# Abstract: Measuring 'stimuli attributes' with simulated phishing attack

Bhardwaj Aditya

A study [3] in 2022 shared some interesting results. The authors studied modern phishing websites to understand what type of user interactions are elicited by phishing websites and how their user experience (UX) and interface (UI) design patterns can help them accomplish malicious attacks. They found that phishing sites took users though multiple steps/stages to lend a sense of professionalism and legitimacy, all while evading phishing detectors and web security crawlers. This has been seen in the wild with Cloudflare Turnstile (an alternative to CAPTHCA) being used to evade static analysis of phishing websites [1]. While they explored more than 50,000 existing phishing websites. It would be interesting to study the same observations with simulated phishing attacks as conducted by [2] via university. This study mentions that students were more likely to click the malicious link embedded within the phishing email, often using mobile devices. They share that

> About a third (32%) of all users who opened the first phishing email went on to click the link embedded within the email.

Learning from these studies, we can conduct similar simulated phishing attacks in the university to investigate stimuli attributes (legitimacy, persuasion, look and feel). As we know better from observations/results shared in the aforementioned research, it would be interesting to see if it affects the numbers of clicks on a malicious link. It can also be extended to see how AI tools and methods like LLMs improve social engineering attempts for the attacker, such as crafting professional-sounding and error-free email body text.

## References

[1] Jan Michael Alcantara. *Evasive Phishing Campaign Steals Cloud Credentials Using Cloudflare R2 and Turnstile*. `https://www.netskope.com/blog/evasive-phishing-campaign-steals-cloud-credentials-using-cloudflare-r2-and-turnstile`. [Online; accessed 15-Sept-2024]. 2023.

[2] David Maimon et al. "A Routine Activities Approach to Evidence-Based Risk Assessment: Findings From Two Simulated Phishing Attacks". In: *Social Science Computer Review* 41.1 (2023), pp. 286–304. DOI: `10.1177/08944393211046339`. eprint: `https://doi.org/10.1177/08944393211046339`. URL: `https://doi.org/10.1177/08944393211046339`.

[3] Karthika Subramani et al. "PhishInPatterns: measuring elicited user interactions at scale on phishing websites". In: *Proceedings of the 22nd ACM Internet Measurement Conference*. IMC '22. Nice, France: Association for Computing Machinery, 2022, pp. 589–604. ISBN: 9781450392594. DOI: 10.1145/3517745.3561467. URL: https://doi.org/10.1145/3517745.3561467.