

FOURTEENTH CONGRESS OF THE REPUBLIC)  
OF THE PHILIPPINES )  
First Regular Session )

7 SEP 20 16:11

SENATE  
S. No. 1626

RECEIVED BY: [Signature]

Introduced by Senator Miriam Defensor Santiago

EXPLANATORY NOTE

The Philippine society is increasingly dependent on the internet for communication, entertainment, commerce, and banking. For the internet to reach its full potential, it must continue to be a trustworthy medium. Internet users should be able to trust the origin of internet communications and the destination of internet hyperlinks.

Internet users around the world are increasingly subjected to scams based on misleading or false communications that trick the user into sending money, or into revealing information that result in financial loss.

One class of such scams is called *phising*. This uses false e-mail return addresses, stolen graphics, stylistic imitations, disguised hyperlinks, and other artifices to trick users into revealing personal information. After obtaining this information, the *phiser* then uses the information to create unlawful identification documents and/or to unlawfully obtain money or property.

This bill seeks to criminalize internet scams involving fraudulently obtaining personal information, commonly known as *phising*.\*

*Miriam Defensor Santiago*  
MIRIAM DEFENSOR SANTIAGO  
*[Signature]*

\* This bill was originally filed during the Thirteenth Congress, First Regular Session.

FOURTEENTH CONGRESS OF THE REPUBLIC )  
OF THE PHILIPPINES )  
First Regular Session )

7 SEP 20 2007

SENATE  
S. No. 1626

RECEIVED BY: [Signature]

Introduced by Senator Miriam Defensor Santiago

1 AN ACT  
2 TO CRIMINALIZE INTERNET SCAMS INVOLVING FRAUDULENTLY  
3 OBTAINING PERSONAL INFORMATION

4 *Be it enacted by the Senate and House of Representatives of the Philippines in Congress*  
5 *assembled:*

6 SECTION 1. *Short Title.* – This Act shall be known as the “Anti-Phising Act of 2007.”

7 SECTION 2. *Definition of Terms.* – For the purposes of this Act, the term:

8 (A) “Phising” means an internet scam based on misleading or false communications that  
9 trick the user into sending money, or trick the user into revealing enough information  
10 to enable various forms of identity theft that result in financial loss.

11 (B) “Phiser” means any person, firm, association, corporation or partnership or other  
12 organization who engaged or commits the act of phising.

13 (C) “Internet” means the combination of computer facilities and electromagnetic  
14 transmission media, and related equipment and software, comprising the  
15 interconnected worldwide network of computer networks that employ the  
16 Transmission Control Protocol/Internet Protocol (TCP/IP) or any successor protocol  
17 to transmit information.

18 (D) “Domain name” means any alphanumeric designation which is registered with or  
19 assigned by any domain name registrar, domain name registry, or other domain name  
20 registration authority as part of an electronic address on the internet.

21 (E) “Electronic mail message” means a message sent to a unique electronic mail address.

22 (F) “Initiate” means to originate or transmit such message or to procure the origination or  
23 transmission of such message, but shall not include actions that constitute routine

1 conveyance of such message. For purposes of this paragraph, more than one person  
2 may be considered to have initiated a message.

3 (G) “Procure” means intentionally to pay or provide consideration to, or induce, another  
4 person to create a website or domain name.

5 (H) “Recipient” means an authorized user of the electronic mail address to which the  
6 message was sent or delivered. If a recipient of a commercial electronic mail message  
7 has one or more electronic mail addresses in addition to the address to which the  
8 message was sent or delivered, the recipient shall be treated as a separate recipient  
9 with respect to each such address. If an electronic mail address is reassigned to a new  
10 user, the new user shall not be treated as a recipient of any commercial electronic  
11 mail message sent or delivered to that address before it was reassigned.

12 (I) “Internet information location tool” means a service that refers or links users to an  
13 online location on the worldwide web. Such term includes directories, indices,  
14 references, pointers, and hypertext links.

15 SECTION 3. *Criminal Offense and Penalty.* –

16 (A) *Website.* — Whoever knowingly, with the intent to carry on any activity which would  
17 be a crime of fraud or identity theft—

18 (1) Creates or procures the creation of a website or domain name that represents  
19 itself as a legitimate online business, without the authority or approval of the  
20 registered owner of the actual website or domain name of the legitimate online  
21 business; and

22 (2) Uses that website or domain name to induce, request, ask, or solicit any  
23 person to transmit, submit, or provide any means of identification to another;

24 shall be imprisoned for a minimum of six (6) months and one (1) day to a maximum of  
25 six (6) years and a fine of not more than Six Thousand Pesos (P6,000) but not less than Two  
26 Hundred Pesos (P200).

27 (B) *Messenger.* – Whoever knowingly, with the intent to carry on any activity which  
28 would be a crime of fraud or identity theft—

- 1 (1) Falsely represents itself as being sent by a legitimate online business;
- 2 (2) Includes an Internet information location tool that refers or links users to an  
3 online location on the world wide web that falsely purports to belong to or be  
4 associated with such legitimate online business; and
- 5 (3) Induces, requests, asks, or solicits a recipient of the electronic mail message  
6 directly or indirectly to provide, submit, or relate any means of identification  
7 to another;

8 shall be imprisoned for a minimum of six (6) months and one (1) day to a maximum of  
9 six (6) years and a fine of not more than Six Thousand Pesos (P6,000) but not less than Two  
10 Hundred Pesos (P200).

11 SECTION 4. *Liability of Officials of Juridical Persons.* – If the phiser is a partnership,  
12 firm, corporation or association, the president or the manager or any officer thereof who knows  
13 or should have known the commission of the offense shall be liable.

14 SECTION 5. *Separability Clause.* – If any provision, or part hereof, is held invalid or  
15 unconstitutional, the remainder of the law or the provision not otherwise affected shall remain  
16 valid and subsisting.

17 SECTION 6. *Repealing Clause.* – Any law, presidential decree or issuance, executive  
18 order, letter of instruction, administrative order, rule or regulation or part thereof, contrary to, or  
19 inconsistent with, the provision of this Act is hereby repealed, modified, or amended accordingly.

20 SECTION 7. *Effectivity Clause.* – This Act shall take effect fifteen (15) days after its  
21 publication in at least two (2) newspapers of general circulation.

22 Approved,