Effects of email users' behaviour and demographics on respond to each step of a phishing attack

Hossein Abroshan, Jan Devos, Geert Poels, Eric Laermans

Abstract— Phishing is a process in which attackers send emails to Internet users and try to convince them to click on a link to steal their sensitive information or open an attachment to compromise their account, computer, organisation systems, etc. Users' behaviour, such as their risk-taking preference and decision-making style, can influence a phishing attempt's success. However, studies did not profoundly investigate the effects of the behaviours on each step of a phishing process (e.g., opening the email, clicking on the link, and submitting sensitive information on the phishing webpage). This study demonstrated the effects of risk-taking level and decision-making style, gender, age, and education level on the users' respond to each selected step of a phishing attempt.

In this real-world study, we measured the behaviours of 135 participants from academia using psychological scales and tests. We then tested their phishability level by sending them simulated phishing emails. The regression analysis results showed that the general risk-taking preference and gender of the users could predict their phishability in the second step, i.e., clicking on the phishing link ($p<0.05$). We could not find any significant relation between their decision-making style and other demographic factors with the users' phishability level in the second step of the phishing. We also could not find any relations between the measured behaviours, age, gender, and education level of the users and their phishability level in the first and second steps (i.e., opening the phishing email and submitting sensitive data to the phishing website).

The results of this study can help us develop proper mitigation actions to minimise phishing success in different steps. Organisations can use this approach to identify risky users and focus on decreasing their phishability level, for instance by providing more training to them or changing the behaviour (if possible). The developed model can be used as a comprehensive framework to investigate other behaviours' effects in each step of phishing.

Keywords— Cyber security, Phishing, Human behaviour, Individual differences, Online scams.

Hossein Abroshan is with the Ghent University (e-mail: hossein.abroshan@ugent.be).
Jan Devos is with Ghent University (e-mail: JanG.Devos@UGent.be@ugent.be).
Geert Poels is with the Ghent University (e-mail: Geert.Poels@UGent.be).
Eric Laermans is with the Ghent University (e-mail: Eric.Laermans@UGent.be).