## Supporting Information

### Participants

Participants were employees of the University of California, Irvine (UCI), including faculty, staff, and student employees. Data from students who are not employed by UCI were not collected, as the university's Office of Information Technology does not routinely survey student compliance with cybersecurity guidelines. In total, data from 14,106 participants were collected ($N$ = 7,059 collected over the week of March 2nd, 2026; $N$ = 7,047 collected over the week of March 9th, 2026). The protocol was deemed exempt from approval by the Institutional Review Board at UCI (protocol #00000544). The data was anonymized by members of the Office of Information Technology at the UCI prior to being transferred to the authors, and no demographic information was collected.

### Materials

A simulated spam email was sent to all participants. The language included in the email was meant to lead the recipient to believe it was sent by a system administrator and to click the included link. The email was sent as part of university-wide campaign, intended to enhance and test vigilance. The previous campaign at UCI was run between November 10th and 21st, 2025 and included ~12,300 participants. A different simulated attack is used for each campaign. The full text of the email used for this experiment is available upon request. It is not included here so it cannot be used in real-life cyber-attacks against our university in the future.

### Procedure

Participants were pseudo-randomly assigned to two groups, equalizing the number of participants in each academic unit across groups. Participant were blinded to the procedure and did not expect receiving the simulated spam email. All participants received the same email on Monday between 9:00 am and 10:00 am Pacific Time. The experimental manipulation revolved around the date when the email was sent. The state of California transitioned to DST on Sunday, March 8th, at 2 am. The control group (CTRL, $N$ = 7,059) received the email on March 2nd, 2026, the Monday before the transition to Daylight Saving Time (DST). The DST group ($N$ = 7,047) received the email on March 9th, 2026, the Monday immediately after the transition to DST. Although I did not measure changes in sleep duration directly, the dates were chosen to be in close proximity to avoid any confounding factors. Responses to the email were monitored throughout the week, up until Friday (March 6th/13th) at 5:00 pm Pacific Time. However, only responses recorded up until 4:00 am on Tuesday morning were analyzed, as pre-registered ($N$ = 13,915 total; $N$ = 6,970 in the CTRL group; $N$ = 6,945 in the DST group).

### Data and Analysis

Upon receiving the emails, participants' responses could have included opening the email, reporting it as spam, clicking the link, and (if clicked) acknowledging having clicked it. The anonymized dataset available for analysis consisted of 14,106 individual records, including the date and time of all responses (when applicable), as well as each participant's academic unit. Analysis methods for all types of responses are detailed below.

Email openings were monitored in two ways. Each email included an invisible image marked as a "tracking pixel". Opening the email in most browsers and software would automatically lead to the presentation of this image. Access to the URL for this image served was therefore used as a marker that the email had been opened and provided the timestamp for most email openings. However, some email software does not load images, leading to false negatives (i.e., undetected openings). The second method for monitoring email opening was therefore used only when the link embedded in it was clicked. If an email was marked as opened based on a click, the opening date and time were set as the click date and time.

Clicking the suspicious link led to a webpage informing the participant that they fell prey to a simulated phishing attack. The date and time of the initial click were recorded. Some malwares preemptively open the links of all received emails, potentially leading to false positives (i.e., emails marked as clicked despite not having been clicked by a human participant). To avoid including these false positives in the analysis, I designed and pre-registered a procedure to mark them and omit them from analysis. If the same IP address appeared for three or more users, any click related to that IP address was considered a false positive. Similarly, if the same domain name appeared for the repeated IP addresses and a different IP address, all entries under this domain name were considered false positives as well. In total, 19.38% of the emails sent out were marked as false positives (19.37% in the CTRL group, 19.4% in the DST group). After removing these participants, the sample size was $N$ = 5,620 for the CTRL group and $N$ = 5,598 for the DST group. There was no difference in the portion of participants marked as false positives across groups ($\chi^2$ = 0.002, $p$ = 0.97). This sample was used for all analyses, unless stated otherwise. Note that this procedure was pre-registered before data collection began. For completeness, the main analysis on click probabilities was run on the full sample, including emails marked as false positives (which were all clicked regardless of group and therefore diluted any group differences). This analysis still showed significantly more clicks in the DST group, providing evidence for the robustness of the effect (total $N$ = 13,915; $\chi^2$ = 4.25, $p$ < 0.05; CTRL = 31.99%, DST = 33.64%; OR = 1.08, 95% CI=[1.004,1.16]; RR = 1.05, 95% CI=[1.002,1.103]).

At the bottom of the webpage at which participants arrived after clicking the link, there was an acknowledgment button, which participants were asked (but not required) to click. The date and time of acknowledgments were recorded.

UCI employees are encouraged to report spam email to the Office of Information Technology by forwarding it to one of two email addresses (spam@uci.edu or security@uci.edu). These reports, along with their dates and times, were collected for all reports.

All statistical analyses were done using MATLAB 2022b (Mathworks Inc, Massachusetts). Most analyses used $\chi^2$ tests. Odd ratios were estimated using Fisher's Exact Test. Additional analyses included a mixed-effects logistic model, which accounted for the random effect of academic units. An additional paired two-sided Wilcoxon signed rank test was used to compare across academic units. Only academic units with at least $N$ = 75 participants per group were included in this analysis (22 of 27 academic units; the omitted units had an average of 7, 12.5, 13.5, 18, and 48.5 participants per group). The included units had a range of 78.5-1,078.5 participants per group on average. All α levels were set at 0.05.

All anonymized data is shared in their raw form at osf.io/5vjxq.