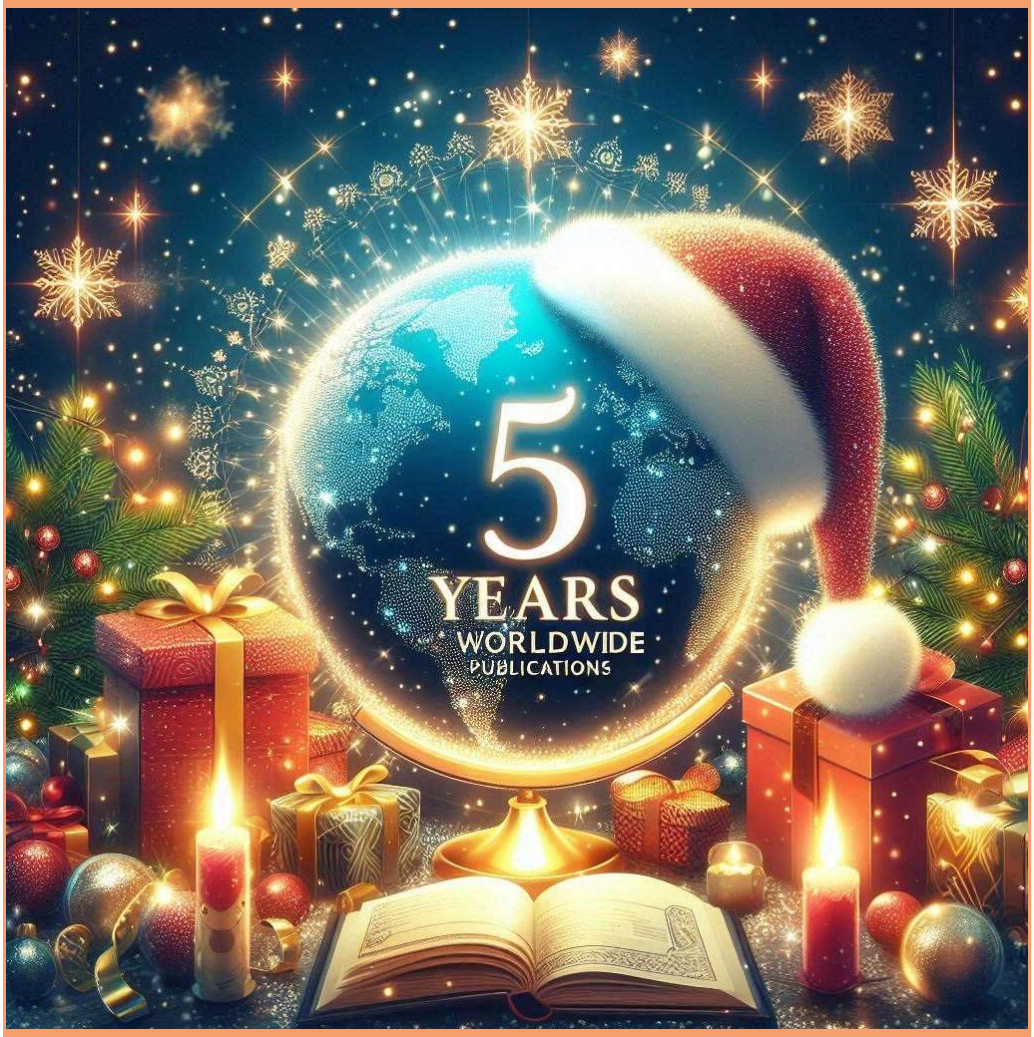
Journal of Digital Science



ISSN 2686-8296

Volume 6 Issue 2 **December 2024**

CONTENTS

The Rise of Sophisticated Phishing. How AI Fuels Cybercrime

Patricia Riurean[1][0000-0003-1683-0052], George Bolog[2][0009-0003-8381-7605], Simona Riurean[3][0000-0002-5283-6374]

[1] Smarttech247, Bucharest, Romania
[2] Booking Holdings, Bucharest, Romania
[3] University of Petrosani, Petrosani, Romania

https://doi.org/10.33847/2686-8296.6.2_2

Received 28.11.2024/Revised 11.12.2024/Accepted 23.12.2024/Published 24.12.2024

Abstract. The rapid evolution of phishing attacks has been significantly accelerated by advancements in artificial intelligence (AI), transforming these schemes into sophisticated, scalable, and highly targeted cyber threats. This article examines the historical progression of phishing, from its early days of generic mass emails to the advent of AI-powered attacks that exploit deepfake technology, adaptive strategies, and hyper-personalization. Key areas of focus include the anatomy of AI-driven phishing campaigns, real-world case studies highlighting their impact, and the unique challenges they pose to traditional security measures. The study further explores countermeasures, emphasizing AI-driven detection systems, adaptive security protocols, and enhanced training programs to mitigate these threats. By analyzing the integration of generative AI tools in phishing schemes, this article underscores the urgent need for innovative and collaborative defenses to address the rapidly evolving landscape of AI-fueled cybercrime and the need for proactive and adaptive security measures to mitigate AI-fueled threats, providing a roadmap for future research and practical implementations.

Keywords: business email compromise, spear phishing, adaptive attacks, SEG, EDR, XDR solutions

1. Introduction

Phishing began as a method for cybercriminals to obtain sensitive information like usernames, passwords, and financial details. The social engineering roots in early 1990 are the exploitation of human trust and urgency. Early examples include spoofed emails and fake login pages [1].

The history of phishing is fascinating, especially considering how far it's come from the AOL account theft scams back in the 90s, to AI driven phishing [2]. The term "phishing" caught on because it describes the tactics so perfectly: much like a fisher lure in a fish, the scammer lures their target into a trap. It's a clever and succinct way to refer to this type of malicious activity.

An article in *Computerworld* discusses the origins of phishing, noting that the term was coined around 1996 by hackers stealing AOL accounts and passwords. The article explains that these scammers used email lures, akin to fishing, to "phish" for sensitive information from internet users [3].

Early phishing emails often used poorly written, generic messages aimed at large numbers of recipients (e.g., the classic "Nigerian Prince" scam that would request money to pay for airline tickets) [4].

Mass phishing in 2000 described the emergence of bulk phishing emails with generic content. It marked a significant shift in cybercrime tactics. These bulk phishing emails were often generic and sent to large numbers of recipients, hoping to trick a

few into revealing personal information or clicking on malicious links. This method relied on the sheer volume of emails to find victims, rather than targeting specific individuals.

The year 2005 marked the transition to targeted attacks as spear phishing and whaling. Spear phishing is a more personalized attacks targeting specific individuals or organizations. It uses the basic data harvesting techniques (e.g., LinkedIn or Meta profiles) to tailor messages. Whaling points to high-value targets like executives or decision-makers, being focused on financial fraud or obtaining company secrets [5].

The evolution of phishing attacks starting from 1990 has some milestones, as presented in Figure 1.

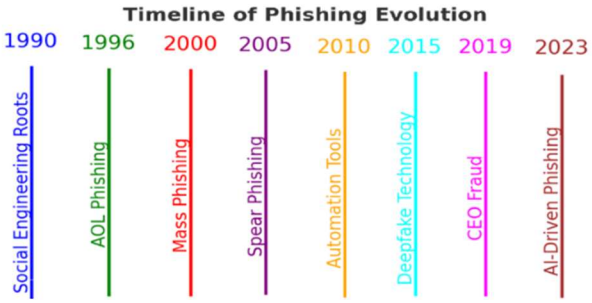


Figure 1. Milestones in phishing evolution. Source: Authors' elaboration

Phishing kits and phishing-as-a-service (PhaaS) arise in early 2010. Automation tools (e.g., phishing kits) to deploy campaigns at scale are introduced and botnets are used to send spam emails, increasing volume and reach. Phishing kits are collections of tools and resources that allow attackers to create and launch phishing campaigns with minimal technical expertise. These kits typically include (i) email templates, (ii) fake websites and (iii) automation tools. Email templates are pre-designed emails that mimic legitimate communications from trusted entities. Fake websites are cloned versions of legitimate websites to trick users into entering sensitive information. Automation tools features to automate the sending of phishing emails and the collection of stolen data [6].

PhaaS emerged as a business model where cybercriminals could purchase or subscribe to phishing services. This model included ready-made phishing kits available for purchase on the dark web. These kits came with all necessary components to launch phishing attacks and support services and support services where some providers offered customer support, updates, and even customization options for their phishing kits. The development of PhaaS lowers the technical barrier for criminals [7].

Since 2015, AI is becoming a powerful game-changer. Content (text, voice and video) can be created with various generative AI tools. AI models for text (such as ChatGPT) drastically improves phishing email quality. Sophisticated grammar, tone, and structure mimic professional communication. AI also enables multilingual phishing, therefore breaking language barriers. AI-generated audio mimicking trusted individuals for voice phishing (vishing) and deepfake video scams impersonates executives for urgent approvals (e.g., wire transfers). Hyper-personalization with Machine Learning such as data scraping profiling and behavior prediction are also advanced techniques supported by a number of "handy" tools. AI analyzes large datasets (e.g., social media, breached databases) to create highly personalized messages, therefore tailored phishing increases trustworthiness and likelihood of success. Machine Learning (ML) models predict target behavior (e.g., response patterns) to time and craft optimal messages, as well. AI systems generate and deploy

thousands of unique phishing messages in minutes and dynamic content creation adjusts messages in real time for different targets.

Conversational AI engages victims, appearing as customer support or trusted individuals and prolongs interaction aim to extract more information or induce compliance.

In 2019, cybercriminals used deepfake audio to impersonate a CEO, tricking a company into transferring a large amount of money.

Deepfake audio fraud highlights how cybercriminals exploit AI to create convincing, hard-to-detect scams.

This type of attack leverages advanced technology to mimic voices and deceive employees, making it a significant threat. However, traditional methods like phishing and business email compromise (BEC) continue to be major attack vectors. Phishing remains one of the most common cyber threats. Attackers send emails that appear to be from legitimate sources, tricking recipients into clicking on malicious links or providing sensitive information. In BEC attacks, cybercriminals impersonate company executives or trusted partners to trick employees into transferring money or revealing confidential information.

These attacks often involve careful research and social engineering to make the requests seem legitimate.

2. Anatomy of AI-Powered Phishing Attacks

AI has fundamentally transformed the phishing landscape, amplifying both the scale and sophistication of attacks. While phishing was once a manual and opportunistic technique relying on poorly crafted emails and wide-net strategies, the integration of AI has elevated phishing into a precision tool for cybercriminals.

This evolution is evident in several critical dimensions, as seen in Figure 2.

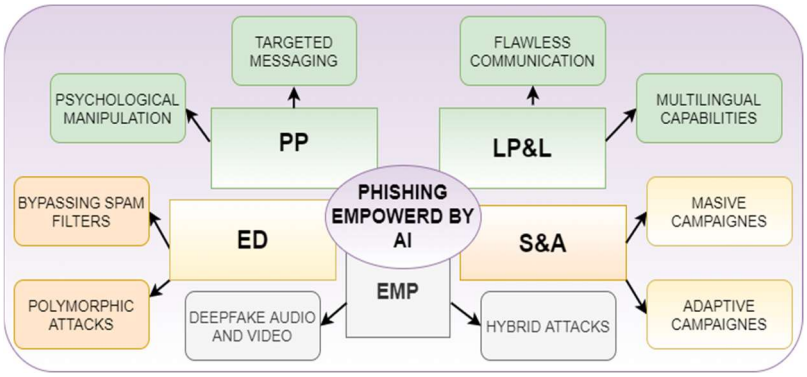


Figure 2. Phishing evolution with critical dimensions empowered by AI.
Source: Authors' elaboration

1. Precision personalization (PP) by targeted messaging and psychological manipulation.

AI enables highly personalized phishing messages by analyzing large datasets, including social media profiles, email threads, and publicly available information. ML models can predict a victim's responses and craft messages that exploit specific vulnerabilities (e.g., urgency, authority, or curiosity). An example can be the situation when AI analyzes an executive's LinkedIn profile and generates an email mimicking their tone, requesting immediate financial action.

2. Language proficiency and localization (LP&L) by flawless communication and multilingual capabilities.

Generative AI models like ChatGPT craft phishing emails that are linguistically perfect, eliminating the red flags of poor grammar or awkward phrasing. AI tools can generate phishing content in multiple languages, enabling attacks on a global scale. As a possible situation can be a phishing campaign targeting employees in different countries can seamlessly adapt language and cultural references.

3. Scale and automation (S&A) by massive campaigns and adaptive campaigns.

AI-powered tools can generate and distribute thousands of unique phishing emails in minutes, each tailored to its recipient. AI dynamically adjusts phishing strategies based on real-time feedback, increasing success rates. For example, if an email bounces or is flagged, AI can tweak the message and resend it to bypass filters.

4. Emergence of multi-modal phishing (EMP) by deepfake audio and video or hybrid attacks.

AI creates realistic audio and video impersonations of trusted individuals, such as CEOs or family members. AI combines phishing emails with deepfake calls to reinforce urgency and legitimacy. A deepfake voicemail instructs an employee to urgently approve a financial transaction initiated by a fraudulent email, can be a good example [8].

5. Evasion of detection (ED) by bypassing spam filters and polymorphic attacks.

AI-generated emails avoid patterns typically flagged by spam filters. AI continuously alters email content to evade signature-based detection systems.

For example, each phishing email contains unique phrasing while maintaining the same malicious intent.

AI has significantly transformed the phishing landscape, making attacks more sophisticated and harder to detect.

There are some key ways AI has impacted phishing, as seen in Figure 3.

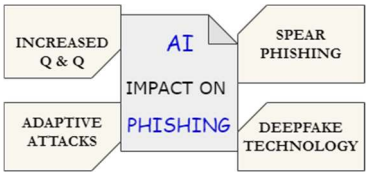


Figure 3. Key ways that AI impact phishing attacks. Source: Authors' elaboration

Increased quantity and quality (Q&Q) - AI enables cybercriminals to generate and distribute phishing content at an unprecedented rate. AI tools can create highly convincing emails that are grammatically correct and tailored to specific targets [9].

Spear phishing - AI can automate the research and targeting process for spear-phishing attacks. By analyzing large datasets, AI can craft personalized messages that are more likely to deceive the recipient [10].

Deepfake technology - AI-powered deepfake audio and video can be used to impersonate executives or trusted individuals, making scams like BEC even more convincing [11].

Adaptive attacks - AI allows attackers to quickly adapt to new security measures, developing more sophisticated scams that can bypass traditional defenses [11].

Adaptive attacks as a sophisticated form of cyber threats, dynamically adjust their tactics in response to the defenses they encounter. Unlike traditional attacks, which follow a predefined method, adaptive attacks continuously evolve to exploit vulnerabilities and bypass security measures. Advanced technologies like ML and behavioral analysis are used to modify these strategies in real-time. This allows

attackers to respond to the defenses they encounter and find new ways to penetrate systems [12].

These attacks often employ multiple tactics simultaneously, such as combining phishing with malware or DDoS attacks. This multi-vector approach makes them more challenging to defend against. Adaptive attacks learn from each attempt, improving their effectiveness over time. The success and/or failure of previous attacks are analyzed to refine novel methods [13].

By continuously monitoring and analyzing their target, adaptive attacks can identify and exploit specific vulnerabilities, making them highly effective against well-protected systems [14].

To defend against adaptive attacks, organizations need to implement adaptive security measures that includes behavioral analysis to continuously monitor user and system behavior to detect anomalies, advanced ML algorithms to predict and respond to evolving threats, and real-time response by implementing systems that can automatically adjust defenses in response to detected threats [12,13].

These strategies help create a more resilient security posture capable of withstanding the dynamic nature of adaptive attacks.

3. AI's Means of Eluding Detection Systems

The adaptability and intelligence of AI bring significant challenges for traditional security systems designed to detect phishing attempts.

By leveraging ML and dynamic content generation, AI-powered phishing attacks have become increasingly proficient at bypassing spam filters and detection mechanisms.

AI makes available dynamic alteration of an email subject lines by modifying it to align with trends, keywords, or personalization that make emails appear legitimate. Also, generative AI tools modify the email content in real time, altering word choices, sentence structures, and formatting to avoid detection by pattern-matching algorithms.

AI dynamically alters URLs by using randomized or contextually appropriate domains that mimic trusted entities while redirecting victims to malicious sites. For example, a phishing campaign targeting HR professionals might adapt email content to reference specific job platforms or hiring trends, enhancing plausibility.

ML algorithms play a critical role in identifying weaknesses in filters and refining success metrics. AI analyzes how spam filters function, and learns which email characteristics are less likely to trigger suspicion. By tracking which emails get delivered and produce responses, AI improves future phishing attempts for maximum effectiveness. If a specific subject line results in higher email delivery rates, AI algorithms can replicate similar patterns across future campaigns.

Polymorphic phishing campaigns build attacks that continuously evolve to stay ahead of detection systems. AI enables real-time adjustments by altering email content between delivery and user interaction to evade detection mechanisms and unique instances by generating different versions of the same phishing email for each recipient to avoid detection by signature-based systems. A polymorphic email campaign might send one version of a message to a user's work email and another to their personal email, each tailored to the context.

AI exploit human and systemic gaps using behavioral mimicry and social engineering synergy. AI tools can emulate human-like behaviors, such as delays in responses or time-based email sends, to mimic legitimate communication patterns. By integrating dynamic content generation with insights from data breaches or social media, AI crafts messages that exploit human trust. For example, AI might generate

a phishing email pretending to be from an IT department, sent precisely during an organizational system update.

There are important implications for traditional security systems since false negatives are considerable increased and defenses mechanisms are overwhelmed and the human oversight is reduced. Traditional systems rely heavily on static rules and known patterns. AI's ability to create unique, ever-changing content renders these rules insufficient. AI enables phishing at scale, overwhelming even sophisticated spam filters with a flood of credible-looking emails. The realism of AI-generated phishing emails makes them harder for users to flag, relying heavily on automated systems for detection.

4. Real-Life Attacks and Alerts

Recent attacks leveraging AI tools like ChatGPT craft realistic spear-phishing emails. Detection becomes harder as phishing messages and interactions resemble legitimate communication, therefore traditional anti-phishing tools struggle against the sophistication of AI-powered tactics [15].

The spear-phishing attack on the RSA (one of the world's top computer-security companies in 2011) was a pivotal moment in cybersecurity history. Attackers used a targeted approach, sending malicious Excel files to specific employees.

Once these files were opened, the attackers gained access to sensitive data, including information related to RSA's SecurID two-factor authentication products [16]. This attack was a textbook example of a sophisticated spear-phishing campaign [17].

The key elements are:

- phishing emails - the attackers sent emails with the subject line "2011 Recruitment Plan" to a small group of RSA employees over two days. These emails were designed to look legitimate and enticing.
- malicious attachment - One employee retrieved the email from their junk folder and opened the attached Excel file. This file contained malware that exploited a zero-day vulnerability in Adobe Flash.
- zero-day exploit - the malware used an unknown flaw in Adobe Flash to install a backdoor on the employee's computer. Adobe later released a patch to fix this vulnerability.
- remote control - once the backdoor was installed, the attackers could remotely control the compromised machine. They stole several account passwords from the employee and used them to access other systems within RSA.
- lateral movement - with these credentials, the attackers moved laterally within RSA's network, gaining access to sensitive data and other employees' accounts.

This breach highlighted several key points:

- targeted attacks - even well-protected organizations can be vulnerable to sophisticated, targeted phishing attacks.
- human factor - the attack underscored the importance of employee awareness and training in cybersecurity.
- widespread impact - the stolen data had far-reaching implications, affecting numerous organizations that relied on RSA's security products.

It was a stark reminder that no organization is immune to phishing and that continuous vigilance and robust security measures are essential. The incident highlighted the importance of patching software vulnerabilities promptly and the need for robust email security and employee training to recognize phishing attempts.

The CEO of an UK-based energy firm believed he was on the phone with his boss, the chief executive of firm's the German parent company while he was asked to transfer more than $200,000. The attackers used AI to create a convincing imitation

of the CEO's voice, complete with a recognizable accent and speech patterns. The fake CEO called the employee, urgently requesting a transfer to a Hungarian supplier, assuring that it was critical and would be reimbursed. Trusting the voice, the employee complied and transferred the funds. The money was then funneled through various accounts, making it difficult to trace. This incident highlighted the growing threat of deepfake technology in cybercrime and the importance of verifying unusual requests, even when they appear to come from trusted sources [18].

The utilisation of secure and encrypted internet connections, such as virtual private networks (VPNs) or HTTPS websites, is instrumental in safeguarding personal data transmitted over networks. It is imperative that Wi-Fi networks employ encryption mechanisms, such as WPA2 or WPA3, to ensure network security. Public Wi-Fi networks that lack encryption are susceptible to cyberattacks. To mitigate this risk, it is essential to disable the personal device's automatic connection to Wi-Fi networks within range. This measure prevents the device from connecting to potentially malicious networks without the user's awareness [19].

The U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) issued an alert (on 13th of November, 2024) to help financial institutions identify fraud schemes associated with the use of deepfake media created with generative artificial intelligence (GenAI) tools [20].

The FinCEN alert [21] highlights the increasing use of deepfake technology by fraudsters to create fake identification documents, photographs, and videos. These deepfakes are used to access other individuals' accounts or open fraudulent accounts, facilitating various types of cybercrime.

The FinCEN alert highlights its commitment to equipping financial institutions with the tools and knowledge necessary to combat the rising threat of AI-enhanced fraud. The alert focuses on: FinCEN categorizes and explains the methods criminals use in AI-enhanced fraud, such as:

- BEC;
- Deepfake identity fraud;
- AI-facilitated phishing and social engineering attacks.

These typologies help financial institutions understand the diverse ways AI can be misused to exploit vulnerabilities in the financial system.

The alert provides red flag indicators that financial institutions can use to detect suspicious activity, including:

- Unusual or inconsistent documentation - AI-generated fake IDs and documents often have subtle anomalies;
- Behavioral patterns - transactions or communications that deviate from an account holder's normal activity;
- High-frequency account openings or transfers - indicators of fraudulent accounts or money laundering schemes.

The alert reminds institutions of their responsibilities under the Bank Secrecy Act (BSA):

- Filing Suspicious Activity Reports (SARs) when AI-enabled fraud is suspected;
- Monitoring and reporting patterns that may indicate broader criminal activity.

Key points from the alert include:

- Criminals use deepfake media to create realistic but fraudulent identification documents to bypass identity verification processes.
- Deepfake technology is also used in BEC schemes, spear phishing attacks, elder financial exploitation, family emergency schemes, romance scams, and virtual currency investment scams.

This alert underscores the need for enhanced vigilance and advanced security measures to combat the evolving threats posed by deepfake technology [22].

5. AI Tools as Countermeasures

To combat the growing threat of AI-driven phishing a number of compulsory measures can be to adopt for defense. The using of ML models to detect anomalies in communication patterns and identify suspicious activities, apply regularly update phishing awareness programs to address AI-enabled tactics and implement multi-factor authentication and secondary approvals for critical transactions. AI-driven tools that analyze communication patterns and flag deviations from typical behavior can be implemented. Systems that check for subtle anomalies in URLs, such as similar-looking characters or misleading domains can be used. Threat intelligence systems to track evolving AI-driven phishing techniques and update defenses in real-time can be also deployed [23].

Secure Email Gateway (SEG) is a critical component of organizational cybersecurity strategies, evolving to address increasingly sophisticated email threats. By integrating machine learning, threat intelligence, and advanced detection techniques, SEGs combat both traditional and modern email threats. SEG is designed to protect organizations from malicious email-based threats. By analyzing email traffic, SEGs block spam, phishing attempts, malware, and advanced threats like BEC.

However, their effectiveness is maximized when paired with complementary security solutions, such as Extended Detection and Response (XDR) and Endpoint Detection and Response (EDR) advanced solutions [24].

XDR solutions have become essential in modern cybersecurity, offering integrated threat detection and response across various digital environments. XDR enables organizations to detect threats across multiple domains (e.g., endpoints, networks, cloud) before they cause harm.

Some of the most powerful XDR platforms available today are CrowdStrike Falcon XDR, enhanced by its AI-driven platform "Charlotte AI," (Figure 4). It provides comprehensive endpoint protection with real-time threat detection and response capabilities. Its cloud-native architecture ensures rapid data processing, enabling security teams to swiftly investigate incidents and proactively hunt for threats [25].

Figure 4. CrowdStrike Falcon XDR. Source [26]

Sentinel One's platform offers autonomous security solutions for various IT environments, focusing on endpoint, cloud, and identity security. It delivers prevention, detection, response, remediation, and forensics within a single platform.

Microsoft Defender Advanced Threat Protection (MDATP), now part of Microsoft Defender for Endpoint, is a comprehensive security solution to protect against, detect, and respond to threats. With the integration of Microsoft Copilot, the platform extends its capabilities to include AI-driven automation.

Palo Alto Networks Cortex XDR is a comprehensive platform that integrates network, endpoint, and cloud data to detect and respond to threats. It utilizes machine learning and behavioral analytics to identify sophisticated attacks and streamline investigations.

Trend Micro's Vision One extends threat detection and response across an organization's digital landscape. It delivers advanced threat intelligence using a layered approach to protect against a wide range of cyber threats.

The most appropriate XDR solution must offer integration capabilities with existing infrastructure, scalability, ease of use, and the specific security needs of organization.

A comparative study of the XDR solutions presented above with details on their key features, strengths, challenges, and ideal use cases is presented in Table 1.

Table 1. Comparative study of the XDR solutions

XDR Solution	Key Features	Strengths	Challenges	Best For
CrowdStrike Falcon XDR (Charlotte AI)	AI-powered insights, guided investigations, global threat intelligence, real-time threat graph	High-speed detection and response, scalability, intuitive AI	Premium pricing, training required for advanced features, potential integration issues with non-Crowd Strike tools	Organizations needing fast, scalable, and AI-driven threat detection and response
SentinelOne Singularity XDR	Autonomous AI, endpoint/cloud/identity security, prevention and remediation within one platform	Comprehensive security coverage, AI-driven automation, user-friendly interface	Cost for advanced features, may require adaptation for non-standard environments	Businesses seeking autonomous, AI-driven security across endpoint and cloud
Microsoft Defender XDR (Copilot)	Cross-domain integration, natural language querying, automated response, scalable cloud-native architecture	Tight integration with Microsoft ecosystem, ease of use, strong threat intelligence	Limited compatibility with non-Microsoft tools, potential privacy concerns in regulated industries	Enterprises heavily reliant on Microsoft tools and services
Palo Alto Networks Cortex XDR	Network, endpoint, and cloud data integration, behavioral analytics, machine learning	Advanced analytics and detection, seamless multi-domain integration, detailed investigation tools	Resource-intensive setup, higher cost for full functionality	Organizations requiring deep analytics across multiple domains
Trend Micro Vision One XDR	Layered threat intelligence, advanced detection for diverse environments, integration across endpoints	Cost-effective for SMBs, strong layered approach to threat detection, efficient cross-domain insights	Limited features compared to other XDR leaders, may require additional tools for full coverage	SMBs and mid-sized enterprises looking for cost-effective layered security

6. Conclusion

The most challenging aspects regarding the AI-driven phishing are their increased complexity wide accessibility and rapid evolution. The realism of AI-crafted content makes phishing harder to detect through traditional methods. The availability of AI tools lowers the barrier for entry allowing even low-skill cybercriminals to launch sophisticated attacks. AI enables constant innovation in phishing techniques outpacing the development of countermeasures. XDR solutions are invaluable for modern organizations, offering comprehensive threat detection, incident response, and operational efficiency across diverse environments. By unifying visibility, automating responses, and enhancing proactive defense, XDR empowers organizations to address increasingly sophisticated threats. Implementing XDR solution can significantly enhance an organization's cybersecurity posture, but it also presents several challenges.

References

1. T. P. Fowdur and L. Veerasoo "An email application with active spoof monitoring and control" 2016 International Conference on Computer Communication and Informatics (ICCCI) Coimbatore India 2016 pp. 1-6 doi: 10.1109/ICCCI.2016.7480002
2. J. Chen and C. Guo "Online Detection and Prevention of Phishing Attacks" 2006 First International Conference on Communications and Networking in China Beijing China 2006
3. Russell Kay Sidebar: The Origins of Phishing 2004 https://www.computerworld.com/article/1325606/sidebar-the-origins-of-phishing.html?utm_source=chatgpt.com last accessed 2024/12/21
4. Okosun O. and Ilo U. (2023) "The evolution of the Nigerian prince scam" Journal of Financial Crime Vol. 30 No. 6 pp. 1653-1663. https://doi.org/10.1108/JFC-08-2022-0185
5. P. Y. Leonov A. V. Vorobyev A. A. Ezhova O. S. Kotelyanets A. K. Zavalishina and N. V. Morozov "The Main Social Engineering Techniques Aimed at Hacking Information Systems" 2021 Ural Symposium on Biomedical Engineering Radioelectronics and Information Technology (USBEREIT) Yekaterinburg Russia 2021 pp. 0471-0473 doi: 10.1109/USBEREIT51232.2021.9455031
6. F. Castaño E. F. Fernañdez R. Alaiz-Rodríguez and E. Alegre "PhiKitA: Phishing Kit Attacks Dataset for Phishing Websites Identification" in IEEE Access vol. 11 pp. 40779-40789 2023 doi: 10.1109/ACCESS.2023.3268027
7. F. Ilca and T. Balan "Phishing as a Service Campaign using IDN Homograph Attack" 2021 International Aegean Conference on Electrical Machines and Power Electronics (ACEMP) & 2021 International Conference on Optimization of Electrical and Electronic Equipment (OPTIM) Brasov Romania 2021 pp. 338-344 doi: 10.1109/OPTIM-ACEMP50812.2021.9590028
8. Gandhi Kashish et al. "A Multimodal Framework for Deepfake Detection." arXiv preprint arXiv:2410.03487 (2024)
9. Fredrik Heiding Bruce Schneier and Arun Vishwanath AI will Increase the Quantity — and Quality — of Phishing Scams 2024 https://hbr.org/
10. URL: https://www.microsoft.com/ How AI is changing phishing scams last accessed 2024/12/21
11. Georg Lindsey AI-Powered Phishing Scams: Smarter and More Dangerous 18 Dec 2024 https://cgnet.com/ last accessed 2024/12/21
12. URL: https://www.bitdefender.com/en-us/blog/businessinsights/principles-of-adaptive-cybersecurity-in-a-dynamic-threat-landscape last accessed 2024/12/21
13. URL: https://www.edgenext.com/what-is-adaptive-threat-modulation-and-why-is-it-key-for-ddos-resilience/ last accessed 2024/12/21
14. URL: https://www.bitsight.com/blog/what-adaptive-security-and-how-it-can-benefit-your-organization
15. M. Corbett and S. Sajal "AI in Cybersecurity" 2023 Intermountain Engineering Technology and Computing (IETC) Provo UT USA 2023 pp. 334-338 doi: 10.1109/IETC57902.2023.10152034

16. J. Epstein "Phishing Our Employees" in IEEE Security & Privacy vol. 12 no. 3 pp. 3-4 May-June 2014 doi: 10.1109/MSP.2014.51
17. E. Weippl "Advanced persistent threats & social engineering" 2014 5th International Conference on Data Communication Networking (DCNET) Vienna Austria 2014
18. Catherine Stupp Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case. Scams using artificial intelligence are a new challenge for companies 2019 https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402 last accessed 2024/12/21
19. Antipova T., Riurean S. Managing cyber resilience literacy for consumer. International Journal of Informatics and Communication Technology (IJ-ICT), 14(1), 2025, 122-131. https://doi.org/10.11591/ijict.v14i1.pp122-131
20. Thomas C. Kost Filipp Kofman Max Bonici and Michael Treves Deepfake Technology to Circumvent Controls. A recent FinCEN alert highlights an increase in reports of deepfake identity fraud and describes ways financial institutions can reduce risk and detect the illicit use of AI tools November 2024 https://www.dwt.com/
21. URL:https://www.fincen.gov/news/news-releases/fincen-issues-alert-fraud-schemes-involving-deepfake-media-targeting-financial last accessed 2024/12/21
22. Kristen E. Larson FinCEN Alert: Fraud schemes using generative artificial intelligence to circumvent financial institutions' identity verification authentication and due diligence controls November 20 2024 https://www.consumerfinancemonitor.com/
23. Moldovan D., Riurean S. Cyber-Security Attacks, Prevention and Malware Detection Application. J. Digit. Sci. **4**(2), 3 – 23 (2022). https://doi.org/10.33847/2686-8296.4.2_1
24. Simona Riurean, Concepte și tehnologii noi de comunicații în arhitecturi de rețele / Novel Communications Concepts and Technologies in Network Architectures, Universitas Petroşani, 2023, 528 pg. ISBN:978-973-741--948-4
25. K. Jakimoski, "Automation Improvement in Cyber Risk Management," 2023 International Conference on Software, Telecommunications and Computer Networks (SoftCOM), Split, Croatia, 2023, pp. 1-6, doi: 10.23919/SoftCOM58365.2023.10271658.
26. URL: https://www.crowdstrike.com/platform/endpoint-security/falcon-insight-xdr/

Aims and Objectives

Published online by Institute of Cited Scientists, Cyprus, two times a year, Journal of Digital Science (JDS) is an international peer-reviewed journal which aims at the latest ideas, innovations, trends, experiences and concerns in the field of digital science covering all areas of the scholarly literature of the sciences, social sciences and arts & humanities.

The main goal of this journal is the effective dissemination of original incites/results generated by the human brain and presented/reflected in articles using modern information/digital technology.

Current Issue is 11th issue of Journal of Digital Science for five years of publishing. The main subjects currently covered include: Telecommunication, Cyber threats, Deep Learning, Neural Network Technologies.

Contact information

Journal URL: https://ics.events/journal-of-digital-science/
Email: conf@ics.evnets
Printed online from the original layout under the imprint at:
1, Vlachou, Nicosia, The Republic of Cyprus