**T5 -machine learning-based anti-phishing detectors have shown vulnerability to evasion attacks . the results provide insights for enhancing machine learning-based anti-phishing detectors. manipulation of phishing HTML pages using obfuscation techniques led to third place in MLSEC 2022 .a field note documents the experience of participating in the machine learning security evasion competition 2022, where manipulation of phishing HTML pages led to a third place in the competition, a field note.**

**Bart** -Evading Anti-Phishing Models: A Field Note Documenting an Experience in the Machine Learning Security Evasion Competition 2022. Machine learning-based anti-phishing detectors have shown vulnerability to evasion attacks. This field note documents the experience of participating in MLSEC 2022, where manipulation of phishing HTML pages using obfuscation techniques led to third place in the competition. The results provide insights for enhancing machine learning- based anti- phishing detectors.

**Gemini** –In the Machine Learning Security Evasion Competition 2022, researchers tested evasion attacks against anti-phishing machine learning models. Participating in the competition, the authors used obfuscation techniques to manipulate phishing HTML pages, achieving third place. This experience highlights the vulnerability of anti-phishing models to evasion attacks and provides valuable insights for strengthening these models. The employed obfuscation techniques can help enhance the robustness of anti-phishing detectors, ensuring greater protection against phishing attacks.

**Gpt-40**  –The Machine Learning Security Evasion Competition 2022 (MLSEC2022) highlighted the vulnerabilities of machine learning-based anti-phishing detectors to evasion attacks. This field note recounts the experiences of participants who engaged in the competition by deploying evasion attacks against these detectors. The competition focused on the manipulation of phishing HTML pages through various obfuscation techniques, which proved to be an effective strategy for evading detection. The participant who documented this experience achieved third place, underscoring the effectiveness of the applied techniques.

The insights gained from MLSEC2022 are critical for the future development of more robust anti-phishing systems. The success of obfuscation methods in evading detection demonstrates that current machine learning models need significant improvements to cope with sophisticated phishing attacks. This field note serves as a valuable resource for researchers and developers aiming to enhance the security features of machine learning-based anti-phishing detectors. By understanding the methods used to bypass these systems, developers can create more secure and resilient anti-phishing tools that can better protect users from evolving cyber threats.

**Gpt-3**  The Machine Learning Security Evasion Competition 2022 (MLSEC2022) was initiated due to the susceptibility of machine learning-based anti-phishing detectors to evasion attacks. This field note recounts the participation experience in MLSEC 2022, where researchers employed obfuscation techniques to manipulate phishing HTML pages, resulting in a third-place finish. The competition highlighted the need to enhance machine learning-based anti-phishing detectors to counter evasion tactics effectively. The vulnerability of these detectors underscores the importance of continuously improving their robustness against sophisticated evasion attacks. The findings from this competition shed light on the challenges faced by anti-phishing models and emphasize the significance of developing more resilient defenses. By documenting the strategies and outcomes of evasion attacks in a real-world competition setting, this field note contributes valuable insights for advancing the security of machine learning-based anti-phishing systems. Overall, the experience in MLSEC 2022 underscores the ongoing arms race between attackers and defenders in the realm of cybersecurity, emphasizing the critical role of innovation and vigilance in safeguarding against evolving threats in the digital landscape.