

Assignment Block 3 Group 5

Reviewed by group 1

Summary:

This paper discusses the security issue that banks and other forms of financial institutions are affected by phishing. The problem owners of this security are thus the financial institutions. The metrics relating to this security issue reveals that almost half of all phishing attack targets are within the financial sector. PayPal is targeted most often, however the issue is unrelated to revenue. The problem owners can follow the four canonical risk strategies: risk mitigation, risk acceptance, risk avoidance and risk transfer. There are other actors which influence the security issue, such as customers, ISPs, LE, legislators and providers. The actors suffering most from phishing mainly use risk acceptance and avoidance as their strategies. A rough approximation of ROSI on mitigating risks leads to a result of 1700%. This takes into account the strategies of educating customers on phishing and having customers use two factor verification.

Strengths of the assignment:

- Clear definition of the problem owner with underlying motivation
- Good and clear connections to course content.
- Really nice well defined ROSI, nicely found case and good use of assumptions (only one minor issue defined in the 'minor issues' section).
- Good use of other resources and literature

Major issues:

The introduction

- Any research article or paper should contain an introduction (and methodology). Starting to answer questions without context makes it difficult to understand for the reader what the paper is about. A description of what this paper will discuss is needed.

Problem owner

- Clear definition of how you got to your problem owner. Perspective is important, so picking one particular section is good. However, you're missing some cohesion within your writing. The second last paragraph is about the banks saving their reputation by means of compensating customers, but the last sentence has absolutely nothing to do with this. Stay close to the matter that needs to be addressed in this section, don't get lost in irrelevant information.

Risk strategies by problem owner

- You've outlined the four canonical instruments. Indeed these are the broader outlines of what risk strategies are available. But in this assignment it is meant to dive much deeper into the various risk strategies within these canonicals. For example, instead of giving an example of risk avoidance (EG finding and removing phishing sites), you should outline how your problem owner should do this and also how this can be evaluated using either your dataset or another measure. The same goes for the other three canonical instruments. With these four canonical strategies it is, for example, not possible to calculate ROSI, for which something more specific is needed.

Other actors that influence security issue

- The graph seems rather random if you don't reference to a source/data (even though it is probably a correct and meaningful graph). Also, it is mentioned, for example, that ISPs are

affected by phishing, but how do they influence the security issue? What you have described is relevant, however it is not an exact answer to the question.

Risk strategies by other actors

- See point 4.

Conclusion:

- Similar to major issue 1, a good report should feature a conclusion of your research.

Minor issues:

- You made a fair amount of punctuation errors. Also your plurals and singulars often didn't match up between verbs and nouns.
- In your ROSI calculation, you should address that it isn't feasible for a bank to force all their customers to play an anti-phishing game. They are customers, not employees.
- References should be formatted properly.
- Your last two plots feature Dutch text, that doesn't belong in an English paper.