# Security Investment - Review of group 10

Reviewed by group 14

## Summary

The authors begin with explaining who their problem owner is and what their responsibilities are. They then discuss the differences in security performance. Afterwards, they address the several strategies that the problem owner can choose to follow. It is followed by a detailed explanation of the other actors' risk strategies who contribute to the goal. Finally, a ROSI calculation is made based on several metrics from literature and estimations. Concluding, phishing is a complex phenomenon and the awareness campaign strategy has a positive ROSI, so companies can directly benefit from this investment.

**Summary of our thoughts:**
The paper addresses the security issue well, and correctly states the involved actors and their reasoning, and an analysis on how to deal with the issue mentioned.
However, the paper also states that the hosting companies are responsible for solving the issue, which is not necessarily true. Also, this is not backed up by any references.
Furthermore, we feel the paper is too long for the amount of information it contains, and could be shortened a bit.
Overall, apart from the issues mentioned, this is a clear description of the security issue, involved actors, and a well-elaborated analysis on the strategy to deal with phishing.

## Strengths

- The paper addresses the different actors involved in the security issue, and elaborates on all these.
- Many references. For example in the introduction, the authors provide multiple definitions of the "problem owner", explaining why they consider the hosting companies as their problem owner.
- Usage of definitions provided in the videos on the edge.edx platform. For example, when answering the second question, you use the four segments of players in the cybersecurity realm. Also, the "ship-now fix-later" strategy is explained in the context of phishing. We really like the fact that you use the existing theory and frameworks in the assignment.
- The arguments are clever and you really thought of all possibilities. For example, when discussing the communication to the security consumers, it is a strong point that you also consider the fact that they might get annoyed by too much communication and that other hosting providers might be considered "safer" when they don't communicate at all (the false perception).

# Major issues

- You state that hosting providers can do very little to increase security awareness, but that they are able to inform the most targeted brands. So they can do a lot about awareness? This is very contradictory. The fact that you hold hosting companies responsible for raising security awareness regarding the customers of specific brands, also seems illogical to us. Why are the hosting companies responsible? The fact that they are in a position to inform the most targeted brands, does not make these hosting companies responsible for the security issue.

# Minor issues

- Some sentences are very broad, and contain a lot of words that don't really say anything and thus are very vague for the reader. For example, sentences like "having more availability or being more secure" or "it spans multiple layers of cyberspace and involves different costs and benefits for different actors". Overall, we feel the paper could be much shorter and contain the same amount of information.
- The claim “If hosting providers provide VPN services, security is their core competence” is not supported with evidence or references. We think this is quite a strange claim; there are probably more aspects companies have in order to consider security as their core competence.
- Minor spelling and grammar mistakes. Nothing that affects the content of the paper, but present anyway.
- Perhaps you could have given a small introduction into the kind of phishing you are discussing; is it spear phishing or fake emails leading to malicious URL’s? Throughout the paper, it becomes clear that you consider fake websites as the ‘real’ phishing, perhaps a small explanation could be present in the introduction.