SENATE STAFF ANALYSIS AND ECONOMIC IMPACT STATEMENT

(This document is based on the provisions contained in the legislation as of the latest date listed below.)

Prepared By: Communications and Public Utilities Committee

BILL: SB 2162

SPONSOR: Senator Posey

SUBJECT: Internet Computer Fraud

DATE: March 16, 2005 REVISED: _____ _____ _____ _____

	ANALYST	STAFF DIRECTOR	REFERENCE	ACTION
1.	Halloran/Wiehle	Caldwell	CU	**Favorable**
2.			CM	
3.			JU	
4.				
5.				
6.				

I. Summary:

The bill protects against internet computer fraud in three ways, by prohibiting phishing or fraud-based web sites, protecting against deceptive acts or practices relating to spyware, and prohibiting collecting specified information without notice and consent. The bill also designates a violation of these provisions a violation of the deceptive and unfair trade practices act and creates civil remedies.

The bill creates an as yet unnumbered section of the Florida Statutes.

II. Present Situation:

The Phoenix Business Journal recently had an article on the growing problems with phishing and spyware. According to the article, “phishing” is when unscrupulous individuals or organizations try to obtain consumer information via fraudulent Web sites. “Spyware” is hidden software that companies and others download onto personal computers when connected to the internet and then use to monitor the use of the computer and report it to the company or individual.

The Florida Deceptive and Unfair Trade Practices Act (FDUTPA), Chapter 501, part II, F.S., makes unlawful unfair methods of competition, unconscionable acts or practices, and unfair or deceptive acts or practices in the conduct of any trade or commerce. “Trade or commerce,” which includes the conduct of any trade or commerce, however denominated, including any nonprofit or not-for-profit person or activity, is defined as the advertising, soliciting, providing, offering, or distributing, whether by sale, rental, or rental, or otherwise, of any good or service, or any property, whether tangible or intangible, or any other article, commodity, or thing of value, wherever situated.

The enforcing authority for the FDUTPA is the local state attorney for violations within a single judicial circuit or the Department of Legal Affairs if the violation occurs in or affects more than one judicial circuit or, in cases affecting a single judicial circuit, when the office of the state attorney defers to the department in writing, or fails to act upon a violation within 90 days after a written complaint has been filed with the state attorney. The act provides for cease and desist orders, remedies by the enforcing authority, civil penalties, and receipt by the prevailing party of attorney's fees and costs in civil litigation.

A willful violation of the FUDTPA subjects the violator to a civil penalty of not more than $10,000 for each violation. In any civil litigation initiated by the enforcing authority, the court may award to the prevailing party reasonable attorney's fees and costs if the court finds that there was a complete absence of a justiciable issue of either law or fact raised by the losing party or if the court finds bad faith on the part of the losing party.

An individual harmed by a violation of the FUDTPA may, without regard to any other remedy or relief to which the person is entitled, bring an action to obtain a declaratory judgment that an act or practice violates the FUDTPA and to enjoin a person who has violated, is violating, or is otherwise likely to violate the act. In such an action, the person may recover actual damages, plus attorney's fees and court.

III. Effect of Proposed Changes:

Section 1 of the bill protects against internet computer fraud in three ways, by prohibiting phishing or fraud-based web sites, protecting against deceptive acts or practices relating to spyware, and prohibiting collecting specified information without notice and consent. The bill also designates a violation of these provisions a violation of the deceptive and unfair trade practices act and creates civil remedies.

Definitions

The bill creates definitions for use in interpreting and implementing these protections, as follows:

- "Authorized user" or "user" means a person who owns or leases a computer or who uses a computer when authorized by its owner or lessee. The term does not include a person who has obtained authorization to use the computer solely through an end-user license agreement.
- "Business entity" means a for-profit or not-for-profit corporation, partnership, limited partnership, proprietorship, firm, enterprise, franchise, association, or trust or a self-employed individual, whether fictitiously named or not, doing business in this state, and includes a contractor or subcontractor of such a business entity.
- "Computer" means an internally programmed, automatic device that performs data processing.
- "Computer program" or "computer software" means a set of instructions or statements and related data which, when executed in actual or modified form, cause a computer, computer system, or computer network to perform specified functions.
- "Computer user" means a person in this state who uses a computer that is connected to the Internet.

- "Computer virus" means a computer program that is designed to replicate itself or affect another program or file in a computer by attaching a copy of the program or other set of instructions to one or more computer programs or files without the consent of the owner or lawful user. The term includes, but is not limited to, programs that are designed to contaminate other computer programs; compromise computer security; consume computer resources; modify, destroy, record, or transmit data; or disrupt the normal operation of the computer, computer system, or computer network. The term also includes, but is not limited to, programs that are designed to use a computer without the knowledge and consent of an authorized user and to send large quantities of data to a targeted computer network without the consent of the network for the purpose of degrading the targeted computer's or network's performance or for the purpose of denying access through the network to the targeted computer or network.
- "Electronic mail message" means an electronic message or computer file that is transmitted between two or more telecommunications devices; computers; computer networks, regardless of whether the network is a local, regional, or global network; or electronic devices capable of receiving electronic messages, regardless of whether the message is converted to hard copy format after receipt, viewed upon transmission, or stored for later retrieval.
- "Internet" means the global information system that is logically linked together by a globally unique address space based on the Internet Protocol (IP), or its subsequent extensions; that is able to support communications using the Transmission Control Protocol/Internet Protocol (TCP/IP) suite, or its subsequent extensions, or other IP-compatible protocols; and that provides, uses, or makes accessible, either publicly or privately, high-level services layered on the communications and related infrastructure described in this section.
- "Personal identification information" means any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual, including:
    - A name, postal or e-mail address, social security number, date of birth, driver's license or identification number issued by a state or the Federal Government, telephone number, mother's maiden name, alien registration number, government passport number, employer or taxpayer identification number, Medicaid or food-stamp account number, bank-account number, credit-card or debit-card number, or personal-identification number or code assigned to the holder of a debit card by its issuer to permit authorized electronic use of the card;
    - Unique biometric data, such as a fingerprint, voice print, retina or iris image, or other unique physical representation;
    - A unique electronic identification number, address, password, or routing code;
    - Medical records;
    - Telecommunication identifying information or an access device;
    - Account balances;
    - Overdraft history;
    - Payment history;
    - A history of web sites visited;
    - A record of a purchase or purchases; or
    - Any other number or information that can be used to access an individual's financial resources.

- "Transmit" means to transfer, send, or make available computer programs or software, or any component of computer software, via the Internet or any other medium, including local area networks of computers, any other nonwire transmission, or any disk or other data storage device.
- "Web page" means a location with respect to the worldwide web which has a single uniform resource locator or other single location with respect to the Internet.

Phishing and fraud-based web sites

The bill provides that a person or a business entity may not, by means of a web page, electronic mail message, or other use of the Internet, solicit, request, or take any action to induce a computer user to provide personal identification information by representing that the person or business entity soliciting or requesting the information, either directly or by implication, is an on-line business, unless the person or entity has the authority and approval of the on-line business to make that representation.

Spyware

The bill provides that a business entity or person who is not the authorized user of a computer may not engage in deceptive acts or practices that involve any of the following conduct with respect to the computer.

- Taking control of the computer by:
  - using the computer to send unsolicited information or material from the computer to others;
  - diverting the Internet browser of the computer;
  - accessing or using the modem or Internet connection or service for the computer and thereby causing damage to the computer or causing the authorized user to incur unanticipated financial charges;
  - using the computer as part of an activity performed by a group of computers to cause damage to another computer; or
  - delivering advertisements that a user of the computer cannot close without turning off the computer or closing all sessions of the Internet browser for the computer.
- Modifying settings related to use of the computer or to the computer's access to or use of the Internet by altering:
  - the web page that appears when the authorized user launches an Internet browser or similar program used to access and navigate the Internet;
  - the default provider used to access or search the Internet, or other existing Internet connections settings;
  - a list of bookmarks used by the computer to access web pages; or
  - security or other settings of the computer which protect information about the authorized user for the purposes of causing damage or harm to the computer or its owner or user.
- Collecting personal identification information through the use of a keystroke logging function.

- Inducing the authorized user to install a computer software component onto the computer, or preventing reasonable efforts to block the installation or execution of, or to disable, a computer software component by:
  - ◊ presenting the authorized user with an option to decline installation of a software component such that, when the option is selected by the owner or authorized user, the installation nevertheless proceeds; or
  - ◊ causing a computer software component that the authorized user has properly removed or disabled to automatically reinstall or reactivate on the computer.
- Misrepresenting that installing a separate software component or providing log-in and password information is necessary for security or privacy reasons, or that installing a separate software component is necessary to open, view, or play a particular type of content.
- Inducing the authorized user to install or execute computer software by misrepresenting the identity or authority of the person or business entity providing the computer software to the user.
- Inducing the authorized user to provide personal identification, password, or account information to another person by misrepresenting the "identify" of the person seeking the information or "without the authority of that user's intended recipient of the information."
- Removing, disabling, or rendering inoperative a security, anti-spyware, or anti-virus technology installed on the computer.
- Installing or executing on the computer one or more additional computer software components with the intent of causing a person to use the components in a way that violates any other provision of this section.

Collection of information

The bill prohibits the collection of certain information without notice and consent. A business entity or person may not:

- transmit to a computer, which is not owned by that business entity or person and for which that business entity or person is not an authorized user, any information-collection program, unless the information-collection program provides notice in accordance with the above requirements before execution of any of the information-collection functions of the program; or
- execute any information-collection program installed on the computer unless before execution of any of the information-collection functions of the program the authorized user of the computer has consented to the execution under the notice required above.

The bill defines the term "information-collection program" to mean computer software that either:

- collects personal identifying information and sends that information to a person other than the authorized user of the computer or uses that information to deliver advertising to, or display advertising on, the computer; or
- collects information regarding the web pages accessed using the computer and uses that information to deliver advertising to, or display advertising on, the computer.

The notice required for an information-collection program must be clear and conspicuous, must be given in plan language, and must satisfy all of the following requirements:

- The notice must be clearly distinguishable from any other information visually presented contemporaneously on the protected computer.
- The notice must contain one of the following statements, as applicable, or a substantially similar statement:
  - For an information-collection program that collects personal identifying information and sends that information to a person other than the authorized user of the computer or uses the information to deliver advertising to the computer, the notice must state: "This program will collect and transmit information about you. Do you accept?"
  - For an information-collection program that collects information regarding the web pages accessed using the computer and uses that information to deliver advertising to the computer, the notice must state: "This program will collect information about web pages you access and will use that information to display advertising on your computer. Do you accept?"
  - For an information-collection program that performs both of the above-mentioned actions, the notice must state: "This program will collect and transmit information about you and your computer use and will collect information about web pages you access and will use that information to display advertising on your computer. Do you accept?"
- The notice must allow the user to grant or deny consent by selecting an option to grant or deny consent and abandon or cancel the transmission or execution without granting or denying consent.
- The notice must allow the user to select to display on the computer, before granting or denying consent, a clear description of:
  - the types of information to be collected and sent, if any, by the information-collection program;
  - the purpose for which the information is to be collected and sent; and
  - in the case of an information-collection program that first executes any of the information-collection functions of the program upon the next execution of other computer software, the identity of that other computer software.
- The notice must provide for concurrent display of the statements and options set forth above until the user:
  - grants or denies consent;
  - abandons or cancels the transmission or execution; or
  - selects the option of displaying the description of the type of information collected and the purpose of collection.

If an authorized user has granted consent to the execution of an information-collection program under this notice, no subsequent notice is required. However, the person who transmitted the program must provide another notice and obtain consent before the program may be used to collect or send information of a type or for a purpose that is materially different from, and outside the scope of, the type or purpose set forth in any previous notice.

Penalties

The bill makes a violation of its provisions a violation of the Deceptive and Unfair Trade Practices Act, set forth in part II of chapter 501, F.S., and subjects the person committing the violation to the penalties of that act.

The bill also creates civil remedies. A computer user, including an individual who is engaged in the business of providing Internet access service or who owns a web page or trademark, whose property or person is injured as a result of a violation of this section may:

- institute a civil action to enjoin and restrain future violations of the statute and to recover actual losses, lost wages, attorney's fees, and other costs incurred by the computer user or resulting from the misappropriation of the personal identification information of the computer user; or
- bring a civil suit for damages in an amount of up to $5,000 for each incident, or three times the amount of actual damages, whichever amount is greater. In such an action, the court may award reasonable attorney's fees to the prevailing party.

The venue for a civil action brought under this statute is the county in which the plaintiff resides or in any county in which any part of the alleged violation took place, regardless of whether the defendant was ever actually present in that county. A civil action must be brought within 5 years after the violation occurred.

A civil action may be filed regardless of whether there is any criminal prosecution for the acts that are the subject of the civil action. The rights and remedies provided by the bill are in addition to any other rights and remedies provided by law.

Section 2 provides that the bill takes effect July 1, 2005.

IV. Constitutional Issues:

A. Municipality/County Mandates Restrictions:

None.

B. Public Records/Open Meetings Issues:

None.

C. Trust Funds Restrictions:

None.

V. Economic Impact and Fiscal Note:

A. Tax/Fee Issues:

None.

B. Private Sector Impact:

Persons and businesses injured by activities made unlawful by the bill will have a cause of action to recover damages.

C. Government Sector Impact:

The Attorney General and a State Attorney bringing an action under the Unfair and Deceptive Trade Practices Act will incur expenses and receive remedies determined appropriate by the court.

VI. Technical Deficiencies:

On page 7, lines 19-25, the bill prohibits taking control of another's computer by "inducing the authorized user to provide personal identification, password, or account information to another person by misrepresenting the *identify* of the person seeking the information or *without the authority of that user's intended recipient of the information*. It appears that "identify" should be identity. Also, the latter prohibition lacks a verb and the intent is unclear.

The provisions on notice and consent to use of information-collecting software do not address issues relating to authority or ability of the computer user to give consent, for example whether the user is a minor.

VII. Related Issues:

None.

VIII. Summary of Amendments:

None.