



**HAWAII HEALTH SYSTEMS**  
C O R P O R A T I O N

*"Touching Lives Every Day"*

## ***COMPLIANCE ALERT 13-7***

### ***Most Phishing Attempts are "Live"***

Phishing "fishing" is when an unauthorized source or person tries to get sensitive information from people to be used in identity theft and/or access to other protected information. Phishing continues to be a huge problem in healthcare organizations.

Many of us are sensitized to phishing attempts by email. Never open an attachment from someone you don't recognize or provide any sensitive, protected, or personal information to an unknown source. **However, we also need to be on their guard if asked for sensitive information over the phone or in person.** According to [Verizon's 2012 Data Breach Investigations Report](#) (page 34), 83% of Social Engineering attacks were conducted live by speaking directly with the victims.

This type of "live" phishing has occurred at HHSC facilities in the last year. Consequently, HHSC staff and employees should also be suspicious when someone calls and ask for sensitive, protected and information.

If you have any further questions, please contact your Regional Compliance Officer, David Lane, Ph.D., Chief Compliance and Privacy Officer [dlane@hhsc.org](mailto:dlane@hhsc.org), or James Brady, Ph.D., HHSC Security Officer [jbrady@hhsc.org](mailto:jbrady@hhsc.org).

Source: [http://www.verizonbusiness.com/resources/reports/rp\\_data-breach-investigations-report-2012\\_en\\_xg.pdf](http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf)