CSU The California State University
WORKING FOR CALIFORNIA

Phishing: Don't Take the Bait

What is Phishing?

Phishing refers to the use of fraudulent email messages that appear to come from a legitimate vendor or an actual employee

The FBI has indicated that imposter fraud that targets colleges and universities is growing. Fraudsters are constantly changing the tactics they employ to dupe organizations out of their funds and thus we must be mindful of this whenever changes are requested or if something seems odd. As a public institution, it can be easily determined who has business contracts with us, which makes it even easier for criminals to pose as contacts for those companies. The following are some tips prevent a loss of funds to your campus or auxiliary.

Do not publish forms to change payment instructions publicly on the web

- ✓ Do not make it easy for fraudsters to request changes to payment instructions. Forms should be available only through formal request from a known vendor contact via phone or previously established e-mail correspondence.

Any requests for changes to payment instructions should be followed up with a phone call to a known phone number of a contact at that vendor

- ✓ Fraudsters will not only create an e-mail address that looks just like that of a vendor, but also will copy e-mail signatures and incorporate vendor logos in many instances. The phone number in the signature line may route to a fraudster's phone as well where they can try to verify the same information they provided in the phony e-mail. Thus, it is best to contact a known source at the vendor company to ensure that the request to change payment instructions is limited. Documentation of this verification is **key**. It is recommended that current banking information be included on the request to revise bank accounts. This will help validate the authenticity of the requesting source.

Beware of voicemail, fax and e-mail phishing

- ✓ Fraudsters may call or leave a voicemail claiming to be a vendor when really they are looking to source information that they can then use to their advantage. If an individual is posing questions that a vendor should already know the answer to, then it may be wise to halt the call and contact a known representative of the vendor to verify the other individual's connection to the vendor.
- ✓ There have been several times where fraudsters have also posed as executives within college campuses requesting payment via e-mail for a specific reason. Campuses and auxiliaries should have protocols for these types of payments and there is rarely a reason that they should be circumvented- pick up the phone and make sure the request is legitimate. A reply back to the e-mail is not sufficient as it could be going back to a fraudulent e-mail address.

Have a policy regarding refunds for overpayment

- ✓ Although not specifically wire or ACH fraud, funds coming in for an unidentifiable or unspecifiable reason should be scrutinized, especially if a student or vendor is requesting a refund for the "excess" funds. If the funds are grossly in excess, then instead of issuing a refund, the full amount should be returned to the originator; ensure we are not unwittingly engaging in money laundering.

Report fraud instances and attempts to management and the Treasury group

We can all learn from one another and form best practices along the way, but this can only occur if experiences and information are shared