OMB Control # 0693-0089
Expiration Date: 09/30/2024

Research on People's Perceptions of Phishing Email Cues Reporters Study

**FOUR STANDARD SURVEY QUESTIONS**

**1. Explain who will be surveyed and why the group is appropriate to survey.**

The Information Access Division (IAD), of the Information Technology Laboratory (ITL), at the National Institute of Standards and Technology (NIST) is leading this information collection.

Organizations across all sectors utilize embedded phishing awareness training programs to prepare their employees for real-world phishing attacks. As a part of these programs, organizations send a simulated phishing email to employees to train them to spot real-world phishing emails. However, it is unknown which phishing email cues – the properties of an email that either compel a user to click on a fraudulent link or attachment or alert the user that the email may be a phish – have a higher impact than others when email recipients make phishing determinations. Therefore, it is necessary and appropriate to survey email users who participate in these training programs.

NIST will conduct this study with federal and non-federal organizations that implement embedded phishing awareness training programs to investigate the differences in people's perceptions when identifying different types of cues in a phishing email. This submission for OMB approval is submitted to cover non-federal participants of the study. The email recipients that are trainees in these programs will be invited to participate via email (see attached Study Participation Email Invitation). See question 3 below for sampling information.

**2. Explain how the survey was developed including consultation with interested parties, pre-testing, and responses to suggestions for improvement.**

The survey instrument was developed and refined based on prior NIST phishing research (Greene, et. al. User Context: An Explanatory Variable in Phishing Susceptibility, 2018). During development, the survey was reviewed by two survey experts and two subject matter experts (SMEs) to ensure the language and questions were accurately and appropriately tailored for the study population. Feedback from the reviewers was incorporated in the final survey instrument. An established method for accurately predicting survey completion time was used to determine the survey instrument's timing (https://verstaresearch.com/newsletters/how-to-estimate-the-length-of-a-survey/).

**3. Explain how the survey will be conducted, how customers will be sampled if fewer than all customers will be surveyed, expected response rate, and actions your agency plans to take to improve the response rate.**

NIST will conduct an anonymous survey online using the Qualtrics survey platform. An email (see attached Study Participation Email Invitation) will be sent to approximately 20,000 individuals 18 years or older who are a part of their organization's embedded phishing awareness training program inviting them to complete the survey. The survey will be closed once 1,000 respondents complete the survey. If participants choose to participate, they will click the link in the email to be directed to the survey instructions and survey (see attached Reporters Information Sheet and Survey Instrument).

The survey will take approximately 15 minutes to complete. The survey will be open for 4 weeks after the phishing email is sent.

**1,000 respondents x 15 minutes per response = 250 burden hours.**

As stated in the provided Information Sheet, to maintain participant confidentiality, no identifiers, data, or information are collected that can be traced back to participants. Individual responses will be assigned an anonymous reference code generated by the Qualtrics platform. NIST will not create or keep a list that links the response reference codes to specific participants. There will be no collection, storage, access, use, or dissemination of personally identifiable information from the survey.

**4. Describe how the results of the survey will be analyzed and used to generalize the results to the entire customer population.**

Data analyses will be conducted by NIST researchers. Both descriptive and inferential statistics will be conducted to understand participants' perceptions of phishing emails. Based on data analyses, the survey results may be generalizable to a broader population of individuals whose organizations conduct embedded phishing awareness training programs.