**Regional Workshop on Frameworks for Cybersecurity and Critical Information Infrastructure Protection (CIIP)**

Document RWBA/2007/NACPEC-E
16 October 2007
Original: English

# Contribution to the Regional Workshop on Frameworks for Cybersecurity and CIIP held in Buenos Aires, Argentina, 16-18 October 2007[1]

**by**

**North American Consumer Project on Electronic Commerce (NACPEC)**
**www.nacpec.org**

## "*An Update on Anti-Spam and Phishing Activities in Mexico*"[2]

[1] ITU Regional Workshop on Frameworks for Cybersecurity and CIIP held in Buenos Aires, Argentina, 16-18 October 2007, www.itu.int/itu-d/cyb/events/2007/buenos-aires/

[2] "Contribution submitted by Cristos Velasco, Director General, North American Consumer Project on Electronic Commerce (NACPEC), www.nacpec.org

# An Update on Anti-Spam and Phishing Activities in Mexico

## *I. Background*

Spam is growing, and eroding consumer trust and the use of e-mail communications at a global scale. Five years ago, spam was not considered a major threat, but gradually it has evolved into a major criminal conduct and is causing strong economic and social repercussion to the information society.
Mexico has not been exempt from the global reach of spam. Mexico has undertaken a number of tasks to control the spam problem at the national level, particularly in the legal and technical areas, and through the spread of education and prevention campaigns.

The purpose of this paper is to offer an update of Mexico's activities to control and fight spam and phishing. This paper will briefly touch on various issues, mainly the governing legal framework; international cooperation of enforcement authorities; and education and awareness campaigns. International and national statistics will also be shown in order to illustrate our readers on the national strategy in the fight against spam in Mexico.

This paper is submitted as a contribution to the ITU Regional Workshop on Frameworks for Cybersecurity and Critical Information Infrastructure Protection to be held in Buenos Aires. It aims to serve as reference not only to the government members of the ITU and the organizations and individuals participating in such regional workshop, but also to all the stakeholders involved in the Internet Governance Forum (IGF) process, the second meeting of which will be held in Rio de Janeiro from 12-15 November 2007.

## *II. Statistics*

There are no official statistics on spam and phishing from the government of Mexico. However, the National CERT, which works under the auspices of Mexico's National Autonomous University (UNAM)[3] and the Cybercrime Police (Policia Cibernetica), have joined efforts to track and pursue Internet crime, including spam and phishing activities.

Said organizations estimate an amount of 2050 phishing websites affecting Mexican institutions during 2006. The numbers were obtained through a large number of technical mechanisms and conduits conducted by the National CERT.
Statistics as of 30 April 2007 amount to 589 phishing websites affecting eight major financial institutions established in Mexico, including the national credit bureau.[4]

Statistics from Netcraft found a total of 14 phishing websites in Mexico as of April 5, 2005. Whereas, Symantec estimates a total of 2,578 of bot-infected computers in Mexico from July to December 2004.

## *III. Legislation*

### A. Against Spam

Under Mexican legislation, spam is a consumer protection issue and is regulated in five provisions of the Federal Consumer Protection Law (FCPL) and its regulation, which are enforced by the Office of the Federal Attorney for Consumer Protection (Procuraduría Federal del Consumidor hereinafter "PROFECO").[5]

Article 76 BIS of the FCPL contains an opt-out clause, which allows consumers to withdraw from receiving commercial notices and advertisement in transactions including those carried out through the Internet.
Furthermore, article 17 of the FCPL offer consumes the right to inform providers or businesses using its

[3] CERT's website is available at: http://www.cert.org.mx/
[4] See UNAM-CERT & Federal Police, "*Taxonomía de Phishing en México*", Congreso de Seguridad en Cómputo 2007 organizado por la Universidad Nacional Autónoma de México (UNAM), available at: http://congreso.seguridad.unam.mx/?liga=download
[5] PROFECO's website is available at: http://www.profeco.gob.mx/

information for marketing or advertising purposes that their personal data may not be transmitted or shared with third parties, unless a judicial authority determines such transmission.

Articles 125 to 128 of the FCPL provide for administrative penalties equivalent from $498.77 to $1'950,747.46 Mexican pesos, (approximately USD $46.00 to $180,467.00) for non-compliance with such provisions, and up to $5'586,000.00 Mexican pesos (approximately USD$516,768.00) in case of backsliding. Article 129 of the FCPL stipulates administrative imprisonment up to 36 hours in case of non-compliance with an order from PROFECO.[6]

In order for PROFECO to assert administrative penalties under the FCPL and its regulation, such agency must first assess the gravity of the infraction, and take the following four elements into consideration: (i) the loss caused to the consumer or to the society in general; (ii) the intentional nature of the violation; (iii) whether it is a case of recurrence; and (iv) the economic condition of the defendant.

**B. Against Phishing**

Phishing is considered a criminal offence under articles 112 Bis and 113 Bis. of the Credit Institutions Law (CIL), which is a federal law governing the financial sector.
Article 112 Bis section (iv) of the CIL prohibits the obtaining and use of information about customers or transactions of the banking system without having the corresponding authorization. This offense is sanctioned with fines from thirty thousand to three hundred thousands days of minimum salary[7] (equivalent to USD$140,432.00 and USD$1'403,488.00) and imprisonment from 3 to 9 years. The penalties may be increased up to a half when an advisor, functionary or employee of a credit institution performs the conduct.

Art. 113 Bis. of the CIL prohibits the use, obtaining and transferring of securities or resources from customers pertaining to credit institutions. Such offense is sanctioned with fines from five hundred to thirty thousand days of minimum salary (equivalent to USD$2,339.00 and USD$140,432.00) and imprisonment from 3 to 10 years.

## *IV. Spam Cases*

Despite the fact that many spam and phishing cases are being traced and investigated by the Cybercrime Police with the support of the National CERT, there is no yet a single case filed in a federal or local court to request the legal prosecution of spammers.

Some of the reasons that not a single spam case has been filed under a court of law in Mexico is due to: (i) the difficulty to track and enforce the law against spammers who are physically established in other jurisdictions; (ii) the current lack of financial and human resources of the Mexican law enforcement authorities; and (iii) the lack of cooperation and coordination as to which federal agency has jurisdiction over spam and phishing issues.

## *V. International Cooperation*

Mexico plays an active role in international government related fora working on spam and e-commerce consumer protection issues.
For instance, PROFECO forms part of the Committee on Consumer Policy (CPC) of the Organization for Economic Cooperation and Development (OECD)[8] since 2000 and of he International Consumer Protection Enforcement Network (ICPEN)[9]. Within such fora, PROFECO participates in the *Sweep Days*

[6] For more detailed information on Mexico's legal framework against spam, see Velasco, Cristos *"Mexico's Experience in Combating Spam. A Legal Perspective from a Consumer Advocate"*, Contribution to the International Telecommunications Union (ITU) Thematic Meeting on Cybersecurity, Geneva, Switzerland, July 2005, available at: http://www.itu.int/osg/spu/spam/legislation/Mexico_Contribution_%2006_%20June_%202005.pdf

[7] The monetary fines contained in some Mexican laws are referred to and express in Minimum Salary Days (*Días de Salario Mínimo*). Currently, a "*Minimum Salary Day*" consists of eight working hours equivalent to an amount of $50.57 (Fifty Mexican pesos 57/100) (USD$ 4.60) depending of the geographic area where the worker is located, see *Comisión Nacional de Salarios Mínimos* at: http://www.conasami.gob.mx/

[8] The website of OECD's CPC is available at: http://www.oecd.org/department/0,2688,en_2649_34267_1_1_1_1_1,00.html

[9] ICPEN's website is available at: http://www.icpen.org/

campaigns, attends meetings, workshops and engages in the elaboration of policy documents on spam and consumer protection. PROFECO is also part of the London Action Plan (LAP).
PROFECO'S participation in such fora and groups seeks not only to improve Mexico's international cooperation with other country members in the area of spam, but also to create awareness and strengthen the protection and defense of consumer rights on electronic commerce in national territory.[10]

The Ministry of Economics (*Secretaría de Economia SE*[11]) though the General Direction of Interior Commerce and Digital Economy (*Dirección General de Comercio Interior y Economía Digital*) plays an active role in the Electronic Commerce Steering Group (ECSG) of the Asia-Pacific Economic Cooperation forum (APEC). SE currently chairs the ECSG and has engaged in workshops, seminars and policy discussions on e-commerce, including topics related on anti-spam issues and privacy and data protection within the Asia-Pacific region.[12]

## *VI. Bilateral Cooperation*

The US Federal Trade Commission (FTC) and PROFECO signed a bilateral Memorandum of Understanding (MOU) in January 2005 in order to promote and enhance cooperation in the fight against cross-border fraud and to facilitate better law enforcement coordination in consumer protection matters affecting both countries.[13]

The MOU between the FTC and PROFECO was the first entered with a Latin American and a non-English speaking country. The MOU sets forth *inter alia* the following objectives: (i) share information and provide mutual assistance to facilitate the enforcement of their respective consumer protection laws to prevent fraudulent and deceptive commercial practices; (ii) coordinate investigations, research, consumer & business education and provide information in relation to investigations, speeches, research papers, compliance education programs and amendments to legislation; and (iii) request for mutual assistance pursuant a list of criteria between the established points of contact on a confidential basis.

Up to now, the MOU between the FTC and PROFECO has not had any practical use and legal effects in the Mexican legal system. However, with the recent enactment of the US SAFE WEB ACT[14], such MOU will probably serve as a vehicle to enhance consumer protection issues in both countries, and facilitate coordination of investigations and cooperation for the prosecution of spamers and cybercriminals affecting American and Mexican citizens.

## *VII. Education and Awareness Campaigns*

Mexico has been very proactive in the education and awareness front through the dissemination of online tools in order to keep consumers informed on the potential dangers of spam, phishing and the evolution of new forms of online crime so as to prevent the population from falling victim of cross-border fraud schemes.

For instance, the website of the Direction General of Computing Academic Services (DGSCA) of the National Autonomous University of Mexico (UNAM)[15] contains information and updates on the latest Internet threats, including viruses, spam and phishing techniques, and provides a list of preventive measures including the use of e-mail filters. That website is mainly addressed to the Internet & ISP's

---

[10] See more on PROFECO's position against the enforcement of spam in Mexico at:
[11] The website of the Ministry of Economics is available at: http://www.economia.gob.mx
[12] The website and documents of the ECSG are available at:
http://www.apec.org/apec/apec_groups/som_special_task_groups/electronic_commerce.html
[13] The Memorandum of Understanding on Mutual Assistance in Consumer Protection Matters between the Federal Trade Commission of the United States of America and the Procuraduría Federal del Consumidor of the United Mexican States is available in English and Spanish at:
http://www.ftc.gov/opa/2005/01/memunderstanding.htm
[14] Undertaking Spam, Spyware and Fraud Enforcement With Enforcers across Border Act (US SAFE WEB Act) is a legislation, the purpose of which is to strengthen international cooperation between law enforcement agencies to share information and investigations in cross- border fraud on the Internet such as spam, spyware and identity theft schemes. It is available at: http://www.ftc.gov/reports/ussafeweb/USSAFEWEB.pdf
[15] DGSCA's website is available at: http://www.dgsca.unam.mx/

industries and academic institutions to help them protect themselves and prevent their computing systems and IT infrastructure from major Internet threats.

The North American Consumer Project on Electronic Commerce (NACPEC)[16] is currently working with other academic institutions in order to enhance consumer education and awareness on the Internet. NACPEC's website contains a section on spam and phishing with updated information and resources such as statistics, international legislation and cases, publications, news and a list of frequently asked questions and advice to Mexican consumers based on the applicable legislation in order to help them identify and reduce spam and prevent them from falling victim of phishing techniques.[17]
The national CERT and the Cyberecrime Police have created e-mail addresses where affected individuals may file reports and complaints as a result of phishing and identity theft schemes.[18]

## *VIII. Recent Developments*

In June 2007, the National CERT with the support of the Cybercrime Police and the Internet and financial industries in Mexico conformed an ad-hoc prevention group known as "*the e-Crime Mexico Group*".
The e-Crime Mexico Group is a multidisciplinary effort with the principal mission of preventing and reducing cybercrime in Mexico. The tasks of this group include *inter alia*: (i) identifying, monitoring and prosecuting Internet related crimes including fraud, phishing, identity theft and all those crimes involving information systems; (ii) analyzing and informing about the latest threats to security systems on the Internet; and (iii) fostering a culture of 'information security' in Mexico. The e-Crime Mexico Group will revisit the works originally undertaken by a multidisciplinary enforcement and prevention group formerly known as Cybercrime-Mexico (DC Mexico).

## *IX. Conclusion*

Mexico has sufficient rules to combat spam and phishing at the national level, however since spam is a cross-border issue, the problem does not only rest on having a good piece of legislation for its control. The problem relies mostly on the effectiveness of the enforcement of the law and the prosecution of spammers by the local enforcement authorities with the assistance of international organizations and law enforcement groups.

Mexico's efforts to control and prevent spam have improved in recent years. Spam, phishing and other online threats will continue to evolve in the coming years. In order to tackle them more effectively, there is the need to improve cooperation and coordination not only between government local agencies and the industry with international organizations, but also between national CERTs and consumer and civil society groups working on prevention of online crime.

The continuous dissemination of information and education campaigns by consumer groups and NGO's about new forms of online crime plays a significant role to prevent the general population from falling victim of the global reach of spam.

[16] NACPEC' s website is available at: http://www.nacpec.org
[17] See the FAQ's on Spam and Phishing in Spanish at: http://www.nacpec.org/es/faq.html?lang=es
[18] See, *supra* note 2.