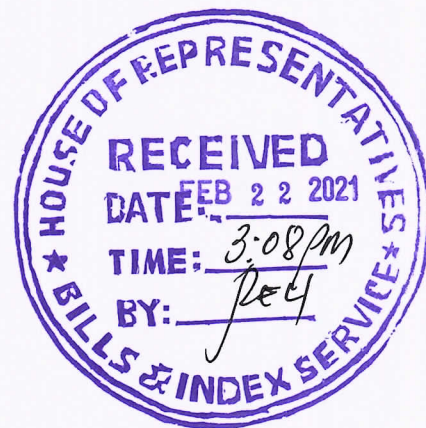


Republic of the Philippines  
HOUSE OF REPRESENTATIVES  
Quezon City

EIGHTEENTH CONGRESS  
Second Regular Session

House Bill. No. **8791**



---

Introduced by  
**Representatives CAMILLE A. VILLAR and  
JOSE FRANCISCO "KIKO" B. BENITEZ**

---

### **EXPLANATORY NOTE**

Phishing is a criminal act to acquire sensitive information, such as usernames, passwords, web site details and credit card accounts, by masquerading as a trustworthy entity in an electronic communication. It is an example of a social engineering technique to fool users of information highway<sup>1</sup>.

Phishing is perilous. On April 18, 2020, at the height of the lockdown, Philippine authorities warned Filipinos of an increase in phishing and other online fraud as more people take to the Internet to pay bills, bank and purchase groceries amid a lockdown due to the coronavirus outbreak. The online transactions have helped many cope with the restrictions of the lockdown on the main island of Luzon, where the capital Manila is located and which is home to some 57 million people or more than half of the country's population.

Both the Cybercrime Division of the National Bureau of Investigation (NBI) and the Bangko Sentral ng Pilipinas (BSP) have reported "a 100% increase in phishing and warned everyone to be cautious when it comes to individuals' bank details<sup>2</sup>.

The Bankers Association of the Philippines (BAP) has urged the public to be vigilant against phishing activities especially now that some people rely on online transactions following the declaration of enhanced community quarantine in most parts of the country.

Scammers usually pretend to be bank employees who ask for account details, while others claim to be members of charitable institutions seeking donations to help those affected by the lockdown.

As a crime, phishing targets are emails, telephone or text messages by someone posing as a legitimate institution to lure individuals into providing sensitive data such as banking and credit card details, passwords and personally identifiable information.

The most common forms of phishing are:

1. Link manipulation or a form of technical deception designed to make a link in an email and the spoofed website it leads to;
2. Filter evasion or the use of masquerade images and being sent to users with a great difficulty of deletion;

---

<sup>1</sup> Wikinedia [www.wikinedia.org](http://www.wikinedia.org) on phishing

3. Website forgery or the act of placing a picture of a legitimate URL over the address bar, or by closing the original address bar and its place, a new legitimate URL is created but is utilized to deceive e-mail users;

4. Phone phishing or the act of acquiring sensitive information through the use of telecommunication facilities including voice over internet protocol (VOIP).

Phishing may be considered as fairly new felony, a concordant effect of technology, with the first phishing technique described in detail only in 1987 but the actual crime committed a decade later, in 1996. Phishers (the term referred to perpetrators of phishing crimes) target large and known organizations known to transact heavily through e-commerce such as eBay, PayPal and banking and travel institutions dealing online.

The damage caused by phishing ranges from denial of access to one's email account to substantial financial loss. Fundamentally, it is an assault to a person's right to privacy. And significantly, they can ruin an individual's trustworthiness, credit standing and worse, deny the victims access to their bank accounts.

In the Philippines, the relevant statutes are the E-Commerce Law of the Philippines and the various issuances of the National Telecommunication Commission. But there is no specific legislation addressing this crime.

This bill seeks to commence the discussion on the enactment of an effective policy against phishing and all other forms of internet and telecommunications fraud. With more than 73 million internet users in the country<sup>3</sup> and online transactions becoming more popular as a mode of doing business in the Philippines, the early deliberation of this proposed measure is recommended.

  
JOSE FRANCISCO "KIKO" B. BENITEZ

  
CAMILLE A. VILLAR

Republic of the Philippines  
HOUSE OF REPRESENTATIVES  
Quezon City

EIGHTEENTH CONGRESS  
Second Regular Session

House Bill. No. 8791

---

Introduced by  
Representatives **CAMILLE A. VILLAR** and  
**JOSE FRANCISCO “KIKO” B. BENITEZ**

---

**AN ACT**  
**FURTHER PROTECTING THE INTEGRITY OF ELECTRONIC**  
**TRANSACTIONS, DEFINING FOR THE PURPOSE THE CRIME OF**  
**INTERNET AND TELECOMMUNICATIONS PHISHING, PROVIDING PENALTIES**  
**THEREFOR**

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

**Section 1.** Any person who shall commit the act of phishing in the internet or instant messaging system shall be punished with imprisonment of not less than two (2) years nor more than ten (10) years, or a fine of not less than Fifty Thousand Pesos (Php 50,000.00) but not more than Five Hundred Thousand Pesos (Php 500,000.00) or both such imprisonment and fine, at the discretion of the court.

The act of internet and message phishing involves securing or getting of sensitive personal information for the purpose of using it in fraud, or for participating in fraudulent business practices, or for the purpose of identity theft and misrepresentation. It is carried out by email or instant messaging or through the use of phone calls, voice over internet protocol or a combination of all those mentioned and other facilities of information technology.

The Act covers the development and possession of phishing kits or materials to commit fraud and the creation of fake websites to send bogus emails in order to defraud another person.

**Sec. 2.** The Department of Justice in coordination with the relevant offices shall establish a framework of comprehensive process of assisting victims of phishing and assist law enforcement agencies in obtaining evidence to apprehend perpetrators.

**Sec. 3. Implementing Rules and Regulations.** Within ninety (90) days after the approval of this Act, the Department of Justice shall promulgate the rules and regulations to supplement the enforcement of this Act.

**Sec. 4.** This Act shall take effect fifteen (15) days after its complete publication in the Official Gazette or in two (2) newspapers of general circulation, whichever comes earlier.

Approved,