ECS - Individual Assignment

Ricky Sewsingh

November 2015

1 Abstract

The main topic in this paper is the combination of legislation and phishing. When attackers decide on a country to host their phishing website, several reasons are involved in this decision. This paper discusses if legislation has a big influence in this decision. The hypothesis used in this paper is that legislation does have a big influence in this decision. In order to obtain a conclusion in this matter, countries with a high and a low amount of phishing websites have been compared. It was found that there was no big difference in the legislations of the countries compared. Then several other reasons have been discussed, which could have an influence in the decision of an attacker. Four different reasons have been discussed: Phishing awareness in a country, Domain names, Country's effort to take down a phishing website and the influence of Domain name registrars, Hosting providers and ISP's.

2 Introduction

Phishing is an ominous threat in the field of cybercrime. Daily lots of victims fall for phishing attacks, resulting into high losses for both consumers and businesses around the world. According to the RSA[1], nearly 450,000 attacks have been recorded in 2013, which led up to estimated losses of over USD $5,9 billion.
Moore and Clayton[2] define phishing as follows: "Phishing is the process of enticing people into visiting fraudulent websites and persuading them to enter identity information such as usernames, passwords, addresses, social security numbers, personal identification numbers (PINs) and anything else that can be made to appear to be plausible. This data is then used to impersonate the victim to empty their bank account, run fraudulent auctions, launder money, apply for credit cards, take out loans in their name, and so on."
Most of the companies targeted in the given dataset were financial institutions such as PayPal and eBay. Since PayPal and eBay have a lot of users, which involves a lot of money, they are obviously attractive targets for attackers. Companies like Facebook and Google are also targeted. When attackers get access to social media accounts like Facebook, they can use those accounts to spread

information through a large network.
A big part in the phishing issue is legislation. Every country (and even every state in the US) has its own legislation regarding cybercrime. This paper analyses if legislation has influences in the decisions of an attacker.

3 Literature Review

Countries have different legislations regarding cybercrime and therefore also phishing. In the UK there are no specific laws regarding phishing, but phishing can be seen as a violation of the Fraud Act of 2005 [3]. Someone is in breach of this section if one: dishonestly make a false representation and intends to make gain for himself or another or to cause loss to another or to expose another to a risk of loss". This does mean that a phishing attack has to succeed before the attacker can be prosecuted. Since for phishing mostly 'spam' is used, the regulations about spam also apply for phishing [4]. For example the Electronic Commerce (EC Directive) Regulations 2002 from the European Union applies for these cases.
In the US, the US Congress promulgated the ITADA (Identity Theft an Assumption Deterrence Act) in 1998 [4]. This made identity theft a federal crime under any applicable state or local law. Because phishing is a form of identity theft, it falls under the ITADA.
Redford M. discusses the differences between the US and EU legislation [5]. He argues that EU legislation works better because it is 'treaty-based', instead of the US legislation, which is 'legislation-based'. Legislation-based means 'that the laws are made for the needs of that country without much collaboration with international communities; therefore, this is the law of a nation' [5]. Whereas treaty-based means 'a limited collaboration system, which works through global voluntary participation. All the participating countries work in conformity to remedy cybercrime causation, with the intent to form laws that will enable them to overcome conflicts of law, choice of laws, and other international legal complexities.'. Treaty-based' approaches supposedly should work better, because this solves the problem of jurisdiction. If a country is targeted by someone living in another country, jurisdiction can be a big problem. The EU wants to target this problem by internationalising the EU law, which now already spans over the EU [5].
Even though Redford M. favours the EU approach over the US approach, Granova A. favors the other way around [4]. She states that the US has the most sophisticated legislative system. This because the US law states several crimes which can and have been successfully linked to phishing. But this could also be because this paper was published in 2005, when the Fraud Act of 2005 was just introduced in the EU. Ranganathan C. also discusses the differences and the effectiveness of the EU/UK legislation and the US legislation regarding spam [6]. It is discussed that the EU approach has implementation issues. This because the member states implement the EU Directive in a different way. Also even though it is an EU Directive, every member has its own implementation.

This also gives the issue of jurisdiction, which should be prevented using this approach. The US legislation contains the 'Can-Spam Act'. The paper discusses that this has a positive impact. This because it makes the use of open proxies or use of false headers illegal. But this means that it still gives the right to spammers to send spam, only if they do not break the act. What also is discussed is the fact that 'Law is only as good as its enforcement'. Since government agencies and ISP's mostly deal with spammers, the Federal Legislation tend not do a lot.
In addition to the disabilities of prosecuting attackers, Yu Beng L. discusses that identifying the source of a phishing campain is the main challenge [7]. Because email systems lack mechanisms to authenticate sender's identities, spammers can conceal their identities.

4 Research Question

There are a lot of subfields in phishing. This paper focuses on the legislation part of phishing. In order to tackle cybercrime, including the phishing problem, many countries and groups like the European Union created laws and acts regarding cybercrime. But whether legislation actually helps in reducing phishing as a whole and what type of legislation is best practice, are interesting topics to discuss. Because of the dataset given, the discussion whether or whether legislation does not have an impact on hosting websites can be evaluated. The research question discussed in this paper is therefore: *Does legislation have an impact in the amount of hosted phishing websites in a country?*

4.1 Hypothesis

Based on the literature review this question can't be answered with a simple yes or no. Many papers discuss the different legislations and explain what helps and what should be improved. A big issue discussed is jurisdiction. Even though if a country has well defined legislation regarding phishing, because the attacker resides in a different country, legislation of the country of residence applies, which can cause problems, if these are not well defined. Therefore many researchers propose a international law, so the issues of jurisdiction does not occur.
But even if legislation is not well defined, it still tackles the issue. If phishers are being prosecuted by this law, it still has an effect, even if it is small. Therefore the hypothesis is: yes, legislation has an impact in the amount of hosted phishing websites.

5 Methodology

The best way to answer the research question is to compare a country with and without legislation and see if when legislation was applied, the amount of hosting websites decreases. Obviously this is infeasible.

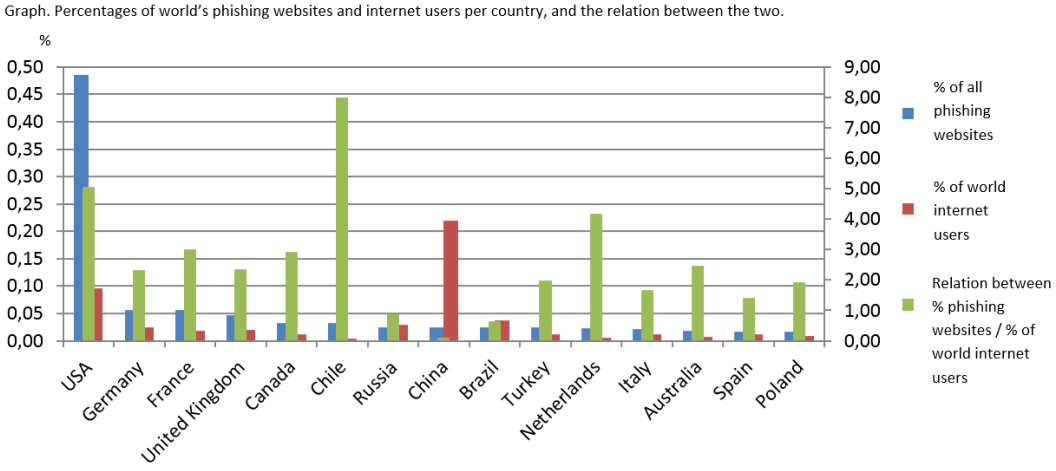
Using the dataset, one can derive the countries hosting a high and low amount of phishing websites. This is valuable information. In this paper legislations of these two types of countries will be compared and see if there is a big difference. This information can be used to determine what differences of legislation influences the amount of phishing websites. But this conclusion can be biased, since attackers could have other reasons to host their websites in a specific country, which does not relate to the legislation involved. Therefore the next thing to do is discuss other reasons why a country is attractive to host phishing websites. If it can be concluded that a country is attractive because of these reasons, but still does not host a lot of websites, one can discuss that the legislation does its job well.

6 Results

6.1 Countries: Amount of Phishing Websites

The first thing discussed in the methodology is using the dataset to derive the countries hosting a high and low amount of phishing websites. Since this has to be as independent as possible, this amount is normalised by the amount of internet users. This resulted in Figure 1.

Figure 1: Amount of phishing websites per country normalised



The top 3 countries in this graph are: Chile, USA and the Netherlands. The lowest 3 countries in this graph are: China, Brazil and Russia. This means these are the countries which going to be compared. The different legislations per country can be found in Appendix A.

6.2 Discussing the different legislations

Of all the legislations, it is noticeable that the US has a significantly higher amount of acts against cybercrime, compared to the other legislations. This was also stated by Granova A. [4]. The most important cybercrime law regarding phishing in the US is: '18 U.S.C. § 1028' [8]. This is prohibits online identity theft, which is a major part of a phishing attack. The cybercrime laws of The Netherlands and Chile are not that complex. But they still make parts of phishing illegal. For example article 2 in the Law on Automated Data Processing Crimes of Chile says: *'Anyone illegally obtains access to or uses information contained in an information processing system, intercepts or interferes with it, shall be liable for imprisonment from a minor to a medium sentence.'* [9]. This means if someone obtains information through a phishing website and uses it to its advantage, this article is breached. The Netherlands has a similar article: Article 138a-1 [10]. But this means that a phisher is not offending any law, if the phisher hasn't had a successful attack.
However comparing this to the similar laws from the other three countries, we can see there is not much difference. The Criminal Law of the People's Republic of China, Article 287 states: *'Whoever uses a computer for financial fraud, theft, corruption, misappropriation of public funds, stealing state secrets, or other crimes is to be convicted and punished according to relevant regulations of this law'* [11]. Since a phishing attack can be seen as financial fraud, this article could be used against a phisher. Brazil's Law no. 9,983, Article 313-A[12] and Russia's Criminal Code, Chapter 28, Article 271.1[13] are similar to these laws.
Since all laws are similar and only punishes phishers if they actually had a successful attack, this should not be a reason for a phisher to host a phishing website in one of the countries.
There are two things that can be noticed about these laws. The first is that all articles are ten or more years old. Updating cyber-crime laws is of utmost importance, since technology keeps advancing. The oldest article is from Chile, which was published on June 7, 1993. The second thing is that there is no law which targets phishing specifically. Every law previously mentioned tackles the results of phishing attacks. This means phishing itself is not illegal, but the consequences of phishing are.

6.3 Other Reasons For Choosing A Hosting Country

Phishing Awareness in a country
If a country is not aware of the phishing websites hosted, attackers prefer to host their websites in that country. This because since the country is not aware of the websites, the likelihood of the websites to be taken down is low. But, as explained in lecture 4.4, once the country is aware of the phishing websites, it takes a small amount of time to take them down. The attackers will then switch to another domain name of another country. Once this country is also aware of the phishing websites, the attackers will switch to another domain name, and so

on. Therefore specialists recommend the increase of information sharing, which tackles this problem.
Instead of saying that awareness of a country contributes to the decision which country the phishing website is going to be hosted, the other way around actually applies. The awareness of a country contributes to the decision which country the phishing website is 'not' going to hosted.

Domain Names
Domain names play a big role in the decision of a hosting country. Once a domain name is used a lot in phishing websites, it becomes suspicious. Once that happens, specific checks will be made towards that domain name, which makes filtering phishing websites with that domain name easier. Therefore, attackers switch domain names if the current domain name has become suspicious. This way they increase the up-time of their websites.

Country's effort to take down phishing websites
As earlier explained, when a country is aware of phishing websites hosted in the country, taking the website down is step two. Some countries tend to not take these matters seriously. This because the targeted country is mostly another country than the hosting country.
Also each jurisdiction has a certain capability and way of dealing with phishing incidents. For example, in North America shutting down phishing sites hosted there can be done in hours/minutes [14]. For more complex phishing sites, communication with government officials and law enforcement is needed, since some ISP's can't block the IP by law. Attackers would prefer countries where jurisdiction helps prolonging the up-time of their phishing website.

Domain Name Registrars, Hosting Providers and ISP's
The Domain Name Registrars, Hosting Providers and IPS's in a country are also a big part in the decision. ISP's which are for example 'un-popular' can be very slow in taking down phishing websites [14]. Also some registrars do not want to intervene due to regulatory reasons. They then request to contact the host, or the registrant of the domain, especially if the phishing site is hosted on a compromised website. Countries with a lot of these types of registrars and ISP's are attractive for attackers to host their websites. The longer a phishing website is online, the more attacks a phisher can have.
Phishing websites can also be dangerous for hosting providers. If a hosting provider hosted phishing websites, and this becomes publicly known, the goodwill of the hosting provider can be damaged. This can result into two things. First the hosting provider becomes careful for phishing websites, and tries to avoid them by means of prevention. But this can be expensive, so for small hosting providers, this can be hard. The second result is that a hosting provider has been hosting phishing websites, but does want this to become public, so tries to avoid the conflict. This type of hosting providers are attractive for phishers.

7 Limitations

In order to get the best answer to the research question, one has to compare a country in two different states. One is with legislation and one is without. Comparing these two states of the country, one can conclude if legislation has an impact in the amount of phishing websites hosted in the country, by simply looking at the amount of phishing websites hosted with and without legislation. If there is a difference, it can be concluded that legislation has an impact. But obviously this is not feasible, since the laws have to be changed for this experiment, besides the fact that a country actually have to cooperate in this experiment.
Something I also wanted to do in this paper is to evaluate actual cases of phishing and discuss if legislation had an impact in these cases. But since in every case I could not link the results to my research question, because the research question is about hosting websites, I left this part out.
To form the conclusion, I compared countries with a high amount of phishing websites compared to countries with a low amount of phishing websites. The countries chosen are obtained from a dataset containing data, e.g. phishing websites and hosting country, from a couple days. In order to get a more accurate result, one should have a dataset containing data from a bigger time span. This could have biased the conclusion, since the countries chosen, could've been different if a larger dataset with a larger time span was used.
One thing that would also be interesting to examine, is the average up-time in a country. This information could also be used in the question if legislation has an impact. But due time-related issues, this is not done in this paper.

8 Conclusion

To form this conclusion, different legislations have been compared from two different kind of countries; countries hosting a high amount of phishing websites, and countries hosting a low amount of phishing websites. This resulted in the fact that there was not a big difference in the different legislations involved between the two cases. The cybercrime laws in each country were similar, except for the cybercrime law in the US, which was more complex.
Several other reasons have also been discussed, why an attacker would choose a certain country to host a phishing website. The reasons included: Phishing awareness in a country, Domain Names, Country's effort to take down phishing websites and the involvement of Domain Name Registrars, Hosting Providers and ISP's. Each reason has its own significance in the decision of a phisher and this has been discussed.
Based on these results, the conclusion is that *legislation does not have an impact in the amount of hosted websites in a country.* Even though the different kinds of legislation does prohibit phishing consequences, like identity theft, there is no law that makes hosting a phishing website itself illegal. Also since there is not a big difference between different legislations in the countries examined, it

can also be concluded that attackers do not decide where to host their website based on the legislation involved. Since the cyber-crime laws in the US are more complex and more specific, this should result into a less amount of hosted phishing websites. But using the dataset, it was found that the US belongs to the top 3, which contradicts the statement. It can also be discussed that the other reasons mentioned have a bigger impact for the decision. If a country is famous for taking down phishing websites fast, this has a bigger impact in the decision of an attacker than if the corresponding legislation is heavier.
It can also be discussed that if a country has no legislation, phishers would take this into account, but since there is no case of a country where websites can be hosted and which has no legislation regarding phishing, this can not be confirmed.
This conclusion differs from the hypothesis. The reason for this is because for the hypothesis, a comparison is made by looking at countries with and without legislation. It says: 'If phishers are being prosecuted by this law, it still has an effect, even if it is small'. This has an influence in the conclusion, if you compare countries with and without legislation, since this type of reasoning only holds for such a case. The reasoning used in the conclusion is the fact that there is not a big difference in the different legislations. So a phisher does not take legislation into account when deciding, because they are all similar. Therefore legislation does not influence the amount of hosted phishing websites in a country.

Appendix A: Legislations

This section is stating the legislation per country regarding cybercrime.

Chile [9]
Chile has a Law on Automated Data Processing Crimes no. 19.223, published June 7, 1993.

Article 1: Anyone that maliciously destroys or makes unusable a system of information processing, or any of its parts or components, or prevents or modifies its operation, shall be liable for imprisonment from average to maximum sentences

Article 2: Anyone illegally obtains access to or uses information contained in an information processing system, intercepts or interferes with it, shall be liable for imprisonment from a minor to a medium sentence.

Article 3: Anyone that maliciously alters, damages or destroys data contained in a system of information processing, shall be liable for imprisonment from a minor to a medium sentence.

USA [8]
UNITED STATES CODE
TITLE 18. CRIMES AND CRIMINAL PROCEDURE
PART I -CRIMES
CHAPTER 47-FRAUD AND FALSE STATEMENTS
Section 1030. Fraud and related activity in connection with computers.

(a) Whoever-
(1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it;
(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains-
(A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602 (n) of title 15, or contained in a file of

a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);
(B) information from any department or agency of the United States; or
(C) information from any protected computer if the conduct involved an interstate or foreign communication;
(3) intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States;
(4) knowingly and with the intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $ 5.000 in any one-year period;
(5) (i) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;
(ii) intentionally accesses a protected computer without authorization, and as a result of such conduct recklessly causes damage; or
(iii) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage; and
(B) by conduct described in clause (i), (ii), or (iii) of subparagraph (A), caused (or, in the case of an attempted offense, would, if completed, have caused)–
(i) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least USD 5,000 in value;
(ii) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;
(iii) physical injury to any person;
(iv) a threat to public health or safety; or
(v) damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defence, or national security;
(6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if
(A) such trafficking affects interstate or foreign commerce; or
(B) such computer is used by or for the Government of the United States;
(7) with intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication containing any threat to cause damage to a protected computer; shall be punished as provided in subsection (c) of this section.

(b) Whoever attempts to commit an offense under subsection (a) of this section shall be punished as provided in subsection (c) of this section.

(c) The punishment for an offense under subsection (a) or (b) of this section is–

The Netherlands (Dutch) [10]

1. Met gevangenisstraf van ten hoogste een jaar of geldboete van de vierde categorie wordt, als schuldig aan computervredebreuk, gestraft hij die opzettelijk en wederrechtelijk binnendringt in een geautomatiseerd werk of in een deel daarvan. Van binnendringen is in ieder geval sprake indien de toegang tot het werk wordt verworven:
a. door het doorbreken van een beveiliging,
b. door een technische ingreep,
c. met behulp van valse signalen of een valse sleutel, of
d. door het aannemen van een valse hoedanigheid.

2. Met gevangenisstraf van ten hoogste vier jaren of geldboete van de vierde categorie wordt gestraft computervredebreuk, indien de dader vervolgens gegevens die zijn opgeslagen, worden verwerkt of overgedragen door middel van het geautomatiseerd werk waarin hij zich wederrechtelijk bevindt, voor zichzelf of een ander overneemt, aftapt of opneemt.

3. Met gevangenisstraf van ten hoogste vier jaren of geldboete van de vierde categorie wordt gestraft computervredebreuk gepleegd door tussenkomst van een openbaar telecommunicatienetwerk, indien de dader vervolgens
a. met het oogmerk zichzelf of een ander wederrechtelijk te bevoordelen gebruik maakt van verwerkingscapaciteit van een geautomatiseerd werk;
b. door tussenkomst van het geautomatiseerd werk waarin hij is binnengedrongen de toegang verwerft tot het geautomatiseerd werk van een derde.

China [11]
Criminal Law of the People's Republic of China
(March 14, 1997)

Article 285. Whoever violates state regulations and intrudes into computer systems withinformation concerning state affairs, construction of defense facilities, and sophisticatedscience and technology is be sentenced to not more than three years of fixed-termimprisonment or criminal detention.

Article 286. Whoever violates states regulations and deletes, alters, adds, and interferesin computer information systems, causing abnormal operations of the systems and graveconsequences, is to be sentenced to not more than five years of fixed-term imprisonment orcriminal detention; when the consequences are particularly serious, the sentence is to benot less than five years of fixed-

term imprisonment.
Whoever violates state regulations and deletes, alters, or adds the data or applicationprograms installed in or processed and transmitted by the computer systems, and causes graveconsequences, is to be punished according to the preceding paragraph.
Whoever deliberately creates and propagates computer virus and other programs which sabotagethe normal operation of the computer system and cause grave consequences is to be punishedaccording to the first paragraph.

Article 287. Whoever uses a computer for financial fraud, theft, corruption,misappropriation of public funds, stealing state secrets, or other crimes is to be convictedand punished according to relevant regulations of this law.

Brazil [12]
Law no. 9,983 of July 7, 2000

Insertion of fake data into systems of information
Article 313-A. -An authorized public servant must not insert or facilitate the insertion of fake data, or alters systems of information, or improperly exclude correct data from these systems, or from any data banks of Public Administration, with the purpose of obtaining undue advantages, for himself or for other people, or causing any harm
Sentence – prison, 2 (two) up to 12 (twelve) years, and fine.

Non-authorized modification or alteration of systems of information
Article 313-B –A public servant must not modify or alter systems of information, or computer software, without authorization or order of a competent authority.
Sentence – prison, 3 (three) months up to 2 (two) years, and fine.
The sentences are increased by one third up to half of it if the modification or alteration performed cause harm to the Public Management or to any of its assets.

Russia [13]
Chapter 28. Computer information crimes

Article 272. Unauthorized access to computer information

1. Unauthorized access to law protected computer information in the electronic computers, their systems or networks or on the machine carriers resulted in erasing, blocking or copying computer information, disturbing the work of electronic computers, their systems or networks is punished with fine from two hundred to five hundred minimum wages, condemned person's wages or another income within the term from two to five months, refinery works within the term from six months to one year, or imprisonment within up to two years.

2. The same action carried out by a group of persons in prior agreement or an organized group or a person abusing his official position and having equally

an access to electronic computers, their systems or networks is punished with fine from five hundred to eight hundred minimum wages, condemned person's wages or another income within the term from five to eight months, refinery works within the term from one to two years, arrest within the term from three to six months or imprisonment within up to five years.

Article 273. Production, use and spread of detrimental electronic computer programs

1. Production of electronic computer programs or introduction of changes into current programs resulted in erasing, blocking, modifying or copying information, disturbing the work of electronic computers, their systems or networks and use or spread of these programs are punished with imprisonment within up to three years with fine from two hundred to five hundred minimum wages or condemned person's wages or another income within the term from two to five months.

2. The same actions entailed serious consequences through imprudence are punished with imprisonment within the term from three to seven years.

Article 274. Violation of electronic computer, system or network operating rules

1. Violation of electronic computer, system or network operating rules on the part of a person having an access to electronic computers, their systems or networks resulted in erasing, blocking or modifying law protested information and caused a considerable damage is punished with denial of particular position or activity privileges within up to five years, obligatory works within the term from one hundred and eighty to two hundred hours or freedom limitation within up to two years.

2. The same action entailed serious consequences through imprudence is punished with imprisonment within up to four years.

References

[1] RSA, "Rsa online fraud report 2014," 2014, http://www.emc.com/collateral/fraud-report/rsa-online-fraud-report-012014.pdf.

[2] T. Moore and R. Clayton, "Examining the impact of website take-down on phishing," in *Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit*. ACM, 2007, pp. 1–13.

[3] C. Wilson and D. Argles, "The fight against phishing: Technology, the end user and legislation," in *Information Society (i-Society), 2011 International Conference on*. IEEE, 2011, pp. 501–504.

[4] A. Granova and J. Eloff, "A legal overview of phishing," *Computer Fraud & Security*, vol. 2005, no. 7, pp. 6–11, 2005.

[5] M. Redford, "Us and eu legislation on cybercrime," in *Intelligence and Security Informatics Conference (EISIC), 2011 European*. IEEE, 2011, pp. 34–37.

[6] E. Moustakas, C. Ranganathan, and P. Duquenoy, "Combating spam through legislation: A comparative analysis of us and european approaches." in *CEAS*, 2005.

[7] N. Dinna, Y. Leau, S. Habeeb, and A. Yanti, "Managing legal, consumers and commerce risks in phishing," *International Journal of Human and Social Sciences*, vol. 3, no. 5, 2008.

[8] U. States, "Cybercrimelaw of the us," 2006, http://www.qcert.org/sites/default/files/public/documents/us-ecrime-compilation_of_cybercrime_laws-eng-2006.pdf.

[9] CyberCrimeLaw, "Cybercrimelaw of chile," 1993, http://www.cybercrimelaw.net/Chile.html.

[10] Wetboek, "Cybercrimelaw of the netherlands," 2008, http://www.wetboek-online.nl/wet/Sr/138a.html.

[11] CyberCrimeLaw, "Cybercrimelaw of the china," 1997, http://www.cybercrimelaw.net/China.html.

[12] ——, "Cybercrimelaw of the brazil," 2000, http://www.cybercrimelaw.net/Brazil.html.

[13] Crime-Research, "The russian federation's criminal code," 1997, http://www.crime-research.org/library/Criminal_Codes.html.

[14] BrandProtect.org, "Phishing attacks: The truth about average takedown times," 2012, http://info.brandprotect.com/Blog/bid/78782/Phishing-Attacks-The-Truth-about-Average-Takedown-Times.