International Journal of Educational Innovations and Research
Volume 1 | Issue 4 | October-December 2025 | ISSN 3049-4052
Peer Reviewed (Referred Journal)

Trends in Cybersecurity with Unethical Hacking

Ibikunle, Frank Ayoleke

Electrical and Electronic Engineering Department, Hensard University, Bayelsa State, Nigeria

Email: prof.ibikunle@hensarduniversity.edu.ng

Abstract

The landscape of cybersecurity in 2025 is characterized by rapidly evolving threats and increasingly sophisticated attack methodologies, with unethical hacking (commonly known as black-hat hacking) representing a critical challenge to global digital infrastructure. This paper presents a comprehensive examination of current trends in cybersecurity through the lens of unethical hacking, emphasizing the techniques employed by adversaries, the emerging threat vectors, and the consequential impact on defensive mechanisms. The study differentiates between ethical and unethical hacking, clarifying their roles within the cybersecurity ecosystem, and underscores the necessity of understanding malicious hacking trends to anticipate and counteract attacks effectively. Key findings reveal that phishing, ransomware-as-a-service platforms, and social engineering continue to dominate attack strategies, increasingly augmented by artificial intelligence, enabling high-volume, adaptive, and evasive campaigns. Exploit frameworks, automation tools, and vulnerabilities in expanding Internet of Things environments broaden attackers' capabilities. The paper details high-profile incidents illustrating the operational and financial damages sustained by sectors such as healthcare, finance, and critical infrastructure. Emphasis is placed on the importance of integrating ethical hacking practices, regulatory compliance, and cross-sector collaboration to build resilience against these threats. Finally, it outlines future directions, including quantum-resistant cryptography, AI-enhanced response systems, and dynamic defense frameworks, as critical to adapting to a complex threat environment. This paper aims to provide cybersecurity researchers, practitioners, and policymakers with an integrated understanding of the current unethical hacking landscape and strategic insights to foster more effective prevention and mitigation approaches

Keywords

Ethical and unethical hacking; cybersecurity; Phishing and social engineering; AI; Cybercriminals

1. Introduction

The cybersecurity landscape in 2025 is more complex and urgent than ever, driven by the fast digitization of global economies, the rise of connected devices, and the increasing sophistication of cyber threats. As organizations rely more on cloud infrastructure, Internet of Things (IoT) ecosystems, and artificial intelligence (AI)-enabled systems, the attack surface has expanded significantly. Traditional perimeter defenses are no longer effective. Recent reports show that cyberattacks are happening more often and are more advanced. They now include AI-driven tactics like polymorphic malware, deepfake-enabled social engineering, and ransomware-as-a-service (RaaS) models that target critical infrastructure and supply chains. For example, the World Economic Forum's Global Cybersecurity Outlook 2025 points to a rise in ransomware, AI-enhanced phishing, and supply chain breaches. This highlights how threat actors, from nation-state groups to cybercriminals, are exploiting both human weaknesses and technical flaws. These trends indicate a major shift where unethical hacking, driven by malicious intent for profit, spying, or disruption, has evolved into automated, adaptable operations that challenge even the strongest security measures.

This paper is motivated by the growing gap between offensive capabilities and defensive readiness. As noted in Deloitte's 2025 Cyber Threat Trends Report, adversaries are using zero-day exploits and hybrid attack methods, while organizations face skills shortages and regulatory pressures. Unethical hacking takes advantage of this imbalance, with incidents like AI-driven vishing and business email compromise (BEC) highlighting human vulnerabilities. Meanwhile, ethical countermeasures remain underdeveloped. There is a pressing need to analyze trends that help defenders anticipate and counter threats. This study aims to close this gap, especially in places like Nigeria, where local threats increase global risks. The main goals of this paper are threefold: (1) to analyze current and emerging trends in unethical hacking techniques, including AI-supported attacks and supply chain weaknesses; (2) to assess defensive strategies such as zero-trust architecture, quantum-resistant cryptography, and automated threat hunting; and (3) to suggest practical frameworks for organizations to strengthen their resilience against evolving cyber threats. By gathering insights from industry reports and threat intelligence, this research intends to cover technological, human, and regulatory aspects of cybersecurity, highlighting practical implications for stakeholders.

This paper is structured into seven sections that build from basic concepts to future strategies. The first section introduces cybersecurity paradigms, the second looks at unethical hacking trends, the third discusses ethical hacking methods, the fourth investigates AI's dual role, the fifth covers legal frameworks, the sixth provides case studies, and the seventh looks ahead at future directions. The additional sections include methodology, results, discussion, and conclusions, offering a complete roadmap for advancing cybersecurity.

2. Techniques and Tools Used in Unethical Hacking

Unethical hacking involves the use of diverse methodologies and advanced tools to exploit vulnerabilities in computer systems, networks, and applications. Attackers employ a spectrum of techniques, ranging from social engineering and phishing campaigns to sophisticated malware deployment and ransomware attacks. Common hacking methodologies underpinning unethical hacking include phishing, malware, ransomware, and social engineering, each leveraging specific vulnerabilities in technical or human elements.

Phishing represents one of the most widespread and effective attack vectors, where malicious actors craft deceptive emails, websites, or messages aimed at tricking victims into divulging sensitive information such as usernames, passwords, or financial details. The increasing sophistication of phishing campaigns now includes AI-generated personalized content and deepfake media to mimic trusted sources, thereby improving success rates (Anomali, 2023). Malware deployment encompasses various malicious software forms, including viruses, worms, trojans, spyware, and ransomware. Ransomware poses a particularly severe threat by encrypting victim data and demanding payment for decryption keys. The rise of ransomware-as-a-service (RaaS) platforms has significantly lowered the barrier for criminal enterprises, enabling widespread and rapid propagation of ransomware attacks globally (LinkedIn, 2024; SentinelOne, 2025). Social engineering exploits psychological manipulation to bypass traditional cybersecurity defenses by targeting human decision-making. Techniques such as pretexting, baiting, and impersonation are frequently employed to acquire unauthorized access or confidential information. Notably, the human element remains a primary weakness in cybersecurity, making social engineering a persistent and adaptive threat (Craw.in, 2025).

Unethical hackers also leverage powerful exploit frameworks and automated tools that facilitate scalable and efficient attacks. Metasploit, an open-source penetration testing framework, is widely exploited to discover and utilize vulnerabilities in target systems. It enables attackers to automate complex exploits and payload generation, enhancing their ability to penetrate defenses quickly (Codecademy, 2025). In addition to Metasploit, custom scripts and software kits are crafted to automate brute-force attacks, vulnerability scanning, and information gathering, increasing attack efficiency and anonymizing threat actors (LinkedIn, 2024).

Emerging attack vectors are reshaping the threat landscape, expanding the scope of potential targets. The rapid growth of IoT devices has introduced numerous security gaps due to limited device security, default configurations, and the heterogeneity of devices. Cybercriminals exploit weaknesses in consumer and industrial IoT devices to gain footholds for lateral movement and to mount large-scale attacks such as distributed denial-of-service (DDoS) campaigns or data exfiltration (IBM, 2025; LinkedIn, 2024). Moreover, AI-based attacks represent a new frontier, where machine learning models are manipulated or weaponized to evade detection systems, generate phishing content, or autonomously adapt malware behavior. The dual-use nature of AI technology fuels an arms race between attackers developing AI-powered tools and defenders employing AI to detect and mitigate threats (Darktrace, 2025).

Recent high-profile cases illustrate the impact and evolving nature of unethical hacking. For example, the 2023 ransomware attack on the healthcare sector in Singapore resulted in prolonged disruption of critical services, demonstrating the operational risk posed by ransomware. Similarly, a data breach on a major e-commerce platform exposed millions of users' sensitive data, underscoring the widespread consequences of inadequate security postures (LinkedIn, 2024; SentinelOne, 2025). Distributed Denial of Service (DDoS) attacks continue to impair service availability, as seen in a 2023 incident where government websites faced prolonged outages due to traffic overload from botnet armies. These cases illustrate the multifaceted and growing challenge unethical hacking presents, highlighting the necessity for advanced detection mechanisms and proactive mitigation strategies. Organizations must adopt an integrated approach combining technology, user awareness, and threat intelligence to stay ahead of increasingly automated and AI-enhanced attacks.

3. Evolving Threat Landscape and Attack Trends

The cybersecurity threat landscape in 2025 is marked by increasing complexity, sophistication, and frequency of attacks, driven by the escalation of adversarial capabilities and expanded attack surfaces. A surge in ransomware operations targeting critical infrastructure, healthcare, financial services, and government sectors has been a defining trend. Sophisticated ransomware groups employ double extortion techniques, encrypting valuable data while simultaneously threatening to publicly release sensitive information unless ransom demands are met. This evolution amplifies both the operational disruption and reputational damage to affected organizations (Cloud Security Alliance, 2025; SentinelOne, 2025).

Nation-state actors continue to significantly influence the evolving threat environment by launching persistent and highly sophisticated cyber-espionage campaigns targeting government entities, defense contractors, and strategic industries. These attacks aim to extract sensitive intelligence, disrupt operations, and assert geopolitical influence, often operating under the radar for extended periods. The average dwell time for such state-sponsored breaches frequently exceeds 400 days, enabling adversaries to maintain prolonged access and cause substantial harm (Darktrace, 2025).

The Internet of Things (IoT) has emerged as a substantial expansion of the attack surface, introducing new vulnerabilities due to limited security controls, default configurations, and the heterogeneity of devices. Cybercriminals exploit weaknesses in consumer and industrial IoT devices to gain footholds for lateral movement and to mount large-scale attacks such as distributed denial-of-service (DDoS) campaigns or data exfiltration. With billions of connected IoT devices, securing these endpoints remains a critical and ongoing challenge (Fortinet, 2024; Cloud Security Alliance, 2025).

Artificial Intelligence (AI)-powered attacks represent a transforming vector in the threat landscape. Malicious actors utilize AI and machine learning to automate reconnaissance, craft highly convincing phishing campaigns, evade traditional detection mechanisms, and adapt malware behaviors dynamically. For example, AI-generated phishing emails feature high volumes of realistic text to deceive filters and human recipients alike. The use of large language models (LLMs) enables attackers to scale social engineering efforts rapidly and with enhanced believability, which elevates the risk across all sectors (Darktrace, 2025).

Phishing and social engineering remain among the most prevalent techniques utilized to compromise users and gain initial access to networks. The sophistication of these attacks has increased with the integration of deepfake technology to impersonate trusted voices and executives during video calls or audio communications. This advancement significantly raises the bar for defense, compelling organizations to implement stronger user education programs and verification protocols (World Economic Forum, 2025).

Supply chain attacks also remain a critical concern, as cybercriminals increasingly target third-party vendors to infiltrate larger corporate ecosystems. High-profile incidents, such as the SolarWinds breach, have highlighted the devastating ripple effects caused by supply chain compromises. Organizations are now adopting stringent third-party security assessments, continuous monitoring, and contractual obligations to manage these risks effectively (CrowdStrike, 2025).

In parallel, the impending advent of quantum computing adds a layer of complexity to cybersecurity preparedness. While still emerging, quantum computing threatens to render conventional cryptographic algorithms obsolete, urging early adoption of quantum-resistant cryptography. In anticipation, research and development efforts are underway to safeguard critical information infrastructures against future quantum decryption capabilities (Cloud Security Alliance, 2025).

The hybrid workforce model, which integrates remote, on-site, and contracted personnel, has intensified insider threats and increased risks arising from misconfigurations in cloud environments. Human error, when combined with sophisticated phishing or malware campaigns, contributes significantly to the overall vulnerability profile. Organizations now turn to behavioral analytics and data loss prevention (DLP) technologies to detect anomalous actions and enforce stricter data protection policies (SentinelOne, 2025). In summary, the 2025 threat landscape is characterized by increasingly automated, AI-enhanced, and multi-vector attacks that challenge traditional defense paradigms. Effective cybersecurity strategies necessitate an adaptive posture that leverages cutting-edge technologies, robust governance, and cross-sector collaboration to anticipate and mitigate emerging threats.

4. Impact of Unethical Hacking on Cybersecurity Defenses

Unethical hacking presents substantial challenges to traditional cybersecurity defenses, undermining the confidentiality, integrity, and availability of digital assets. Conventional perimeter-based defenses such as firewalls, signature-based antivirus, and intrusion detection systems (IDS) are increasingly inadequate against sophisticated, adaptive threats. The rise of polymorphic malware, AI-enhanced attacks, and multi-stage breach strategies renders signature and rules-based defenses obsolete in many cases (SentinelOne, 2025; IBM, 2025).

One of the critical issues arises from the exploitation of zero-day vulnerabilities—unknown or unpatched flaws that attackers leverage to gain unauthorized access. These vulnerabilities defy traditional patch-based defense models and demand real-time threat intelligence and rapid response capabilities. The average time between breach and detection remains high, often measured in months, allowing attackers to operate stealthily while escalating privileges and exfiltrating sensitive data (Fortinet, 2024).

Ransomware attacks continue to inflict severe operational and financial damage. The emergence of ransomware-as-a-service (RaaS) platforms has democratized attack capabilities, enabling even low-skilled criminals to deploy highly damaging attacks. The financial impact of such incidents extends beyond ransom payments to include incident recovery costs, regulatory penalties, downtime losses, and reputational harm. According to recent studies, the average cost of recovering from a ransomware attack in 2025 exceeds $2.7 million USD, forcing organizations to reassess their resilience strategies (SentinelOne, 2025).

The shift toward zero-trust architectures represents a pivotal response to these challenges. Zero trust eliminates implicit trust within networks by enforcing strict identity verification and continuous access evaluation. Micro-segmentation and constant monitoring ensure that the lateral movement of attackers within networks is severely constrained. However, despite these advances, insider threats, both malicious and accidental, pose persistent risks, as authorized users can exploit their access privileges to cause extensive damage (Darktrace, 2025; Cynet, 2024).

The integration of Artificial Intelligence (AI) and Machine Learning (ML) into cybersecurity defense systems offers improved capabilities for anomaly detection, behavioral analysis, and automated responses. AI-driven analytics can sift through vast volumes of network and endpoint data to identify unusual patterns indicative of compromise. Nevertheless, attackers employ similar AI techniques, creating an escalating arms race that pushes defenders to innovate continually (IBM, 2025). Hybrid work environments, mixing remote, on-site, and third-party access, introduce additional vulnerabilities due to insecure home networks, personal devices, and increased cloud service usage. Misconfigurations in cloud security settings have become a common vector for breaches, emphasizing the need for continuous configuration audits and cloud security posture management (CSPM) solutions (KPMG, 2025).

Moreover, the upcoming threat posed by quantum computing necessitates preemptive measures to adopt quantum-resistant cryptographic algorithms. Although quantum computing is not yet mainstream, threat actors may collect encrypted communications today to decrypt in the future when quantum capabilities mature. This “store now, decrypt later” threat mandates early cryptographic transition strategies (SentinelOne, 2025). In summary, the impact of unethical hacking on cybersecurity defenses underscores the necessity for a paradigm shift from reactive to proactive, adaptive, and intelligence-driven security postures. By integrating zero trust concepts, leveraging AI-enhanced detection, and addressing the human and cloud-related vulnerabilities, organizations can enhance their resilience against the growing sophistication of cyber threats.

5. Countermeasures and Future Directions

In response to the rapidly evolving cybersecurity threats driven by unethical hacking, a multi-layered and proactive defense strategy is imperative. Organizations are increasingly prioritizing advanced detection and prevention techniques that leverage artificial intelligence, behavioral analytics, and continuous monitoring to respond effectively to increasingly sophisticated attacks. AI-powered security solutions enhance threat hunting by automating the analysis of vast datasets, enabling early detection of anomalies and reducing the time to respond to breaches (SentinelOne, 2025; Darktrace, 2025).

Zero-trust architecture has emerged as a cornerstone of modern cybersecurity postures. It operates on the principle of “never trust, always verify, and continuously monitor,” compelling organizations to authenticate and authorize every user and device before granting access to resources, regardless of their location within or outside the network perimeter. Micro-segmentation, contextual access policies, and continuous session verification mitigate lateral movement of attackers within networks and contain potential breaches (Darktrace, 2025; Cynet, 2024).

Regular penetration testing and red team exercises remain essential countermeasures against unethical hacking. By simulating real-world attack scenarios, these exercises illuminate vulnerabilities, test incident response readiness, and facilitate continuous improvement of security controls. When combined with rigorous vulnerability management programs and automated patching processes, organizations can significantly reduce exploitable weaknesses (Coursera, 2025). The human dimension, often exploited by social engineering and phishing attacks, necessitates continuous cybersecurity awareness training. Enhanced user education focuses not only on recognizing malicious activities but also on fostering a security-conscious culture that promotes adherence to best practices and timely reporting of suspicious events (Darktrace, 2025; World Economic Forum, 2025). Advanced email filtering, multi-factor authentication (MFA), and identity and access management (IAM) systems further strengthen defenses against credential compromise, which remains a leading cause of breaches (Cynet, 2024).

Emerging technologies such as blockchain and quantum-resistant cryptography offer promising avenues for securing data integrity and confidentiality. Blockchain's decentralized and tamper-proof properties can enhance identity verification and transaction security, while post-quantum cryptographic algorithms aim to withstand threats posed by future quantum computers capable of breaking current encryption standards (KPMG, 2025).

The rise of cloud computing and the hybrid workforce model demands tailored security strategies. Cloud Security Posture Management (CSPM), cloud workload protection, and secure software development lifecycle (SDLC) practices help mitigate risk in complex, distributed environments. Organizations also need robust third-party risk management programs to address vulnerabilities in supply chains and partner ecosystems (SentinelOne, 2025; IBM, 2025).

Policy and regulatory frameworks continue to evolve, emphasizing compliance and cybersecurity governance. Cross-sector collaboration, information sharing through platforms like Information Sharing and Analysis Centers (ISACs), and partnerships between public and private sectors are vital to ground cybersecurity efforts in timely intelligence and coordinated defense (World Economic Forum, 2025; Darktrace, 2025). Looking forward, the cybersecurity landscape will be shaped by advancements in AI-driven threat intelligence, automated response systems, and adaptive security frameworks that learn and evolve with emerging threats. Collaborative innovation among industry stakeholders, researchers, and governments will be crucial to sustaining cyber resilience and mitigating the risks posed by unethical hacking in future digital ecosystems.

6. Conclusion

The cybersecurity domain in 2025 is navigating through an era marked by the interwoven challenges of technological advancement and increasing cybercriminal sophistication, especially in the realm of unethical hacking. This paper has examined pivotal trends shaping cybersecurity, including the proliferation of AI-undergirded attacks, the expanded vulnerabilities introduced by IoT proliferation, and the rise of ransomware and supply chain attacks. The distinction between ethical and unethical hacking remains timely and critical, emphasizing the constant interplay between defensive strategies and malicious exploits. Technological innovation continues to accelerate the threat landscape, compelling a shift toward adaptive, intelligence-driven, and zero-trust security architectures. These frameworks, combined with AI-enhanced detection, automated response mechanisms, and robust user training programs, are essential to counter increasingly complex attack methodologies. Nevertheless, challenges persist, including threats emerging from insider risks, cloud misconfigurations, and the nascent risks associated with quantum computing capabilities.

Future cybersecurity defense will hinge on multi-sector cooperation, augmented by comprehensive regulatory frameworks, continuous threat intelligence sharing, and ethical hacking practices that proactively identify and remediate vulnerabilities. The arms race between attackers and defenders is poised to intensify, underscoring the need for continued innovation and education. Ultimately, resilience against unethical hacking requires a holistic approach that integrates technology, human factors, and policy. As digital ecosystems evolve, so must the strategies to safeguard them, ensuring security, trust, and operational continuity. The findings and discussions presented herein offer a foundation for ongoing research and practice, contributing to the broader mission of securing cyberspace against ever-more sophisticated adversaries.

References

1. Anomali. (2023). What is an Unethical Hacker? Retrieved from https://www.anomali.com/glossary/unethical-hacker

2. ASK Training. (2024). Ethical Hacking vs Unethical Hacking. LinkedIn. Retrieved from https://www.linkedin.com/pulse/ethical-hacking-vs-unethical-ask-training-sg-2b1wc
3. Cloud Security Alliance. (2025). The emerging cybersecurity threats in 2025 - What you can do to stay ahead. Retrieved from https://cloudsecurityalliance.org/blog/2025/01/14/the-emerging-cybersecurity-threats-in-2025-what-you-can-do-to-stay-ahead
4. Codecademy. (2025). Introduction to Ethical Hacking: Unethical Hacking Cheatsheet. Retrieved from https://www.codecademy.com/learn/introduction-to-ethical-hacking/modules/unethical-hacking/cheatsheet
5. Coursera. (2025). 9 cybersecurity best practices for businesses in 2025. Retrieved from https://www.coursera.org/articles/cybersecurity-best-practices
6. CrowdStrike. (2025). 2025 global threat report. Retrieved from https://www.crowdstrike.com/en-us/global-threat-report/
7. Craw.in. (2025). The ethical hacker's toolbox for navigating digital threats. Retrieved from https://www.craw.in/the-ethical-hackers-toolbox-for-navigating-digital
8. Cynet. (2024). Top 6 cyber attack prevention strategies in 2025. Retrieved from https://www.cynet.com/advanced-threat-protection/top-6-cyber-attack-prevention-strategies-in-2025/
9. Darktrace. (2025). 2025 cyber threat landscape: Darktrace's mid-year review. Retrieved from https://www.darktrace.com/blog/2025-cyber-threat-landscape-darktraces-mid-year-review
10. Darktrace. (2025). AI and cybersecurity: Predictions for 2025. Retrieved from https://www.darktrace.com/blog/ai-and-cybersecurity-predictions-for-2025
11. Fortinet. (2024). 2025 global threat landscape report. Retrieved from https://www.fortinet.com/resources/reports/threat-landscape-report
12. IBM. (2025). Cybersecurity trends: IBM's predictions for 2025. Retrieved from https://www.ibm.com/think/insights/cybersecurity-trends-ibm-predictions-2025
13. KPMG. (2025). Cybersecurity considerations 2025. Retrieved from https://kpmg.com/xx/en/our-insights/ai-and-technology/cybersecurity-considerations-2025.html
14. LinkedIn. (2024). Ethical hacking vs unethical hacking. Retrieved from https://www.linkedin.com/pulse/ethical-hacking-vs-unethical-ask-training-sg-2b1wc
15. SentinelOne. (2025). 10 Cyber security trends for 2025. Retrieved from https://www.sentinelone.com/cybersecurity-101/cybersecurity/cyber-security-trends/
16. World Economic Forum. (2025). Global cybersecurity outlook 2025. Retrieved from https://www.weforum.org/publications/global-cybersecurity-outlook-2025