Phish Out of Water: A Large-Scale Study of Phishing Email Cues

Jody Jacobs, Shanée Dawkins, Julia Sharp, *National Institute of Standards and Technology*
Katherine Garcia, *Rice University*
Brandon Pearson, Warda Usman, Alycia Carey, Joshua Reynolds, Chris Fennell, *Walmart*

Abstract

This poster presents the results of a study on people's perceptions of phishing email cues. The study, conducted in collaboration with Walmart's information security research team, examined whether the presence of certain cues impacts human phishing email detection. 26 unique cues across five cue types were tested with more than 50,000 Walmart employees; nearly 3,000 participants completed a follow-up survey. The simulated phishing campaign resulted in a 16.81% report rate and a 7.22% click rate. Preliminary survey results suggest that there are no differences in clicking behaviors between cue types.

1. Introduction

Simulated phishing emails sent as a part of an organization's embedded phishing awareness training program typically contain one or more cues that either compel the recipient to click on a fraudulent link or attachment or alert them that the email may be a phish [1]. Phishing awareness research has typically focused on why people fall for phishing emails [2] [3] or the efficacy of phishing training [4]. The phishing awareness research community has yet to fully evaluate whether some of these cues have a higher influence than others on email recipients' decision-making during phishing determinations. Since cues vary in their location, size, premise, and frequency, current phishing awareness evaluation methods may be limited; this presumes that the difficulty of spotting a phishing email is not influenced by the style and severity of the cue. The study reported here was designed to address this limitation by examining people's perceptions of phishing emails and whether the presence of certain cues influences their detection of phishing emails. We report a subset of the results of the research question, *what differences, if any, exist in people's perceptions of phishing email cues when determining whether an email is a phish or not?* This study will help us better understand which cues are most strongly associated with human perceptions and behaviors.

USENIX Symposium on Usable Privacy and Security (SOUPS) 2026. August 23 -- 26, 2026, Hannover, Germany.

2. Methodology and Study Design

To collect operational data, the study was designed so that Walmart researchers could seamlessly integrate the phishing simulations into their existing phishing awareness training program. Using the comprehensive list of phishing cues from the NIST Phish Scale [5] [6], 26 controlled simulated phishing emails about an Artificial Intelligence (AI) conference registration (each email having one cue) were sent to Walmart associates (employees) in place of their regularly scheduled monthly phishing training campaigns (see Appendix for list of cues by cue type and example of the simulated phishing email). In August 2025, Walmart distributed the emails evenly across 57,785 associates, so that each cue email was sent to 2,222 or 2,223 associates (U.S.-based, selected randomly).

One week after the phishing emails were sent, study participants were invited via email to take an anonymous post-exercise survey, aimed at analyzing their reactions to the phishing email and their perceptions of phishing emails overall. Cues were represented in the survey both individually and by the five NIST Phish Scale cue types: common tactic, error, language and content, technical indicator, and visual presentation indicator [7]. The survey remained open for three weeks, with reminder emails sent to study participants. Participants were not required to respond to any questions in the survey. A subset of the survey findings is presented here (see Appendix for survey questions presented here).

2.1 Data Collection

Exercise Data. Study participants' actions during the simulated phishing exercises were categorized by:

- Clickers – clicked on a link or attachment in the phishing email and did not report the email to Walmart.
- Reporters – reported the email to Walmart and did not click on a link or attachment.
- Clickers and Reporters – clicked on a link or attachment and also reported the email to Walmart.
- No Action – neither clicked on a link or attachment nor reported the email to Walmart.

Survey Data. The NIST-hosted Qualtrics survey included quantitative and qualitative questions. Participants were organized into three groups according to their exercise action (i.e., no action, reporters only, and clickers – which refers to both the clickers only group and the clickers and reporters group in the survey data). Respondent data where Qualtrics indicated the survey progress was 0% were excluded prior to analyses.

2.2. Limitations

Emails used for the study were not subject to Walmart's security protections, and therefore, exercise results may not fully reflect participants' phishing email behaviors. Additionally, survey response rates may have been affected by Walmart's security practice of blocking links in the survey invitation email; associates needed to retype or copy/paste the link text into a browser to access the survey.

3. Results

Of the 57,785 Walmart associates sent emails as part of the study, 70.96% took no action; 16.81% reported the email but did not click; 7.22% clicked but did not report the email; and 5.01% clicked and reported the email. The five cue types had similar percentages of clicked only, clicked and reported, reported only, and no action taken (see Appendix Section 9.4 Exercise Data). The five cue emails with the highest click rates (not including those that clicked and reported) were 'Poses as a friend, colleague, supervisor, authority figure (common tactic cue type; 8.24%); 'Lack of signer details' (language and content cue type; 8.01%; 'Spelling errors' (errors cue type; 7.92%); 'Domain spoofing in email address' (technical indicator cue type; 7.87%); and 'No/minimal branding/logos' (visual presentation indicator cue type; 7.78%); and 'No/minimal branding/logos' (visual presentation indicator cue type; 7.78%).

3.1 Survey Results

A total of 2,535 associates completed the survey: 1,005 clickers; 993 reporters only; 537 no action (see Appendix Section 9.5 Survey Data for detailed results of the survey questions presented in this section). Of those that responded to the question about what they did next after seeing the phishing email (N=717 clickers, N=716 reporters only, and N=244 no action), reporters only and clickers groups predominantly responded that they "reported the email" (83.10% of reporter respondents and 62.62% of clicker respondents). The no action taken respondents for this question predominantly "ignored it and continued [their] work" (59.43%).

Participants were also asked whether they noticed anything unusual about the phishing email they received. Notably, across all cue emails, 90.00% of clickers responding to this question (N=710) indicated that they thought the email looked suspicious. All respondents that received the cue email 'You're special' (N=26), 'Generic greeting' (N=24), and 'URL hyperlinking' (N=23) thought the email looked suspicious and yet clicked one of its links.

Regarding phishing email detection behaviors more broadly, survey participants were asked about their likelihood of looking for the individual cues when identifying a phishing email. It is notable that the percentage of respondents, for each of the groups (clickers, reporters only, and no action), who indicated that they were extremely likely to look for the 'Poses as a friend, colleague, supervisor, authority figure' cue was among the lowest compared to the other cues in the common tactic cue type. However, when put in the context of the exercise data, 'Poses as a friend, colleague, supervisor, authority figure' had the highest click rate. Additionally, respondents in all three groups indicated that they were extremely likely to look for the cues within the errors cue type, yet the 'Spelling errors' cue was in the top five emails clicked.

4. Discussion

The preliminary findings from this study suggest that the type of phishing email cue does not impact clicking behaviors. Additionally, those who fall for phishing emails and click the links within them may do so even if the email looks suspicious. Lastly, there may be a disconnect between participant actions and the cues they typically look for when determining if an email is a phish or not. Careful consideration should be given to the content of simulated phishing emails and supplemental training materials, aligning the cues people look for and the cues that compel them to click in phishing emails, to have effective training in modern phishing awareness programs.

5. Ethical Considerations

The study protocol was reviewed and approved by NIST's Research Protections Office in accordance with NIST human subjects research guidelines and ethical principles. This study meets the criteria for exempt human subjects research. Participation in the survey was voluntary. We protected participant confidentiality by using an anonymous reference code for the research records and by redacting any identifiable information from the data prior to analysis.

6. Acknowledgments

NIST would like to acknowledge Lorenzo Neil for his contributions to the study design. The authors would also like to thank Walmart's phishing awareness training team for assisting with coordinating email dissemination and analysis efforts. This material is based upon work supported by Rice University NIST Graduate Student Measurement Science and Engineering Fellowship Program under Award Number 70NANB21H090.

7. Disclaimer

Any mention of commercial products or companies is for information only and does not imply recommendation or endorsement by the National Institute of Standards and Technology, nor does it imply that the products are necessarily the best available for the purpose.

This manuscript was edited with the assistance of Google Gemini. Google Gemini was used to refine R code for data wrangling and summarization in accordance with the authors' instructions. All content, scientific claims, and conclusions have been reviewed and verified by the authors to ensure accuracy and originality.

8. References

1. Fennell, C., (2023). Email Challenges and Phishing with Chris Fennell. Sp4rkCon 2023. https://internal.walmart.com/content/sp4rkcon/wmeo/sp4rkcon-home/sp4rkcon-2023/agenda/email-challenges-and-phishing.html
2. Auton, J. C., Sturman, D., (2025). Persuasion under pressure: the influence of persuasion principles and time constraints on phishing email susceptibility. *Information and Computer Security*, Vol. 33 No. 5 pp. 845–859, doi: https://doi.org/10.1108/ICS-07-2024-0163
3. Butavicius, M., Taib, R., & Han, S. J. (2022). Why people keep falling for phishing scams: The effects of time pressure and deception cues on the detection of phishing emails. *Computers & Security*, *123*, 102937. https://doi.org/10.1016/j.cose.2022.102937
4. Ho, G., Mirian, A., Luo, E., Tong, K., Lee, E., Liu, L., Longhurst, C., Dameff, C., Savage, S., & Voelker, G. M., (2025). Understanding the Efficacy of Phishing Training in Practice, 2025 IEEE Symposium on Security and Privacy, San Francisco, CA, pp. 37-54. https://doi.org/10.1109/SP61157.2025.00076
5. Steves, M. P., Greene, K. K., & Theofanos, M. F., (2019). A phish scale: rating human phishing message detection difficulty. Proceedings 2019 Workshop on Usable Security. Workshop on Usable Security, San Diego, CA. https://doi.org/10.14722/usec.2019.23028
6. Steves, M., Greene, K., & Theofanos, M., (2020). Categorizing human phishing difficulty: A Phish Scale. Journal of Cybersecurity, 6(1), tyaa009. https://doi.org/10.1093/cybsec/tyaa009
7. Dawkins, S., Jacobs, J., (2023). NIST Phish Scale User Guide. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Series TN 2276. https://doi.org/10.6028/NIST.TN.2276

9. Appendix

9.1 Phishing Cues

The 26 phishing cues tested in this study are based on the NIST Phish Scale cues, grouped into five types (see Table 1. List of Cues by Cue Type) [7].

Table 1. List of Cues by Cue Type

Technical Indicator Cues
Sender display name and email address
Domain Spoofing in email address
Attachment Type
URL Hyperlinking
Domain Spoofing in links
Visual Presentation Indicator Cues
No/minimal branding/logos
Logo imitation
Out-of-date branding/logos
Unprofessional looking design or formatting
Security indications and icons
Language and Content Cues
Generic greeting
Lack of personalization
Lack of signer details
Legal language/copyright info/disclaimers
Distracting detail
Requests for sensitive information
Sense of urgency
Threatening language
Error Cues
Spelling errors
Grammar irregularities
Inconsistency
Common Tactics Cues
Poses as a friend, colleague, supervisor, authority figure
Humanitarian appeals
Too good to be true offers
You're special
Limited time offer

9.2 Sample Simulated Phishing Email

Figure 1. Spelling Error Phishing Email Template shows the phishing email sent to study participants for the "spelling errors" cue using the conference registration template.

Figure 1. Spelling Error Phishing Email Template

The text below is from the email image above:

Dear [associate name]

Thank you for registering to participate in CogNeatoCon AI Summit 2025! Your registration has been processed. In this email you will find important information about your conference registration.

There is complementary parking onsite.

Your registration ID is: 13454982345

You can view yur receipt and update your registration status here: CogNeatoConAI.chkpt-ecommerce.com.

If you need any other information for the conference, please visit our website at CogNeatoConAI.chkpt-ecommerce.com.

If you have received this email in error, please click here: CogNeatoConAI.chkpt-ecommerce.com.

Thank you,
CogNeatoCon AI Summit 2025
CogNeatoConAI.chkpt-ecommerce.com

9.3 Phishing Survey Questions

The survey included questions related to participants' overall perceptions of phishing emails and their specific perceptions of the email they received in the study. This paper presents results from the following survey questions:

Q2c: When you saw the email, what did you do next? (Select all that apply.)

- Replied to the email
- Ignored it and continued my work
- Showed it to someone I know
- Opened the sender's website in a separate browser window

- Forwarded it to my organization's IT department or other trusted authority
- Reported the email
- I did something else [open ended]

Q4: Did you notice anything unusual about the email? (Select one.)

- No, I thought the email looked legitimate.
- Neither suspicious nor legitimate.
- Yes, I thought the email looked suspicious.

Q7b: How likely or unlikely are you to look for the following when you are trying to decide if an email is a phish or not? *[grid list of cues with Likert scale response options]*

- Extremely unlikely
- Unlikely
- Neither likely nor unlikely
- Likely
- Extremely likely

9.4 Exercise Data

Figure 2 and Table 2 depict overall participant actions by cue type.

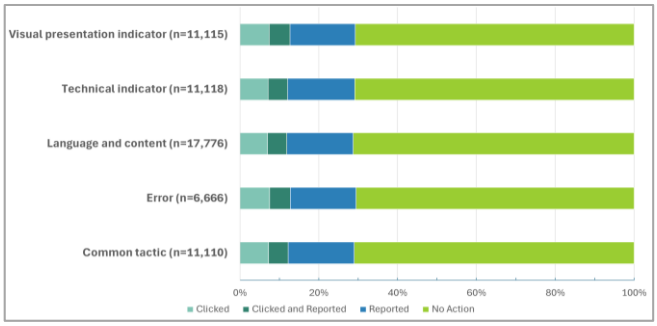

Figure 2. Participant Actions by Cue Type

Table 2. Participant Actions by Cue Type

Cue Type	Clicked Only	Clicked and Reported	Reported Only	No Action
Visual presentation indicator (N=11,115)	7.42%	5.26%	16.55%	70.77%
Technical indicator (N=11,118)	7.11%	4.95%	17.08%	70.86%
Language and content (N=17,776)	7.01%	4.85%	16.88%	71.26%
Error (N=6,666)	7.56%	5.22%	16.71%	70.51%
Common tactic (N=11,110)	7.26%	4.95%	16.76%	71.03%

N=total number of associates sent emails with cues in the corresponding cue type

9.5 Survey Data

Figure 3 and Table 3 show the survey data for survey question 2c, "When you saw the email, what did you do next?"

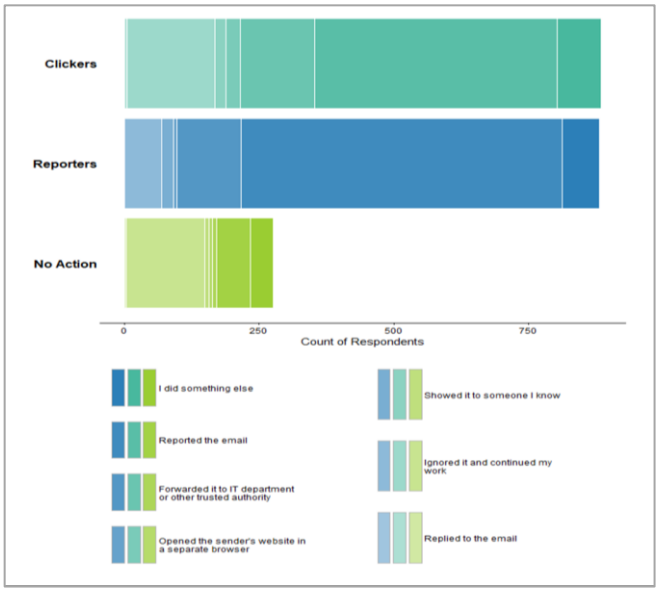

Figure 3. When you saw the email, what did you do next?

Table 3. Survey data – actions after seeing phishing email

Action	Clickers	Reporters Only	No Action
Replied to the email	0.68% (6)	0.11% (1)	1.4% (4)
Ignored it and continued my work	18.42% (163)	7.71% (68)	52.35% (145)
Showed it to someone I know	2.5% (19)	2.61% (23)	3.25% (9)
Opened the sender's website in a separate browser window	3.16% (28)	0.68% (6)	1.81% (5)
Forwarded it to my organization's IT department or other trusted authority	15.59% (138)	13.49% (119)	3.25% (9)
Reported the email.	50.73% (449)	67.46% (595)	22.38% (62)

I did something else.	9.27% (82)	7.94% (70)	15.52% (43)
Total Respondents (N)	*717*	*716*	*244*

Table 4 shows the clickers group survey data for survey question 4, "Did you notice anything unusual about the email?". The list of cues here is limited to those with the highest 'yes' percentages (those greater than 95%).

Table 4. Clickers group survey data – perceived suspicion

Cue	"Yes, I thought the email looked suspicious"
You're special (N=26)	100.00%
Generic greeting (N=24)	100.00%
URL hyperlinking (N=23)	100.00%
Spelling errors (N=30)	96.67%
Sender display name and email address (N=30)	96.67%
Requests for sensitive information (N=23)	95.65%
Distracting detail (N=21)	95.24%

N=total number of Clickers Respondents

Figure 4 and Table 5 show the survey data for survey question 7b, "How likely or unlikely are you to look for the following when you are trying to decide if an email is a phish or not?" for the Spelling errors and Poses as a friend, colleague, supervisor, authority figure cue types.

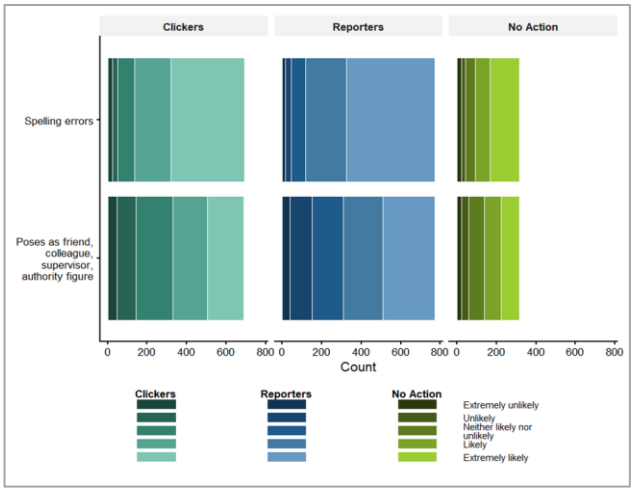

Figure 4. Likelihood of looking for cues when identifying phishing email

Table 5. Survey data – likelihood of looking for cue when identifying phishing email

Cue	Response	Clickers	Reporters	No Action
Spelling errors	Extremely unlikely	3.32% (23)	1.94% (15)	7.28% (23)
	Unlikely	3.75% (26)	3.63% (28)	5.7% (18)
	Neither likely nor unlikely	12.7% (88)	9.59% (74)	16.14% (51)
	Likely	26.41% (183)	26.68% (206)	24.37% (77)
	Extremely likely	53.82% (373)	58.16% (449)	46.52% (147)
	Total Respondents (N)	*693*	*772*	*316*
Poses as friend, colleague, supervisor, or authority figure	Extremely unlikely	6.97% (48)	4.% (37)	7.64% (24)
	Unlikely	13.93% (96)	14.62% (113)	11.46% (36)
	Neither likely nor unlikely	26.85% (185)	20.57% (159)	24.84% (78)
	Likely	25.4% (175)	26% (201)	27.39% (86)
	Extremely likely	26.85% (185)	34.02% (263)	28.66% (90)
	Total Respondents (N)	*689*	*773*	*314*