Kern Community College District

Phishing Campaign Plan

Intro

Phishing is a cyber technique that is used in most attacks today to infiltrate a network, compromise user data, or spread ransomware. Phishing is an email that is sent from an adversary that has malicious links embedded, request users to enter passwords, or used to identify the users contact list.

The phishing campaign will be a training tool to give users awareness of what techniques are being used and know how to report potential phishing emails. The phishing campaign will be conducted every semester to ensure users are vigilant in the trends of what is being seen. There will be a training opportunity for users that may click on the link or give out passwords. The training will provide the things to review in an email that is not expected.

Plan

The phishing campaign will be conducted each semester to provide user awareness and to be aware of trending phishing attacks that occurring.

Steps:

1. The email address will be updated with all staff, 2 weeks before the training is conducted. Updating the email addresses will ensure if there are any changes in staff that will also be included in the training and the phishing campaign.
2. Training will be provided to all staff per the schedule below. The training will provide awareness of the threat and what things to look in a phishing email.
3. The phishing campaign will be conducted over a week span. All users will receive an email tailored for the trending categories and different method that may be seen in today's environment. The phishing campaign will provide a report on staff that open the email, click the active link, provide a password, or download the attachment. The reports will be available for awareness of the effectiveness level of success with an attack and determine better ways to provide training in the future.
4. If staff open the email, click the active link, provide a password, or download the attachment there will be another email sent for additional training. The training will be a refresher of what things to look for and remind staff to report suspicious email. Training that is completed will be available in a report to further analysis how to improve user awareness to staff.

Schedule

The following is the schedule for phishing training that will be provided to all staff. The training will be logged and available for reporting on completion. The schedule also includes the phishing campaign for all staff. Users can report identified phishing emails and further training will be available thru an email if the user clicks on the suspicious links.

Training for all Staff Schedule

Semester Quarter	Training Dates
Summer 2022 12 Week Classes	May 9-13, 2022
Summer 2022 8 Week Classes	May 31-Jun 3, 2022
Fall 2022	Aug 15-19, 2022
Winter 2023	Jan 9-13, 2023

Phishing Campaign Schedule

Semester Quarter	Phishing Campaign
Summer 2022	Jun 6-10, 2022
Fall 2022	Sept 5-9, 2022
Winter 2023	Jan 30-Feb3, 2023

User Impact

The phishing campaign will include an email that is sent out during scheduled times and may last up to a week in duration. Users that identify the email should report the to the Help Desk or enter a ticket on the main website.

Phishing Email Tactics: Included below are tips to review emails for phishing. If there are any suspicious emails report to the Help Desk for further review.

- Do not open emails that you are not expecting.
- Email address from the senders that have misspelling or a domain that is not recognized should not be opened.
- Vendors and common companies will have recognized branding, however if there are misspellings in the body of the message or poor grammar the email may not be from the company.
- Before clicking on a link in an email, hoover your mouse over the link. The link should start with a known domain and then have further file extensions before clicking.
- If you are prompted for a password reset, ensure the website you are pointed to is a known site. Also, most sites do not have you put in your password, a temporary password or code is given to you in a separate email to change to.