December 10, 2015

To: Campus Community

Fr: Matthew Hall, Associate Vice Chancellor for Information Technology & Chief Information Officer

Re: **What All UCSB Faculty And Staff Need To Do To Protect Against Cyber Threats**

Did you know the cost of an identity breach at UCSB is up to $12 million? Additional reputational costs could impact grants, faculty and student recruitment, and donors.

The University of California is taking active steps to improve cybersecurity across the system. Cyber threats come from nation states, criminals, hackers, and extremists. Each time you log on to the UCSB network or a campus system, you hold the key to protecting university information.

Cyber attackers target weaknesses in our servers, the campus network, office computers, and the devices you bring to campus. They only have to be successful once to cause significant damage.

As part of the UC-wide initiative, and the start of a campaign to raise awareness and improve overall cybersecurity here at UCSB, please follow these best practices to keep our campus network and systems secure:

- **When In Doubt, Throw It Out.** Links in email, tweets, posts, and online advertising are often the way cybercriminals compromise your computer. If it looks suspicious, even if you know the source, it's best to delete, or if appropriate, mark as junk email.

- **Enable Dual Factor Authentication.** Passwords are not as strong as they used to be. Two-factor authentication requires something you KNOW (a password) and something you HAVE (a phone). After you enter your password on a website, you'll get a second code sent to your phone. Only after you enter it will you get into your account. Many services now support two-factor authentication, including Google/Gmail, Microsoft accounts, Apple ID, Amazon Web Services, PayPal, Facebook, and LinkedIn.

- **Secure Mobile Devices With A Lock Screen.** Use a lock screen (with a PIN, fingerprint, or pattern to unlock) on phones and tablets. Set your device to automatically lock after one minute.

- **Simple Passwords Can Be Easily Hacked.** Combine capital and lowercase letters with numbers and symbols to create a more secure password. Separate passwords for each account helps to thwart cybercriminals.

- **Protect Sensitive Data.** Sensitive data (social security numbers, student information, credit card numbers) should be eliminated where possible from all computers and devices. If it absolutely must be stored, then encrypt it. Encryption of sensitive data with a strong password key prevents an attacker from reading its contents if the computer or device is compromised.

- **Stay Safe On Social Media.** Set the privacy and security settings on websites to your comfort level for information sharing. Think twice before posting pictures you wouldn't want your coworkers or future employers to see. The more information you post, the easier it may be for a hacker or someone else to use that information to steal your identity, access your data, or commit other crimes, such as stalking. If someone is harassing or threatening you, remove them from your friends list, block them, and report them to the site administrator.

Complacency about cybersecurity makes UCSB vulnerable to compromises that could significantly affect our mission of teaching, research, and public service. Your commitment to these cybersecurity best practices will protect the information entrusted to our campus.

Respectfully,

John Ajao
Director, Library Systems & Repository Operations

Matthew Hall
Associate Vice Chancellor for Information Technology & Chief Information Officer

Richard Kip
Assistant Dean for Academic Technology, College of Letters & Science

Antonio Manas-Melendez
Senior Internal Auditor, Audit & Advisory Services

Ben Price
Director, Administrative & Residential IT

Joe Sabado
Acting Executive Director, Student Information Systems & Technology

Andy Satomi
Director, Academic Affairs Information Technology

Jim Woods
Director of Computing, Marine Science Institute