CAMPUS NOTICE

ADMINISTRATIVE COMPUTING AND TELECOMMUNICATIONS (ACT)

November 1, 2010

ALL ACADEMICS, STAFF AND STUDENTS AT UCSD

SUBJECT: WARNING – Security Warning - WiFi Hotspot Hijacking

Everyone should be aware that a recently released Firefox browser extension called "Firesheep", allows anyone on a shared unencrypted wifi hotspot to easily hijack network traffic and take over web applications that communicate insecurely such as Twitter, Facebook, Webmail or other applications.

If you must conduct things like email and other business via a WiFi hotpot, you should ensure that all of your network applications use end-to-end encryption to protect the confidentiality and integrity of the data. You should know that not all services support end-to-end encryption. Until they do, users of mobile devices should take precautions to protect their network communications.

WiFi does have encryption, but only the most recent version will offer any protection from this issue. The use of the UCSD protected network because it has WPA2 encryption will prevent the disclosure of application data on the wireless segment of the network and is strongly recommended for all faculty, staff and students on campus. To protect you when you travel, be aware of what services you are using on open networks. Services such as instant messenger, printing, filesharing, and many web sites are not using end-to-end encryption and are easily visible to snooping and data theft. If you are off campus and you need to use one of these services, using the campus VPN first to encrypt your traffic over the wireless segment offers you significantly more privacy and security then using these services over an open wireless connection. Using the UCSD Protected Network while on campus with its WPA2 encryption will prevent the disclosure of application data and is strongly recommended for all faculty, staff and students on campus.

We also strongly encourage any and all users of the UCSD guest network to take precautions to protect their communications. The UCSD Guest network is not encrypted, so all communications should happen to SSL encrypted web sites or over a VPN connection.

Info on using the campus VPN:
http://blink.ucsd.edu/technology/network/connections/off-campus/VPN/

Info on the campus protected wireless:
http://blink.ucsd.edu/technology/network/connections/wireless/

Please contact security@ucsd.edu with any questions.

Charlotte Klock

Executive Director, IT Infrastructure
Interim Chief Security & Privacy Officer