**Interim Report**

**DNS Abuse Transparency**

Contents

[Detailed Project Description 2](#_Toc155793548)

[Literature Review 2](#_Toc155793549)

[Project Work Plan 3](#_Toc155793550)

[Ethical Issues Review 4](#_Toc155793551)

[References: 5](#_Toc155793552)

# Detailed Project Description

The" DNS Abuse Transparency " project aims to improve the transparency of mitigations used in the face of bad actors, such as phishing sites, abusing DNS names. It focuses on how DNS infrastructure providers, registrars, and registries, among others handle abuse reports and how transparently they work. With the goal of creating best practices for openness in combating DNS abuse, the project includes collecting data from these organisations and researching them to comprehend and classify their existing transparency reports. In this project, the crucial problem of Domain Name System (DNS) abuse, a developing concern in the digital age is the focus. A crucial component of internet operations, the DNS is being used more and more maliciously, threatening user privacy, corporate security, and national security. The goal of this project is to improve DNS abuse mitigation's transparency. There is a noticeable gap in the way infrastructure providers report and handle DNS abuse, despite the urgency. Analysing present processes and transparency reports and providing a thorough evaluation of their effectiveness and clarity is the main goal. Through an evaluation of current protocols for reporting and managing DNS abuse, the study seeks to identify the main challenges to improving transparency. These challenges include registrars being unable to devote much resource, limited public awareness and uneven reporting requirements. The research will examine transparency reports in a systematic way from some leading DNS infrastructure providers, reviewing the information, techniques, and public relations tactics employed. The idea is to put out a framework that encourages DNS abuse mitigation that is more effective, standardised, transparent, and easily available. By doing this, the project hopes to contribute to a more secure online environment were addressing DNS abuse transparently is both prioritised and can be successfully executed. The intended result is a set of guidelines for DNS infrastructure providers with the intention of enhancing their transparency policies eventually building more confidence among internet users and other stakeholders.

# Literature Review

To elaborate, the literature on DNS abuse offers more profound understandings of the complexity of cybersecurity issues. The investigation of DNS vulnerabilities by Schmid (2021) highlights the necessity for more advanced security measures. This is especially important considering how sophisticated cyberthreats are becoming. In their exploration of the potential of AI to transform network forensics, Rizvi et al. (2022) point out that AI can improve detection skills and offer more potent solutions for DNS abuses.

The study of Blockchain solutions by Chaganti, Bhushan, and Ravi (2023) introduces a new direction in DNS security by putting out a decentralised strategy that might provide more effective defences against DNS attacks. The study conducted by Kapoor et al. (2021) offers a critical viewpoint on the detection of ransomware, which is a crucial aspect of DNS security. The authors highlight the interdependence of different cyberthreats and the significance of a complete cybersecurity strategy.

The integration of AI into cybersecurity operations by Kaur, Gabrijelčič, and Klobučar (2023) demonstrates how AI may be used not only for detection but also for DNS abuse detection and avoidance. This proactive strategy is claimed to be essential in an environment where dangers are ever-changing. Goethals, Volckaert, and De Turck (2021) conclude by focusing on the application of AI in intelligent networks, which is (again) claimed to be essential to future developments in cybersecurity and underlines the necessity of constant technological innovation to keep up with hreats.

Together, these works offer a framework for comprehending the present difficulties in mitigating DNS abuse and highlight the necessity of continued study and advancement in this area. Yet they are clearly lacking in terms of transparency, a lack that this project aims to improve.

# Project Work Plan

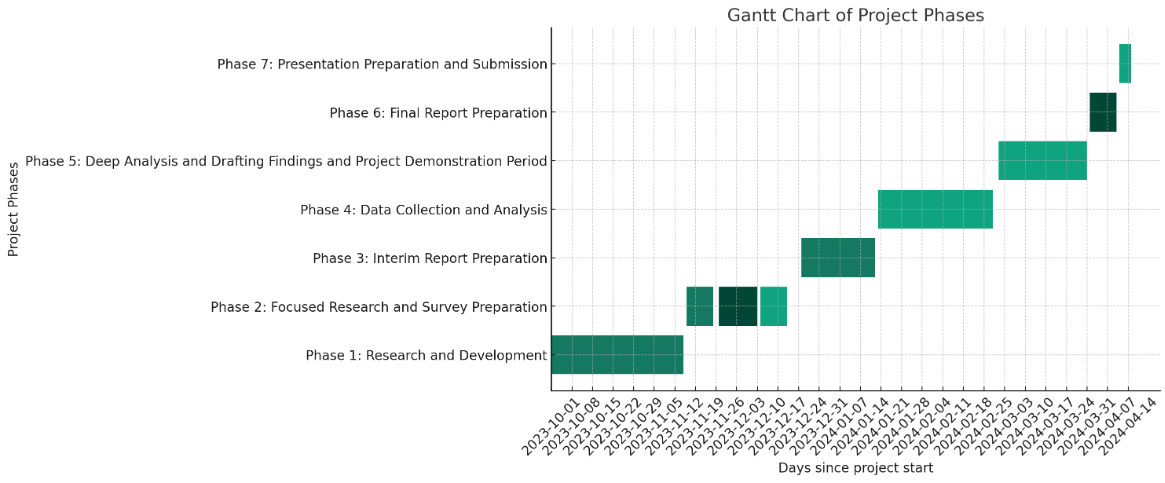


Figure [1]: The accompanying Gantt chart vividly illustrates this progression, providing a visual timeline of milestones and task dependencies.

To guarantee the careful review and improvement of DNS Abuse Transparency, the Project Work Plan is divided into seven stages. The journey begins with the Research and Development phase, during which a basic understanding of DNS abuse and mitigation techniques is built. The development of the technical and documentation abilities required for the project depends heavily on this phase. After that, creating questionnaires and speaking to stakeholders is what's known as the Focused Research and Survey Preparation phase, which aims to collect information on transparency in current DNS abuse mitigation mechanisms. To prepare the groundwork for the Data Collection and Analysis phase, the subsequent Interim Report Preparation phase focuses on combining these findings into a cohesive report. This is when the theoretical work from earlier stages comes together with the actual collection and initial analysis of data.

After then, the project moves on to the Deep Analysis and Drafting Findings phase, when a thorough examination of the data obtained identifies patterns and weaknesses in the methods used now. In preparation for the final report preparation, this analysis is shaped into an document on which we will seek feedback from stakeholders to ensure accuracy and clarity. The project is refined into a presentation that summarises the conclusions and suggested tactics for boosting DNS Abuse Transparency during the last phase, Presentation Preparation and Submission. This presentation acts as a platform for suggesting future paths as well as an overview of the project's results.

# Ethical Issues Review

Ethical issues are critical to the DNS Abuse Transparency initiative, especially when it comes to cybersecurity and digital health solutions. The study by Fisher, Bragard, and Bloom (2020) on eHealth HIV intervention research emphasises that research participants and their data are handled with rigorous adherence to confidentiality and informed consent norms. The difficulties and moral dilemmas surrounding permission processes, data management, and recruitment particularly about online tactics are highlighted by this study.

When collecting or analysing data, special attention is paid to avoiding bias or prejudice of any kind. This guarantees that participant gender, colour, or socioeconomic class has no bearing on research findings, which is in line with the ethical standards recommended in public health research conducted in social media environments, as Massey et al. (2023) outline. Their research highlights how crucial it is for public health and social media studies to take vulnerability into account and advance ethical standards. Additionally, a thorough analysis of the project's effects on various demographic groups is conducted to determine the possible effects of DNS abuse on these groups. As part of this, mitigation techniques must be inclusive and equitable to contribute to a safer online space that values diversity and encourages fair access to digital resources. Additionally, through addressing the difficulties experienced by underrepresented groups in cybersecurity, the project hopes to promote an inclusive culture. This strategy considers a broad range of cultural and social contexts, recognising the value of different viewpoints and levels of experience when addressing DNS abuse.

To sum up, this project's ethical evaluation highlights the dedication to respecting the strictest guidelines for research ethics, encouraging an impartial and fair investigation, and making sure that everyone, regardless of background, benefits from the research. This moral position supports the larger objective of building a safe and welcoming virtual community, which is supported by the previously mentioned studies (Fisher, Bragard, & Bloom, 2020; Massey et al., 2023). It also lends legitimacy to the research.

# 

# References:

Fisher, C., Bragard, E. and Bloom, R., 2020. Ethical Considerations in HIV eHealth Intervention Research: Implications for Informational Risk in Recruitment, Data Maintenance, and Consent Procedures*. Current HIV/AIDS Reports, [online] 17(3), pp.215-222.*

Goethals, T., Volckaert, B. and De Turck, F., 2021. Enabling and Leveraging AI in the Intelligent Edge: A Review of Current Trends and Future Directions. *IEEE Open Journal of the Communications Society*, *2*, pp.2311-2341

Kapoor, A., Gupta, A., Gupta, R., Tanwar, S., Sharma, G. and Davidson, I.E., 2021. Ransomware detection, avoidance, and mitigation scheme: a review and future directions. *Sustainability*, *14*(1), p.8.

Kaur, R., Gabrijelčič, D. and Klobučar, T., 2023. Artificial intelligence for cybersecurity: Literature review and future research directions. *Information Fusion*, p.101804.

Massey, P.M., Murray, R.M., Chiang, S.C., Russell, A.M. and Yudell, M.A., 2023. Social Media, Public Health Research, and Vulnerability: Considerations to Advance Ethical Guidelines and Strengthen Future Research. *JMIR Public Health and Surveillance, [online] 9(1), e49881.*

Rizvi, S., Scanlon, M., McKinney, J. and Sheppard, J., 2022. Application of artificial intelligence to network forensics: Survey, challenges and future directions. *IEEE Access*, *10*, pp.110362-110384.

Schmid, G., 2021. Thirty years of DNS insecurity: Current issues and perspectives. *IEEE Communications Surveys & Tutorials*, *23*(4), pp.2429-2459.