Did you know that global telecommunications company AT&T was the corporate co-chair in 2011?

Anti-Phishing Act

Summary

This Act will help ensure that phishing and pharming are illegal and that the state has the ability to prosecute the bad actors that prey on the residents of this state. Phishing or Pharming are acts that defraud someone by using a false web site or pretending to be a legitimate business on the Web and fraudulently obtaining identifying information. This act also enables lawsuits by Internet service providers and owners of web pages or trademarks that are used without authorization in the conduct of a violation. It includes an immunity provision narrowly tailored to only those properties that are "controlled or operated" by the internet service provider or internet registrar.

Model Legislation

Section 1. {Definitions} As used in this Act:

1. "Entity" includes corporations, business trusts, estates, partnerships, limited partnerships, limited liability partnerships, limited liability companies, associations, organizations, joint ventures, governments, governmental subdivisions, agencies, or instrumentalities, or any other legal entity, whether for profit or not-for-profit.

2. "Individual" means a natural person.

3. "Identifying information" means any information that can be used to access an individual's financial accounts or to obtain goods and services, including, but not limited to: address, birth date, Social Security number, driver's license number, non-driver governmental identification number, telephone number, bank account number, student identification, credit or debit card number, personal identification number, unique biometric data, employee or payroll number, automated or electronic signature, computer image, photograph, screen name or password. The term does not include information that is lawfully obtained from publicly available information, or from Federal, State, or local government records lawfully made available to the general public.

4. "False pretenses" means the representation of a fact or circumstance which is not true and is calculated to mislead.

5. "Web page" means a location that has a single uniform resource locator (URL) with respect to the World Wide Web or another location that can be accessed on the Internet

Section 2. {Phishing and Pharming}

1. Phishing. – An individual or entity is guilty of phishing if, with intent to defraud or injure an individual, or with knowledge that he is facilitating a fraud or injury to be perpetrated by anyone:

(a) the actor makes any communication under false pretenses purporting to be by or on behalf of a legitimate business, without the authority or approval of the business; and

(b) the actor uses that communication to induce, request, or solicit any person to provide identifying information or property.

2. Pharming. – An individual or entity is guilty of pharming if, with intent to defraud or injure an individual, or with knowledge that he is facilitating a fraud or injury to be perpetrated by anyone:

(a) creates or operates a webpage that represents itself as belonging to or being associated with a legitimate business, without the authority or approval of such business, and that may induce any user of the Internet to provide identifying information or property; or

(b) alters a setting on a user's computer or similar device or software program through which the user may search the Internet and thereby causes any user of the Internet to view a communication that represents itself as belonging to or being associated with a legitimate business, which message has been created or is operated without the authority or approval of such legitimate business and induces, requests or solicits any user of the Internet to provide identifying information or property.

Section 3. {Immunity for Disabling Phishing and Pharming Sites} No Internet registrar or Internet service provider may be held liable under any provision of the laws of this State or of any political subdivision of this State for removing or disabling access to an Internet domain name controlled or operated by such registrar or by such provider or to content that resides on an Internet website or other online location controlled or operated by such provider and that such provider believes in good faith is used to engage in a violation of this Subchapter.

Section 4. {Violations}

1. A person who violates this section is guilty of a Class XX felony, a fine not to exceed $XXX or imprisonment not to exceed XX years, or both.

2. The following persons may bring a civil action against a person who violates this subchapter.

(a) an Internet service provider who is adversely affected by the violation;

(b) an owner of a web page, computer server, or a trademark that is used without authorization in the violation; or

(c) the Attorney General

3. Except as provided by paragraph 3, a person permitted to bring a civil action may obtain either actual damages for a violation of this Act or a civil penalty not to exceed $150,000 per violation of this act.

4. A violation of this Act by a state-chartered or licensed financial institution shall be enforceable exclusively by the financial institution's primary state regulator.

Section 5. {Applicability} This Act shall apply to the discovery of phishing or pharming incident that occurs on or after the effective date of this section. This act does not apply to a telecommunications provider's or Internet service provider's good faith transmission or routing of, or intermediate temporary storing or caching of, identifying information.

Section 6. {Effective Date} This Act shall take effect in 120 days after the date of enactment.

Section 7 {Preemption} This Act deals with subject matter that is of Statewide concern, and it is the intent of the Legislature that this Act shall supersede and preempt all rules, regulations, codes, statutes or ordinances of all cities, counties, municipalities and other local agencies within this state regarding the matters expressly set forth in this Act.

Adopted by the Telecommunications & Information Technology Task Force at the Annual Meeting, July 20, 2006. Approved by the ALEC Board of Directors August, 2006.