



1 to a protected computer, by causing a computer program  
2 or code to be copied onto the protected computer, and by  
3 means of that program or code—

4 “(1) intentionally obtains, or transmits to an-  
5 other, personal information with the intent to de-  
6 fraud or injure a person or cause damage to a pro-  
7 tected computer; or

8 “(2) intentionally impairs the security protec-  
9 tion of the protected computer;

10 shall be fined under this title or imprisoned not more than  
11 2 years, or both.

12 “(c) No person may bring a civil action under the  
13 law of any State if such action is premised in whole or  
14 in part upon the defendant’s violating this section. For  
15 the purposes of this subsection, the term ‘State’ includes  
16 the District of Columbia, Puerto Rico, and any other terri-  
17 tory or possession of the United States.

18 “(d) As used in this section—

19 “(1) the terms ‘protected computer’ and ‘ex-  
20 ceeds authorized access’ have, respectively, the  
21 meanings given those terms in section 1030; and

22 “(2) the term ‘personal information’ means—

23 “(A) a first and last name;

24 “(B) a home or other physical address, in-  
25 cluding street name;



1 “(C) an electronic mail address;

2 “(D) a telephone number;

3 “(E) a Social Security number, tax identi-  
4 fication number, drivers licence number, pass-  
5 port number, or any other government-issued  
6 identification number; or

7 “(F) a credit card or bank account number  
8 or any password or access code associated with  
9 a credit card or bank account.”.

10 (b) Conforming Amendment- The table of sections at  
11 the beginning of chapter 47 of title 18, United States  
12 Code, is amended by inserting after the item relating to  
13 section 1030 the following new item:

“1030A. Illicit indirect use of protected computers.”.

14 **SEC. 3. AUTHORIZATION OF APPROPRIATIONS.**

15 In addition to any other sums otherwise authorized  
16 to be appropriated for this purpose, there are authorized  
17 to be appropriated for each of fiscal years 2005 through  
18 2008, the sum of \$10,000,000 to the Attorney General  
19 for prosecutions needed to discourage the use of spyware  
20 and the practice commonly called phishing.

21 **SEC. 4. FINDINGS AND SENSE OF CONGRESS CONCERNING**  
22 **THE ENFORCEMENT OF CERTAIN**  
23 **CYBERCRIMES.**

24 (a) FINDINGS.—Congress makes the following find-  
25 ings:



1           (1) Software and electronic communications are  
2           increasingly being used by criminals to invade indi-  
3           viduals' and businesses' computers without authoriza-  
4           tion.

5           (2) Two particularly egregious types of such  
6           schemes are the use of spyware and phishing scams.

7           (3) These schemes are often used to obtain per-  
8           sonal information, such as bank account and credit  
9           card numbers, which can then be used as a means  
10          to commit other types of theft.

11          (4) In addition to the devastating damage that  
12          these heinous activities can inflict on individuals and  
13          businesses, they also undermine the confidence that  
14          citizens have in using the Internet.

15          (b) SENSE OF CONGRESS.—Because of the serious  
16          nature of these offenses, and the Internet's unique impor-  
17          tance in the daily lives of citizens and in interstate com-  
18          merce, it is the sense of Congress that the Department  
19          of Justice should use the amendments made by this Act,  
20          and all other available tools, vigorously to prosecute those  
21          who use spyware to commit crimes and those that conduct  
22          phishing scams.

