ECS Assignment Block 4 - Group 5

Maaike Bak, Federico Falconieri, Angela Plomp, Ricky Sewsingh

19 October 2015

1 Introduction

The first part of this paper focuses on three actors from the previous assignment. These three actors are financial institutions (the problem owner), the customers of these financial institutions and Internet service providers. For each of them one security countermeasure will be proposed and a cost/benefit analysis of this countermeasure will be provided. Also externalities on the other actors will be taken into account.

2 Countermeasures and relative cost/benefit analysis on three actors affected by phishing

2.1 Problem owner: financial institutions

2.1.1 Countermeasure: Spread Awareness

A countermeasure financial institutions could make, and mostly are doing, is spreading awareness about the problem. Since this issue mostly starts at a customer, it is obvious to tackle this problem at this stage. If a customer has more knowledge about phishing, he/she can prevent these kind of attacks by simply use this knowledge to avoid phishing websites.

2.1.2 Cost/benefit for other actors

- *Customers*: there would be a great benefit for customers. Customers who have acquired knowledge about phishing are less likely to be a victim of a phishing attack. But since the customer actually has to acquire the knowledge, means the customer has to put effort in this matter. This can be seen as a cost.
- *Legislators*: they would not have particular costs or benefits.
- *Law enforcement*: less people involved in phishing attacks probably means less concrete victims of it. This would reflect on a benefit, even if marginal, for law enforcement entities, because their workload would be reduced and their resources could be used to tackle other crimes.
- *ISPs*: they would not have particular costs or benefits.
- *Hosting providers*: they would not have particular costs or benefits.
- *Email providers*: they would not have particular costs or benefits.

2.1.3 Incentives

Financial institutions have a great incentive for this countermeasure. The benefit/cost rate is very high, depending on what measures are taken. One can do it as simply as making customers read a small paper or email about phishing, or

extensively as making customers go to a seminar about phishing. If the simple measure is taken, the biggest problem is the fact that customers actually have to read the paper. Making sure this happens as an insitution is hard, since you can't force people to read it. Putting effort in this matter is the biggest cost for the institutions, but since this will greatly reduce the amount of phishing attacks, if done correctly, the benefits could exceed the costs, which is a great incentive.

2.1.4 Externalities

It is quite clear what externality emerges from this countermeasure. The customers didn't choose for this, yet they are a big part of this countermeasure. But the customer also has an incentive in this matter. A customer also wants to reduce the risk of being a victim in a phishing attack. Therefore, if the cost of doing so isn't very time consuming, a customer would not mind putting effort in reducing this risk.

2.2 Actor: customers

2.2.1 Countermeasure: risk avoidance

The best countermeasure that customers can put in place is not using internet banking at all. Risk avoidance is the most effective way to reduce risk for them. This, though, has a very high cost on customers, and at this point in time it is hard to believe that it will be adopted pervasively. This cost would be in the form of time loss.

2.2.2 Cost/benefit for other actors

- *Financial institutions*: they would have no benefit whatsoever from this countermeasure and, in the other hand, a very high cost. Internet banking allows banks to have less subsidiaries open to the public and personell.
- *Legislators*: they would not have particular costs or benefits.
- *Law enforcement*: less people exposed to phishing probably means less concrete victims of it. This would reflect on a benefit, even if marginal, for law enforcement entities, because their workload would be reduced and their resources could be used to tackle other crimes.
- *ISPs*: they would not have particular costs or benefits from customers implementing this countermeasure. Altough it can be assumed that this countermeasure would imply a reduction of internet traffic and hence ISPs workload, this reduction percentage is probably not significant.
- *Hosting providers*: they would not have particular costs or benefits.
- *Email providers*: they would not have particular costs or benefits.

2.2.3 Incentives

Customers are not really incentivised in taking this countermeasure, because the costs probably overcome the benefits. This is especially true when the fact that in many countries financial institutions completely refund their client in case of phishing is taken into account. So in general the cost of adopting this countermeasure is higher than the benefit, hence this probably is main reason why this countermeasure is not adopted by most bank customers.

2.2.4 Externalities

The benefits of adopting this strategy fall mainly on the customer itself, whereas the costs fall both on them and on financial institutions.

2.3 Actor: ISPs

2.3.1 Countermeasure: DNS blacklisting

A very concrete countermeasures that ISPs can adopt is DNS blacklisting or DSNBL. Most ISPs provide DNS service to their customers and at the same time most ISPs customers rely on these DNS. The idea is pretty simple: ISPs, following instruction given by other actors like the financial institutions victims of phishings or law enforcement, stop translating the domain names of phishing websites for their customers. Customers then, when trying to load the page of a phishing website, will end up with an error and thus will not be able to see the phishing website at all.

2.3.2 Cost/benefit for other actors

- *Financial institutions*: they benefit greatly from this countermeasure. It is the most quick and efficient way to obscure phishing websites.
- *Customers of financial institutions*: customers benefit greatly from DNS blacklisting, and this solution is transparent to them so it cost them nothing.
- *Legislators*: legislators do not have particular benefit or cost from this countermeasure.
- *Law enforcement*: law enforcement entities do not have particular benefit or cost from this countermeasure, aside from the fact that this will probably reduce the number of victim and hence their workload.
- *Hosting providers*: they have no benefit from this countermeasure and a significant cost. As a matter of fact this solution obscure domains owned by the hosting providers. In the past hosting providers filed lawsuits against ISPs , but usually without success.
- *Email providers*: email providers do not have particular benefit or cost from this solution.

2.3.3 Incentives

ISPs do not really have an incentive to adopt blacklisting and are usually forced by law enforcement and financial institutions to do so. (check) Most of the cost, including the indirect one deriving from being lawsuited by hosting websites, fall on them and in exchange they do not receive any benefit.

2.3.4 Externalities

Given that in economics an externality is the cost or benefit that affects a party who did not choose to incur that cost or benefit [1], a picture emerges quite clearly. ISPs have a lot of power but are not motivated to solve the issue because the benefit of this effort would fall completely on other actors, namely banks and customers, and at the same time all the costs, both direct and indirect (e.g. lawsuites from involved hosting providers, retaliation from criminal groups through DDoS etc.) would fall on the them.

3 Explaining the variance in uptime and amount of attacks

The metric shows the amount of attacks and uptime distribution per targeted firm in the financial sector. This relates to the security performance of those firms, regarding their succes in e.g. raising awareness under customers and taking action against noticed phishing sites in time.

3.1 Possible factors explaining the variance in number of attacks and uptime

First of all it should be mentioned that the dataset must be assumed to be representative in order to perform any statistical analysis. However, it may be clear that not all banks notify their phishing websites to Clean-mx. Also Clean-mx only stores data for about 10 days due to the large amount of data. When looking for plausible factors that can explain the variance, a few come to mind:

- *Number and size of transactions per time unit*
- *Average money deposited per account*: This is a metric for the wealth of a bank's customers. Probably there is more to gain when the customers of a bank are wealthier.
- *Number of customers*: Next to the wealth of a bank's customers, a large number of customers can also make a bank an attractive target because this increases the reach of a phishing site. This is comparable to the choice hackers make when they hack a Windows computer instead of an Apple.

- *Revenue of the bank*: Because only few banks provide information about the average money deposited per account, or about the number of transactions per day, the bank's revenue is a more realistic approach and could be used as a proxy for a bank's cash flows. The more cash flows through a bank, the more attractive it is to throw in some phishing sites.

- *Awareness measures taken by firms*: The more measures taken, the less attractive a bank should be to a phisher. Very good spam filters or the use of tokens in internet banking will decrease the probability of succes of phishers, which should negatively influence the amount of attacks.

- *Responsiveness of firms*: There should be an explaining factor for the uptime of a site, but it is hard to capture this in a concrete factor. Perhaps the amount of fte (man hours) dedicated to taking down phishing sites would explain some variance, but it is impossible to retrieve this for all banks.

- *Level of awareness amongst customers*: This is partly the result of the awareness measures mentioned above, and partly the outcome of public norms and awareness in certain countries or groups within societies. For example, elderly people might be much more aware of the dangers of online banking, while young adults are less critical because they grew up with it and all of their friends use it. Also, the more aware people are, the more likely they are to notify a phishing website immediately so that the bank can take it down fast.

3.2 Collecting data on the above factors

At the moment we are collecting data on the 60 of the 103 banks who are attacked most often - thereby only excluding banks who are attacked less than 5 times in the 10 days covered by the dataset. The factors which are feasible to collect are: Number of customers; Revenue of the bank; Average money deposited per account. Since there is no common database for this information, it has to be found manually. Not all data can be found for each bank, so we will exclude cases without any data but will still use cases that miss one of the factors. Also, we tried to find information about the use of tokens in internet banking as a proxy for the awareness measures taken by firms. Unfortunately this is very hard to look up in all the different websites of the banks so we are not sure whether this is feasible. It might explain though why Dutch banks are attacked so few.

3.3 Linear regression

We plan to do a linear regression in SPSS to explore the relation between the explaining factors and the dependent factor (being number of attacks, as uptime is hard to explain with concrete factors).

References

[1] J. M. Buchanan and W. C. Stubblebine, "Externality," *Economica*, vol. 29, no. 116, pp. pp. 371–384, 1962. [Online]. Available: http://www.jstor.org/stable/2551386