October is National Cyber Security Awareness Month

To: Campus Community

Fr: Sam Horowitz, Chief Information Security Officer
Kip Bates, Associate Chief Information Security Officer

Don't be a victim of social engineering. In the information technology context, social engineering refers to miscreants that want you to do something that's against your best interest. Sometimes that's giving up your password. Other times it's giving up your hard-earned money.

October is National Cyber Security Awareness Month. This month we'll highlight actions that you can take to protect yourself from social engineering attacks. You will see posters in your departments and an article in The Current. Stop for a moment, and take note.

The most common form of social engineering is phishing. That's when a criminal sends you an email promising something wonderful or threatening dire consequences if you don't take action. Usually, there's a sense of urgency to do something now. With any of these, you should see flashing red lights.

Look carefully at the author's email address. Is it legitimate? Consider the tone. Is it something that is in character for our workplace or from the sender? Be careful when you click links. In Gmail, hover over them. You will see the actual URL in the lower left of your window. Look carefully to determine if the website referenced is what you think it should be.

If the link says it's a UCSB website, but the link ends in something other than .edu, then it may be a phishing message. Misspellings and bad grammar are hallmarks of many phishing messages. Remember the three signs: promises, threats, and urgency.

Some of the university's suppliers, like Anthem and Health Net, send legitimate messages to members of our community, but they shouldn't have the three signs and they shouldn't have misspellings or bad grammar. There is no substitute for your critical judgment.

It's not enough to protect yourself from being a victim. You can help protect the rest of the campus community! Mark your message as phishing. In Gmail, you do this by three dots near the date. Select "Report Phishing" if you believe the message is phishing. If it's just an unwanted email that isn't trying to trick you into supplying information, you can click "Report spam." Doing so will improve Google's ability to filter the messages before they reach other users.

Remember that social engineering messages can arrive by telephone or text message. You need to be vigilant there, too.

Share this information with our friends and family. Follow the UCSB Information Security team on Twitter, Facebook, and Instagram to get more information about protecting yourself from cyber threats. Together, we can keep our corner of the Internet a little bit safer for everyone.

Regards,
Sam Horowitz, Chief Information Security Officer
Kip Bates, Associate Chief Information Security Officer

Join us on social media:
- Twitter: @UCSB_ITSECURITY
- Facebook: @UCSB.Infosec
- Instagram: ucsb_itsecurity