The Role of Auditory Environments and Anxiety in Detecting Phishing Emails

Reza Ghaiumy Anaraky
School of Electrical Engineering and Computer Science
Louisiana State University
Baton Rouge, Louisiana, USA
rganaraky@lsu.edu

Mark Cartwright
New Jersey Institute of Technology
Newark, New Jersey, USA
mc232@njit.edu

Oded Nov
Tandon School of Engineering
New York University
New York, New York, USA
onov@nyu.edu

Abstract

This work explores the effects of auditory environments and anxiety on users' ability to identify phishing emails. In an experimental in-person study, sixty participants evaluated twelve different phishing and legitimate emails while immersed in four different auditory environments (silence, lecture, ambient street noise, concert), at low or high playback (i.e., volume) levels. Using a path model, we found that (1) all non-silent auditory environments induced some level of anxiety, reducing participants' ability to correctly identify phishing emails, and (2) low (vs. high) playback level of ambient noise led to lower levels of anxiety and, in turn, higher accuracy in identifying phishing emails. These findings highlight the importance of auditory environments in managing anxiety for improving phishing detection capabilities. We discuss the theoretical and practical implications of this work.

CCS Concepts

• **Security and privacy** → **Usability in security and privacy**; • **Human-centered computing** → *HCI theory, concepts and models*; *Empirical studies in HCI*.

Keywords

Phishing detection, anxiety, environmental noise, auditory environment, decision-making

ACM Reference Format:
Reza Ghaiumy Anaraky, Mark Cartwright, and Oded Nov. 2025. The Role of Auditory Environments and Anxiety in Detecting Phishing Emails. In *Extended Abstracts of the CHI Conference on Human Factors in Computing Systems (CHI EA '25), April 26–May 01, 2025, Yokohama, Japan.* ACM, New York, NY, USA, 10 pages. https://doi.org/10.1145/3706599.3720272

1 Introduction

Phishing is one of the most prevalent forms of cybercrime, where attackers use deceptive messages to obtain the victims' personal information or access. One of the most common types of phishing attacks is phishing emails that are designed to steal the recipient's personal information and subject their victims to financial risks. In 2022, cybercriminals were able to steal over $44 million through phishing emails [1]. In 2023, there were 300,000 phishing victims in the US, which has increased more than ten times since 2018 [2].

When using smartphones, people are susceptible to receiving phishing emails anywhere, from a quiet library to a noisy street. The context in which individuals evaluate potential phishing content is important since it may affect the individual's cognitive capacity to detect such content [26, 52, 60]. In this work, we study how various auditory environments directly and indirectly affect users' security decisions. An auditory environment can directly affect decisions by inducing a cognitive burden [60] or can indirectly affect decisions through other means. Anxiety is one of the factors that reduces users' ability to identify phishing content [3, 25]. However, previous research has not explored the potential indirect effects of users' auditory environments on their security decisions through mitigation or exacerbation of their anxiety levels. In this work, we evaluate the effects of the auditory environment on individuals' anxiety and, in turn, their ability to identify phishing content.

RQ: *Does users' auditory environment influence their susceptibility to phishing attacks by affecting their level of anxiety?*

To study the effects of auditory environments on phishing detection, we designed a within-subject experiment where participants classified 12 emails as phishing or legitimate. While evaluating the emails, participants used noise-canceling headsets provided by the researchers that exposed them to one of two auditory environment types: a *silent* auditory environment or *non-silent* auditory environment including concert, lecture, and street traffic) in either *high or low playback levels* (randomly assigned). Our results show that a silent environment leads to a lower level of anxiety than any non-silent environment, which, in turn, increases participants' accuracy in identifying phishing emails, making them less susceptible to such attacks. Additionally, a low (vs. high) playback level of ambient noise leads to lower levels of anxiety and, in turn, higher accuracy in identifying phishing content.

This paper makes theoretical and practical contributions. To our knowledge, this is the first study that explores the effects of auditory environments on security decisions through anxiety. Theoretically, we contribute to the literature by showing that the effect of the auditory environment on decision-making is mediated by anxiety. Practically, our findings advocate for a holistic approach to cybersecurity, where, in addition to technical solutions such as machine learning for phishing detection, contextual factors such as auditory environment are considered to provide more supportive decision-making environments for users.

CHI EA '25, Yokohama, Japan

ACM ISBN 979-8-4007-1395-8/25/04
https://doi.org/10.1145/3706599.3720272

2 Literature Review and Hypotheses Development

This work lies at the intersection of cybersecurity, soundscape studies, and cognitive psychology. In the following, we review the literature on phishing. We then discuss prior work on the effects of auditory environments on human decision-making and anxiety, considering the cognitive burdens that auditory environments impose on decision-makers.

2.1 Phishing Attacks and the Need for Human-Centered Approaches in Combating Them

In phishing attacks, an attacker uses various techniques to obtain the victim's personal information. For example, an attacker may impersonate a trusted source (e.g., a familiar person or a reputable company—email spoofing) and ask for sensitive information, such as login credentials or financial data. Alternatively, the attacker may redirect the victim to a fraudulent website where the victim discloses their sensitive information[13, 42]. Phishing attacks are on the rise, and phishing content keeps victimizing users: phishing attacks increased by 61% in the six months ending October 2022 compared to the previous year [55]. With a phishing attack occurring every eleven seconds, an estimated 33 million records were extorted before 2023 [18].

Security researchers developed many tools that can automatically detect phishing content. However, these tools have shortcomings [20, 39, 41]. Quang et al. [20] conduct a systematic literature review to evaluate modern deep learning approaches in phishing detection. After studying 81 papers, they concluded that modern phishing detection techniques fall short in performance accuracy and have common issues such as manual parameter-tuning, long training time, and deficient detection accuracy. The shortcomings of technical solutions highlight the role of human factors in this domain and the need to understand how to help users not fall prey to phishing content.

Phishing emails can be difficult for users to detect as they vary in their level of sophistication [17, 40, 47]. For example, an attacker may increase their phishing efficacy by various techniques, such as calling for immediate action that triggers some sense of urgency, leading a recipient to disclose information [47]. As another example, a phishing email can claim to represent the United States Postal Service (USPS) and invite users to click on a non-legitimate URL (e.g., WWW.abcdef.com/324591). However, a more sophisticated attack could embed this non-legitimate URL in USPS's legitimate URL of "www.usps.com," making victims believe they would be redirected to the legitimate website. Such emails that are more difficult to identify can be more effective in victimizing people, leading to the following hypothesis:

H1: Emails with higher identification difficulty lead to lower identification accuracy.

To make phishing detection easier, most human-centered anti-phishing attempts focus on increasing users' awareness about attacks via education [8, 12, 17, 28]. For example, Weaver et al. [57] designed a phishing training program and conducted a between-subject study, where half of the participants interacted with the training program and the other half interacted with a control filler task. Their results show that those who viewed the training materials were more likely to correctly distinguish legitimate emails from phishing emails. However, research also shows that the effect of education wears off over time so that there is no significant difference in identifying phishing content six months after education and training [11, 43]. Additionally, scholars have started to point out various hidden costs associated with training and education [14, 30, 56]. For example, Brunken et al. [14] studied six stakeholders involved in a phishing training campaign in a large European corporation over a period of five months and estimated the in-person hours cost of training to be € 50,000 across all stakeholders.

Despite such shortcomings and extant research on phishing mitigation through education, there has been little research on the effects of users' environment and anxiety levels on phishing susceptibility. Both anxiety and environment can affect decision-making and task performance. In the following, we highlight the role of anxiety in phishing susceptibility. We then explore the effects of the users' auditory environment on their anxiety and decision-making.

2.2 The Role of Anxiety in Phishing Susceptibility

Anxiety is a feeling of worry and uneasiness and is one of the major human factor variables that affect decision-making and task performance [25]. Anxiety triggers worriedness, impairing performance in tasks with high attentional or short-term memory demands [27, 32, 33, 46]. Additionally, studies show a positive association between anxiety and task difficulty [5, 49]. For example, Spielberger et al. [49] studied computer-assisted learning among 29 students and found that difficult learning materials peak anxiety. Wu et al. [59] studied writing performance among English major students in China and found that more complex writing tasks elevate writing anxiety among students. In line with these findings, we pose the following hypotheses:

H2: A higher anxiety leads to lower phishing email identification accuracy.

H3: Emails with greater identification difficulty lead to higher levels of anxiety.

Furthermore, anxiety is more likely to effectively impair performance in more difficult tasks [24]. For example, Spielberger et al. [49] found that individuals with high anxiety make more errors in difficult tasks, suggesting an interaction effect between anxiety and task difficulty on performance. Therefore, we hypothesize that the performance-impairing effects of anxiety are larger for more difficult tasks.

H4: The effect of anxiety on identification accuracy is stronger for more difficult emails.

2.3 Cognitive Effects of Noise

Prior research has shown that, similarly to anxiety, environmental noise hinders cognitive performance on tasks that require attention [10, 15, 44, 52, 58, 60]. For example, Cassidy et al. [16] studied the effects of auditory environments, such as classroom and library noises and silent environments, on word recall tasks. They found that a silent environment leads to recalling more words than a non-silent environment. In addition to the cognitive impairing

effects of noise, studies highlight the role of playback level and report more severe cognitive impairing effects for louder noises [19, 48]. For example, noises with high playback levels impair driving performance more so than noises with lower playback levels [19]. In line with these findings, we hypothesize similar cognitive impairing effects for noise and high playback levels:

H5: Users' ability to correctly identify phishing and legitimate emails is higher in silent environments than in any non-silent auditory environments.

H6: Users' ability to correctly identify phishing and legitimate emails is stronger in auditory environments with low playback levels than in those with high playback levels.

Evidence suggests that noise adversely affects cognitive performance by inducing anxiety (e.g., though arousing the central nervous system [15]). For example, Edsell [21] conducted a study by exposing students to different levels of white noise. They showed that the environment with high noise levels (61-75 dB) induces higher anxiety levels than the environment with low noise levels (50 dB). These results were subsequently confirmed and strengthened in other studies [9, 31, 50]. Therefore, we hypothesize the following:

H7: Silent auditory environments induce lower anxiety levels than non-silent auditory environments.

H8: Auditory environments with high playback levels induce greater anxiety than those with low playback levels.

Figure 1 summarizes our hypothesized model.

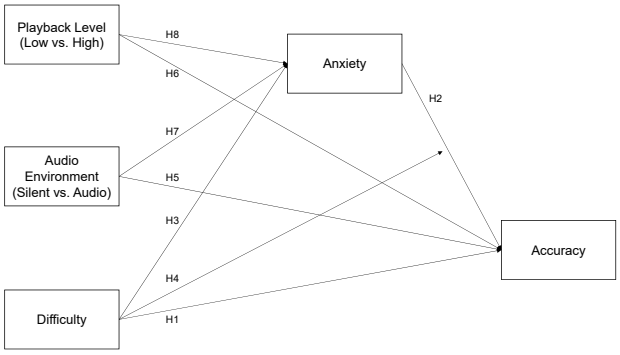


Figure 1: Hypothesized model.

3 Research Methods

3.1 Experimental Design

To study the effects of the auditory environment on users' ability to distinguish legitimate emails from phishing emails, we designed an in-person, within-subject experiment where users had to evaluate emails while randomly exposed to various auditory environments. Our auditory environments included silent (as the baseline), concert[1], lecture[2], and street traffic[3] sounds.

The study was approved by our university's institutional review board (IRB). It took place in person, and we used Qualtrics [4] to present the emails, administer the audio files, and collect users' responses. After giving consent to participate in the study, participants were given a set of noise-cancelling headphones. In order to protect participants' health, we have sanitized and cleaned these headphones before handing them over. Then, participants evaluated a total of twelve emails, five legitimate and seven phishing. The distribution of emails is in line with similar past work [29, 57]. These emails were presented in random order. From our four audio files, one random file was played with each email. We controlled the audio files so that every participant listened to each of the four audio files three times. Furthermore, we randomly set the playback level of each audio file as low or high. These low and high playback levels were chosen based on the literature [21], so that a low noise level is around 50 dB and a high noise level is 61-75 dB. The average dBs for low and high playback for concert, lecture, and street traffic environments were 46/65, 48/64, and 47/71 dBs, respectively. After evaluating each email, participant self-reported their anxiety levels and then had to wait for 15 seconds before proceeding to the next email. The audio files were played only during the email evaluation task and not when responding to questions or during the 15-second wait. Upon finishing the survey, participants received a $5 Amazon gift card.

The emails used in this study were designed based on guidelines and examples used in previous research [37, 47]. The authors discussed these emails in several meetings and iteratively made improvements. The goal was to include emails with varying levels of phishing identification difficulty. The criterion for the level of difficulty was based on the subtlety of cues known to be common in phishing emails [40, 47]. For example, phishing emails may include offers that are too good to be true (e.g., a free ticket to Hawaii), induce a sense of urgency (e.g., act by the end of the day), and involve non-legitimate URLs (e.g., xyzrandomurl.com). Ultimately, the sender's email domain is visible, serving as a key indicator of legitimacy. Two independent privacy and security researchers rated the emails' difficulty levels from 1 to 5 and met together to agree on a score for each email. We used this score as a categorical variable in our analyses. The emails' fonts were Gmail's default fonts, and the layout was designed to mimic Gmail's environment. Figure 3 and Figure 4 show screenshots of the emails.

3.2 Measurement Instruments

3.2.1 Dependent Variables. After reading each email, participants used a radio button to report whether they believed the email was legitimate or phishing. In the analysis, we used this response to measure the accuracy of participants' responses, with one suggesting that they correctly identified a phishing or legitimate email

[1]The source was a trimmed 1-minute long audio from https://youtu.be/1T6utlXm6dM?si=UcPN1k6oByrJQcnQ&t=54. For any audio file, if participants were still reading the email after one minute, the audio replayed from the beginning.
[2]The source was a trimmed 1-minute long audio from https://youtu.be/lZ3bPUKo5zc?si=Riy6YQMdcQX2hEV5&t=1644
[3]The source was a trimmed 1-minute long audio from https://www.youtube.com/watch?v=ATq9ihuhBO4
[4]https://www.qualtrics.com/

and zero as misclassifying a phishing or legitimate email. Additionally, we measured participants' level of anxiety with a 3-item scale, adopted from the Zsido et al.s' five-item scale [61], to keep the survey shorter since we measured anxiety after each email evaluation. These items had a high internal consistency (see Section 3.3). For these questions, participants reported their agreement with the following statements using a 5-point scale: "I feel jittery," "I feel upset," and "I feel confused." We used a sum score of these items as a measure of anxiety. Therefore, our anxiety score could range from three to 15.

3.2.2 Independent Variables. We used the level of difficulty and experimental manipulations as independent variables. Additionally, we measured proactive awareness [22] as a control for participants' security practices. This construct measures the extent to which individuals are attentive to links and whether they are cautious when they navigate through various URLs (e.g., "When someone sends me a link, I open it without first verifying where it goes."). Since this variable was not significantly associated with any of the dependent variables, we removed it from the analysis.

3.3 Participant recruitment and Data Analysis

We recruited 60 participants in a campus library in the northern United States, including 32 males, 26 females, one non-binary, and one with "other" gender identities. Participants' ages ranged from 18 to 25 years old (Mean = 20.03, SD = 1.99). Eighteen participants had a high school degree, 19 had a bachelor's degree, 18 had a master's degree, and six had an associate degree. Four participants reported using the internet several times a day, while 56 reported using it almost constantly. Additionally, one participant reported checking their email once a week, two reported checking emails several times a week, six checked their emails at least once a day, 33 checked their emails several times a day, and 18 checked their emails almost constantly. All of our participants passed the attention check questions.

We conducted a repeated measure path model to study our hypotheses. We created two orthogonal contrasts of silent vs. any audio and high vs. low playback level. In these analyses, we used a sum-score of anxiety items. Cronbach's alpha for these three items was 0.82, suggesting a high internal consistency [53].

4 Results

4.1 Descriptive Statistics

Out of 720 email classifications, participants correctly classified 549 (76.25%) emails, including 199 legitimate emails and 350 phishing emails. However, they misclassified emails in 171 instances, where 101 legitimate emails were incorrectly identified as phishing and 70 phishing emails were incorrectly identified as legitimate. The average level of anxiety was 7.23 (SD = 2.50) overall, 7.22 (SD = 2.51) for the lecture, 7.38 (SD = 2.46) for the traffic, 7.36 (SD = 2.63) for the concert, and 6.96 (SD = 2.40) for the silent audio environments.

4.2 Hypotheses Testing

We conducted a path model to test the hypotheses. Overall, this model accounted for 29.8% of the variance in accuracy and 1.9% of the variance in anxiety. As we used a robust maximum likelihood estimator and specified accuracy as a categorical dependent variable, the model did not report traditional fit measures. Therefore, in addition to reporting the R-squares as a fit measure, we assessed the model fit by comparing the model with interaction effects against the model without interaction effects and studied fit improvements [38]. The model comparison suggests a significant improvement of fit ($\chi^2(1) = 13.027$, $p < 0.001$). Therefore, we report it in the following.

In line with H1, we found that it was less likely for participants to identify phishing emails that are more difficult to identify. By one standard deviation increase in the difficulty level, identification accuracy decreased by 48.2 percent (OR = 0.518, $p < .001$, **H1 confirmed**). Additionally, we found support for H2, suggesting that by one standard deviation increase in anxiety, identification accuracy decreased by 29.9 percent (OR = 0.701, $p < .001$, **H2 confirmed**). Furthermore, we found support for H3 suggesting that by one standard deviation increase in identification difficulty, individuals experienced more anxiety by 0.065 standard deviations (β = 0.065, $p = .004$, **H3 confirmed**). We also found an interaction effect between difficulty and anxiety predicting accuracy, suggesting that by one standard deviation increase in task difficulty, the effects of anxiety on accuracy increased by 58.5 percent (OR = 1.585, $p < .001$, **H4 confirmed**).

We did not find direct effects of the auditory environment on prediction accuracy. A silent environment did not lead to different prediction accuracy than any audio ($p = .159$, **H5 rejected**). Similarly, an auditory environment with a high playback level (volume) did not lead to different accuracy levels compared to an auditory environment with a low playback level ($p = .467$, **H6 rejected**). However, a silent environment induced less anxiety than any non-silent auditory environment (β = -0.059, $p = .007$, **H7 confirmed**). Similarly, a low playback level induced less anxiety than a high playback level (β = -0.099, $p = .006$, **H8 confirmed**). Table 1 and Figure 2 report the results.

Overall, the indirect effect of the auditory environment (silent vs. non-silent) on accuracy was significant, such that a silent environment led to improved identification accuracy due to mitigating anxiety (β = 0.021, $p = .021$). Similarly, the indirect effect of playback level on identification accuracy was significant such that a low-playback level auditory environment led to higher identification accuracy than a high-playback level auditory environment as it leads to lower anxiety (β = 0.035, $p = .031$). These results suggest that the effects of the auditory environment for both cases of silent vs. non-silent and low vs. high playback levels on accuracy were fully mediated by anxiety.

4.3 Post-hoc Analyses

We conducted an additional exploratory model to study any difference between various auditory environments (lecture, traffic, and concert) with high and low playback levels. We only found an effect of playback level on anxiety, such that higher playback levels lead to higher anxiety levels (β = 0.113, $p = .006$). Lecture, traffic, and concert auditory environments did not have significantly different effects on anxiety levels or accuracy ($ps > .05$). Therefore, we do not report the statistical results for this post hoc test further.

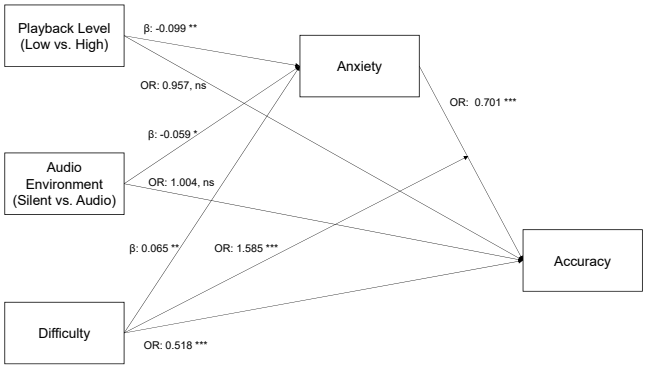


Figure 2: Results of path analyses.

5 Discussion

In this work, we studied the effects of auditory environments on user's anxiety and email phishing susceptibility. Showing the mechanisms through which environmental noise may increase the likelihood of putting users' privacy and security in jeopardy, this work has theoretical and practical contributions.

Our work makes a theoretical contribution by uncovering the mechanisms through which noise can affect performance. Previous research showed that environmental noise can decrease performance [10, 15, 52, 58, 60]. We showed that one of the mechanisms through which noise hinders performance is by elevating anxiety: compared to a silent environment, the mere presence of noise increases individuals' anxiety and, consequently, decreases their ability to identify phishing emails. In our experiment, the performance-impairing effects of lecture, concert, and traffic auditory environments were fully mediated by anxiety. In addition to the presence of noise, we found similar effects for higher playback levels, such that they increase anxiety levels and, hindering phishing detection performance.

Additionally, while the auditory environments that we examined increased anxiety levels and decreased performance, it is possible that more soothing auditory environments can mitigate anxiety and raise performance. For example, in the field of music therapy, studies have shown that music can be effective in relieving anxiety [34]. However, studies measuring the positive effects of soundscapes on physiological responses and cognitive performance were less conclusive [4, 23, 35, 51, 54]. It is possible that some of these discrepancies are due to differences in personal auditory preferences [45]. If so, we can elicit an individual listener's musical preferences to present them with music stimuli that are most effective for them in reducing anxiety. Improving individuals' security decision-making abilities through personalized auditory stimuli would be a novel approach that can complement other methods, such as giving individuals privacy clues [6, 7, 36].

By showing the effects of users' environment on phishing susceptibility, our results underscore the need for a holistic approach to cybersecurity that not only addresses the technical aspects but also the contextual factors surrounding the users. A holistic approach is crucial as research highlights shortcomings in technical solutions [20, 39] and human-centered-base educational attempts [11, 43] in combating phishing threats. Our work opens another avenue in combating such attacks by accounting for contextual factors. This has implications for users, suggesting that they should become aware that their environments can affect their decision-making ability. When users know that environmental parameters such as background music can adversely affect their decision-making, they may decide to boost their performance with less exposure to such parameters. For example, they may not make crucial decisions in noisy or uncomfortable environments and postpone consequential decision-making until they are in a more appropriate environment.

Furthermore, organizations and cybersecurity professionals should acknowledge that the context where employees and users evaluate potential phishing content can significantly affect their phishing susceptibility. Implementing strategies to minimize the adverse effects of the environment may lessen the need for costly intervention campaigns [14]. For example, organizations may consider noise reduction techniques when designing office spaces for their employees. Noise reduction techniques involve using soundproof pods and designing the office space that keeps team members who work with each other closest to help maintain a quiet office environment.

Finally, classification difficulty was one of the strongest predictors of accuracy. Ideally, those more educated about various types of phishing attacks find it less challenging to identify phishing content. Therefore, education should be part of a holistic solution to cybersecurity threats. Since previous research shows that the effects of education wars off over time [11], researchers should keep exploring novel educational methods with more lasting effects, even when users are busy with their daily activities and reluctant to phishing content they may be exposed to.

6 Limitations and Future Work

Our study used a limited set of auditory stimuli, and our sample was limited to college students. Additional experimentation with a more diverse population is needed to see if our findings are generalizable. For example, our sample of college students may not be a representative sample in terms of digital literacy as they interact with emails frequently due to their academic needs, and our results may be different if we study a population with less experience with emails.

Furthermore, future studies should consider more diverse auditory stimuli, such as soothing and relaxing soundtracks, to study the potential anxiety-mitigating effects of such soundtracks. Additionally, future work should try to understand what characteristics of the auditory environment lead to increased anxiety and study the extent to which these effects are universal or if they may depend on the listener and their preferences.

Finally, while we only studied phishing susceptibility, future studies can explore various decision-making contexts and study if the effects of noise on decision-making vary across different decision-making tasks and, if so, what task-specific features may contribute to this difference.

7 Conclusion

Our findings show that auditory environments that elevate anxiety can impair one's ability to protect themselves against phishing attacks. This underscores the importance of factors that go beyond

digital environments to mitigating cybersecurity threats, emphasizing the need for holistic strategies that consider both digital and physical parameters.

References

[1] [n. d.]. *The Latest Phishing Statistics (updated February 2023) | AAG IT Support.* https://aag-it.com/the-latest-phishing-statistics/ Section: Business.

[2] [n. d.]. *Phishing: Number of Victims in the United States.* https://www.statista.com/statistics/1390362/phishing-victim-number-us/ Accessed: May 25, 2024.

[3] Hossein Abroshan, Jan Devos, Geert Poels, and Eric Laermans. 2021. Covid-19 and phishing: Effects of human emotions, behavior, and demographics on the success of phishing attempts during the pandemic. *Ieee Access* 9 (2021), 121916–121929.

[4] Jesper J. Alvarsson, Stefan Wiens, and Mats E. Nilsson. 2010. Stress Recovery during Exposure to Nature Sound and Environmental Noise. *International Journal of Environmental Research and Public Health* 7, 3 (March 2010), 1036–1046. https://doi.org/10.3390/ijerph7031036

[5] Hyejin An and Shaofeng Li. 2024. Anxiety in task-based language teaching. *Individual differences and task-based language teaching* 16 (2024), 52.

[6] Reza Ghaiumy Anaraky, Bart P Knijnenburg, and Marten Risius. 2020. Exacerbating mindless compliance: The danger of justifications during privacy decision making in the context of Facebook applications. *AIS Transactions on Human-Computer Interaction* 12, 2 (2020), 70–95.

[7] Reza Ghaiumy Anaraky, Tahereh Nabizadeh, Bart P Knijnenburg, and Marten Risius. 2018. Reducing default and framing effects in privacy decision-making. (2018).

[8] Nalin Asanka Gamagedara Arachchilage and Melissa Cole. 2011. Design a mobile game for home computer users to prevent from "phishing attacks". In *International conference on information society (i-society 2011)*. IEEE, 485–489.

[9] Aylin Aydın Sayılan, Nurşen Kulakaç, and Samet Sayılan. 2021. The effects of noise levels on pain, anxiety, and sleep in patients. *Nursing in Critical Care* 26, 2 (2021), 79–85.

[10] Simon P Banbury and Dianne C Berry. 2005. Office noise and employee concentration: Identifying causes of disruption and potential improvements. *Ergonomics* 48, 1 (2005), 25–37.

[11] Benjamin Berens, Katerina Dimitrova, Mattia Mossano, and Melanie Volkamer. 2022. Phishing awareness and education–When to best remind. In *Workshop on Usable Security and Privacy (USEC)*.

[12] Benjamin Maximilian Berens, Florian Schaub, Mattia Mossano, and Melanie Volkamer. 2024. Better Together: The Interplay Between a Phishing Awareness Video and a Link-centric Phishing Support Tool. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*. 1–60.

[13] André Bergholz, Jan De Beer, Sebastian Glahn, Marie-Francine Moens, Gerhard Paaß, and Siehyun Strobel. 2010. New filtering approaches for phishing email. *Journal of computer security* 18, 1 (2010), 7–35.

[14] Lina Brunken, Annalina Buckmann, Jonas Hielscher, and M Angela Sasse. 2023. {"To} Do This Properly, You Need More {Resources"}: The Hidden Costs of Introducing Simulated Phishing Campaigns. In *32nd USENIX Security Symposium (USENIX Security 23)*. 4105–4122.

[15] Duane C Button, David G Behm, Michael Holmes, and Scott N Mackinnon. 2004. Noise and muscle contraction affecting vigilance task performance. *Occupational ergonomics* 4, 3 (2004), 157–171.

[16] Gianna Cassidy and Raymond AR MacDonald. 2007. The effect of background music and background noise on the task performance of introverts and extraverts. *Psychology of Music* 35, 3 (2007), 517–537.

[17] Xiaowei Chen, Margault Sacré, Gabriele Lenzini, Samuel Greiff, Verena Distler, and Anastasia Sergeeva. 2024. The Effects of Group Discussion and Role-playing Training on Self-efficacy, Support-seeking, and Reporting Phishing Emails: Evidence from a Mixed-design Experiment. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*. 1–21.

[18] Sam Cook. [n. d.]. *Top Phishing Statistics and Facts for 2019–2023.* https://www.comparitech.com/blog/vpn-privacy/phishing-statistics-facts/

[19] Brian H Dalton, David G Behm, and Armin Kibele. 2007. Effects of sound types and volumes on simulated driving, vigilance tasks and heart rate. *Occupational Ergonomics* 7, 3 (2007), 153–168.

[20] Nguyet Quang Do, Ali Selamat, Ondrej Krejcar, Enrique Herrera-Viedma, and Hamido Fujita. 2022. Deep learning for phishing detection: Taxonomy, current challenges and future directions. *Ieee Access* 10 (2022), 36429–36463.

[21] Richard D Edsell. 1976. Anxiety as a function of environmental noise and social interaction. *The Journal of psychology* 92, 2 (1976), 219–226.

[22] Serge Egelman and Eyal Peer. 2015. Scaling the security wall: Developing a security behavior intentions scale (sebis). In *Proceedings of the 33rd annual ACM conference on human factors in computing systems*. 2873–2882.

[23] Mercede Erfanian, Andrew J. Mitchell, Jian Kang, and Francesco Aletta. 2019. The Psychophysiological Implications of Soundscape: A Systematic Review of Empirical Literature and a Research Agenda. *International Journal of Environmental Research and Public Health* 16, 19 (Jan. 2019), 3533. https://doi.org/10.3390/ijerph16193533

[24] Michael W Eysenck and Manuel G Calvo. 1992. Anxiety and performance: The processing efficiency theory. *Cognition & emotion* 6, 6 (1992), 409–434.

[25] Annastasia Falkenberg. 2019. *The Role of Cue Utilisation and Anxiety on Phishing Email Susceptibility.* Ph. D. Dissertation.

[26] Tzipora Halevi, Nasir Memon, and Oded Nov. 2015. Spear-phishing in the wild: A real-world study of personality, phishing self-efficacy and vulnerability to spear-phishing attacks. *Phishing Self-Efficacy and Vulnerability to Spear-Phishing Attacks (January 2, 2015)* (2015).

[27] Michael S Humphreys and William Revelle. 1984. Personality, motivation, and performance: a theory of the relationship between individual differences and information processing. *Psychological review* 91, 2 (1984), 153.

[28] Emaan Bilal Khan, Emaan Atique, and Mobin Javed. 2024. Investigating Phishing Threats in the Email Browsing Experience of Visually Impaired Individuals. In *Extended Abstracts of the CHI Conference on Human Factors in Computing Systems*. 1–11.

[29] Ponnurangam Kumaraguru, Justin Cranshaw, Alessandro Acquisti, Lorrie Cranor, Jason Hong, Mary Ann Blair, and Theodore Pham. 2009. School of phish: a real-world evaluation of anti-phishing training. In *Proceedings of the 5th Symposium on Usable Privacy and Security*. 1–12.

[30] Daniele Lain, Kari Kostiainen, and Srdjan Čapkun. 2022. Phishing in organizations: Findings from a large-scale and long-term study. In *2022 IEEE Symposium on Security and Privacy (SP)*. IEEE, 842–859.

[31] Yuliang Lan, Hannah Roberts, Mei-Po Kwan, and Marco Helbich. 2020. Transportation noise exposure and anxiety: A systematic review and meta-analysis. *Environmental research* 191 (2020), 110118.

[32] Gavin P Lawrence, Michael A Khan, and Lew Hardy. 2013. The effect of state anxiety on the online and offline control of fast target-directed movements. *Psychological Research* 77 (2013), 422–433.

[33] Delila Lisica, Maida Koso-Drljević, Birgit Stürmer, and Christian Valt. 2024. Reduction of anxiety symptoms during systemic family therapy results in a concurrent improvement of cognitive performance: a study on people with high anxiety. *Cognition and Emotion* 38, 2 (2024), 245–255.

[34] Guangli Lu, Ruiying Jia, Dandan Liang, Jingfen Yu, Zhen Wu, and Chaoran Chen. 2021. Effects of Music Therapy on Anxiety: A Meta-Analysis of Randomized Controlled Trials. *Psychiatry Research* 304 (Oct. 2021), 114137. https://doi.org/10.1016/j.psychres.2021.114137

[35] Oleg Medvedev, Daniel Shepherd, and Michael J. Hautus. 2015. The Restorative Potential of Soundscapes: A Physiological Investigation. *Applied Acoustics* 96 (Sept. 2015), 20–26. https://doi.org/10.1016/j.apacoust.2015.03.004

[36] Y. Meier and N. C. Krämer. 2022. The privacy calculus revisited: an empirical investigation of online privacy decisions on between- and within-person levels. *Communication Research* 51 (2022), 178–202. Issue 2. https://doi.org/10.1177/00936502221102101

[37] Tamir Mendel and Eran Toch. 2023. Social support for mobile security: Comparing close connections and community volunteers in a field experiment. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*. 1–18.

[38] Mplus. 2023. *Chi-Square Difference Testing Using the Satorra-Bentler Scaled Chi-Square.* Accessed: 2023-11-18.

[39] Ammar Odeh, Ismail Keshta, and Eman Abdelfattah. 2021. Machine learningtechniquesfor detection of website phishing: A review for promises and challenges. In *2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC)*. IEEE, 0813–0818.

[40] Daniela Oliveira, Harold Rocha, Huizi Yang, Donovan Ellis, Sandeep Dommaraju, Melis Muradoglu, Devon Weir, Adam Soliman, Tian Lin, and Natalie Ebner. 2017. Dissecting spear phishing emails for older vs young adults: On the interplay of weapons of influence and life domains in predicting susceptibility to phishing. In *Proceedings of the 2017 chi conference on human factors in computing systems*. 6412–6424.

[41] Sharvari Patil and Narendra M Shekokar. 2023. A Study of Recent Techniques to Detect Zero-Day Phishing Attacks. In *Intelligent Approaches to Cyber Security*. Chapman and Hall/CRC, 71–83.

[42] Salvi Siddhi Ravindra, Shah Juhi Sanjay, Shaikh Nausheenbanu Ahmed Gulzar, and Khodke Pallavi. 2021. Phishing Website Detection Based on URL. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology (USRCSEIT)* 7, 3 (2021), 589–594.

[43] Benjamin Reinheimer, Lukas Aldag, Peter Mayer, Mattia Mossano, Reyhan Duezguen, Bettina Lofthouse, Tatiana Von Landesberger, and Melanie Volkamer. 2020. An investigation of phishing awareness and education over time: When and how to best remind users. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*. 259–284.

[44] James Reynolds, Alastair McClelland, and Adrian Furnham. 2014. An investigation of cognitive test performance across conditions of silence, background noise and music as a function of neuroticism. *Anxiety, Stress, & Coping* 27, 4 (2014), 410–421.

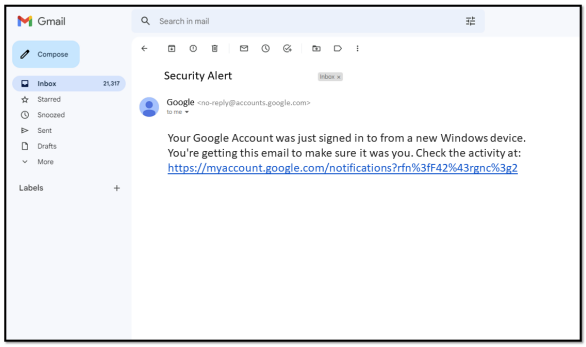
[45] Elliott Salamon, Steven R. Bernstein, Minsun Kim, and George B. Stefano. 2003. The Effects of Auditory Perception and Musical Preference on Anxiety in Naive

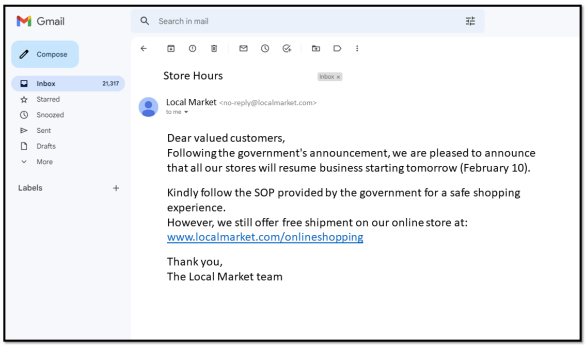
Human Subjects. (2003).
[46] Irwin G Sarason. 1988. Anxiety, self-preoccupation and attention. *Anxiety research* 1, 1 (1988), 3–7.
[47] Anastasia Sergeeva, Björn Rohles, Verena Distler, and Vincent Koenig. 2023. "We Need a Big Revolution in Email Advertising": Users' Perception of Persuasion in Permission-based Advertising Emails. In *Proceedings of the 2023 chi conference on human factors in computing systems*. 1–21.
[48] Andrew Smith. 1990. Noise, performance efficiency and safety. *International archives of occupational and environmental health* 62 (1990), 1–5.
[49] Charles D Spielberger, Duncan N Hansen, et al. 1969. Effects of state anxiety and task difficulty on computer-assisted learning. *Journal of Educational Psychology* 60, 5 (1969), 343.
[50] Lionel Standing and Greg Stace. 1980. The Effects of Environmental Noise on Anxiety Level. *The Journal of General Psychology* 103, 2 (Oct. 1980), 263–272. https://doi.org/10.1080/00221309.1980.9921007
[51] Emil Stobbe, Josefine Sundermann, Leonie Ascone, and Simone Kühn. 2022. Birdsongs Alleviate Anxiety and Paranoia in Healthy Participants. *Scientific Reports* 12, 1 (2022), 16414.
[52] David L Strayer, Jonna Turrill, Joel M Cooper, James R Coleman, Nathan Medeiros-Ward, and Francesco Biondi. 2015. Assessing cognitive distraction in the automobile. *Human factors* 57, 8 (2015), 1300–1324.
[53] Keith S Taber. 2018. The use of Cronbach's alpha when developing and reporting research instruments in science education. *Research in science education* 48 (2018), 1273–1296.
[54] Stephen C. Van Hedger, Howard C. Nusbaum, Luke Clohisy, Susanne M. Jaeggi, Martin Buschkuehl, and Marc G. Berman. 2019. Of Cricket Chirps and Car Horns: The Effect of Nature Sounds on Cognitive Performance. *Psychonomic Bulletin & Review* 26, 2 (April 2019), 522–530. https://doi.org/10.3758/s13423-018-1539-1
[55] Bob Violino. [n. d.]. *Phishing attacks are increasing and getting more sophisticated. Here's how to avoid them.* https://www.cnbc.com/2023/01/07/phishing-attacks-are-increasing-and-getting-more-sophisticated.html
[56] Melanie Volkamer, Martina Angela Sasse, and Franziska Boehm. 2020. Analysing simulated phishing campaigns for staff. In *Computer Security: ESORICS 2020 International Workshops, DETIPS, DeSECSys, MPS, and SPOSE, Guildford, UK, September 17–18, 2020, Revised Selected Papers 25*. Springer, 312–328.
[57] Bradley W Weaver, Adam M Braly, and David M Lane. 2021. Training users to identify phishing emails. *Journal of Educational Computing Research* 59, 6 (2021), 1169–1183.
[58] Muriel M Woodhead. 1958. The effects of bursts of loud noise on a continuous visual task. *British Journal of Industrial Medicine* 15, 2 (1958), 120.
[59] Libo Wu and Hasliza Binti Abdul Halim. 2024. Task complexity and foreign language writing emotions as predictors of EFL writing performance. In *Frontiers in Education*, Vol. 9. Frontiers Media SA, 1323843.
[60] Adriana A Zekveld, Sophia E Kramer, and Joost M Festen. 2011. Cognitive load during speech perception in noise: The influence of age, hearing loss, and cognition on the pupil response. *Ear and hearing* 32, 4 (2011), 498–510.
[61] Andras N Zsido, Szidalisz A Teleki, Krisztina Csokasi, Sandor Rozsa, and Szabolcs A Bandi. 2020. Development of the short version of the spielberger state—trait anxiety inventory. *Psychiatry research* 291 (2020), 113223.

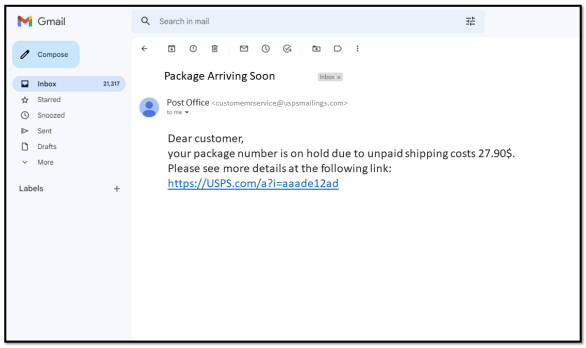
A Appendix

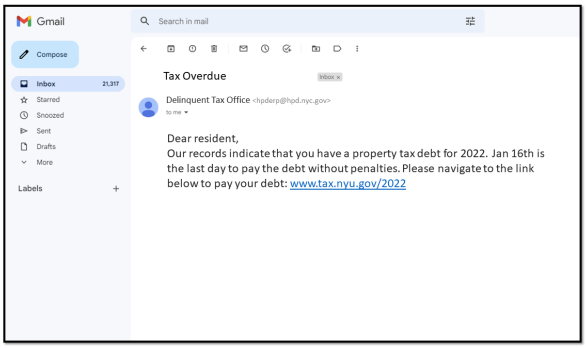
Variable Names	Standardized coefficients	Odds Ratio	Standard error	*p-value*
DV: Accuracy	R.squared = 0.298			
H1: Difficulty	-0.655	0.518	0.092	<.001
H2: Anxiety	-0.355	0.701	0.089	<.001
H4: Anxiety X Difficulty	0.461	1.585	0.120	<.001
H5: Auditory Env: Silent vs. non-silent	-0.043	0.957	0.043	.159
H6: playback level: Low vs. high	0.004	1.004	0.046	.467
DV: Anxiety	R.squared = 0.019			
H3: Difficulty	0.065	-	0.025	.004
H7: Auditory Env: Silent vs. non-silent	-0.059	-	0.024	.007
H8: Playback Level: Low vs. high	-0.099	-	0.039	.006

Table 1: Path model results. Since anxiety is a continuous variable, the odds ratio is not applicable.









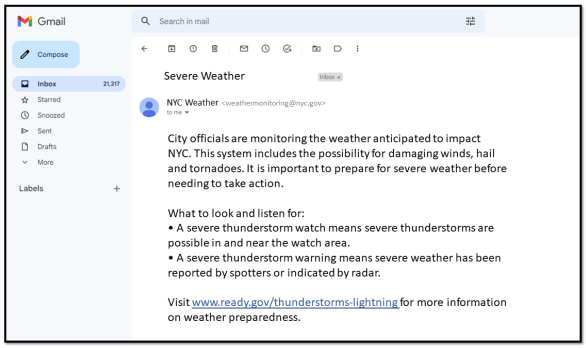
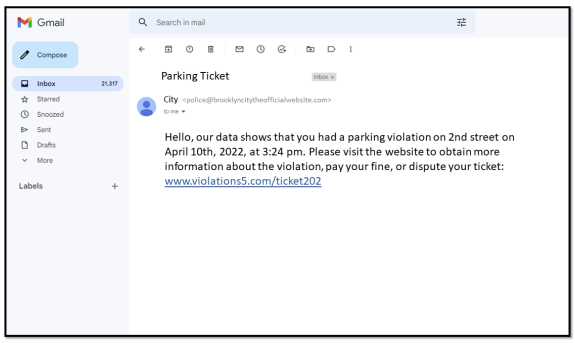
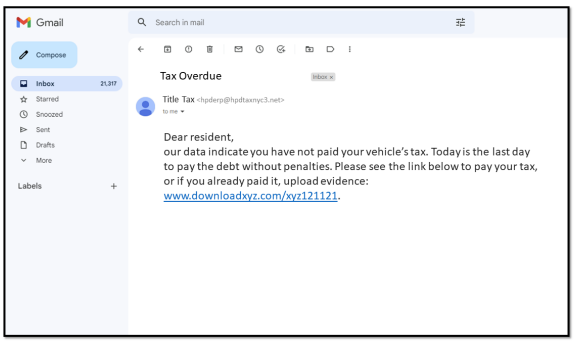
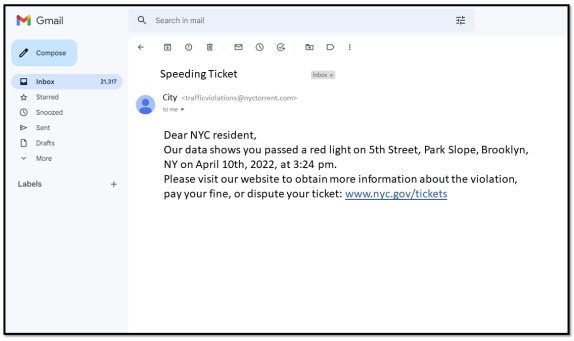
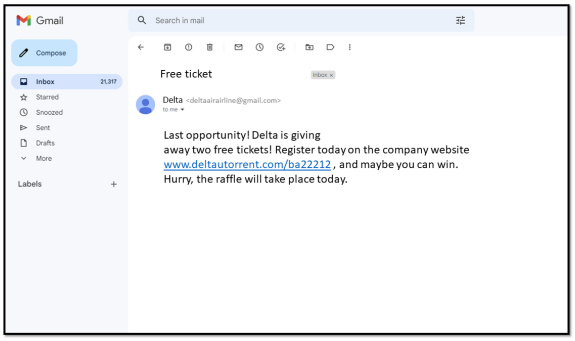


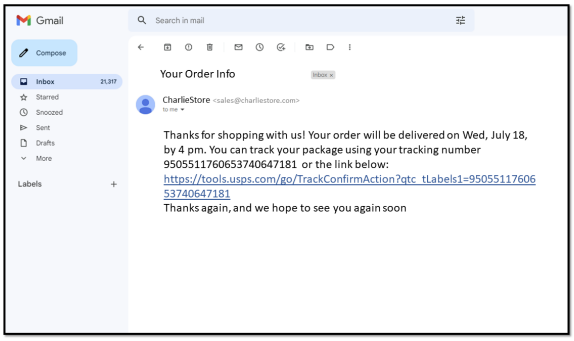
Figure 3: Legitimate emails that we used in this study.

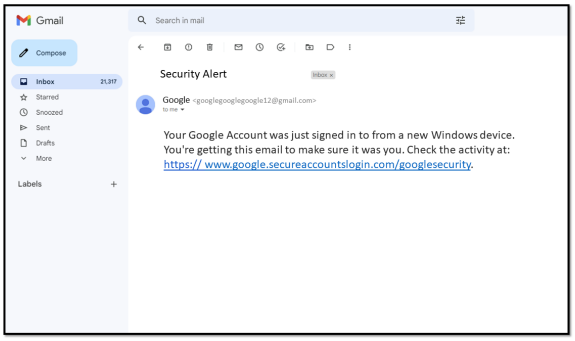












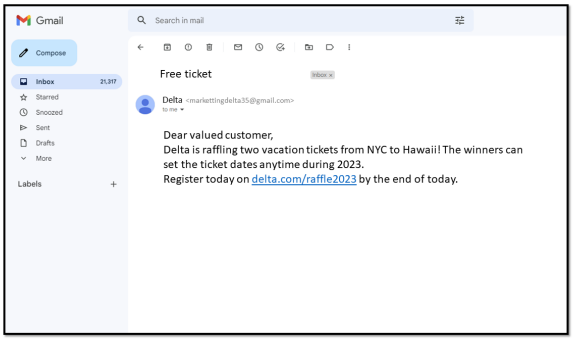


Figure 4: Phishing emails that we used in this study.