations must adopt AI-driven security solutions to counteract these threats effectively, ensuring proactive defence mechanisms in an evolving cyber landscape.

[7] The paper presents a proactive approach to detecting phishing attacks using AI and ML. It highlights the increasing sophistication of phishing techniques and the limitations of traditional security measures. The proposed system operates across multiple platforms, automatically detecting phishing attempts in real time. By leveraging ML models like Support Vector Machine, Random Forest, and Logistic Regression, it achieves accuracy in distinguishing between legitimate and malicious URLs. The study concludes that AI-driven detection enhances cybersecurity and suggests future improvements for even faster and more accurate phishing prevention.

[8] The paper explores the growing threat of phishing emails created using AI, which makes them harder to detect due to their unique and human-like writing style. It presents a dataset of AI-created phishing emails and evaluates various ML models for detecting them. The study finds that AI-generated phishing emails differ significantly from human-written ones, allowing machine learning tools to identify them with high accuracy. The paper concludes that training detection systems with AI-generated phishing emails is crucial for strengthening cybersecurity and preventing advanced phishing scams.

[9] The paper explores the increasing threat of phishing, vishing, and smishing, emphasizing their impact on financial transactions and personal security. It highlights the limitations of existing anti-phishing solutions and proposes an intelligent detection tool combined with a security awareness program. The study introduces a fuzzy logic-based system to classify phishing emails based on both visible and hidden features. By enhancing user awareness and integrating AI-driven phishing detection, the paper aims to decrease the success rate of phishing attacks and improve cybersecurity defences.

[10] The article examines the dual impact of AI-driven chatbots on cybersecurity. It highlights how these AI models—ChatGPT, Google Gemini, and Microsoft Bing Copilot—can be both beneficial and risky. While they enhance cybersecurity

by detecting threats and aiding cyber defence, they can also be exploited by attackers to generate phishing emails, malware, and bypass security filters. The paper discusses various attack techniques, AI vulnerabilities, and strategies to improve AI defences, ultimately advocating for stronger content filtering mechanisms and ethical AI practices to mitigate cybersecurity threats.

[11] The paper explores how artificial intelligence (AI)-based ensemble learning techniques can improve phishing attack detection across websites, emails, and SMS. By reviewing 37 studies from 2019 to 2023, the research identifies commonly used methods such as AdaBoost, Bagging, and Gradient Boosting, highlighting their effectiveness in detecting phishing threats. It emphasizes the importance of open-access datasets for benchmarking AI models and suggests the expansion of optimized methods to enhance phishing detection accuracy. The study concludes that AI-driven ensemble learning provides a robust approach to mitigating phishing threats in the digital landscape.

3. OBJECTIVE OF THE STUDY

To analyse evolving phishing techniques, assess the role of AI in both attacks and defence, and study AI-driven solutions adopted for enhancing cybersecurity in IT organizations.

4. RESEARCH METHODOLOGY

The research methodology for the study involves a wide-ranging review of existing literature and categorization of various AI based phishing techniques. The data in this study were recovered from databases such as Digital Library, Springer Link, IEEE, Science Direct, Google Scholar, Internet, and etc. The study examines various AI enabled cyber-attacks and also AI based prevention techniques. The purpose of the study is to know the strengths and limitations of these methods and suggests future research directions to enhance automated systems for better phishing detection.

5. EVOLVING PHISHING THREATS FACED BY IT ORGANIZATIONS

IT organizations today are grappling with increasingly sophisticated phishing threats that exploit emerging technologies and advanced tactics. These challenges include:

1. **AI-Driven Phishing Attacks:** Cybercriminals are harnessing artificial intelligence to craft highly convincing phishing emails. These AI-generated messages can replicate the tone, style, and writing patterns of executives or trusted partners, making them more difficult to identify as fraudulent.

Case Study: In **2024**, Gmail alerted 2.5 billion users about AI-enabled phishing attacks: 2.5 billion users were targeted by malicious actors who are using AI to trick users.

2. **Business Email Compromise (BEC):** Attackers are increasingly targeting corporate email accounts to impersonate executives or vendors. These scams often involve meticulously planned tactics, sometimes enhanced by AI, to trick employees into approving fraudulent transactions.

Case Study: Ubiquiti Networks, a company, fall victim to a Business Email Compromise attack resulting loss of approximately **$46.7 million**. Hackers imitated company executives and duped employees into transferring funds to fake overseas accounts. This incident highlights the importance of verifying email requests for fund transfers, especially those that are unexpected or involve significant amounts.

3. **QR Code Phishing ("Quishing"):** A growing phishing trend involves embedding malicious QR codes in emails or documents. When scanned, these QR codes direct victims to fake websites or prompt them to unknowingly share their credentials. This tactic has been used to target government officials and can easily be adapted for corporate attacks.

Case Study: In **2023**, India witnessed a significant rise in QR code phishing scams, commonly referred to as "quishing." A prevalent tactic involved scammers sending QR codes to individuals, instructing them to scan the code to "accept" a payment of a nominal amount, such as 1 rupee. Instead of receiving money, victims unknowingly authorized a transfer, resulting in financial loss. This method was widely reported across the country.

4. **Abuse of Trusted Platforms:** Cybercriminals are leveraging legitimate services such as Google Forms and Yandex Forms to carry out phishing campaigns. Because these platforms are widely recognized and trusted, phishing attempts using them are more likely to bypass traditional security measures and appear credible to victims.

Case Study: In **2023**, cybercriminals exploited Google Forms to conduct phishing attacks. They crafted deceptive emails that appeared to be legitimate subscription notices, urging recipients to click on a link leading to a Google Form. This form, designed to look authentic, prompted users to provide personal information or credentials. The use of Google Forms, a trusted platform, allowed these phishing attempts to bypass traditional security measures and appear credible to victims.

5. **Deepfake Technology:** AI-driven deepfake audio and video are emerging as a major threat. Attackers can

manipulate voice and video recordings to convincingly impersonate executives, tricking employees into sharing sensitive data or authorizing financial transactions.

Case Study: In **2024**, Wiz, a cybersecurity company, experienced an AI-driven phishing attempt where attackers used a deepfake of CEO Assaf Rappaport's voice. The perpetrators collected audio from his conference speeches to create a convincing imitation, aiming to deceive employees into taking unauthorized actions. Fortunately, the attempt was identified and thwarted.

6. **High Frequency of Attacks:** Many organizations now face phishing attempts on a weekly or even daily basis. This relentless wave of attacks rises the threat of successful breaches and puts significant pressure on IT security teams to stay ahead of threats.

Case Study: According to the report, organizations—especially in North America—face an average of 300,000 to 400,000 telephone-based phishing attempts every day, with attack volumes peaking as high as 600,000 attempts in August 2022. This massive, relentless stream of phishing attempts illustrates how organizations are under constant threat, forcing IT security teams to work continuously to detect, block, and mitigate these attacks.

7. **Advanced Social Engineering:** Modern phishing schemes rely on extensive background research to create highly targeted and believable attacks. By gathering detailed information about their victims, attackers increase the likelihood of successfully deceiving employees, making phishing attempts even harder to detect.

Case Study: In 2023, a significant cyberattack targeted MGM Resorts, resulting in a $100 million loss. Attackers employed advanced social engineering techniques, utilizing AI to mimic voices and deceive employees into divulging sensitive information. This incident underscores the growing complexity of phishing attacks facilitated by AI, making more convincing and puzzling to detect.

Following figure shows the top 5 industries targeted for phishing scams in 2024:

- Finance & Insurance
- Manufacturing
- Services
- Technology
- Retail & Wholesale

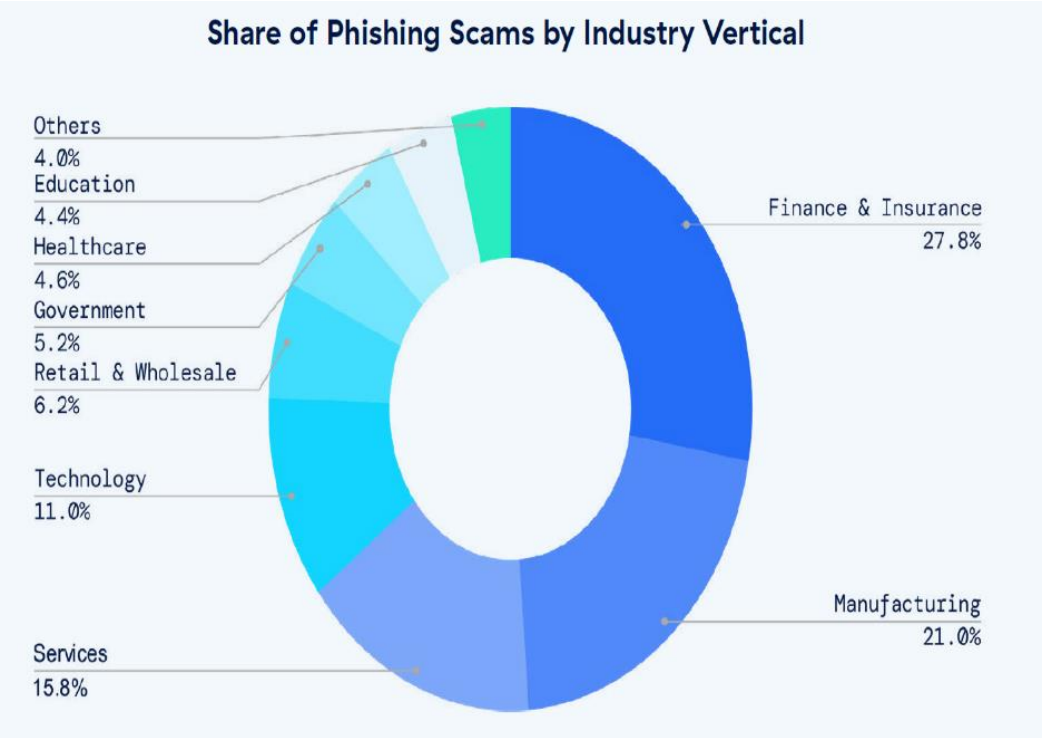

Fig 1: Top 5 industries targeted for phishing scams in 2024 [10]

The following figure shows the top 10 brands most frequently imitated in phishing scams:

- Microsoft, OneDrive, Okta, Adobe, SharePoint, Telegram, pCloud, Facebook, DHL, WhatsApp

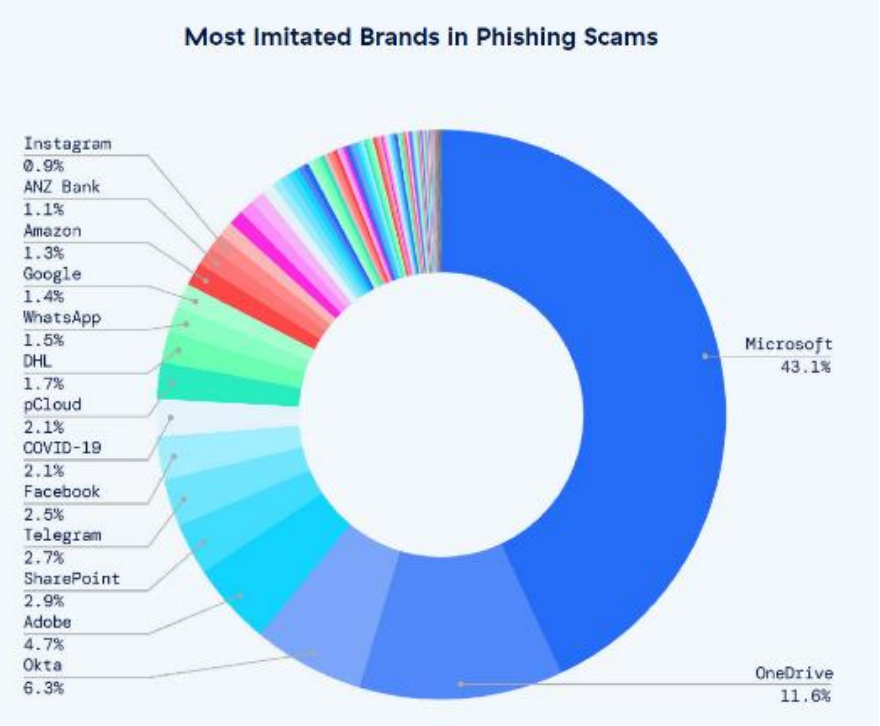

Fig 2: Most Imitated Brands in Phishing Scams [10]

6. AI TOOLS USED FOR PHISHING ATTACKS

AI-powered phishing attacks have become more sophisticated with advancements in natural language processing (NLP), image generation, and automation. Following are some AI tools and techniques used in real-world phishing attacks:

1. AI-Based Phishing Email Generators

- **Chatbots & LLMs** (e.g., ChatGPT, Gemini, Claude)
  - Attackers use generative AI models to craft convincing phishing emails, avoiding common grammatical errors that traditional phishing emails had.
  - These models help create personalized and context-aware phishing messages.
- **Deep Learning-Based Email Spoofing**
  - AI analyses email patterns and styles of a specific target to generate near-identical emails from trusted contacts.

2. AI-Powered Social Engineering & Voice Phishing (Vishing)

- **Deepfake Voice Tools** (e.g., ElevenLabs, Voicify AI)
  - AI can mimic the voice of a trusted person (e.g., CEO or manager) to trick employees into revealing sensitive information.
- **Automated Social Media Scrapers** (e.g., Maltego, OpenAI Whisper for transcribing calls)
  - AI scrapes social media to gather personal details, which attackers use to make phishing messages more convincing.

3. Image-Based Phishing (Deepfake & CAPTCHA Bypassing)

- **Deepfake Image Generators** (e.g., Stable Diffusion, MidJourney, DeepFaceLab)
  - Attackers create realistic fake images of executives to impersonate them in phishing attacks.
- **AI-Based CAPTCHA Solvers** (e.g., AI-based OCR tools like Tesseract OCR)

- Bypassing website protections to automate phishing attacks.

4. AI-Enhanced Phishing Websites

- **Automated Website Cloners** (e.g., Evilginx, Modlishka)
  - AI can generate realistic fake login pages to steal credentials.
- **AI-Powered Keystroke & Behaviour Analysis**
  - AI-based tools analyse typing behaviour to bypass 2FA protections.

5. Automated Spear Phishing Campaigns

- **AI-Based Automation Bots** (e.g., Selenium, Puppeteer)
  - Attackers use AI bots to send phishing emails at scale with adaptive responses.
- **AI-Powered Malware Generators** (e.g., WormGPT, FraudGPT - Black Hat AI models)
  - These are malicious AI variants of ChatGPT designed for cybercrime, used for phishing and malware development.

Following is the comparison table between **Traditional Phishing Attacks** and **AI-Driven Phishing Attacks**:

Table 1: It explains the comparison of traditional and AI based Phishing attack

Aspect	**Traditional Phishing Attacks**	**AI-Driven Phishing Attacks**
Attack Execution	Manually crafted emails and messages	AI automates and personalizes attacks
Email Quality	Often contains spelling and grammar errors	AI-generated messages are highly polished and convincing
Targeting	Broad, random attacks (mass emails)	Highly targeted (spear-phishing using AI data analysis)
Personalization	Uses basic data like names and emails	Uses AI to analyse social media, emails, and behaviours for personalization
Voice Phishing (Vishing)	Typically uses human impersonation	Uses deepfake AI to mimic real voices in phone scams
Website Cloning	Manually copies login pages	AI automates website cloning and makes real-time adaptive pages
Social Engineering	Relies on standard phishing scripts	AI adapts and learns from user interactions
CAPTCHA Bypass	Requires manual solving	AI-powered OCR tools solve CAPTCHAs automatically
Malware Delivery	Uses pre-programmed malware	AI-generated malware evolves to bypass security
Attack Speed & Scale	Time-consuming, requires human effort	AI automates phishing at scale, increasing efficiency
Defensive Measures	Traditional spam filters, employee awareness	Requires AI-powered security solutions to counteract

7. AI-POWERED STRATEGIES WHICH CAN BE PRACTICED FOR PHISHING PREVENTION IN IT ORGANIZATIONS

IT organizations are increasingly leveraging AI-driven solutions to combat phishing attacks. Below are some of the key AI-based strategies and tools implemented to enhance cybersecurity:

1. AI-Powered Email Security Solutions

- **Machine Learning (ML)-Based Email Filtering:** AI models analyse email metadata, content, attachments, and

sender reputation to identify potential phishing attempts.

- **Natural Language Processing (NLP):** AI detects suspicious language patterns, impersonation attempts, and social engineering tactics commonly used in phishing emails.
- **Computer Vision for Image Analysis:** AI scans embedded images to identify fake logos, brand impersonation, and QR code-based phishing attacks.
- **Behavioural Analysis:** AI monitors user email behaviour to detect anomalies, such as unexpected requests for credentials or financial transactions.

2. AI-Based Web Filtering and Threat Detection

- **Real-Time URL Analysis:** AI evaluates URL structures, domain age, and associated IP addresses to determine link legitimacy.
- **Automated Blacklisting:** AI continuously updates databases of known phishing domains, blocking access to malicious websites.
- **AI-Powered Browser Extensions:** AI-integrated browser plugins provide real-time warnings when users visit potentially harmful websites.

3. AI-Enhanced Multi-Factor Authentication (MFA) and Biometric Security

- **Adaptive Authentication:** AI assesses login behaviour, device fingerprints, and location data to determine access risks before granting entry.
- **Behavioural Biometrics:** AI analyzes factors like typing speed, mouse movements, and login patterns to detect unauthorized access attempts.

4. AI for Threat Intelligence and Incident Response

- **Automated Threat Hunting:** AI-powered Security data and Event Management systems detect phishing indicators in real time.
- **AI-Powered Security Orchestration and Response:** AI automates threat detection, blocks phishing attempts, and notifies security teams for further investigation.
- **AI Chatbots for Security Awareness Training:** AI-powered tools benefits employees to recognize and handle phishing attempts effectively.

5. Deep Learning and AI for Advanced Threat Detection

- **Deep Neural Networks for Anomaly Detection:** AI can be used to identify advanced phishing techniques, including deepfake phishing and voice phishing (vishing).
- **AI-Based Phishing Simulation & Training:** AI-driven phishing simulations enhance employee awareness and improve organizational resilience against cyber threats.

1. Some Cases of AI Solutions Adopted by Organizations for Prevention

1. Google (Gmail AI-powered Security)

- Google uses ML to spot phishing in Gmail.
- AI analyses email patterns, sender behaviour, and content to block suspicious emails.
- Google's Safe Browsing feature warns users about phishing sites.

2. Microsoft (Defender for Office 365)

- Microsoft leverages AI in **Microsoft Defender for Office 365** to identify phishing attempts.
- Uses machine learning to analyse email metadata, URLs, and attachments.
- Protects enterprises from business email compromise (BEC) attacks.

3. IBM (Watson for Cybersecurity)

- IBM's **Watson AI** assists security teams in detecting and responding to phishing attacks.
- Uses natural language processing (NLP) to analyse emails and detect anomalies.

- Enhances **IBM QRadar**, an AI-powered security information and event management (SIEM) tool.

4. Cisco (Secure Email Threat Defence)

- Cisco uses AI-powered threat intelligence in its **Secure Email Threat Defence** solution.
- Detects phishing emails based on sender reputation, behaviour analysis, and language processing.
- Cisco Umbrella provides cloud-based AI security for organizations.

5. Amazon Web Services (AWS GuardDuty)

- AWS **GuardDuty** uses AI to detect unusual login patterns and phishing attempts.
- Monitors network activity, DNS requests, and user behavior.
- Integrated with AWS security tools for cloud protection.

6. PayPal (AI Fraud Detection)

- PayPal employs machine learning to prevent phishing attacks targeting online transactions.
- AI tracks suspicious payment patterns and account activities.
- Helps identify fraudulent transactions before they happen.

7. **Cloudflare (Zero Trust AI Security)**

- Cloudflare's AI-driven **Zero Trust** security model prevents phishing by analyzing web traffic.
- Uses behavioural analytics to detect and block malicious sites.
- Protects enterprise employees from clicking on phishing links.

8. Meta (Facebook & Instagram AI Security)

- Meta employs AI to detect phishing scams on Facebook and Instagram.
- Machine learning identifies fake login pages and suspicious messages.
- Protects users from phishing links sent via Messenger.

9. O2 (Telefónica UK) – AI-powered Call Defence

- **Partnered with Hiya** to launch "Call Defence," an AI-driven scam call protection system.
- **Analyses call behaviour in real time** to detect fraudsters and alert users about suspicious calls.
- **Automatically enabled** on Android devices and iPhones with iOS 18+, protecting against voice phishing (vishing) attacks.

10. GoFundMe (AI-powered Fraud Prevention)

- **Partnership with Adyen** to implement a machine learning solution for security.
- **Launched in 2021,** the system detects fraud rings, updates block lists, and assigns risk scores.
- **Enhances protection against phishing** and fraudulent activities, ensuring a safer platform.

11. Proofpoint and Barracuda

- These products also provide sophisticated functionality like email filtering, URL scanning, and real-time threat detection.
- These products offer multi-layered defences by easily integrating with current security frameworks, including firewalls and endpoint protection.
- Proofpoint asserts that it uses AI, LLMs, NLP, and other technologies to verify over 250 data points in each email.

8. CONCLUSION

The integration of artificial intelligence into cybersecurity has fundamentally changed the way organizations combat phishing attacks. As cybercriminals employ increasingly sophisticated tactics—using AI to generate deepfakes, launch adaptive phishing campaigns, and execute social engineering scams—IT teams must deploy equally advanced defence mechanisms. This study explores how AI-driven solutions, such as machine learning-powered email filtering, natural language processing,

real-time threat detection, and behavioural analytics, are helping organizations stay ahead of these evolving threats.

However, while AI has proven to be highly effective in detecting and mitigating phishing attempts, it cannot function as a standalone solution. A comprehensive cybersecurity strategy must combine AI technologies with employee awareness programs, continuous monitoring, and shared threat intelligence. By fostering a proactive and adaptable security culture, IT organizations can outpace attackers and minimize the risks associated with phishing.

In the modern cybersecurity landscape, AI-powered systems are not just an advantage—they are essential. Investing in AI-driven innovations and ensuring their responsible implementation will allow organizations to safeguard critical assets, protect users, and reinforce trust in the digital world.

REFERENCES

[1] Abdul Basit, Maham Zafar. "A comprehensive survey of AI-enabled phishing attacks detection techniques"

[2] Shakeel Ahmad, Muhammad Zaman "Across the Spectrum In-Depth Review: AI-Based Models for Phishing Detection"

[3] Meraj Farheen Ansari, "Prevention of Phishing Attacks Using AI-Based Cyber security Awareness Training"

[4] Bhagyashree D. Shendkar, "Enhancing Phishing Attack Detection Using Explainable AI: Trends and Innovations"

[5] Muhammad Saeed Liaqat, "Exploring Phishing Attacks in the AI Age: A Comprehensive Literature Review"

[6] Blessing Guembe, Ambrose Azeta, Sanjay Misra, "The Emerging Threat of Ai-driven Cyber Attacks: A Review"

[7] Dr. K. Sudha1, S. Agalya, "AI Based Advanced Real-time Phishing Detection System Using Supervised Machine Learning Model"

[8] Chibuike Samuel Eze and Lior Shamir, "Analysis and Prevention of AI-Based Phishing Email Attacks"

[9] O. Salem , A. Hossain, M. Kamala, "Awareness Program and AI based Tool to Reduce Risk of Phishing Attacks"

[10] Muhammad Arsal, "Emerging Cybersecurity and Privacy Threats of ChatGPT, Gemini, and Copilot: Current Trends, Challenges, and Future Directions"

[11] Yazan A. Alsariera, " An Investigation of AI-based Ensemble Methods for the Detection of Phishing Attacks"

[12] Figure 1 & 2 are taken from the 2024 Phishing report of Zscaler ThreatLabz.