UNIVERSITY OF HAWAI‘I SYSTEM

TESTIMONY

SB 2869

RELATING TO CONSUMER PROTECTION

Testimony Presented Before the
Senate Committee on Media, Arts, Science, and Technology and
Senate Committee on Commerce, Consumer Protection, and Housing

February 10, 2006

By

David Lassner
Chief Information Officer
University of Hawaii

Testimony Presented Before the
Senate Committee on Media, Arts, Science, and Technology and
Senate Committee on Commerce, Consumer Protection, and Housing

February 10, 2006
By
David Lassner
Chief Information Officer

SB 2869 Relating to Consumer Protection

Chairs Fukunaga and Menor, Vice Chairs Ige and Baker and Members of the Committees:

The University of Hawaii supports SB 2869, which would establish a new set of prohibited acts and associated penalties for a variety of cybercrimes relating to "phishing" and "spyware."

The University of Hawaii (UH) experiences numerous instances of “phishing” and “spyware” impacting our students, faculty and staff. We regularly advise members of the UH community of potential dangers and hazards of these activities. These activities are increasing and more people are being victimized each year. A survey conducted by the Gartner Group in 2005 estimated that 57 million U.S. adults believe they received a phishing email. From the same survey, “2.4 million online consumers report losing money directly because of the phishing attacks. Of these, approximately 1.2 million consumers lost $929 million during the year preceding the survey” [http://www.gartner.com/press_releases/asset_129754_11.html].

What follows is a brief overview on “phishing” and “spyware” and an explanation of why they are so dangerous.

Phishing is attempt to steal personal information from an unsuspecting victim generally using email and a fraudulent website designed to look like the official company’s website. The email appears to be from a legitimate organization stating that an attempt has been made to compromise the potential victim’s account or personal information and that the recipient must go to a website to verify and/or correct their information. The email usually threatens account suspension or non-completion of a financial transaction such as a purchase or payment. The email often appears to come from an organization’s “security” or “fraud prevention” department.

Once a victim submits his/her personal information, it can be captured, sold and used to commit financial fraud. Often the victim does not realize he/she is a victim of identity theft until they apply for loans or receive notification of delinquent payments. It can often take between 3-5 years to repair the damage to one’s financial history and to restore their credit rating.

Spyware is another category of malicious software. Once installed on a computer it can run without the user's or owner's knowledge. Spyware is generally introduced into a computer through email attachments, pop-up ads, websites, and downloadable software such as peer-to-peer filesharing software and games.

Spyware can exhibit a variety of undesirable and dangerous behaviors:

- It can track which websites you visit and gather information about you to send you targeted advertisements.
- It can generate pop-up ads. In extreme cases, so many pop-ups ads start running that it renders the computer unusable.
- It can "hijack" your browser. It changes your "home" page on your browser to some other website that you didn't specify.
- It can record your keystrokes and send it to a server where the information can be used or sold. It's particularly dangerous if on-line financial transactions are captured including account numbers and passwords.
- It can disable your computer security software such, as turning off your antivirus software and Internet firewall leaving the computer vulnerable to other Internet threats.
- It can turn your computer into a "zombie" or "bot". Once compromised in this way, your computer becomes part of a network of "controlled" computers. These "controlled" computers can be used to disrupt network activities through activities such as Distributed Denial of Service attacks, which prevent the target site(s) from conducting their normal business. More frequently, these "controlled" computers become part of a spam-generating network. Millions of malicious spam messages are sent from these computers and are difficult to trace back to the original spammers. This spam may itself be part of phishing or spyware-related activities.

Recent statistics demonstrate the extent of these activities:

"Phishing represented an average of one in every 304 e-mails in 2005, up substantially from one in every 943 in 2004."
[http://www.itsecuritymagazine.com/its/News%20Documents/2006/Jan/IBM%20releases%20cybercrime%202006%20report.htm]

"The average number of spyware components per computer was 93 with one computer having well over a thousand."
[http://www.infosecwriters.com/texts.php?op=display&id=392]

Phishing and spyware activities are increasing. The imposition of strong penalties on the perpetrators of these activities can only help in our attempts to control this type of behavior and help prevent victimization of more innocent members of our community.

Thank you for this opportunity to testify in support of SB 2869.