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: Awareness Campaigns

A countermeasure financial institutions could apply, and mostly are doing, is spreading awareness about the problem. Since this issue mostly starts at the 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. This means they lose less time into reporting the incidents and trying to get their money back. Also since there is a chance their money will be lost, since under certain circumstances the customer can be held liable, the chance of money being lost is also reduced. But since the customer actually has to acquire the knowledge, means the customer has to put effort in this matter. This the biggest cost made by the customer [1].

- *Legislators*: in some cases legislators educate the population by for example advertisements on the television. This is, if the population is educated, not necessary. Therefore the legislators benefit from this counter-measure.

- *Law enforcement*: If customers are more educated about phishing, it can result into less victims. 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*: more awareness could lead to two possible outcomes. First customers are more aware of phishing websites and avoid them. This means less reports of phishing websites, since they are not being visited anymore. This results into a decrease of workload (no blacklisting, lawsuits

etc), which is obviously a benefit. The second outcome is that, because people are more aware of phishing websites, they are better spotted and therefore also faster reported. This means an increase of reports for the ISP's, so a bigger workload and more potential lawsuits. Although, in an optimal situation, this workload should decrease, since the phishing websites are taken down, which should result into less attacks.

- *Hosting providers*: the results for hosting providers are pretty far-fetched, since it is an extremely indirect consequence. As explained for ISP's, more awareness could lead to more blacklisting. If sites from the hosting provider are being blacklisted, the image of the hosting provider will be damaged. This is a major cost of the hosting providers. Therefore hosting providers tend to lawsuits, which also results into a lot of administrative costs.

- *Email providers*: more awareness could also lead to the customers better reporting spam emails containing phishing attacks. Email-providers can then use this information to improve their filtering algorithms. But the cost on the other hand is the fact that they have to process all the reports.

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.
There are a couple of benefits related to this countermeasure. First off all the reduction of incidents will result into a reduced usage of customer service. In these cases financial institutions are required to put a lot of time into refunding and helping the customer by for example resetting passwords. This will be reduced, since the amount of victims will be fewer.
Also a possible benefit would be the fact that fewer websites will be reported, since customers will not fall for the phishing attack that easily anymore. This results into less administrative work, for example reporting the phishing websites to ISP's, hosting providers and law enforcement, will reduce. But from another perspective, one can say that the amount of reports will increase, since phishing websites will be spotted more easily. This results into more administrative work. But reporting these websites has its benefits too, since this will also reduce the amount of attacks. Which of the effects will take place, depends on which type of customer is involved. If the customers are active, they will report the websites, if not, the company ends up in case one.

Another incentive the financial institutions might have, is the fact that in some countries, awareness campaigns reduce the amount the institution has to refund victims of phishing attacks [2]. This is also a great incentive to apply the counter-measure.

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 too high, a customer would not mind putting effort in reducing this risk [1].

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. Figure 1 shows the current trend in the United States of America. [3]
The cost of this countermeasure would be in the form of time loss.

2.2.2 Cost/benefit for other actors

- *Financial institutions*: they would have a very high cost from this countermeasure since Internet banking allows banks to have less subsidiaries open to the public and less personell. On the other hand, though, they would also have a very small benefit: less people using internet banking would allow financial institutions to reduce their expenses on IT services. To be more specific this countermeasure qualifies as an opportunity cost for financial institutions. Jakobsson and Myers [4] describe opportunity costs as those costs that are associated with forgone opportunity because people refuse to use online services because of the fear of phishing, or are otherwise suspicios of them.

- *Legislators*: less people using internet banking means less phishing and thus less need to tackle the problem from a legislative perspective. So customers applying risk avoidance would translate in a, even if very small, benefit for legislators.

- *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.

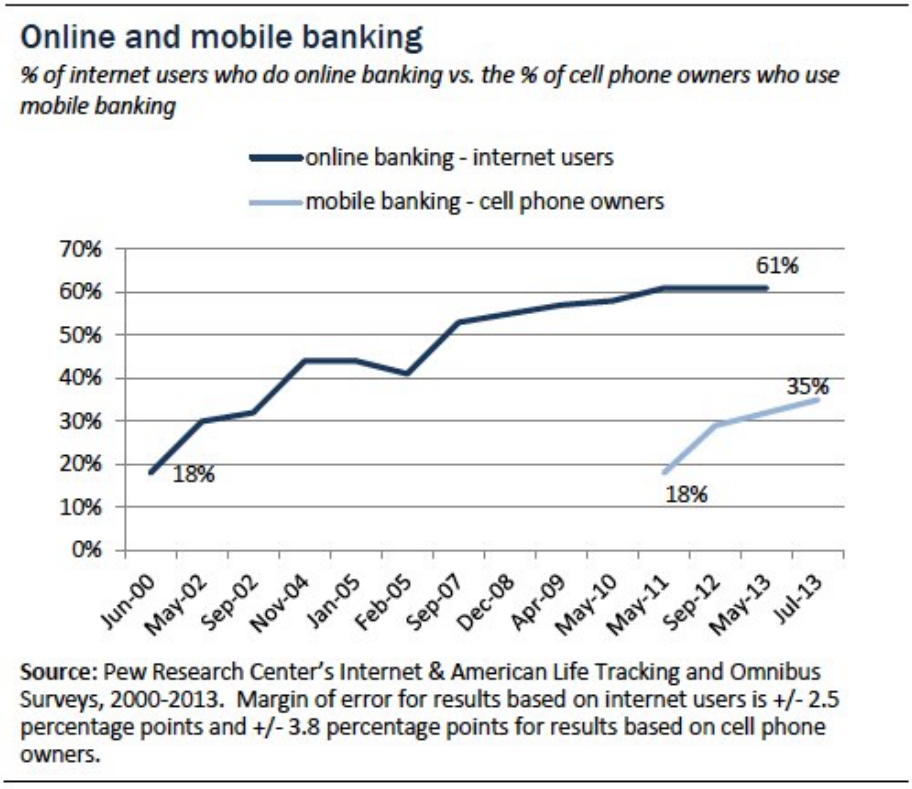

Figure 1: Progression of percentage of Internet Users who use Internet banking from 2000 in the USA

- *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. Also less potential victims means less interest from criminals to set up phishing websites and, thus, less reports to ISPs (and then less blacklisting etc). So this would translate in the benefit of less productivity costs due to taking care of this reports. Also, even more indirectly, less blacklisting implies less possible lawsuits against them from hosting providers.

- *Hosting providers*: again, if it is assumed that less potential victims implies less phishing websites, hosting providers will have the benefit of less costs related to having their websites blacklisted from ISPs (less reports, less damage on public image etc). On the other hand less phishing websites could mean a reduction of their business.

- *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 (time lost in physically going to the bank) is higher than the benefit. This explains why this countermeasure is not adopted by most bank customers.

2.2.4 Externalities

The benefits of adopting this strategy fall mainly on the customers itself and extremely marginally on ISPs, legislators, law enforcement and hosting providers. The costs fall mainly on customers and financial institutions, and marginally on hosting providers.

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 entities, stop translating the domain names of phishing websites for their customers. Customers then, when trying to load the page of the phishing website blacklisted, will end up with an error and thus will not be able to see the phishing website at all.

DNSBL is not an expensive countermeasure, and can be implemented quite easily by ISPs.

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. Also, since blacklisting implies less victims, financial instutitons will spend less resources on incidents (refunds, reporting to law enforcement and hosting providers).
- *Customers of financial institutions*: customers benefit greatly from DNS blacklisting, and this solution is transparent to them so it costs them nothing. This countermeasure, though, at the same time limit their "freedom". ISPs can blacklist domains at their will, without involving their customers in the decisional process. It is hard to express this in terms of a cost for the customers of the financial institutions, but since these people are also customers of the ISPs then it is worth mentioning. Also citizens might prefer this kind of decisions to be made by their government rather then by private companies.
- *Legislators*: legislators have the cost of writing laws in order to regulate blacklisting, since it interferes with freedom of information.
- *Law enforcement*: law enforcement entities benefit from DNSBL because it reduces the number of victims and hence their workload, but also have to deal with new lawsuits from hosting providers towards ISPs.
- *Hosting providers*: they have no benefit from this countermeasure and a significant cost. As a matter of fact this solution obscures domains owned by the hosting providers. In the past hosting providers filed lawsuits against ISPs for DNS blacklisting, for example see [5], but usually without success. Their public image obviously suffer from being blacklisted and thus they become less attractive compared to competitors.
- *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 requested by law enforcement and financial institutions to do so. 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 [6], a picture emerges

quite clearly. ISPs have a lot of power but are not motivated to proactively use blacklisting and do that mainly when requested 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.
- *Language(s) spoken by bank*: Similarly, a bank with a commonly spoken language like English, Spanish, Arab or Chinese, is more interesting to target as phishers can easier produce phishing sites in these languages. Languages like Swedish have less reach.
- *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.

- *Use of tokens*: The use of a security token to prevent the PIN code from being used online via two-step authorisation is a common known example of an anti-phishing measure. It may be used as a proxy for the awareness measures taken by firms.

3.2 Collecting data on the above factors

We have collected 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; Language spoken; Use of tokens. 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.

3.3 Performing statistical analysis

We planned to do a linear regression in SPSS to explore the relation between the explaining interval factors and the dependent factor (being number of attacks, as uptime is hard to explain with concrete factors). For the ordinal variables "Language spoken" and "Use of tokens", a two-sample independent T-test would be appropriate.

3.3.1 Interval variables: Testing for normality and indication of correlation

However, when testing all interval variables for normality, it turned out none of them are normally distributed or have a distribution that looks like a normal distribution. Please see the cumulative percentages of the data and the frequency graphs. Therefore non-parametric tests should be used. However, also the scatter plots (please see the figure) do not indicate any kind of correlation between any of the variables. Therefore further analysis is not promising. PLease note: in order to create sensible scatter plots, a few outliers had to be removed, such as the extreme high number of attacks targeted at PayPal. Also the number of Mastercard and Visa users had to be left out.

3.3.2 Ordinal variables: Problems with sample size

Regarding the ordinal variables - Use of Tokens and Language Spoken - the sample group is too small to make meaningful interpretations. Otherwise, a Mann-Whitney test for independent samples would have been appropriate.

- *Use of Tokens*: Only 11 of the banks do not use a token system, and eleven items is much too small for most statistic tests. A quick exploration tells that all except 3 are attacked less than 40 times, which is not exactly often regarding the data. Although not significant, it also does not support the hypothesis that not using tokens increases the probability of attacks.
- *Language Spoken*: 32 of the 59 banks have English as main language. 9 of them use multiple languages, like Mastercard, PayPal and ING do. However, the other banks are scattered amongst Spanish (3), French (2), Italian (4), Russian (1), Malay (1), German (2) and Portugese (4), resulting in groups no larger than 4. This is much too small to draw significant conclusions from.

Concluding, to our regret it is impossible to point out any relation between the explaining factors and the dependent number of attacks per company. It is realistic to suspect that this is due to a bias the dataset surely contains - not all financial institutions will bother to notify phishing sites to Clean-mx and although there is a lot of data, the timeframe of the dataset is limited to 10 days. Next to that, all explaining factors were retrieved manually from a great amount of different sources. It would have been great to compare the number of attacks based on data from a trustworthy source like the World Bank, as was done in the first assignment with GDP.

	A	B	C	D	E	F	G	H	I
1		Number of attacks	Cumulative percentage	Total money deposited	Cumulative percentage	Revenu	Cumulative percentage	Number of customers	Cumulative percentage
2	TOTAL	7267	100%	$ 18.886.674.552.637,70	100%	$ 76.585.889.093.468,10	100%	75428258044	100%
3	MIN	5	0%	$ -	0%	$ -	0%	0	0%
4		6	0%	$ -	0%	$ -	0%	0	0%
5		6	0%	$ -	0%	$ -	0%	0	0%
6		6	0%	$ -	0%	$ -	0%	13380	0%
7		7	0%	$ -	0%	$ 1.465.000,00	0%	60000	0%
8		7	1%	$ -	0%	$ 3.826.901,87	0%	70000	0%
9		8	1%	$ -	0%	$ 9.564.000,00	0%	89500	0%
10		8	1%	$ -	0%	$ 13.610.822,00	0%	154497	0%
11		9	1%	$ -	0%	$ 13.815.224,06	0%	431000	0%
12		10	1%	$ -	0%	$ 158.000.000,00	0%	500000	0%
13		10	1%	$ -	0%	$ 319.357.234,49	0%	500000	0%
14		11	1%	$ -	0%	$ 343.252.799,06	0%	900000	0%
15		13	1%	$ -	0%	$ 455.000.000,00	0%	1400000	0%
16		13	2%	$ 158.000.000,00	0%	$ 483.373.000,00	0%	1500000	0%
17		14	2%	$ 330.617.835,77	0%	$ 695.700.000,00	0%	2600000	0%
18		14	2%	$ 447.809.377,40	0%	$ 777.470.841,01	0%	3000000	0%
19		14	2%	$ 464.000.000,00	0%	$ 920.000.000,00	0%	3000000	0%
20		14	2%	$ 549.734.000,00	0%	$ 1.649.785.144,26	0%	4000000	0%
21		15	3%	$ 3.251.000.000,00	0%	$ 1.918.412.348,40	0%	4600000	0%
22		16	3%	$ 3.555.585.410,00	0%	$ 2.080.000.000,00	0%	6000000	0%
23		16	3%	$ 3.973.000.000,00	0%	$ 2.750.082.900,41	0%	6173000	0%
24		16	3%	$ 5.400.000.000,00	0%	$ 2.800.000.000,00	0%	6700000	0%
25		16	3%	$ 6.913.000.000,00	0%	$ 3.200.000.000,00	0%	7000000	0%
26		17	4%	$ 7.780.000.000,00	0%	$ 3.600.000.000,00	0%	7100000	0%
27		17	4%	$ 7.900.000.000,00	0%	$ 4.114.000.000,00	0%	7500000	0%
28		18	4%	$ 8.391.000.000,00	0%	$ 4.200.000.000,00	0%	7600000	0%
29		21	4%	$ 8.600.000.000,00	0%	$ 6.300.000.000,00	0%	8600000	0%
30		21	5%	$ 13.700.000.000,00	0%	$ 8.305.000.000,00	0%	9000000	0%
31		24	5%	$ 16.600.000.000,00	0%	$ 8.471.000.000,00	0%	9000000	0%
32		24	5%	$ 24.157.600.000,00	1%	$ 9.473.000.000,00	0%	10400000	0%
33		26	6%	$ 29.877.800.000,00	1%	$ 9.945.371.775,42	0%	10500000	0%
34		28	6%	$ 31.000.000.000,00	1%	$ 10.421.000.000,00	0%	10700000	0%
35		28	7%	$ 32.595.000.000,00	1%	$ 11.200.000.000,00	0%	11000000	0%
36		32	7%	$ 41.452.000.000,00	1%	$ 13.376.000.000,00	0%	11000000	0%
37		33	7%	$ 44.590.000.000,00	2%	$ 13.877.433.309,30	0%	12700000	0%
38		34	8%	$ 44.607.000.000,00	2%	$ 16.600.000.000,00	0%	13400000	0%
39		36	8%	$ 56.796.300.000,00	2%	$ 17.740.000.000,00	0%	14000000	0%
40		38	9%	$ 65.600.000.000,00	2%	$ 17.900.000.000,00	0%	14000000	0%
41		39	9%	$ 66.232.000.000,00	3%	$ 18.530.000.000,00	0%	16000000	0%
42		39	10%	$ 71.998.000.000,00	3%	$ 23.176.000.000,00	0%	18000000	0%
43		40	11%	$ 133.742.000.000,00	4%	$ 23.289.777.094,54	0%	22000000	0%
44		41	11%	$ 184.518.000.000,00	5%	$ 24.033.000.000,00	0%	23000000	0%
45		41	12%	$ 199.000.000.000,00	6%	$ 29.532.667.179,09	0%	23400000	0%
46		42	12%	$ 210.400.000.000,00	7%	$ 29.961.000.000,00	0%	30000000	0%
47		47	13%	$ 228.000.000.000,00	8%	$ 31.700.000.000,00	0%	32000000	0%
48		59	14%	$ 261.000.000.000,00	10%	$ 37.300.000.000,00	1%	41666667	1%
49		71	15%	$ 261.000.000.000,00	11%	$ 47.012.127.894,16	1%	48000000	1%
50		87	16%	$ 300.384.657.897,65	13%	$ 48.000.000.000,00	1%	48000000	1%
51		167	18%	$ 414.903.000.000,00	15%	$ 56.100.000.000,00	1%	50000000	1%
52		170	21%	$ 461.600.000.000,00	17%	$ 61.240.000.000,00	1%	53000000	1%
53		207	23%	$ 489.000.000.000,00	20%	$ 71.651.000.000,00	1%	57000000	1%
54		214	26%	$ 546.128.000.000,00	23%	$ 84.300.000.000,00	1%	65000000	1%
55		215	29%	$ 642.120.000.000,00	26%	$ 85.110.000.000,00	1%	70000000	1%
56		225	32%	$ 687.317.448.116,83	30%	$ 179.000.000.000,00	1%	157000000	1%
57		249	36%	$ 690.000.000.000,00	33%	$ 673.518.000.000,00	2%	169000000	1%
58		429	42%	$ 1.350.642.000.000,00	41%	$ 6.215.000.000.000,00	10%	2000000000	4%
59		743	52%	$ 1.757.000.000.000,00	50%	$ 29.659.000.000.000,00	49%	2300000000	7%
60	MAX	3491	100%	$ 9.473.000.000.000,00	100%	$ 39.014.320.000.000,00	100%	70000000000	100%

Figure 2: Cumulative Percentages showing skew distributions

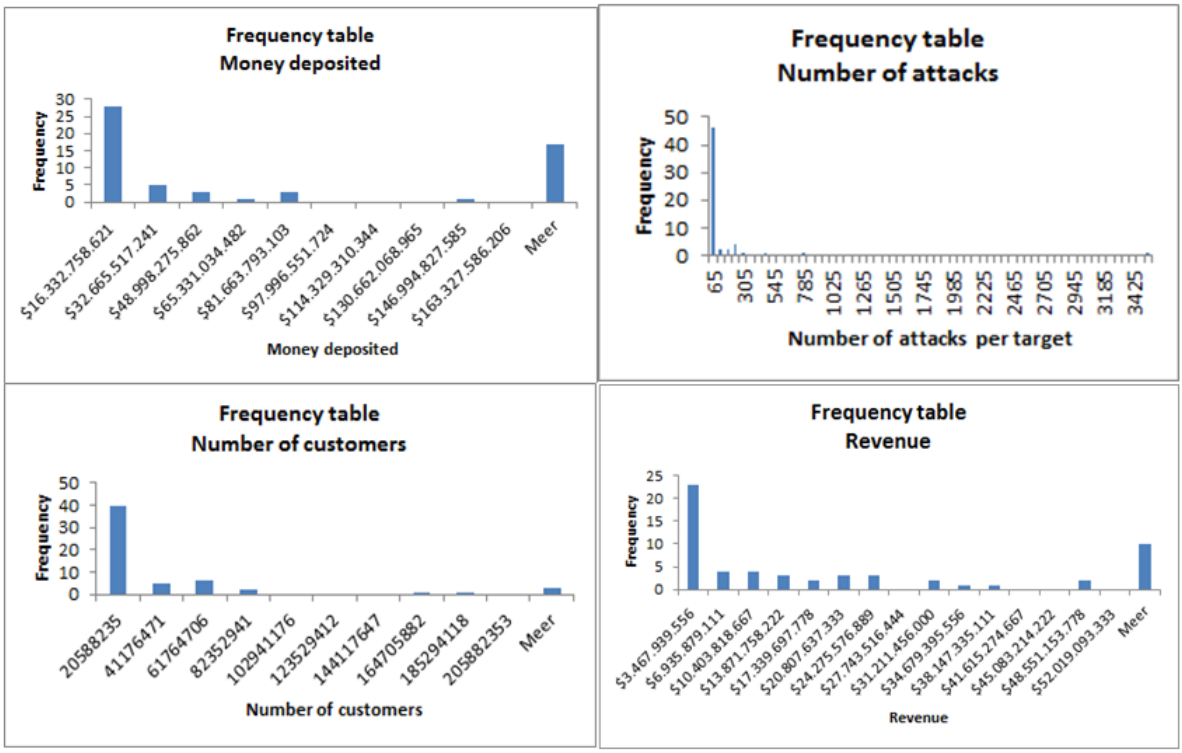

Figure 3: Frequency Graphs of independent interval variables

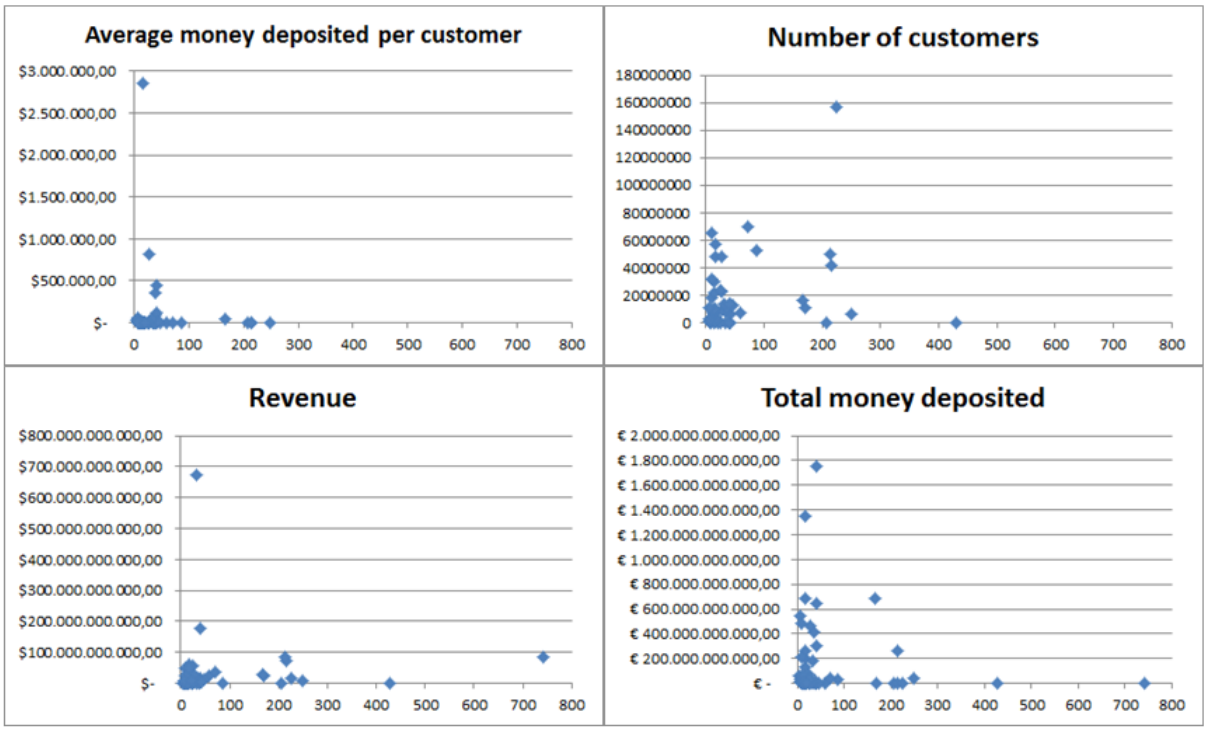

Figure 4: Scatter Plots of independent interval variables, not indicating correlation

References

[1] `https://www.mwrinfosecurity.com/articles/why-security-awareness-campaigns-fail/`.

[2] `https://www.wbs-law.de/eng/privacy-law-eng/phishing-bank-customer-liable-50027/`.

[3] "Pew research center's internet american life tracking and ombibus surveys: 51% of u.s. adults bank online," 2013, http://www.pewinternet.org/2013/08/07/51-of-u-s-adults-bank-online/.

[4] M. Jakobsson and S. Myers, *Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft*. Wiley, 2006. [Online]. Available: https://books.google.nl/books?id=xxAbEcNlIwwC

[5] "Emarketersamerica vs dnsbl operators in florida," 2003, http://www.linxnet.com/misc/spam/slapp.php.

[6] 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