



NEWS RELEASE

FOR IMMEDIATE RELEASE

Date: June 4, 2009

Contact: Ann Nishida-Fry
(808) 546-1888
Ann.nishida@hawaiiantel.com

Hawaiian Telcom Urges Customers to be Vigilant and Protect Their Personal Information from Fraud *Broadband Customers Receive Free Security Services from McAfee*

HONOLULU – With cybercrime on the rise, Hawaiian Telcom advises customers to always be alert and protect their personal information. In particular, customers should treat with caution and suspicion any emails that purport to come from Hawaiian Telcom that request personal information, such as the customer's user name, password or account number. The messages are fraudulent and should be deleted without replying.

"Hawaiian Telcom never sends email messages asking for this type of information," said John Komeiji, Senior VP and General Counsel for Hawaiian Telcom. "Phishing scams are increasing in occurrences and sophistication, and we must rely on the good sense of our customers to be the first defense against these threats so they do not become victims of fraud or identity theft."

"We take our customers' security seriously. That is why Hawaiian Telcom's consumer High-Speed Internet package comes with free security services from network security expert McAfee," added Komeiji.

The free McAfee [www.mcafee.com] services (\$70 retail value) provide comprehensive PC and identity protection to keep consumers safe from online threats and shield them from risky websites. It offers anti-virus, anti-spyware, anti-phishing, anti-spam, two-way firewall protection, parental controls and a powerful website safety advisor so users can safely surf the Web.

Phishing, a term coined in the 1990's, refers to the process of fraudulently attempting to acquire personal information such as passwords, account numbers or credit card numbers through electronic communication. Phishing messages may also include a Website link that takes you to a phony scam site or a pop-up window that looks exactly like a company's official site.

When Hawaiian Telcom becomes aware of such a scam, network security personnel take quick action to identify the source and administer a block to filter out phishing emails. However, as the frequency of such scams increases, customers should be vigilant about protecting their personal information to avoid fraud.

(more)

Tips to tell if an email message is fraudulent:

- It requests personal information, such as your password, user name, or social security number. Hawaiian Telcom never asks for this type of information through email.
- It conveys a sense of urgency. To encourage immediate response without giving a consumer time to think, the message may include verbiage such as “Respond within 48 hours or your account will be closed.” Phishing emails may also suggest your urgent response is required because your account was compromised.
- It is not personalized. Phishing emails are usually sent out in bulk and do not contain your first or last name.
- It encourages you to click on an embedded link within the message.
- It contains misspelled words. Phishers often use incorrect spelling in an attempt to evade a virus protection or computer security software’s identifying the email as spam or junk mail.

If email messages contain any of the elements above, use caution and verify its legitimacy with the company before responding. Hawaiian Telcom customers can visit www.hawaiiantel.net for information or call our technical support department at 643-4375.

About Hawaiian Telcom

Hawaiian Telcom is the state's leading communications provider, offering a wide spectrum of communications products and services, which include local and long-distance service, High-Speed Internet and wireless services. For more information, please visit www.hawaiiantel.com.

###