A solution to minimise the success of phishing attempts using the effects of human behaviour and emotions on falling into a phishing scam.

Phishing is a social engineering scam that can cause data loss, reputational damages, identity theft, money loss, and many other damages to people and organisations. Multiple studies showed the effects of human behaviour, such as risk-taking and decision making, on Internet users' security behaviour. Researchers also investigated how email users' behaviour can influence the success of a phishing attempt. Moreover, the number of phishing attempts has been increased rapidly since the beginning of the COVID-19 outbreak. Several studies demonstrated the effects of the COVID-19 pandemic on human behaviour, impacting phishing attempts' success.

Organisations can use the results of these studies to find potential high-risk users by measuring the users' behaviour and emotions, which are associated with falling into a phishing scam. In this study, we have developed a solution and guideline using previous studies to identify risky users (i.e., those at risk of clicking on phishing links). The solution will then suggest or assigns proper mitigation actions for those users. The system contains measurement (psychological scales), scoring (machine learning), and mitigation modules that can become more mature and accurate over time. Furthermore, specific situations, such as the pandemic, is also considered in the solution- that is, when a situation like the COVID-19 pandemic happens, the solution will consider the impacted human emotions in finding the high-risk users and might suggest other types of mitigations. We have used regression models for the machine learning module.

The proposed solution will help organisations focus more on high-risk users and reduce cyber risks. This solution, however, should be used in combination with technical anti-phishing systems and cybersecurity awareness training campaigns to achieve better results.