Does the Take9 Cybersecurity Awareness Campaign Work?

Ginger Smith, Michael Stoneman, Risa Shishido, Lorrie Faith Cranor
Carnegie Mellon University

1 Introduction

Despite decades of technical countermeasures, phishing continues to succeed largely because it exploits human behavior rather than software flaws. **Take9**, a U.S. cybersecurity awareness campaign launched in September 2024, addresses this by urging users to pause nine seconds before acting on suspicious messages. By October 2025, the campaign reported reaching 44 million people and 28 million video views through social media and other channels [7].

The videos use a narrative format: a character opens a suspicious email attachment, triggering a chain of consequences shown visually: identities are stolen, banking information is compromised, and power grid transformers are damaged, leaving ordinary people without electricity [2]. The longer video includes additional consequences (device infections, password theft), and brief advice (strengthen passwords, contact IT). [1] The campaign frames cybersecurity not as a technical problem but as a matter of everyday habit, aiming to shift behavior without requiring technical understanding.

Prior work found that users respond to cybersecurity communications based on their mental models of who is at risk and why, rather than the content of a threat. Wash found that many users justify ignoring security advice by reasoning that they are too insignificant to be targeted, or that their individual actions could not have large-scale consequences [9]. Vishwanath et al. found that even users who recognize a potential threat may not respond deliberately: urgency cues in phishing emails tend to trigger heuristic, impulsive processing rather than careful evaluation [8]. Together, these studies suggest that effective security communications must account for both users' prior beliefs about their own vulnerability and the cognitive conditions under which they encounter threats.

We explored how Take9's consequences framing might motivate people to follow security advice and compared it to the **Take5** campaign, which has a similar message to pause (for 5 seconds instead of 9). Instead of the narrative structure, Take5 shows advice with bullet points, such as to type links into your browser instead of clicking on them [4].

Despite its reach, Take9 has attracted criticism. Schneier and Vishwanath argue that the campaign instructs users to pause but provides no guidance on what to do during that pause, leaving users without the cognitive scaffolding needed to evaluate whether an email is genuinely suspicious [6].

We present the first empirical evaluation of the Take9 campaign. Our research questions are as follows:

- RQ1: What security advice do participants take away from each video?
- RQ2: After watching the video, do participants believe that: A) Their actions online can negatively impact others beyond themselves? B) They should pause and act on the security advice shown in the video? C) A situation similar to the one depicted could happen to them?
- RQ3: Do participants improve their ability to identify phishing emails after watching the video?

2 Methods

We conducted an online between-subjects survey study with 45 U.S. adults recruited through Prolific. Quota sampling ensured balanced representation across five age brackets (18–29 through 60+), gender, and programming experience. Participants completed a phishing email identification task before and after watching one of three randomly assigned video conditions: the 30-second Take9 video ($n = 14$), the 80-second Take9 video ($n = 15$), or the 55-second Take Five video

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

($n = 16$) [1,2,4]. Participants were paid $5 for participation in the 20 minute study.

Each phishing task showed four email screenshots in random order: one phishing attachment, one phishing link, one legitimate attachment, and one legitimate link. Participants classified each as a scam, legitimate, or uncertain and explained their answer. Open-ended questions after the videos captured participants' primary takeaways and self-reported behavioral changes. Email cues were coded using the NIST Phish Scale [3] as an a priori codebook; takeaway and behavioral change responses were coded inductively. Within-condition pre-to-post comparisons used the Wilcoxon signed-rank test; between-condition comparisons used Kruskal-Wallis.

Ethical considerations: The risks associated with this study were minimal: links and attachments were presented in a non-clickable screenshot format, and no identifying information beyond Prolific IDs was collected. Participants provided their consent to participate. This study was determined exempt by the CMU IRB as a benign behavioral intervention with no greater than minimal risk.

3 Results

3.1 Participant Takeaways and Beliefs

3.1.1 RQ1: Security Advice from Videos

We performed qualitative coding on responses to *What were your main takeaways from this video?* "Pause before acting" was the most common code: 25/29 participants for Take9 and 7/16 for Take5. The next most common codes for Take9 were "Scrutinize email details" and "Harm can spread beyond the individual," with 9 and 4 participants. 4 participants in the Take5 condition said "Avoid clicking links; type URLs manually," and the rest of the advice was mentioned by 3 or fewer participants.

3.1.2 RQ2: Participant Beliefs After Videos

A. Their actions online can negatively impact others beyond themselves? We asked: *If you clicked the link on a phishing email, do you think there would be any consequences? If so, on what levels? (Select all that apply)* All participants selected "personal." The second most popular option was "organization (like school or work)" (Take9: 20/29 and Take5: 7/16), followed by community (13/29 Take9). Only a few participants in each condition selected "state" or "country."

B. They should pause and act on the security advice shown in the video? Although 32 participants said the video advised to "Pause before acting," when asked what they did differently in the post-video phishing task only 2 participants mentioned pausing. The most common reported behavioral change was increased scrutiny of specific email elements—checking sender addresses, inspecting link URLs, and noting urgency cues—mentioned by about a third of participants across all conditions. In addition, from the timing data it does not appear that people paused more in the post task than the pre task.

C. A situation similar to the one depicted could happen to them? While the majority of participants said the scenario could happen to them or someone they know (Take9 83%, Take5 75%), only about half related to the character in the video (Take9 48%, Take5 44%).

3.2 Phishing Detection Accuracy

Overall we did not see much of a change in phishing detection accuracy before and after watching any of the videos. The mean percent correct pre and post for Take9 short was 73% and 70%, for Take9 long 63% and 58%, and for Take5 64% and 66%, with no statistically significant change in correct scores from pre to post task. Although the number of uncertain ("I don't know") responses nearly doubled across all conditions post-video, from 5.6% to 12.8% of all responses, this was also not statistically significant. At $n = 14$–16 per condition, the study is underpowered for small effects; therefore, the absence of significance should be interpreted with caution rather than as evidence of no impact.

4 Discussion

Take9's consequences narrative appears to have landed: more Take9 participants than Take5 participants believed phishing consequences extend beyond the personal level. However, we have limited evidence of the campaign's behavioral message being implemented. Most participants cited pausing as a takeaway, but few did so during the post-video phishing task, and we found no improvement in detection accuracy. These findings are consistent with the critique that Take9 tells users to pause without specifying what to do during that pause [6], and with Marshall et al.'s characterization of low-intensity, no-practice interventions as the least effective tier of anti-phishing training [5].

Future work should increase the sample size to detect smaller effects, if present, improve ecological validity through realistic simulated workflows, and test whether adding cue-specific instruction to Take9's narrative framing produces measurably better outcomes.

5 Acknowledgments

This material is based upon work supported by the National Science Foundation Graduate Research Fellowship Program under Grant No. DGE2140739. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

References

[1] Take 9. Pause take9, 2024. URL: https://www.youtube.com/watch?v=GlmplblxsGM.

[2] Take 9. Take9 - pause for 9 seconds to stay safe online, November 2024. URL: https://www.youtube.com/watch?v=Oe-hQRkKPlE.

[3] Shanee Dawkins and Jody Jacobs. NIST Phish Scale user guide. Technical Report NIST TN 2276, National Institute of Standards and Technology (U.S.), Gaithersburg, MD, November 2023. URL: https://nvlpubs.nist.gov/nistpubs/TechnicalNotes/NIST.TN.2276.pdf, doi:10.6028/NIST.TN.2276.

[4] U. K. Finance. Type don't tap - take five to stop fraud, October 2025. URL: https://vimeo.com/1128219562.

[5] Nina Marshall, Daniel Sturman, and Jaime C. Auton. Exploring the evidence for email phishing training: a scoping review. *Computers & Security*, 139:103695, April 2024. doi:10.1016/j.cose.2023.103695.

[6] Bruce Schneier and Arun Vishwanath. Why Take9 won't improve cybersecurity. Dark Reading, May 2025. URL: https://www.darkreading.com/cybersecurity-operations/why-take9-will-not-improve-cybersecurity.

[7] Shorty Awards. Take9 cybersecurity campaign. 10th Annual Shorty Impact Awards, 2025. URL: https://shortyawards.com/10th-impact/take9-cybersecurity-campaign.

[8] Arun Vishwanath, Tejaswini Herath, Rui Chen, Jingguo Wang, and H. Raghav Rao. Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. *Decision Support Systems*, 51(3):576–586, June 2011. doi:10.1016/j.dss.2011.03.002.

[9] Rick Wash. Folk models of home computer security. In *Proceedings of the Sixth Symposium on Usable Privacy and Security (SOUPS '10)*, pages 1–16, New York, NY, USA, July 2010. Association for Computing Machinery. doi:10.1145/1837110.1837125.

A Additional Acknowledgments

Steven Deng helped implement the survey on Qualtrics and the with project. Thank you to our friends, family, and CyLab Usable Privacy and Security lab members who gave feedback on the surveys and piloted the phishing emails. Thank you Mandy Lanyon for supporting us with the IRB process.

B Survey Instrument

Study: Internet Use Survey Study
Institution: Carnegie Mellon University
Researchers: Ginger Smith, Michael Stoneman, Risa Yoshida, and Steven Deng
Contact: gasmith@andrew.cmu.edu
Platform: Prolific (online panel)
Estimated Time: 20 minutes **Compensation:** $5.00
Eligibility: 18 years or older, currently residing in the United States
SPARCS Study Number: STUDY2026_00000114

Section 1: Consent Form

We are inviting you to take part in a research study conducted by Ginger Smith, Michael Stoneman, Risa Yoshida, and Steven Deng at Carnegie Mellon University. Participation in this study is voluntary. If you choose to take part, you will watch a brief video with sound or closed captions on, and complete an online survey that will help us learn more about your internet use. You qualify if you are 18 or older and currently live in the US. The study (including watching the video) will take about 20 minutes to complete, and should be taken on a computer. You will be compensated $5 for your time through Prolific. You may stop at any time.

Any identifiers collected as part of this survey (i.e., Prolific ID) will be deleted once data analysis is complete. Study data that have been stripped of any information that could identify you (de-identified) may be shared, made public, or used for future research or commercial purposes.

For questions or concerns you can contact the principal investigator Ginger Smith at gasmith@andrew.cmu.edu. This study is fulfilling a course requirement for Usable Privacy and Security; the course instructor is Lorrie Cranor, lorrie@cmu.edu. If you have questions or concerns about your rights as a research participant, you can contact the Carnegie Mellon IRB at (412) 268-4721, IRB-review@andrew.cmu.edu.

You are not allowed to use generative AI tools (such as ChatGPT) to complete this survey or answer questions for you, and you will not be paid if you do so.

Q1. I confirm that: ○ I consent to participate *(required to proceed)*

Section 2: Pre-Video Phishing Task

Note: Participants are shown the following instructions, then 4 email screenshots presented in randomized order (one per page). Each email page includes a page timer. Randomization is implemented via JavaScript embedded in Qualtrics; email images are injected into question slots (`pre_mc_1`–`pre_mc_4`) based on an embedded `preOrder` field assigned at the start of the survey.

Q2. *[Instructional text block — not a response item]*
In this section you will be shown screenshots of 4 emails and asked if you think they are scam emails or legitimate. Emails with links show a mouse hovering over the link, next to the full link. Imagine that you are Gerald Grey who works for Contoso Corp. He travels internationally for work, and uses his email for work purposes like scheduling meetings and personal purposes like getting notifications for online orders. *The following four question sets are each presented on a separate page. Each page consists of an email screenshot, a scam-identification question, an open-ended explanation question, and a hidden page timer.*

pre_mc_1-4. *[Email image displayed]* Email 1/1-4. Imagine that you are Gerald Grey who works for Contoso Corp. He travels internationally for work, and uses his email for work purposes like scheduling meetings and personal purposes like getting notifications for online orders. Do you think this is a scam email?

○ Yes ○ No ○ I don't know

pre_sa_1-4. Please briefly explain why you chose your answer. What specific elements of the email influenced your decision? *[Open-ended text entry]*

Section 3: Experimental Condition (Video)

Note: One of three conditions below is displayed per participant, selected by random block randomization in Qualtrics (even presentation). Each video page includes a hidden page timer enforcing a minimum viewing time before the participant can advance.

Instructions: Please watch the following <#> second video from the <> campaign. Please watch the video with sound or closed captions (cc) on. After watching the video, click the button below to continue.

Condition A — Take9 (30-second video)
https://www.youtube.com/watch?v=Oe-hQRkKPlE

Condition B — Take9 (2-minute video)
https://www.youtube.com/watch?v=GlmplblxsGM

Condition C — Take Five (55-second video) *(Note: The only audio present is background music.)*
https://vimeo.com/1128219562

Section 4: Post-Video Phishing Task

Same as the pre-video phishing task, with the other 4 screenshots.

Section 5: Post-Task Debriefing

Q5.1. Did the video give you any new tools or information to help you identify phishing emails?

○ Yes ○ No ○ I'm not sure

Q5.2. Describe the new tools or information to help you identify phishing emails.

[Open-ended text entry — displayed only if participant answered "Yes" to Q5.1]

Q5.3. Did you do anything different for this set of emails? If so, what and why? *[Open-ended text entry]*

Section 6: Video Reaction & Attention Check

Q6.1ab and Q6.2ab are attention checks for Take9 conditions.

Q6.1ab. Which best describes the video?

- ○ A dance performance to a song called Take 9
- ○ Someone clicks a link in an email which causes a power outage *(correct)*
- ○ A tutorial for how to use a new website that helps manage your email inbox
- ○ A description of how people visually scan information when viewing messages
- ○ A tutorial on how to open and use email attachments on your computer

Q6.2ab. When does the video suggest pausing?

- ○ Before posting on social media
- ○ Before sending email
- ○ Before opening attachments *(correct)*
- ○ Before sending text messages
- ○ Before entering your password

Q6.1c and Q6.2c are attention checks for the Take5 condition.

Q6.1c. Which best describes the video?

- ○ A tutorial on installing security software to prevent cyberattacks
- ○ Encourage people to quickly respond to urgent financial requests
- ○ Advice on how to recognize and prevent fraud by stopping, challenging, and protecting yourself *(correct)*
- ○ Fraud scenarios without any actionable advice
- ○ A step-by-step explanation of the sequence of events leading up to money being stolen from a bank account

Q6.2c. What was NOT mentioned in the video?

- ○ Do not click the link in an email, type it into your search bar instead
- ○ Turn on the alerts in your banking app
- ○ Contact your bank immediately if you notice something suspicious *(correct)*
- ○ If someone's asking for your information or money, you should do what they say immediately
- ○ Treat your one-time passcodes carefully

Q6.3. What were your main takeaways from this video? *[Open-ended text entry]*

Q6.4. Will you change anything about your behavior online after watching this? If yes, what will you do differently? *[Open-ended text entry]*

Q6.5. If you clicked the link on a phishing email, do you think there would be any consequences? If so, on what levels? (Select all that apply)

- ☐ Personal
- ☐ Community
- ☐ Organization (like school or work)
- ☐ State
- ☐ Country
- ☐ Other (please specify): _____
- ☐ No consequences

Q6.6. Have you heard of the Take9 campaign before today?
○ Yes ○ No ○ Not sure

Q6.7. Have you seen videos or content about cybersecurity advice on social media before?
○ Yes ○ No ○ Can't remember

Section 7: Video Reaction — Sentiment

Q7.Likert. Rate the following statements from strongly disagree to strongly agree.

(1 = Strongly Disagree, 2 = Disagree, 3 = Neither Agree nor Disagree, 4 = Agree, 5 = Strongly Agree)

I enjoyed watching the video.
I learned something new from the video.
I would recommend the video to a friend.
I relate to the character in the video.
I would like to watch the video again.
The scenario in the video is something that might happen to me or people I know.
The video offered advice that I plan to use going forward.

Q7.2. How did you find the tone of the video?
○ Too serious ○ Just right ○ Too comical ○ Other

Q7.3. Would you change the length of the video?
○ It should be longer ○ The length is just right ○ It should be shorter

Section 8: Security Knowledge

Note: Knowledge quiz administered across all conditions. Correct and distractor options are marked.

Q8.1. What are things you can do to stay safe online? (Select all that apply)

- ☐ Pause before clicking a link that looks suspicious *(correct)*
- ☐ Use multi-factor authentication *(correct)*
- ☐ Use a unique password for each website where you have an account *(correct)*
- ☐ Use a search engine to go to a website to login, rather than clicking on a link in an email or text *(correct)*
- ☐ Check my accounts regularly and contact providers if I notice anything suspicious *(correct)*
- ☐ Do not share my one-time passcodes or PIN with anyone *(correct)*
- ☐ Reuse passwords for accounts that you don't care about that much *(distractor)*
- ☐ Visit websites that start with `http`, not `https` *(distractor)*
- ☐ Turn off all app notifications because they could be scam messages *(distractor)*

Section 9: Security Experience and Opinions

Q9.1. As far as you know, have you ever… (Select all that apply)

- ☐ Had important personal information stolen (SSN, credit card, bank info)?
- ☐ Had inaccurate information show up in your credit report?
- ☐ Had an email or social networking account compromised?
- ☐ Been the victim of an online scam and lost money?
- ☐ Experienced persistent and unwanted contact from someone online?
- ☐ Lost a job or educational opportunity because of something posted online?
- ☐ None of the above

Q9.2. Who have you asked—or where have you gotten advice—about how to protect your personal information online? (Select all that apply)

- ☐ Friend or Peer
- ☐ Family Member
- ☐ Coworker
- ☐ Librarian or resource at library
- ☐ Government website
- ☐ Website run by a private organization
- ☐ Teacher
- ☐ Social media
- ☐ I have never sought advice on this topic

Q9.3. Do you feel as though you already know enough about avoiding phishing scams?
○ Already know enough ○ Would like to learn more ○ Not sure

Q9.4. Who do you think is most vulnerable or most targeted for online scams or phishing? *[Open-ended text entry]*

Section 10: Demographics

Note: Age, gender, race, and ethnicity are collected by Prolific.

Q10.2. Do you have a degree or employment in computer science or a related field?
○ Yes ○ No

Q10.3. Have you ever received formal training on how to identify phishing or other online scams (e.g., through an employer, school, or online course)?

○ Yes ○ No ○ Not sure

End of Survey

Participants are redirected back to Prolific with their completion code upon submitting the final page.

Phishing Email Stimuli

Participants were shown screenshots of emails. Links in screenshots appear in blue but are not clickable. Phishing email stimuli were drawn from recently identified phishing sites catalogued by PhishTank (https://www.phishtank.com), with body text drafted internally by the research team. Legitimate email samples were drawn from actual emails received by team members with personally identifiable information masked. All emails are framed through the "Gerald Grey" persona (a Contoso Corp. employee who uses email for both work scheduling and personal online-order notifications).

Both the pre- and post-video sets consist of 4 emails each, presented in a randomized order determined per-participant. Emails contained an attachment (A) or link (L), and were phishing (P) or legitimate (L). Table 1 summarizes the eight stimuli.

Filename	Type	Vector
AL1	Legitimate	Attachment
AL2	Legitimate	Attachment
AP1	Phishing	Attachment
AP2	Phishing	Attachment
LL1	Legitimate	Link
LL2	Legitimate	Link
LP1	Phishing	Link
LP2	Phishing	Link

Table 1: Phishing email stimuli used in the pre- and post-video tasks.

Email Stimuli Screenshots

Note: Four emails are drawn from this pool for each task (pre- and post-video) and presented to participants in a randomized order determined per-participant at runtime.

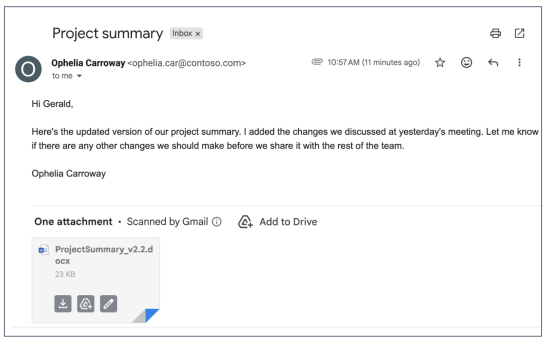

Figure 1: Legitimate, attachment-based email 1 (AL1)

Figure 2: Legitimate, attachment-based email 2 (AL2)

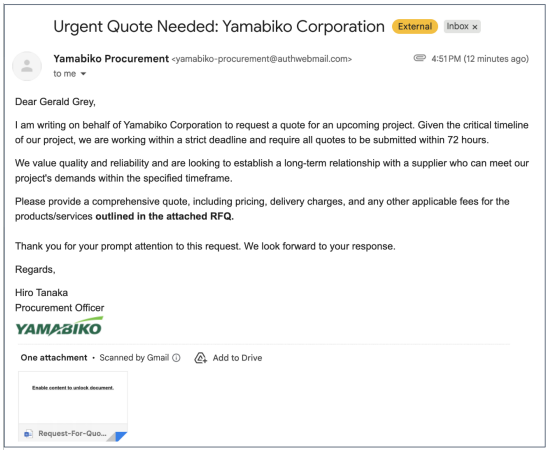

Figure 3: Phishing, attachment-based email 1 (AP1)

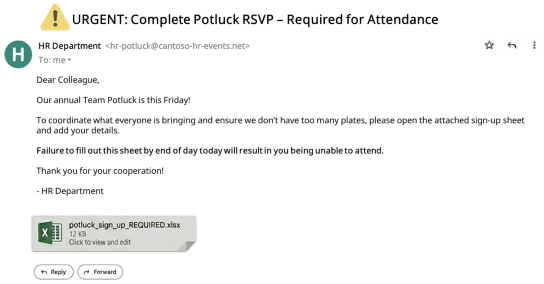

Figure 4: Phishing, attachment-based email 2 (AP2)

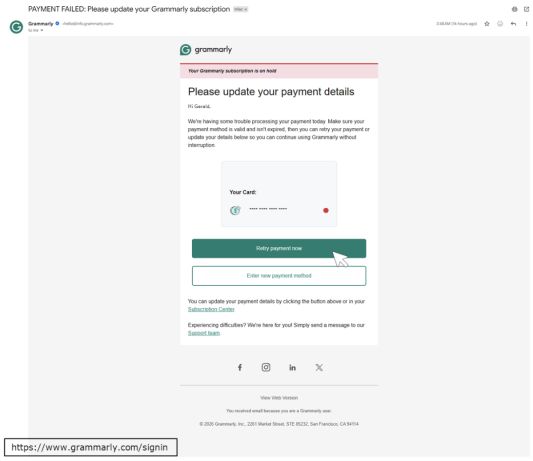

Figure 5: Legitimate, link-based email 1 (LL1)

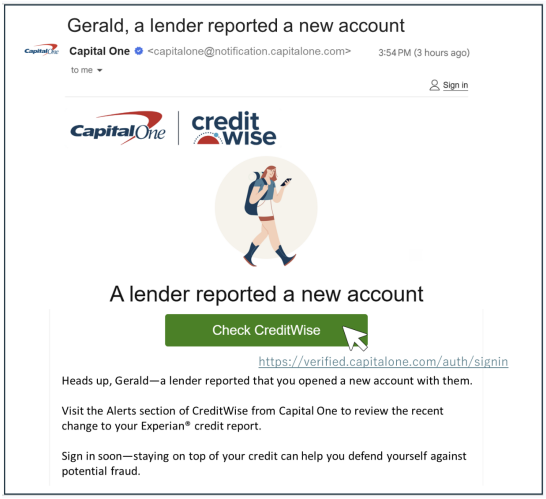

Figure 6: Legitimate, link-based email 2 (LL2)

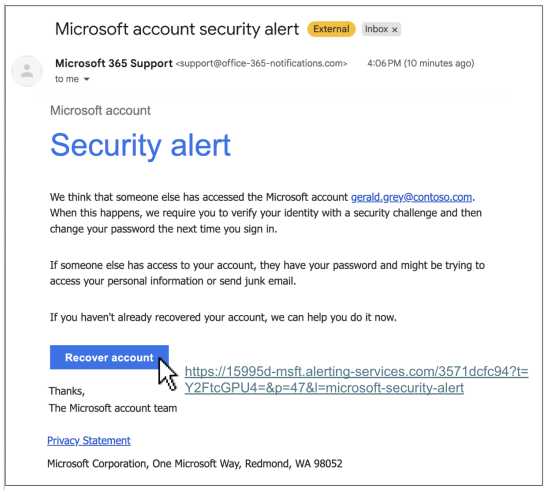

Figure 7: Phishing, link-based email 1 (LP1)

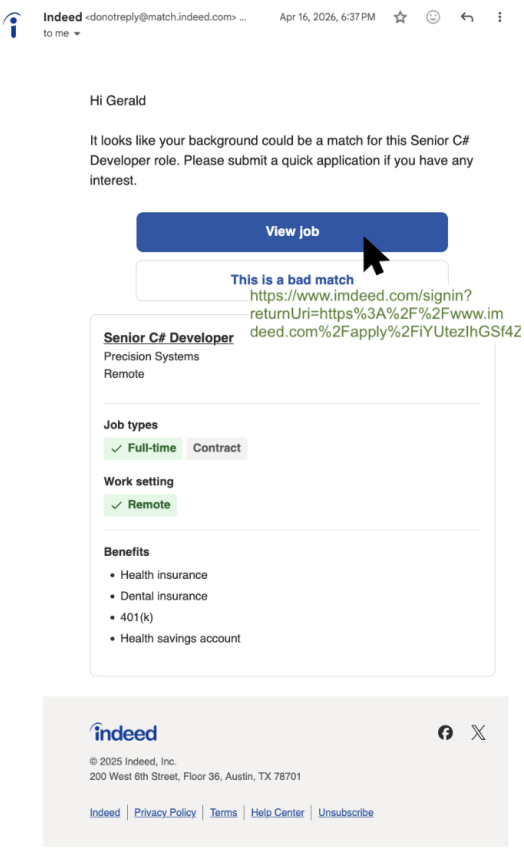

Figure 8: Phishing, link-based email 2 (LP2)

C Data and Statistical Tests

C.1 Demographics

We used Prolific's quota sampling for age (18–29, 30–39, 40–49, 50–59, and 60+), men and women, and people with and without programming experience. We required a prior approval rate of 95%.

	Take9 short n = 14	**Take9 long** n = 15	**Take Five** n = 16
Male	57%	53%	56%
Female	43%	47%	44%
Average age	42 years	44 years	47 years
Programming experience	57%	53%	44%
CS degree or job	50%	13%	31%
Formal phishing training	50%	40%	50%

Table 2: Participant demographics in each condition.

C.2 RQ1

Table 3 contains the counts of codes from the open-ended takeaways from the videos, discussed in section 3.1.1.

Code	**Take9 short**	**Take9 long**	**Take Five**	**Total count** n= 45
Pause before acting	12	13	7	32
Scrutinize email details	5	4	1	10
Harm can spread beyond the individual	2	2	0	4
Scams can be sophisticated; anyone is a target	1	2	3	6
Avoid clicking links; type URLs manually	1	1	4	6
Verify w/IT or sender	0	1	0	1
Monitor accounts regularly	0	0	2	2
Too vague to code	1	1	4	6

Table 3: Frequency of codes for main takeaways from the video.

C.3 RQ2

Table 4 contains data for consequences of clicking a phishing link (select all), discussed in section 3.1.2.

Table 5 contains data for what participants said they did differently in the post-video phishing task, discussed in section 3.1.2.

Level	**Take9 short**		**Take9 long**		**Take Five**	
Personal	14	(1.000)	15	(1.000)	16	(1.000)
Organization	10	(0.714)	10	(0.667)	7	(0.438)
Community	7	(0.500)	6	(0.400)	1	(0.063)
State	2	(0.143)	1	(0.067)	1	(0.063)
Country	3	(0.214)	1	(0.067)	1	(0.063)
Other	0	(0.000)	0	0.000	1	0.063

Table 4: Number participants who selected each level of phishing link consequences, proportion is in parentheses.

Code	**Count**
Pause before acting	2
Scrutinize email details	17
Avoid clicking links; type URLs manually	1
Scams can be sophisticated; anyone is a target	1
Too vague or incomplete to code	2
No change	26
Yes, change reported	3
More cautious or suspicious	3
Used skills they already had	1
Learned at work	1
Context matters	2

Table 5: Self-reported behavioral changes during the post-video phishing task.

C.4 Statistics for RQ3

Comparing within conditions

From running the Wilcoxon signed rank test, no condition showed a statistically significant change in correct scores from pre to post task. Take9 short n=14, V = 18, p-value = 0.6078. Take9 long n=15, V = 35, p-value = 0.7731. Take5 n=16, V = 34.5, p-value = 0.9277.

From running the Wilcoxon signed rank test no condition showed a statistically significant change in not sure scores from pre to post task. Take9 short n=14, V = 10, p-value = 0.08897. Take9 long n=15, V = 8, p-value = 0.3447. Take5 n=16, V = 16, p-value = 0.2795.

Comparing across conditions

Scores across video conditions: Based on Kruskal-Wallis chi-squared = 0.1068, df = 2, p-value = 0.948 we fail to reject the null hypothesis, so there does not seem to be a statistically significant difference in change in scores across video conditions.

Not sures across video conditions: Kruskal-Wallis chi-squared = 0.56243, df = 2, p-value = 0.7549.