Assignment 3

1. Who is the problem owner of the security issue as measured in your first assignment?

A problem owner is affected by the security issue or benefits from the solution to this issue [1]. The security issue discussed is phishing.

Originally the first assignment was focused on the targeted countries of the phishing websites. Metrics and measurements were made, but due to a misunderstanding of one of the variables they did not measure as intended. Therefore focus has now shifted towards the targeted companies.

The dataset consists of the 24.000 most recently closed phishing sites on Clean-mx. Looking at the data, it can be seen that most of the targets - nearly 50% - are either banks or other financial transaction organisations. This is an obvious finding, since the ultimate goal of the attacker is to acquire money [2].

Because of this finding and because it makes this assignment a lot more relevant, the focus in this assignment will be laid on the *banks and financial transaction organisations affected by the phishing websites.*

In The Netherlands, most banks offer financial compensation for victims of phishing, unless they have been very neglectful, even if they are not always obligated to do so. It is the responsibility of banks to warn their clients against phishing tactics [3] - also see paragraph 3.

The loss for the targeted organizations does not only consist of the direct costs of compensating victims of phishing, but a high number of incidents may affect the reputation of the organization and it may decrease the willingness of its customers to use internet banking or other digital services. Consumers see security as a commodity. The CSO of PayPal, one of the world's most often targeted organizations, said that phishing is an overestimated threat and that it's not even in the top 5 threats [4].

One could think of the concept of network externalities in relation to phishing, but it seems like a phishing incident is as bad for the targeted organization as for the actual consumer/victim. The phishers however use money mules to shift the costs of being caught unto them, by letting the mules transfer the money to them via non-refundable operations. In this way, the mule is liable for the costs.

2. What relevant differences in security performance does your metric reveal?

The metric measures the amount of phishing sites targeted at a certain company per time unit - in this case, attacks per 24 hours - and the distribution of uptime at that company in hours, visualized in a histogram (see appendix). Since this assignment focusses at financial institutions, it was analysed how many of the targets are in this sector. Almost half of the targets is in the financial sector, while the other targets are scattered amongst various sectors. Not surprisingly, over 7.300 of the 13.600 attacks at known targets is aimed at a financial institution.

An important finding is that PayPal is targeted most often (almost 3.500 phishing sites in 10 days) - far more often than credit card providers like MasterCard, Visa and American Express, who are at the bottom with at less than 1 phishing site per day. The unpopularity of credit cards can be explained by the possibility of pulling back payments within a certain amount of time, making phishing less attractive. However, PayPal offers a similar service, only excluding private money transactions from this policy [5]. This is called the PayPal Purchase Protection and it allows consumers to reclaim their money when sellers do not deliver what they promise - which is often the case with phishing. This makes the huge difference in amount of attacks odd.

Furthermore, the two most targeted companies (PayPal and Wells Fargo) seem to deal with phishing sites in a similar tempo. 30-40% of the phishing websites is taken down within 1 hour, and the uptime of 30-40% of the sites is pretty much evenly spread over 2 to 6 days.

Lastly, the revenue of a target does not directly correlate to the amount of phishing sites targeted at the company. This is illustrated by for example Poste Italiane, who is number 4 in number of attacks, but whose revenue is about three times smaller than the number 6 and 7, and similar to the number 8. One would expect more attacks when a company handles more money. This discrepancy might indicate a lower level of security, but interestingly this is disproven by 97% of the Poste Italiane phishing sites being put down within 2 hours.

3. What risk strategies can the problem owner follow to reduce the security issue as measured in your first assignment?

Rainer Böhme [6] explained that business drives security strategies for security providers. Security is not the core competence of security providers. He mentions that the economics of information goods create an environment with significant network externalities and economies of scale. Because a monopoly position is at stake, it is rational to ship the product as early as possible and to add security features later.

However, although this might be the case for new companies and services, the situation is a little different for banks. Banks have been providing services in which security is a core feature for many years, in fact people put their money on a bank to keep it safe and to get financial services. People do not get involved with online banking unless they are convinced of its security. eBay is a company that is targeted very often by phishers and this fits Böhme's description much better.

There are 4 strategies banks and other financial transaction organisations can follow to reduce the security issue.

Firstly the banks and other financial transaction organisations can apply risk mitigation. This is an important strategy. Risk mitigation tries to reduce the likelihood and severity of loss events by protecting vulnerable assets with technical and organisational measures. This can be done by, for example, finding and removing the phishing websites, educating customers in order to prevent them to use the phishing websites, or finding and stopping attackers that are at the source of phishing websites.

The second strategy discussed is risk acceptance. Overall this is done quite a lot. For big companies such as PayPal, a lot of phishing websites are created throughout a small period of time. It is hard to mitigate at a high level. The obvious measure a bank can take is to mitigate through better educating their customers about phishing. But there will always be people that fall for the deceit. So, to some extent it is not profitable to put much effort in mitigating this issue and companies choose to accept the issue to a certain level. This is often combined with some sort of compensation for the customer involved in the attack.

The third strategy is risk avoidance. This is very hard for banks and other financial transaction organisations. In order to avoid the risk, one would have to remove the features which are being exploited, such as online banking or online payment systems. Since these are big features which are very convenient for the customers, and are excessively used, it is unthinkable to remove these features.

The last strategy is risk transfer. The impacts that the organisations experience are mostly indirect. Attackers don't focus on the organisation but on the customers. Because the customers play an important role, risk transfer also has its role in the overall strategy. This is done by policy specifications [7]. Because the attacks are customer driven, the organisation can't always be held responsible for the incident. Therefore every organisation has a policy specification regarding phishing attacks, which can decide who is responsible for the incident. Since organisations might exploit this in disadvantage of their customers, there are also certain laws towards this issue. For example, in the Netherlands, if a bank has not warned a customer enough about phishing, they are required to compensate the customer in case he/she becomes a victim [8].

4. What other actors can influence the security issue as measured in your first assignment?

There is a large number of actors involved in the phishing issue. The most important are:

Bank customers: clients are, along with the banks, the main victim of phishing. Usually some form of refund policy exists between them and the bank: if this is the case they will not lose their money, but the bank does. For example, in the UK the FCA Rules state that banks must refund any unauthorised transaction, with the burden of proof on the bank to show that the customer either gave their explicit authorisation or that there was "gross negligence" in how they protected their card or login details [9-10]. A 13-month time limit applies for reporting theft. It must be stressed, though, that even if bank customers do not incur in financial loss, other forms of personal loss exist. Among them there are loss of time, stress, decreased trust and use of the internet and embarrassment [11].

Law enforcement. This category contains the police, attorneys, judges, courts and in general every entity that, under the guidance of a state, tries to arrest and prosecute phishers while protecting citizens and companies from them. All these entities do not suffer direct losses from banking phishing. They definitely have an influence on the problem though. For example the amount of resources a country spends in law enforcement can change the behaviour of phishers, and same goes for the time it takes to catch and prosecute this individuals.

Consortiums of banks: banks sometimes cooperate in high level associations like, for example, the Dutch Banking Association (Nederlandse Vereniging van Banken, NVB). With these consortiums banks try to tackle security problems, phishing included, together. These actors definitely have some influence on the problem, but lack real power. When it's the time to apply the policy they might come up with, each bank still has the freedom acts on its own.

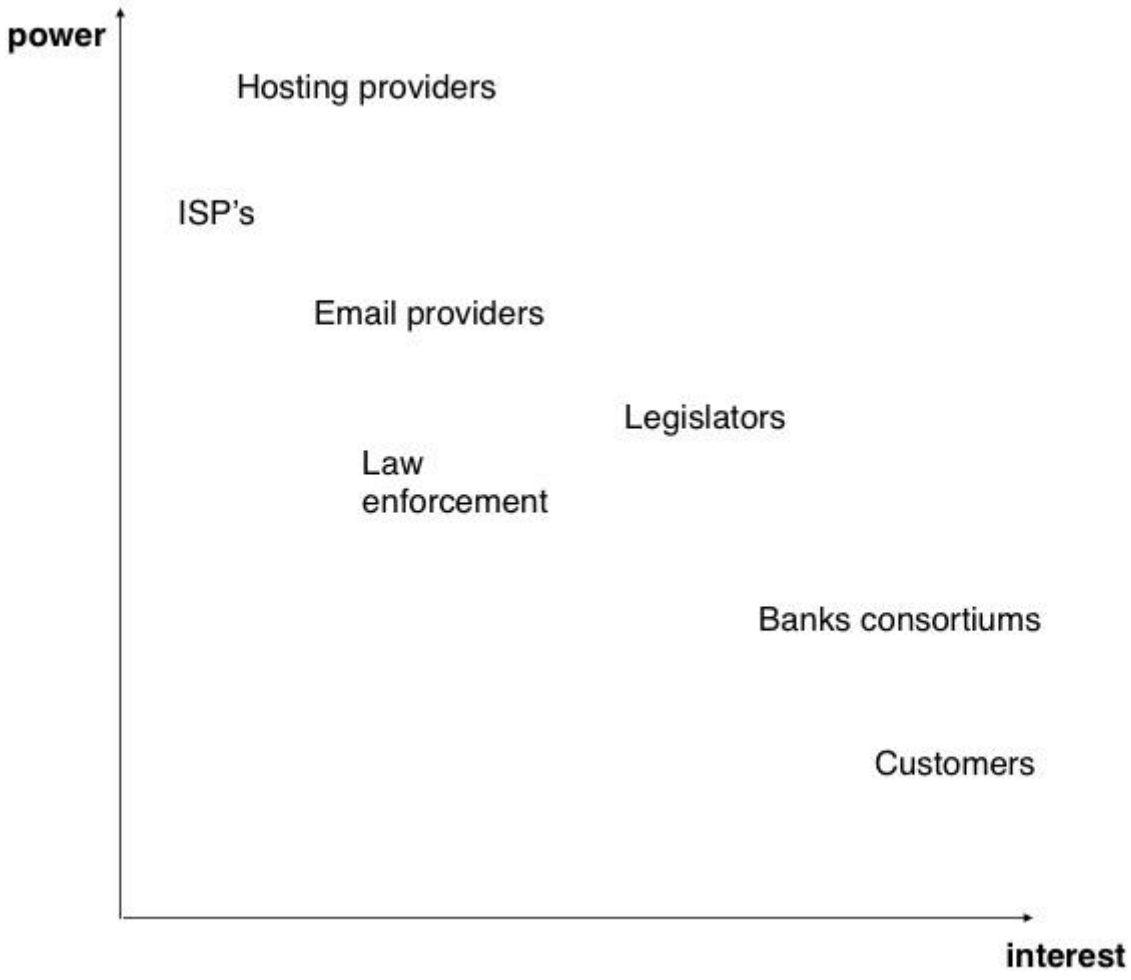
Hosting providers: these are the companies that provide an IP address to phishing websites and sometime host them on their servers. Some popular names are GoDaddy, HostGator and DreamHost. Sometimes the ISPs provide this service to their customers. These actors are the ones that actually have the power to shut down the phishing websites when requested by law enforcement or by the damaged institutions (in this case banks). However they do not really suffer direct losses from bank phishing, hence they are not extremely motivated to act as fast as possible and to prevent the phenomenon.

Internet Service Providers: they are the owners of (a part of) the network and they provide internet to citizens and companies. Just to name a few ISPs in The Netherlands: Vodafone, KPN, Ziggo, Tele2 etc. Like the hosting providers they do not suffer direct losses from banking phishing but they are marginally damaged, since a percentage of their resources, even if very small, is used for these activities. In other words ISPs allocate resources for people that should not be able to use the service at all. Since most internet users use the DNS of ISPs, they can have a big effect on phishing websites because they can easily blacklist and thus obscure them from public access.

Email providers: similarly to ISPs a percentage of their resources is used. For example they spend resources to store all their clients emails in servers, including phishing ones. They carry the messages that contain the links to the phishing websites, and they do this for free. Email providers themselves suffer from phishing. This makes them more interested in solving the general issue if compared to ISPs or hosting providers. Being the main distribution channel of banking phishing, ISPs are a very important actor to involve in order to disrupt the phishers killchain.

Legislators: they decide how to solve this issue from the legal perspective (how to punish criminals, cooperation agreements with other countries etc.) and how much budget law enforcement should get.

The power-interest graphic at the end of this paragraph gives an idea of why phishing is so hard to fight. The Y-axis measures power that is an indicator of how much an actor can do to solve the phishing problem. The X-axis, on the other hand, measures the interest that actors have on getting rid the problem. The more powerful entities, like ISPs and Email providers, do not have a real incentive in being more effective against phishing because they do not suffer the consequence from it, whereas the actors that are actually being hit, mainly banks' customers and banks, do not have enough influence to solve the problem by themselves.



5. Identify the risk strategies that the actors can adopt to tackle the problem. Are there actors with different strategies? Why? Have the strategies changed significantly over time in a way that reduces or increases risks?

Bank customers: banks' clients most effective strategy is risk avoidance. They can choose not to use internet banking at all in order to avoid phishing losses. This is obviously a very helpful, though extreme, measure. As explained in section 4 sometimes banks refund their clients completely if they are victims of phishing and other cybercrimes. This could qualify as a form of risk transfer since the agreement moves the risk from them to the bank. Customers could clearly apply risk mitigation by being extremely careful when logging into banks' websites and by getting more aware. Also customers' risk strategy is clearly shifting from risk avoidance to risk acceptance, since each year more and more people start using internet banking [12]. This rapid increase in the volume of people doing home banking (potential victims) has definitely increased risk: now cybercriminals are way more interested in performing banking phishing than for example 5 years ago because the potential victim population is now way bigger.

Law enforcement entities put a lot of efforts in risk mitigation strategies. They run awareness campaigns as well as investigating crimes and arresting criminals. In this last sense they try to reduce the risk by reducing the threat population. Risk avoidance is not an option for law enforcement, as well as risk transfer. Risk acceptance is contemplated in the sense that clearly in no country 100% of law enforcement resources are used to fight phishing, since there are a lot of other problems to deal with. Hence it's assumed that some of this accidents will happen.

Consortium of banks: Their main risk mitigation and risk acceptance. Examples of mitigation measures are awareness campaigns, the discussion of best practices, the establishment of cooperation agreements between banks (information sharing regarding incidents especially) etc. Risk acceptance is a strategy that banks must adopt at this point, since risk avoidance is not really an option. If a bank was to shut down its online banking services, the loss due to being less attractive than competitors would be probably higher than the actual loss due to phishing. Risk strategies changed in the last years because banks have decided together against phishing. An example is the adoption of the iDeal system in The Netherlands. This system is shared by all the main banks of the country and realize a high level of security by using two-factor authentication, namely a challenge-response access token based on the chip embedded in the debit card or ATM card [13]. In this country banks decided to explicitly not compete on security [14].

ISPs. It is hard to determine which risk strategy ISPs are applying, since they are hit so marginally by the issue. For sure they do not have enough motivation to use risk reduction, and this is extremely unfortunate since they could do a lot - for example, analysing traffic and locating sources of phishing. Strategy has not changed significantly over time.

Hosting providers. The same assumptions made for ISPs are applicable to hosting providers. They do not apply risk reduction. They do risk acceptance in the sense that by not trying to prevent the problem in any way they accept that eventually they will lose resources (mainly time and productivity) to shut down phishing websites when requested by authorities. Strategy has not changed significantly over time. These actors could apply risk mitigation for example by checking regularly the content of the websites that they host.

Email providers. Email providers mainly apply risk reduction by the development and deployment of technological solutions like anti-spam filters. Similarly to ISPs they are hit only marginally by phishing, so they do not have enough incentives to do more. Competition between providers, though, had

some effect, in the sense that some email providers are investing resources to make their anti-spam filters better. So these actors are reducing risk, even if not incentivised by the issue itself.

Legislators clearly apply risk reduction. For example by running awareness campaigns and by developing specific policies and laws. Risk transfer and avoidance are not really suitable options for governments. Since more and more of their citizens are performing internet banking, and therefore are vulnerable to phishing, governments are in general more aware of the issue and are now doing more compared to the past. It's hard to quantify the impact this efforts had in reducing the risk, though it's even harder to imagine that awareness campaigns, as an example, did have not even a small effect on the risk.

Concluding, a clear pattern is visible. The actors suffering the most from banking phishing mainly put a lot of effort in risk reduction and risk acceptance, whereas the actors with more power (but less interest in solving the problem) do not really put enough real effort in any risk strategy. For some actors, namely banks' customers and bank consortiums (again the ones suffering more consequences of the issue), the strategy adopted changed significantly over time; as an example the shift from avoidance to acceptance is quite noticeable for bank's customers.

6. Pick one of the risk strategies identified previously and calculate the Return on Security Investment (ROSI) for that particular strategy. I.e.,

- **Estimate the costs involved in following that strategy**
- **Estimate the benefits of following that strategy (assume a particular loss distribution)**

In 2014, Dutch banks lost €4.7 million because of phishing [15]. ING Bank holds around 40% of the checking accounts. We estimate that ING Bank lost around 0.4* €4.7 million = € 1.9 million.

If ING Bank would like to mitigate the risks of phishing, two important strategies come to mind:

- Educating customers more about phishing tactics,
- Having customers use two factor verification.

Two factor verification methods combines both knowledge of the customer (a password) with property of the customer (a token retrieved from a mobile phone or a device with a card reader). This method is already widely used in internet banking. ING Bank implements this by sending a code to the customer's mobile phone every time the customer wants to transfer money. Although most customers are aware that they should never tell their password to anyone, it is less known that they should also not give to anyone the tokens produced by the card reader device or sent to the mobile phone. If a customer has already given up his password to a phisher and is unaware of this, the phisher can call him under the disguise of a bank clerk and ask for a token, while pretending that there is a problem with the victim's bank account.

Using two factor verification is useless if customers are not sufficiently aware of phishing and cannot recognize a phishing attempt. This is why we will focus on 'educating customers more about phishing tactics' for calculating the Return on Security Investment.

In order to mitigate the financial risk of phishing for ING Bank by educating and warning customers about phishing, the bank could make it mandatory for new internet banking customers to complete a short tutorial about phishing before they can use their online account. An example of a suitable tutorial is 'Anti-phishing Phil', a serious game created by researchers at Carnegie Mellon University [15]. This game teaches users to identify phishing URLs, to look for cues for trustworthiness in web browsers and to use search engines to verify if the site is legitimate. After playing the serious game, 60% less fraudulent websites were incorrectly assumed to be legitimate [16]. Therefore we estimate that if all internet banking users would play this game, it could save around 0.6*€1.9 million = €1.1 million.

In these tables, an overview of the costs and benefits of this strategy can be found:

Costs

Resource	Cost estimate	Justification
Buying/developing a serious game	€10.000 per year	A price of €20.000 is reasonable for a serious game. The game needs to be updated every two years to reflect changes in phishing strategies.
Helpdesk employees for answering questions about the game	€44.000 per year	Two employees are working full time on helping customers with their questions about the game and phishing in general.
Adding mandatory serious game to online banking environment	€9.000 per year	Three experienced software developers work for a month to add the serious game to the existing system. Then every year for maintenance.

Total solution costs: €63.000

Benefits

Result	Benefit estimate	Justification
Higher ability of customers to recognize a phish	€1.1 million	The amount of phishing sites incorrectly assumed to be legitimate sites fell with 60% in the research: 0.6*€1.9 million = €1.1 million

The risk exposure is still €1.9 million, but now there is a risk mitigation of 60%.

ROSI = ((1.9 million * 60%) - €63.000)/ €63.000 = 1700%

This seems like a very high estimate. It could be possible that the risk mitigation is overestimated because participants in the study are more aware just after learning about phishing, but the effect wears off over time. However, it would be interesting to further research the benefits of introducing a serious game about phishing for internet banking customers. An additional benefit of this approach is that ING Bank decreases its liability in cases where a phishing victim seeks compensation from the bank, because ING Bank could easily prove that they did warn customers enough about phishing.

References:

[1] http://www.igi-global.com/dictionary/problem-owner/23507

[2] Jakobsson, Markus, and Adam L. Young. "Distributed Phishing Attacks." IACR Cryptology ePrint Archive 2005 (2005): 91.

[3] http://www.geldenrecht.nl/artikel/2013-08-19/geen-compensatie-voor-phishing-slachtoffer

[4] PayPal CSO: Phishing threat overstated: http://www.darkreading.com/attacks-breaches/paypal-cso-phishing-threat-overstated/d/d-id/1128582

[5] https://www.paypal.com/nl/webapps/mpp/paypal-safety-and-security, accessed October 2015

[6] Böhme, R. (2015). Security Strategies. Lecture in the TU Delft course WM0824, October 2015

[7] Bradbury, J. A. (1989). The policy implications of differing concepts of risk.Science, technology & human values, 14(4), 380-399.

[8] https://www.nvb.nl/nieuws/2013/2365/regels-voor-veilig-internetbankieren-bij-alle-banken-gelijk.html

[9] https://www.moneyforce.org.uk/Managing-crises/Fraud-scams-and-identity-theft/Are-you-liable

[10] http://www.fca.org.uk/consumers/financial-services-products/banking/your-rights/unauthorised-payments

[11]Kelley, C. M., Hong, K. W., Mayhorn, C. B., & Murphy-Hill, E. SOMETHING SMELLS PHISHY: EXPLORING DEFINITIONS, CONSEQUENCES, AND REACTIONS TO PHISHING. Age, 32, 13-06.

[12] http://www.pewinternet.org/2013/08/07/51-of-u-s-adults-bank-online/

[13] https://en.wikipedia.org/wiki/IDEAL

[14] https://www.thehaguesecuritydelta.com/news/newsitem/320

[15] S. Sheng et al. Anti-Phishing Phil: The design and Evaluation of a Game That Teaches People Not to Fall for Phish. Proceedings of the 3rd symposium on Usable privacy and security. Pp 88-99. New York, USA.

[16] ‘60% minder fraude in het betalingsverkeer’. Kirsi Rautiainen, Nederlandse Vereniging van Banken. Press release, March 11 2014.

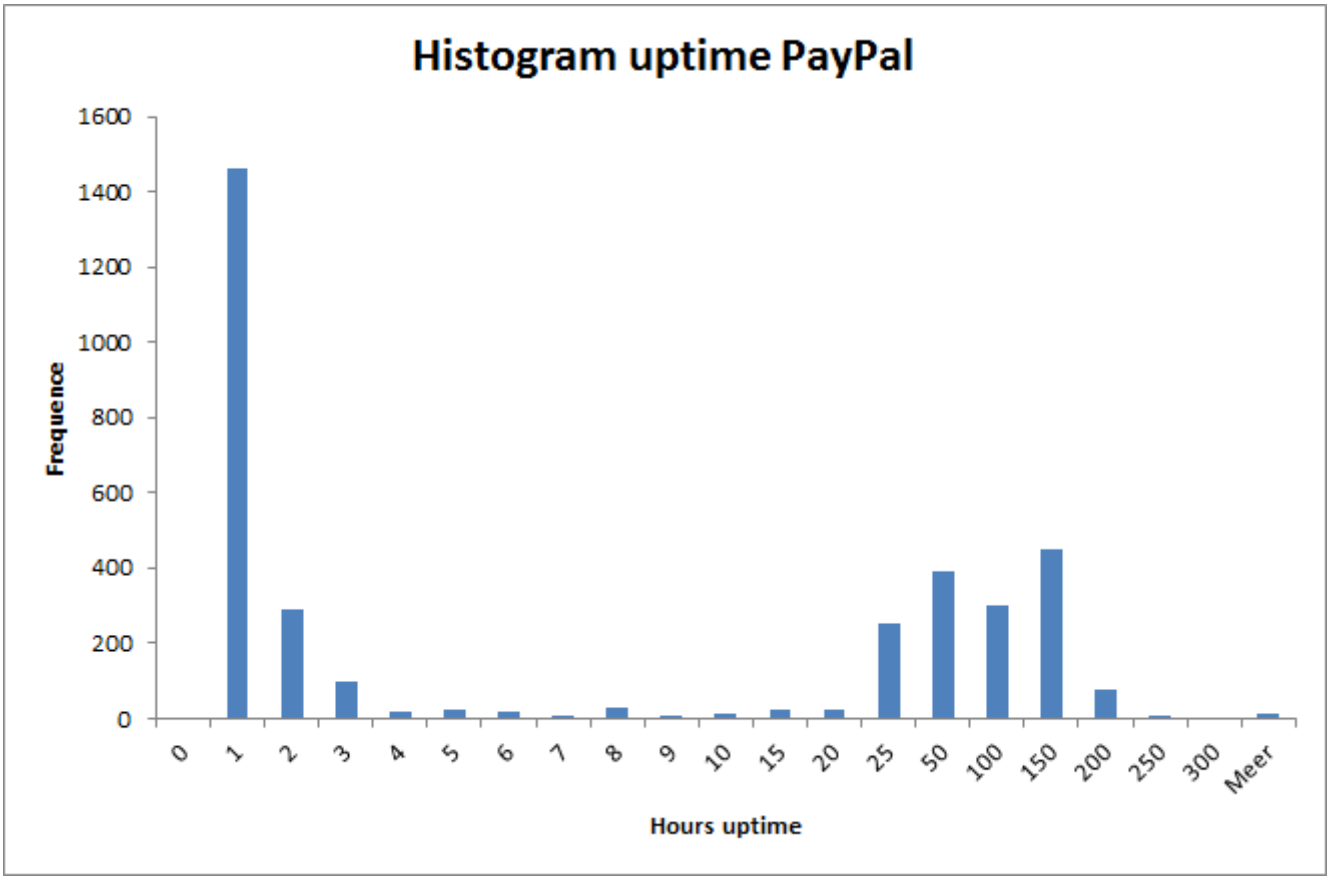
Appendix A

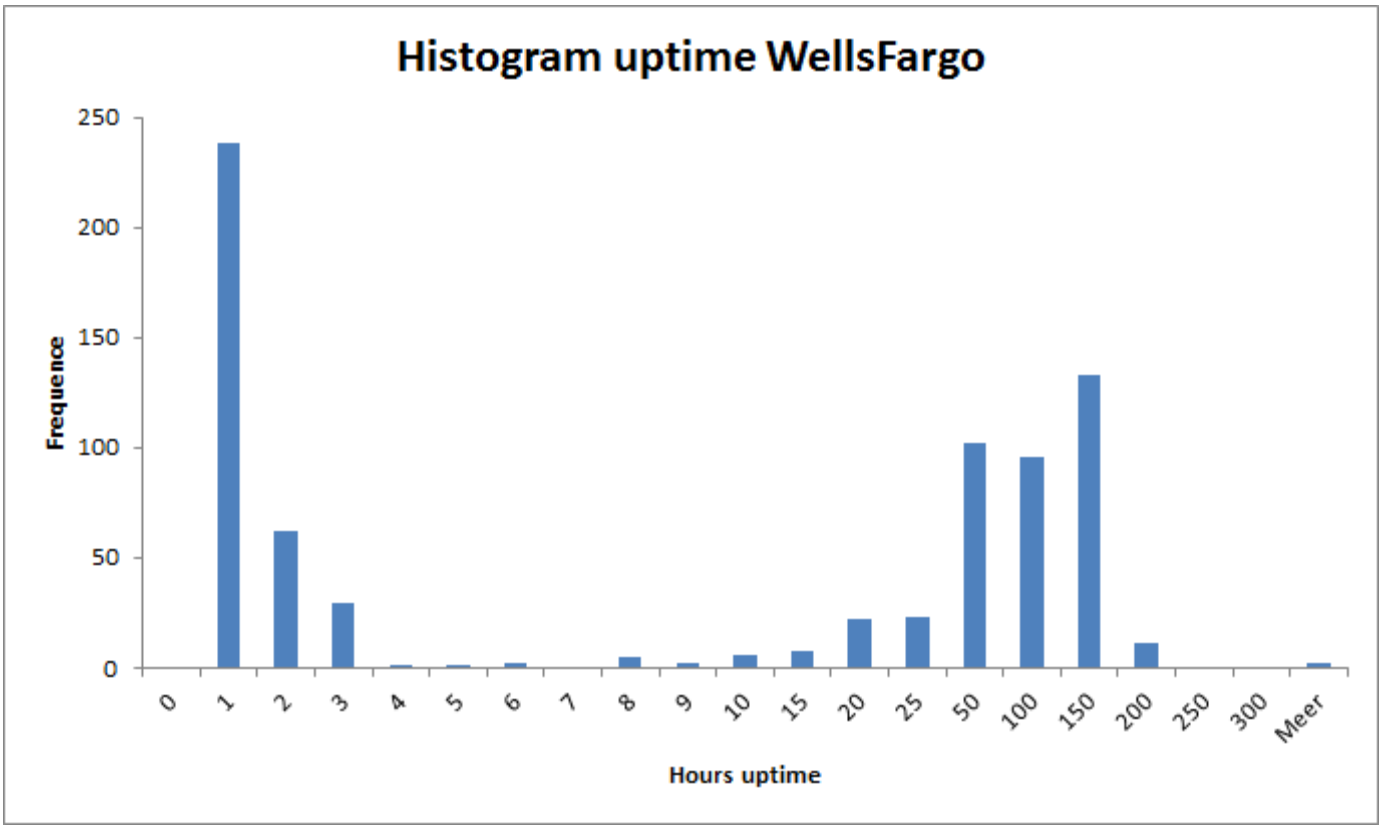
Statistics table for phishing sites						
	PayPal		Wells Fargo		Poste Italiane	
Number of phishing sites during data collection	3491		743		249	
Probable number of phishing sites in 24 hours	347		74		25	
MAX [h]	401.185,86		3.118,4		121,0	
MODUS [h]	24		0,5		0,1	
MEDIAAN [h]	1,82		17,3		0,3	
MEAN [h]	380,56		48,7		2,6	
Frequencies of uptime						
Interval [hour]	Frequency	% chance	Frequency	% chance	Frequency	% chance
0	0	0%	0	0%	0	0%
1	1464	42%	238	32%	221	89%
2	292	8%	62	8%	21	8%
3	99	3%	29	4%	0	0%
4	19	1%	1	0%	1	0%
5	21	1%	1	0%	0	0%
6	17	0%	2	0%	0	0%
7	8	0%	0	0%	0	0%
8	28	1%	5	1%	0	0%
9	9	0%	2	0%	0	0%
10	13	0%	6	1%	0	0%
15	21	1%	8	1%	0	0%
20	23	1%	22	3%	0	0%

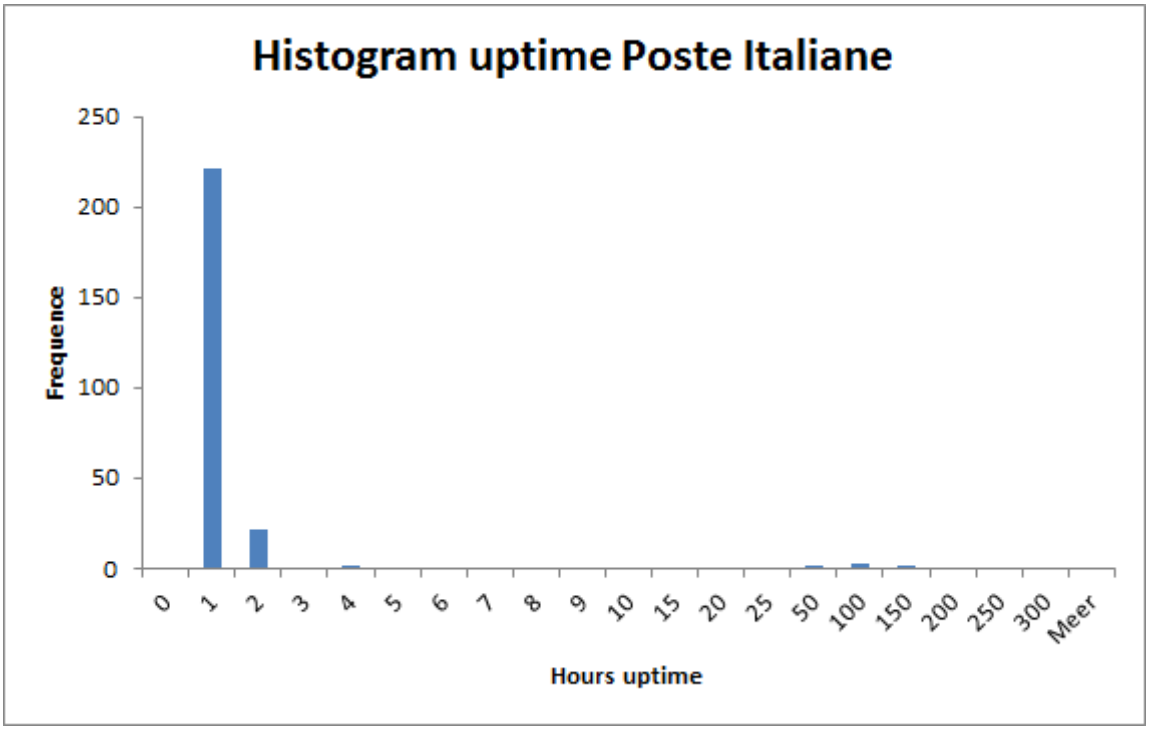
25	252	7%	23	3%	0	0%
50	391	11%	102	14%	1	0%
100	298	9%	96	13%	3	1%
150	448	13%	133	18%	2	1%
200	75	2%	11	1%	0	0%
250	2	0%	0	0%	0	0%
300	0	0%	0	0%	0	0%
Meer	11	0%	2	0%	0	0%

The frequency intervals are chosen in a way that allows a meaningful interpretation of the histogram. It shows the difference in the first few hours, but is less sensitive to difference between an uptime of 3 or 3.1 days. Higher uptimes are caught in larger intervals. The first ten hours are measured in intervals of 1 hour, then the intervals take steps of 5 hours until the uptime is 1 day, then the intervals take steps of ~1 day until 6 days have passed. Uptimes higher than 6 days are rare.

Appendix B


Histogram uptime PayPal
Frequence
1600
1400
1200
1000
800
600
400
200
0
0 1 2 3 4 5 6 7 8 9 10 15 20 25 50 100 150 200 250 300 Meer
Hours uptime


Histogram uptime WellsFargo
Frequence
250
200
150
100
50
0
0 1 2 3 4 5 6 7 8 9 10 15 20 25 50 100 150 200 250 300 Meer
Hours uptime


Histogram uptime Poste Italiane
Frequence
250
200
150
100
50
0
0
1
2
3
4
5
6
7
8
9
10
15
20
25
50
100
150
200
250
300
Meer
Hours uptime