User Experiences with Suspicious Emails in Virtual Reality Headsets: A Study in Realistic Settings

Filipo Sharevski
DePaul University
fsharevs@depaul.edu

Jennifer Vander Loop
DePaul University
jvande27@depaul.edu

Sarah Ferguson
DePaul University
sfergu12@depaul.edu

Viktorija Paneva
LMU Munich
viktorija.paneva@ifi.lmu.de

***Abstract*—For all the immersive potential offered by Virtual Reality (VR) headsets, the technology itself is also conducive to perceptual manipulations. Altering user perception in VR could negatively affect security behavior, as translating prior experiences into an immersive environment might introduce an atypical susceptibility to phishing. A case in point is the routine evaluation of potentially suspicious emails for links or attachments, a task that people might be proficient in traditional interactive environments but fall for when doing so via a VR headset. To explore VR's potential for such manipulative alterations, we devised a study exploring user assessment and action on suspicious emails and warnings through virtual reality (VR) headsets. A balanced set of (*n*=20) Apple Vision Pro users and (*n*=20) Meta Quest 3 users were invited to evaluate their *own* Gmail messages. Prior to doing so, we covertly sent a *false positive* suspicious email – containing either a URL or attachment – that contained a warning banner but was nonetheless legitimate. Our observations showed that two Apple Vision Pro participants clicked the link, and one Meta Quest 3 participant opened the attachment. In all three cases, the susceptibility to phishing was due to the headsets' hypersensitive click response and poor ergonomic precision during the email evaluation task. Although the perceptual manipulation in these cases could be deemed as unintentional, we nonetheless provide evidence of VR's potential to negatively affect users' defenses against immersive social engineering manifestations. Based on these findings and the participation experience, we offer recommendations for implementing suspicious email warnings tailored for VR environments.**

***Index Terms*—VR, phishing, warnings, spam**

I. Introduction

The commercial proliferation of virtual reality (VR) head-mounted displays (or headsets) offered users the possibility to participate in various activities in more immersive ways than before [1]. Gaming was the go-to VR activity, though activities such as social collaboration [2], clinical care [3], education [4], and shopping [5] quickly capitalized on the immersiveness. The ability to interact with superimposed 3D virtual objects in the real world, for example, has tempted 13% of US consumers to acquire a VR headset [6] and at least 21% of the consumer base to do so in the near future [7].

Symposium on Usable Security and Privacy (USEC) 2026
27 February 2026, San Diego, CA, USA
ISBN 978-1-970672-07-7
https://dx.doi.org/10.14722/usec.2026.23028
www.ndss-symposium.org, https://www.usablesecurity.net/USEC/

As interest in VR headsets grows strong [7], companies like Apple and Meta are looking for ways to accelerate the adoption of their products, such as *productivity* [8]. The Apple Vision Pro is marketed as a productivity tool or a "workspace with infinite space" [9], and the Quest offers the "Infinite Office," a full-fledged virtual workspace [10]. Though still an experimental idea, the early adopters hailed the VR headsets as "the ultimate work-from-home devices" that allow for "peripersonal task organization," "direct attention," and "full-body interaction" experiences [11], [12], [13].

Transferring desktop and mobile interactivity into the virtual reality environment, especially for work, is not a trivial task, as immersive interaction is foreign to most people [8]. The slow roll-out, so far, is focused on experiential tasks such as Zoom meetings, individual tasks such as training, maintaining interaction among physically distanced coworkers, and providing workers with private spaces in public settings [14]. PricewaterhouseCoopers (PwC), for example, used VR headsets to help employees combat Zoom fatigue and conduct soft-skills training [15].

A task integral to any productivity-driven use of VR headsets is *email correspondence*. Emails are the key element for a seamless transition to complete workplace immersion and VR headsets have a particular advantage when it comes to multitasking [16]. Dealing with emails, some of which are phishing or spam, is a known problem affected not just by multitasking [17] but also by the general pressures of the working environment [18], [19]. As such, a question arises of how people would respond to suspicious emails when they access them through VR headsets. VR headsets are conducive to manipulative rendition of the immersiveness as the properties of spatiality and perception are shown to result in user deception both intentional and unintentional [20], [21]. For example, the VR platform could spatially place the email client or a particular email message outside the predicted visual focus area of the user, or the email sorting task could be implemented using unfamiliar or unintuitive input gestures [22], [23].

In conventional desktop and mobile computing, people have the aid of warnings in cuing about suspicious emails [24], [25], so another question arises regarding how these warnings render the necessary deception protection in virtual reality environments. In the context of the perceptive manipulation possibilities of VR, unfamiliar or misleading precision, sensitivity, haptic feedback, sound, or color while interacting with

emails could lead people to ignore or second guess these warnings [26]. Equally, one could block out just the warning banner part of an email, exposing a user directly and only to the phishing content itself [27]. Early evidence shows that interactive user security and privacy interventions (e.g., password managers, permissions dialog windows, cookie banners) do not intuitively transfer within an immersive environment [28], [29], [30]. As suspicious email warnings are another type of popular usable security intervention, we devised a study to learn how immersiveness might affect users' security behavior when it comes to phishing URLs and attachments:

- **RQ1:** How do users assess suspicious emails sent to their *own* email addresses in immersive environments, in particular: (i) Meta Quest 3; and (ii) Apple Vision Pro VR headsets?
- **RQ2:** How do immersive environments affect users' actions related to suspicious emails sent to their *own* email addresses when accessed through (i) Meta Quest 3; and (ii) Apple Vision Pro VR headsets?
- **RQ3:** What recommendations do users have for usability and VR immersiveness/ergonomics improvements of banner warnings about suspicious emails when accessed through VR headsets?

Our findings indicate that the warnings were effective in discouraging users from interacting with suspicious emails [26]. About 75% of participants who encountered a warning indicated they would not interact with the email, whereas only 20% of participants who did not encounter a warning banner chose not to interact with the email. Participants expressed reservations about the way the warnings were formatted (see Figure 5), as they felt it failed to help people correctly decide what action to take with an email through a VR headset. The suggestions included implementing a color-coding system [26], a detailed safety description (including a severity indicator), and adding spatial pop-ups in the viewing focus of the user. Having the option of using a VR headset for productivity intrigued our participants, though many found that the VR headset itself created additional challenges for routine sorting and interacting with their emails.

Participants reported they were "spatially" distracted [20] by seeing their physical surroundings and felt it would help if their focus were better directed towards their email. Five, or 25% of the Apple Vision Pro participants complained about how atypically "frictionless" it was to click on a link or any button as an affordance perceived with a dose of friction in traditional interactive contexts (conjecturing that this might result in accidental phishing that, even if rectified, would result in loss of productivity) [21]. Four, or 20% of the Meta Quest 3 participants felt that they were not able to click with the precision needed to perform a task such as inspecting a URL or an attachment by hovering over it, underlying the ability of VR to manipulate an otherwise routine task, even in the presence of warnings [28], [29]. These interactive hurdles led two participants from the Apple Vision Pro group to click on our test *false positive* link and one Meta Quest participant to open the test *false positive* attachment.

II. Background Work

A. Deception by Immersion in VR

VR interfaces expand the attack surface through persistent environmental sensing, novel input modalities, and the blending of physical and digital contexts—observations that extend directly to modern VR headsets [31]. Recent work highlights how sensory immersion in extended Reality (XR) environments can be exploited to introduce deceptive or manipulative patterns that prompt users to make decisions or perform actions that might not be in their best interest, or that they would not otherwise make if fully informed. The combination of immersive capabilities and extensive data collection enables subtle yet powerful manipulation strategies, such as altering user perception, influencing emotions, exploiting sensory immersion, or distorting user memory or sense of reality, all of which have severe implications for user autonomy, security, and privacy [21]. Gray et al. [32] characterize these practices as dark patterns in UX design, which exploit asymmetries in information, attention, and control—risks that may be amplified in immersive systems.

Krauß et al. [20] identified XR-specific properties that facilitate deceptive patterns, including perception, spatiality, physical/virtual barriers, and XR device sensing (e.g., eye tracking, body movement, and location). These properties not only allow for the integration of known deceptive patterns into XR but also give rise to new manipulative strategies specific to immersive environments. For example, perceptual manipulations could involve photorealistic virtual objects, context-aware stimuli, or sensor-driven personalization that renders deceptive content more convincing. Spatial manipulations could manifest as an imbalance of options – making one choice easier to reach, closer, and more salient, while rendering alternatives distant, awkward to reach, or effectively "hidden" in 3D. Tseng et al. [33] further describe Virtual-Physical Perceptual Manipulations (VPPM), in which XR systems alter the human multi-sensory perception of our physical actions and reactions to nudge the user's physical movements.

B. VR Security Threats

Prior security evaluations of VR systems have largely focused the threat evaluation concerning authentication and leakage of private information. As immersiveness is seen as an alternative interaction affordance to the conventional entry of credentials, for example [1], threats to VR headsets could come from adversaries with and without access to the VR headset. An adversary without access or a "shoulder-surfer" might not be able to directly snoop on the credential-entering process of VR users [34] but could craft a careful observation-based attack that would enable deciphering approximately between 75-80% of text inputs made in VR headset [35], [36], [37], [38], [39], coming effectively close to conventional keylogging attacks. Beyond such side-channel threats, recent

work shows that established authentication practices themselves, such as passwords and password managers, are poorly suited to immersive environments. Cumbersome text entry in VR, the absence of cross-application autofill, and the difficulty of applying credential-management workflows designed for desktop or mobile contexts all contribute to higher error rates and reduced authentication reliability [28].

To mitigate observational attacks that focus on variations in users' head pose and hand gestures, Apple Vision Pro relies on an eye tracker to minimize the need for any movements while authenticating or entering sensitive information. But an adversary with access, particularly one able to exploit the Apple Persona, is still able to infer eye-related biometrics from the avatar image to reconstruct text entered via gaze-controlled typing [40]. Or worse, an adversary with access could simply launch an immersive hijacking attack on a Meta Quest 3, or control a user's interaction with their VR headset by trapping them inside a malicious app that masquerades as the full VR interface, effectively gaining access to all the users' private information, including credentials [41].

With the accelerated adoption of VR headsets for productivity, we see a third type of adversary that, regardless of the type of access, can recondition the well-known approach to stealing users' credentials or installing malware through phishing and spam emails. This adversary is not bound to a particular VR headset type, nor does it need any specific and complicated computational setup to be able to successfully launch an attack. Granted, biometric authentication schemes that do not depend on user input [34] might alleviate this threat to an extent, though many of them might still not be integrated with traditional productivity applications, and it will take some time to do so.

C. Threat Vector: Suspicious Emails

Suspicious emails potentially contain malicious URLs and attachments aiming to steal users' credentials or install malware. Spotting a suspicious email is a delicate task that the majority of users have not yet fully mastered, as malicious URLs and attachments still get "clicked" in concerning numbers – the average successful click rate for a phishing attack consistently remains close to 20% over the years [42]. As email communication allows for easy deception through impersonation and influencing pretexts, users must rely on "warnings" or cues that alert them about impending phishing emails, usually generated by their email providers (when providers like Gmail correctly detect phishing or a spam attempt; however, a non-negligible amount of suspicious emails still manage to reach users' inboxes undetected, while some legitimate emails get incorrectly flagged as suspicious [43]).

Suspicious email warnings are thus implemented as *in situ* interventions within user interfaces, presented while the user is engaged in an email correspondence task, such as sorting, reading, or responding to an email [44]. The goal is to either force the attention of a user to a suspicious element like a URL or attachment (usually within an email client) [24] or offer options for users to "go back to safety" or "proceed to a website" (usually in a browser). This is done by placing warnings in banner variants before the email subject lines [45], [46], displaying warning signs in the graphical avatar icon of the sender [47], or showing just-in-time, just-in-place URL trustworthiness tips in the email body [25]. Often, interactive warnings are accompanied by additional informative messages that communicate potential threats to "inoculate" users against future suspicious email correspondence [48].

Evidence from user evaluations of interactive warnings suggests that users tend to adhere to interactive warnings [44], provided the wording is comprehensible, and the design prevents habituation. Adherence and phishing safety, however, come at a cost – usually, the forced attention is distracting, time-consuming, and tedious [49], especially with the high number of emails a user receives a day and the fractured attention due to multitasking [50]. There is also a difference in effectiveness whether the warning "friction" happens within an email client as a banner (the usual vector for delivery of phishing attacks [42]) or in a browser as a splash screen, with the latter implementation being better at preventing participants from reaching phishing websites [24].

D. VR and Suspicious Emails

Virtuality itself is yet to be explored from an adversarial perspective in the context of phishing, spamming, or scamming. So far, AR glasses have been evaluated for their potential to help users analyze images of URLs displayed across devices for improved phishing detection [51]. A usability test showed that the AR glasses helped users improve the correct identification of phishing attempts compared to a baseline condition. An educational "social engineering" VR game exists where players perform voice phishing attacks [52]. Similarly, a VR social engineering game was developed to teach users about cues of deception in phishing emails (e.g., anomalies in the senders' email address, grammar and spelling mistakes in the email body, and principles of influence) [53]. A preliminary test involving five students showed that all of them scored higher on the HAIS-Q scale after having played the game compared to their scores previously.

III. Study

A. Study Methodology

We obtained approval from our Institutional Review Board (IRB) to conduct a mild deception study with a sample of n=40 participants (20 in the Apple Vision Pro group and 20 in the Meta Quest 3 group) who had previous experience with VR headsets. As the Apple Vision Pro is prohibitively expensive to purchase in bulk, we invited participants to join a physical collaborative space and use this headset or the Meta Quest 3 for the purpose of studying how users utilize virtual reality headsets to interact with emails in general. We used this "cover" in order to situate our study to allow participants to interact with emails sent to their *own* email address and *own* phone device, per the methodology guidelines outlined in [54]. Once they set up the VR headset and logged into their email address (we used Gmail as a preferred provider), we asked

the participants a couple of preliminary questions to frame the study in a broader suspicious email context (to avoid priming effects). The first question was how familiar they are with VR headsets, and the second was how they prefer to check their emails. These answers allowed us to provide the opportunity to frame the subsequent request to sort several emails from the spam folders as a task towards the assessment of suspicious emails that are not expected to be phishing or spam by default, just because they have been filtered as such by Gmail.

The first task was to select several emails of their choice in their spam folder and review only the subject line and sender. We did this to ensure that these emails were not dangerous (e.g., resembled standard spam or phishing), both by checking for pretext and formatting patterns found in databases of known spam/phishing emails [55] and using our own assessment experience. If we were uncertain, we asked the participant to proceed to the next one (during the debriefing, we advised them that it was best to delete it). We then asked the participants to open the email, assess the legitimacy of the email (**RQ1**) (with a baseline established beforehand, as described in Appendix 4), and share with us what the most likely action they would perform on it (**RQ2**) (without actually clicking any links or downloading any attachments). To ensure that participants encountered both phishing and spam banner warnings (appearing regularly in the spam folder), we secretly sent a *false positive* phishing email to their own email address — one that Gmail classifies as "phishing," assigns a phishing banner warning, and puts it in the spam folder — but in reality, the email is legitimate. Once we completed the assessment tasks, participants offered their recommendations for improving the email correspondence experience relative to immersive suspicious email warnings (**RQ3**). During the study, we offered the participants to do other tasks in the VR while sorting their emails to mimic their natural task-switching behavior, such as browsing the news, typing a memo, or exploring the VR settings.

B. Study Elements: Warnings

Gmail varies the warning banners per the type of suspicious email. Figure 5 shows the banner for *spam* messages, in gray, that, instead of signaling the danger of email [56], invites the user to go through the suspicious email and "report it not spam" if the user disagrees with Gmail's classification (based on the "similar passages identified in the past"). A variant of this banner, also in gray, is shown in Figure 6, where Gmail has taken action to "hide the images" as known phishing elements that conceal suspicious URLs or malware, warning the user that "this message might be suspicious or spam." A user here has the option to either "see the images" or help with automated detection by confirming that the message is actually spam. If a user has blocked a sender of suspicious emails, Gmail also displays the banner shown in Figure 7 that tells the user "subsequent emails would be sent in spam" and offers the option to either "unblock the sender" or move the existing messages from this sender to their spam folder.

Figure 8 shows the general banner for high certainty phishing messages, in bright red, that not only alerts the user that the email is "dangerous" but also explains the perils of "clicking on a link or downloading an attachment" (personal information stolen). If a user is certain that this email is "safe," Gmail offers an option for them to ignore the warning and report it as a false positive. Figure 9 shows an alternative banner for *phishing* messages where Gmail cannot determine with high certainty that the email might be phishing and urges the user to be "careful with the message." If the user, presuming they are versed in spotting phishing cues, determines the email is indeed phishing, then the warning offers the option to report it as such. Otherwise, the user could proceed and deem the message safe.

C. Study Stimuli: Emails

While a prior check of multiple researcher-controlled email addresses revealed to us that encountering spam messages with the associated banner variants would not be a problem, that was not the case for encountering a phishing email in the participants' spam folders. To ensure that this would happen for the purpose of the study, we have prepared a couple of *false positive* suspicious emails – one with a suspicious URL and one with a suspicious attachment that we knew the filters would assign some of the aforementioned warnings and move them to the spam folder. We decided to use false positive suspicious emails, that is, an email which was *not* suspicious but was classified as such by Gmail, to avoid exposing our participants to greater than minimal risk with other, *true positive* spam or phishing emails.

This means the emails could not cause any harm to users as they did not actually contain malicious links (the actual URL included resolved to a legitimate Amazon Web Services – AWS page), and the attachment was just a blank Word document. We created the first *false positive* suspicious email by initiating an AWS account creation verification email, shown in Figure 10. We chose to randomly target half of our participants with this *false positive* email (10 in the Apple Vision Pro group and 10 in the Meta Quest 3 group). The other half we randomly targeted with another *false positive* suspicious email that contained a blank Word document that was part of a "here is your invoice" pretext that "confirms a recently placed order," as shown in Figure 11. Both *false positive* suspicious emails were directed on the day before participation to the participants' emails they used to sign up for the study (we did not want to tip them off that something might be amiss if we sent the email right before their session).

We chose these emails as we encountered similar ones in our own spam folders. We refer to it as "mild deception," as our participants did not know we were the ones who "sent" this email to their addresses. We assumed the participants might already have spam, but we were less sure about them having suspicious emails containing links and attachments sitting in their spam folders, so that we could test all the interactive warning banner variants. Both of the *false positive* emails were necessary to invoke a realistic scenario where our participants

access either a spam or a phishing banner warning assigned to an email because such an occurrence might not happen frequently enough to be reasonably observed as part of the email correspondence sorting task during the study.

We were aware that the classification of untrustworthy emails was predicated on the individual's email correspondence and behavior, and we expected that we might encounter a case where the *false positive* suspicious emails might not end up in participants' spam folders or get assigned any interactive warning. For those cases, we decided to proceed only with what they had in their spam folder as emails addressed to them without going to their primary inbox or attempting to ask them to perform additional steps. Our IRB has approved the study, and we used an extensive debriefing (see Appendix E) in which we pointed out our methodology, discussing any events during the interviews that might affect the participants' future engagement with suspicious emails.

We believe that our methodological approach is appropriate because it strikes a good balance between the acceptability/manageability of our participants' participation under realistic conditions while we grasp their real-time experiences with their personal email correspondence through a VR headset. Participants were randomly assigned to two groups, in which they either used the Apple Vision Pro device to check their emails via Apple's web application, shown in Figure 1, or the Meta Quest 3 device to check their emails via the Gmail Chrome web browser, shown in Figure 2. As of the study, Meta did not offer a dedicated email application available to use on the Meta Quest platform, so we decided to use the standard browser access to Gmail.

Fig. 1: Apple Vision Pro Email Application [9]

D. Participant Recruitment

We recruited participants who have used a VR headset and regularly use web/email clients. They had to be individuals 18 years of age or older, with internet access on their own device, client, and browser, and were English-speaking and literate. We recruited potential participants through the university's research participant system. We choose to work with students in our university for several reasons. First, students use emails regularly for productivity and might adopt VR for such tasks in the future [57]. Second, across the entire population in the US, college students are in the age group that mostly uses or has used VR before (gaming, for example) [6]. And third, we were limited to using the (expensive) VR sets in a physical collaborative space so we could reasonably invite students to such a place on our campus. We had no access to the participants' email, and we did not record any of their authentication credentials. The interviews were confidential, recorded through an audio-only Zoom session (for the purpose of generating a transcript), lasted on average 30 minutes, and students were provided with extra credit for a class that participates in our university's participant pool program.

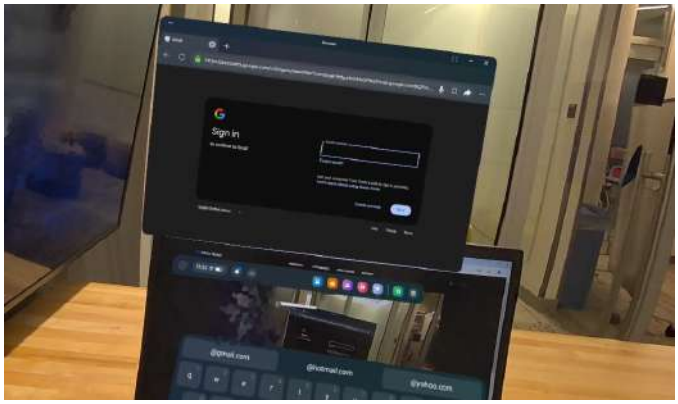

Fig. 2: Meta Quest 3 Gmail through Chrome Browser

E. Trust and Ethical Considerations

As this was a study concerning the participants' *own* email addresses, during the consent process, we offered them the option to choose not to participate and to choose which email address they would use, if they had multiple ones. We noted they could select any email they wanted to communicate to us from their spam folder, and they were free to stop and abandon any question at any point in time if they felt like doing so. Prior to doing any of the tasks and the interview, we told them they could ask us to stop the interview, stop the recording, or remove any answers or readings at any point in time. As the VR headsets might also cause uneasiness or mild dizziness, we also allowed the participants to stop, take off the headset, take a break, and continue when they were ready. We also offered inserts for participants wearing glasses if they needed them for better comfort in using the VR headset, particularly the Apple Vision Pro, in case they wore glasses.

We pointed out to our participants that they could act on the emails from the study as they ultimately wished (e.g., delete, move to inbox, report, etc.). After we collected their answers, we verbosely debriefed them about the mild deception we used and that we were the ones who initiated a *false positive* suspicious email to their spam folder (if they received one or chose to verbalize one during the study). We pointed participants to general suspicious email resources if they wished to further raise or check their awareness [58]. We employed lengthy explanations to reassure our participants that we were not involved with the filtering nor with the formatting and

implementations of the email banner warnings they saw during the study or in the past. We were also careful not to appear in favor nor support of particular types of warnings in order to maintain full researcher impartiality. We communicated that our ultimate goal is to create meaningful detection of phishing when these banner warnings are present in VR headsets. We pointed out that this goal, however, does not prevent from misusing or misinterpreting our findings in making compromises for suspicious email detection, implementation of VR-specific email productivity applications, or abandoning the use of VR for productivity altogether.

F. Data Collection and Analysis

Each interview was done with open-ended questions listed in the interview script (see Appendix C). Due to the nature of the study, not all the participants used a similar set of emails, and in some cases, Gmail either entirely filtered out the *false positive* suspicious emails (shown in Figures 10 and 11) or moved them to the main inbox without any warnings assigned. The responses from participants conveyed their experience, and we set out to conduct a thematic analysis to offer a "compelling, coherent, and useful story" [59] about the intersection between emails, warnings, and immersive interfaces. We pragmatically judged the completion of our data collection by the *information power* of the data collected, instead of judgments based on data saturation [60]. *Information power* suggests that the adequacy of qualitative data depends on its relevance, richness, and specificity to the research questions, such that datasets with higher informational value may require fewer participants. Accordingly, data collection was concluded when the accumulated data were deemed sufficiently robust to address the study objectives comprehensively. As we aimed on a specific case of suspicious emails, with a specific target group in mind (VR headset users), and interpretive engagement underpinned by prior theoretical work on suspicious email assessment in the presence of email banner warnings [44], we deemed a sample of around 40 participants (20 per VR headset) with varying experiences and exposures to suspicious emails sufficient to provide information power for our empirical study. The sample demographics are given in Table I.

To analyze the participants' responses, we followed the steps of the practical guide for doing thematic analysis outlined in [59]. Each of the research members situated themselves both as *insiders* (in the sense that we also had experiences with email sorting through VR headsets) and *outsiders* (in the sense that we have experiences related to how users deal with suspicious emails). Two researchers from the team engaged in a mostly deductive coding process, through multiple rounds, for the purpose of collaboratively gaining richer or more nuanced insights. Whenever necessary, they added new codes for concepts not yet covered by the codebook. Instead of reaching an agreement about every code (codebook listed in Appendix D). Whenever necessary, they added new codes for concepts not yet covered by the codebook. We specifically did not include inter-rater-reliability calculations in our process, as our goal was to freely explore diverse topics associated with user experiences with suspicious email while using the VR headsets.

TABLE I: Survey Demographic Distribution

	Vision Pro	Quest 3
Gender Distribution		
Male	11	16
Female	9	4
Race/Ethnicity		
Asian	12	14
White	1	5
Latinx	3	1
Black	3	0
More than One	1	0
Age		
18-19	1	0
20-24	12	14
25-29	6	2
30-34	1	3
35+	0	1

We then shifted our focus from codes to themes in order to develop the patterns or meaning across our dataset and cluster the codes around central organizing concepts about email sorting through VR headsets. We first generated initial themes, then, working through a thematic mapping, we developed and reviewed the resultant themes. The continuous analytical refinement enabled us to define and name the themes. Lastly, we wrote our results around the themes, selecting data extracts (in order of participation and **A** denoting Apple Vision Pro; **M** denoting Meta Quest 3) to evidence our claims and allow one to independently judge the fit between the data and our understanding and interpretation of them.

IV. Results

The goal of our study was not to quantitatively measure the success rate of phishing or spam but more so to bring the outcomes of the email correspondence task sorting into conversation with how VR headset users access emails and decide upon them from an immersion point of view, given that the email interface – including the banner warnings – is naturally designed for traditional desktop or mobile computing experiences. Therefore, we developed three themes with their own central organizing concepts, corresponding to each of our three research questions.

A. RQ1: Immersive Email Assessment

1) Suspicious Email Warnings Encounters: The full breakdown of the suspicious email warning encounters per VR headset type is shown in Table II. More than half of the participants in each group ***encountered*** the general spam banner warning (Figure 5) as they sorted through emails in their spam folder. The "invoice attachment" email was flagged as a potentially dangerous phishing email (Figure 8) for one participant using the Apple Vision Pro and one using the Meta Quest 3. One Apple Vision Pro participant and one Meta

Quest 3 participant encountered the email banner warning that notified users about hidden images in the message (Figure 6).

One of the participants who encountered the "invoice attachment" email saw the report phishing banner instead (Figure 9). Another participant blocked the email address that the *false positive* suspicious email (Figure 10) came from prior to the interview. When sorting their email, they observed a blocked sender warning, as shown in Figure 7. Referring to the service, **P15M** stated: "*I did block them because I didn't need them (AWS), but my email didn't get released from their data, I guess; It says because you have blocked that site, so it's in the spam folder, and it gives me the option to unblock the sender.*"

TABLE II: Suspicious Email Warnings Encountered

Warnings	Vision Pro	Quest 3
Spam Email	11	13
Phishing Email	1	1
Images Hidden	1	1
Report Phishing	1	0
Block Sender	0	1
No warning	6	4

Ten participants were presented but nonetheless ***failed to notice the interactive banner warnings*** in the first place for both of the *false positive* suspicious emails. To protect participants' privacy, we were not able to see what they were seeing through the VR headsets, access their Gmail settings, or view any rules they may have set up. This limited our ability to determine why the participants were not getting the interactive banner warnings in these cases or if they only failed to notice the warning. Some of the participants were confused by the inconsistency of the warning banners and the fact that not all emails in their spam folders have warnings assigned to them. For example, **P11A** encountered a marketing email that they "*wanted it to go to spam; Usually, I get a warning, but now there is none.*" Even though they found the *false positive* suspicions email with an attachment in their spam folder, **P13A** commented, "*it doesn't have any warnings, and I'm glad it went here; I wouldn't have really opened it, anyway.*"

2) Cues for Accessing Suspicious Emails: Our participants said they usually relied on elements in the email itself to determine if it was spam or phishing, as shown in Table III (further broken down in Table IV). The ***context*** of the email (the pretext and the circumstances in which it was sent) was the most dominant cue that our participants relied on when sorting suspicious emails without being affected by the immersiveness or the type of VR headset they used. Here, participant **P7A** stated that emails where "*the subject line has too many exclamations, or the message required urgent attention to something*" are dead giveaways of a phishing email. The second most cited cue was the ***unknown sender***, in addition to other cues. For example, **P15M** pointed to "*the sender's email address, and also the subjects and the attachments*" as the three elements that indicate deception.

TABLE III: Dealing with Suspicious Emails

Assessment Method	Structure		Logic		Grammar	
Spam Email	10	11	5	6	5	6
Phishing Email	1	1	0	0	0	0
Images Hidden	1	0	0	1	1	0
Report Phishing	1	0	0	0	0	0
Block Sender	0	1	0	0	0	0
No warning	6	3	3	3	0	1

The third most dominant cue was the ***interactive warnings*** themselves. **P20M** indicated that the banner "*gets me right into the mindset to think about whether or not the email is spam.*" Our participants also relied on the ***presence (or absence) of images*** in the email body to determine if an email could be spam or phishing. Participant **P2A** was concerned that an email may be dangerous when "*it appears that the sender did not finish putting in all the images.*" Participants also used the ***formatting*** of the email body or "*the way sentences were structured, written, and organized*" (**P9A**) to notice that a suspicious email deviates from a usual message format with a greeting, a main part, and a signature element. Some indicated that they assess the ***links*** in an email in detail. For example, participant **P11M** felt that an email containing a link with a domain that seems "*random, long, and has dispersed special characters*" is a clear sign of phishing.

They identified scenarios with improbable situations, indicating they considered an email phishing if the sender said, "*I'm in danger; I need money; I'll loan you money first; They randomly want to give away things*" (**P5M**). Other participants found an email concerning when these two deception components were used together, for example, "*the emails are like really pushy saying you're pre-approved for a credit card, or you are automatically entered in this competition*" (**P9A**). Participants who encountered no warning used logical cues as often as email elements, identifying an email as suspicious as it was "*pushing urgency by saying that something happened, even though it didn't*" (**P9M**).

Our participants also found ***grammatical cues*** as helpful as logical ones. They encompassed not only grammatical mistakes, but misspellings and out-of-order symbols. Those who used grammatical cues scrutinized the details of the text within the email for "*spelling, font, things like that, special symbols*" (**P17A**) and were tipped off "*if there's typos, that's a big red flag*" **P12M**. Others generalized that they "*don't think the hackers have good grammar*" (**P3M**) and saw this as a way to determine if an email sender was attempting to

TABLE IV: Suspicious Emails – Cues

Cues	Context		Sender		Warning		Images		Formatting		Attachments		Links	
		∞		∞		∞		∞		∞		∞		∞
Spam Email	9	12	4	4	2	5	6	4	3	5	0	0	1	1
Phishing Email	1	1	1	1	1	1	0	0	0	1	0	1	0	0
Images Hidden	1	0	1	0	1	1	1	1	1	0	0	0	0	0
Report Phishing	1	0	1	0	1	0	1	0	0	0	0	0	0	0
Block Sender	0	0	0	1	0	1	0	0	0	0	0	0	0	0
No warning	5	2	3	0	0	0	0	0	0	0	2	0	0	0

be deceitful.

B. RQ2: Immersive Email Action

1) Avoiding a Phish/Spam: During the session, participants were asked about the actions they would take with spam emails. Because the *false positive* suspicious email in either variant was sent prior to their participation session, some participants had already taken action on this email, but they recalled what action they took. For example, **P10M** knew they had deleted our email because they "*make sure that all spam and all my junk is emptied regularly*." Table V shows the actions they took based on the warning banner message they encountered. Upon reviewing the *false positive* email, the majority were satisfied with the email going to their spam folder. Some participants who encountered the spam warnings conducted a ***cursory investigation***, saying they would "*open up an email, but [they] won't really dive too deep into it if there's something sketchy or off with it*" (**P14M**).

The participants who encountered the phishing email warning took additional precautions when evaluating the emails and elected ***not to interact*** with them. One of these participants, **P11M**, stated that when they see that banner, "*usually [they] don't click on it; [they] just ignore the email altogether*." The participants who encountered the "hidden images" warning indicated that they ***wouldn't interact*** with the email, and they found it convenient. One of them, **P17A** stated, "*I like that the banner makes you have to opt-in to view images; No skin off my back to click the little button if I think it's a legitimate email.*" The participant who encountered the report phishing banner warning indicated that they "*would say it makes you think twice about logging or clicking on any links*" (**P19A**) and opted not to interact with the email as well. In both VR groups, the participants who ***did not encounter any warning*** during the sorting task indicated that they would be more likely to closely inspect and interact with the elements of the email in order to "*check to see how legit it is*" (**P9M**).

2) Falling for a Phish: Three of the participants who encountered our test *false positive* suspicious emails ***clicked*** on the link or opened the attachment. Two Apple Vision Pro participants clicked on the link in the email, which brought them to a legitimate Amazon Web Services (AWS) page (as the email was legitimate in nature). They acknowledged that they did so and stated shortly that they did it "*unintentionally*" (**P15A**), but both of them were hesitant to go into more detail. We did not probe them further as both of them felt uncomfortable that they fell for the phish (we observed their body language, avoiding eye contact, and looking to proceed with the other questions in the interview). Instead, we shared our experience pilot testing the Apple Vision Pro headset, feeling it very ***hypersensitive when clicking on links*** in general. Both participants acknowledged that this is the reason why they might have fallen for the phish, adding that "*getting used to it*" as an interface might help, but to be on the safe side, they noted that they would "*probably use the phone for emails as a fallback while using the VR*" (**P8A**) for now.

One Meta Quest 3 participant erroneously opened our blank Word document attached to the email, vocalizing what appeared to be an accidental misclick as "*Oh, sh*t! I actually opened the document!*" (**P2M**). Discussing the specific immersive experience that led them to fall for the phish, the participants referred to the ***lack of ergonomic precision*** of the VR headset when navigating the Gmail web interface. Reflecting that "*it doesn't happen that often to click by mistake on a routine action such as checking an email*," the participant pointed to the spatial vastness characteristic of immersive environments as "*a lot of space where one could misclick when doing multiple things at once*" as the looking and tapping is yet in perfect, seamless synchronization.

C. RQ3: Immersive Usable Security

1) Warning Banner Usability: While most participants heeded the banner warnings, many said they found them to be only partially usable. Half of the participants indicated that they had to go into their spam folder to look for important emails, including one-time passwords, newsletters they opted in for, and contacts from potential employers, resulting in a need to assess the legitimacy of the emails in their spam folder. They thought it was helpful to get some kind of warning but the warning banner could be improved to help users better understand what elements of the email to look at and what actions to take with the email, especially when

TABLE V: Actions Taken During Email Sorting

Actions	Ignore		Investigate		Unsubscribe		Delete		Report		Block	
Spam Email	8	8	2	2	1	2	0	1	0	0	0	0
Phishing Email	1	1	0	0	0	0	0	0	0	0	0	0
Images Hidden	1	1	0	0	0	0	0	0	0	0	0	0
Report Phishing	1	0	0	0	0	0	0	0	0	0	0	0
Block Sender	0	0	0	0	0	0	0	0	0	0	0	1
No warning	1	0	2	1	1	1	0	2	1	0	1	0

multitasking in an immersive context. Table VI shows the usability recommendations made by our participants.

Participants who encountered the general spam warning were underwhelmed by the message and color coding they encountered. For example, **P8M** reflected that the warning should be ***more alerting*** or "*say, 'this is definitely spam.' because [they] didn't feel that [they] have to be careful*" with the email. Participants also said that the color of the banner could be updated to fit the immersiveness of the VR, as colors could be used as a ***risk indicator***. Participant **P16M** suggested "*that the color coding would definitely help because it can be tough to see the difference in there, especially during multitasking*." Here, participant **P17A** felt that in a VR environment, it would be fitting and useful to have a full palette of warnings, for example, include a "*green indicator about legitimate emails that's not necessarily a banner but something small that people won't ignore over time*." Participant **P13A** worried about ***vulnerable populations***, as the color coding would help "*make the suspiciousness more obvious, maybe because I know a lot of people, especially my dad, who's old, so he would definitely press something if he had to open an email through a VR headset*" (**P13A**).

The overall satisfaction with Gmail's sorting and assignment of banners was low. Most of the participants indicated that they regularly had spam go to their inbox or important emails go to their spam, and most felt that the banner warnings were assigned inconsistently. Participant **P20M** suggested that anyone wanting to use their email through a VR headset should go through an "***explicit training*** *period so they train the engine to respond according to their interactions.*" As the immersiveness is the key feature that would accelerate the adoption of VR headsets, participant **P18M** reasoned that such training could be good in the context of "*allowing people to maneuver email messages with gestures like they would do with real mail*" (alluding to the action of tearing spam mail or physically discarding it). Some thought that a "***three-dimensional pop-up*** *in the VR headset would help*" as it would be helpful to add the ability to drag, scale, position, and orient various windows simultaneously with both hands (**P7M**). Participants were unsure if it the ***warning multidimensionality*** was the responsibility of Gmail, the VR headset, or a shared one. Here, participant **P11M** surmised that "*if something is labeled as spam in my inbox, I can see there would be ways, scaling or immediate decluttering for the headset to make it harder to click on something in the spam or bring your focus that you're about to click on something*."

2) Virtual Reality Usable Security: While performing the email sorting tasks, participants in both groups worried about the hypersensitivity and precision involved in clicking using a VR headset, accurately predicting the accidental ***misclicks*** that actually occurred. As shown in Table VII, there were differences between the Apple Vision Pro and the Meta Quest 3 recommendations based on the device used. The Apple Vision Pro uses vision tracking, and to click on something using this VR headset, the user looks at the object they would like to select and then taps their index finger and thumb together to select it. The Meta Quest 3, on the other hand, has two controllers with buttons. The user holds the controllers in their hands, points the cursor at the object , and then clicks the trigger button on the controller to make a selection.

The Apple Vision Pro participants stated that "*the touch is a little too sensitive*" (**P8A**) and that perhaps even after calibration, it would create situations where, in the words of participant **P1A**, it's "*hard to zero-in on a single button, and I would probably accidentally move my head and click on another thing I don't mean to.*" The Meta Quest 3 participants commented on the noticeable glitches with the precision fix of the VR headset. Participant **P9M** confessed, "*[they] almost clicked three times on random other buttons out there*." Speaking for the overall experience with the Meta Quest 3, participant **P11M** explained that...:

> "*...you have to move the cursor around with your hand, and sometimes that's not as accurate as using a mouse or your finger, so I can see that you could actually then maybe click a bad link from a spam message accidentally. I suppose there must be ways to make the friction, feedback, and response configurable so it feels more natural*."

Two participants from each group said that the screen setup is too distracting to be able to trust themselves when

TABLE VI: Warning Banner Usability Recommendations

Recommendations	Color Coding		Algorithm Control		Message Content		Pop-up		Risk Indicator	
Spam Email	4	2	2	2	1	5	0	1	0	1
Phishing Email	1	0	0	0	1	0	0	1	1	0
Images Hidden	1	0	0	0	0	0	1	0	1	0
Report Phishing	1	0	0	0	0	0	0	0	0	0
Block Sender	0	0	0	0	0	0	0	0	0	1
No warning	0	1	4	1	1	0	0	0	0	0

determining phishing emails while performing other tasks. For example, **P1M** said, "*with a VR headset you have more going on, so it's easier not to read a warning as thoroughly, as your focus might be on another task or orientation*." In response to the multitasking, participant **P1M** recommended:

> "*When you open your browser or email client, everything else should be dimmed down by default, so it creates kind of a place where the focal point of your attention should be just the email. When I was going through my emails, everything else remains in full focus and brightness, so I was easily distracted and could have very much clicked on something.*"

TABLE VII: Virtual Reality Usability Recommendations

	Sensitive Clicking	Precise Clicking	Multitasking	Email App
Vision Pro	5	0	1	0
Quest 3	0	4	1	3

While the Apple Vision Pro has a dedicated email application (Figure 1), Meta Quest 3 offered only the Gmail Chrome web browser to access participants' inboxes (Figure 2). We did not observe any specific differences between the app and the browser, but we probed the participants in the Meta Quest 3 group about the experience of sorting the correspondence through a browser. Three of them felt that their challenges with navigation and the potential to misclick might be resolved with "*an application which is specifically designed for this kind of space, both for work and especially for gaming*" (**P8M**), alluding to natural multitasking productivity scenarios envisioned by Apple and Meta.

V. Discussion

Our study provides empirical evidence that VR's perceptive manipulation possibilities could be misused against victims and lead them to "*misclick*" on a phishing link or attachment. This is consistent with similar findings regarding the lack of intuitive transfer of usable security and privacy interventions within an immersive environment [28], [29], [30]. The perceptive manipulation possibilities of VR, in the context of resilience, are hindered due to the need for users to extend their mental models developed for interactive resistance to security and privacy threats [61]. The gesture discoverability, the elicitation of spatial dimension in the interactive sequence of actions when sorting emails, and the shifting focus between detecting deception and avoiding accidental clicking while multitasking [62] are some of the new and *unfamiliar* affordances that users need to first internalize for full immersion and then conceive as possible avenues of social engineering victimization. The immersive multitasking also plays a part in the sudden exposure to security threats as the task representation, spatial and multimodal switching, and the ability for frictionless passthrough parallel tasks (e.g, using a voice assistant to open an email attachment while the user's focus is on another task) [63] also requires security-aware reconceptualization. The traditional security mental models, though, should not just be subject to an unidirectional extension. The natural *cross-reality tasks* — where users switch between VR and desktop or mobile environments [64] – also could lead to user deception (emails combined with text messages etc, links transferred in VR, and so on) so the "*fallback*" approach noted by our participants are worthy of consideration for coordinated, user-centered protection across interactive contexts.

A. Implications: Suspicious Email Warnings

For long, the interplay between phishers/spammers and first-line email detection has been defined by the ability of adversaries to craft emails with clever formatting, spelling, keyword selection, and sender spoofing [42]. We expect these tactics to remain, but the immersiveness itself offers an opportunity to expand the space for experimenting further with deceptive affordances. For example, adversaries could include images, fonts, and animation in emails that might distract a user away from the warning, the link, and the overall email. The concept of *external* distractions is already available in medical VR applications aiming to reduce patients' pain and anxiety [65], and we believe that it is not unlikely that an adversary would resort to *internal* distractions as a means of deception. Distraction is such an important susceptibility factor that advanced

suspicious email warnings incorporate a temporal component or a delay of a few seconds in rendering the email content in order to eliminate possible in-situ distractions [50], [66]. In a multitasking environment such as VR, such delays might not be possible to prevent phishing/spamming distractions, or worse, they could be of an adversarial advantage.

B. Virtual Reality Deceptive Patterns

To operationalize our findings in the context of the deceptive possibilities of VR, we cross-evaluated the themes and manipulative mechanisms identified by both Hadan et al. [21] and Krauß et al. [20] in Appendix F.

Regarding the *adverse effects on user experience*, the use of a VR headset for multitasking involving email sorting tasks could be misused when spatially presenting a link or attachment preview that obscures traditional phishing cues [67], even if users – like participant **P9M** – habitually check the links in emails in a traditional interactive context. These effects are equally relevant for deception as they could convey a heightened realism of the email communication. For example, in VR, a QR code send in an email could be decoupled from the email body and spatially present to the user in the 3D environment corresponding to the pretext (a document signature, a credit card payment, etc [68]) so users pay attention to completing this task instead of inspecting the potentially phishing URL embedded in the QR code [69], [70].

In terms of *obscuring reality and disguising risks*, other tasks might be placed in a way that obscures only the suspicious banners or even manipulates the usual color schemes of the banners themselves [26]. For example, the current palette of banner warnings shown in the Appendix A could be either replaced by a green overlay color, or, even more convincing, with a green glow to indicate the safety of an email. Gesture-wise, the *data fuels privacy risks and manipulation*, i.e., the very interaction with emails that mimics balling up and tossing away an envelope in a bin, could reveal the current focus of a user – for example, cleaning up their spam inboxes, like many of our participants indicated – and offer an opportunity for a timed follow-up spear phishing email. Our results offer the first evidence of the *interaction insecurity increases manipulation risk* threat as a possibility where an adversary – in the absence of VR-specific warnings – could intentionally manipulate input sensitivity and gesture precision to force users to open a suspicious link or attachment.

This form of *ergonomic vulnerabilities amplify manipulation*, could create a multiplying effect in immersive email interactions. Adversaries could not just manipulate the interaction with links/attachments but also manipulate any email-specific gestures and affordances in a similar way. This is evident considering the possibility of a pervasive *perception hacking* and *imbalancing options* where an adversary launches a 'gesturejacking' and 'pixelnapping' attack in VR by embedding the malicious payloads behind seemingly innocuous interactive renditions [71], [23]. Regarding *hyperpersonalization* in the context of email deception, a conceivable threat is the potential use of email personification with holographic recreations of

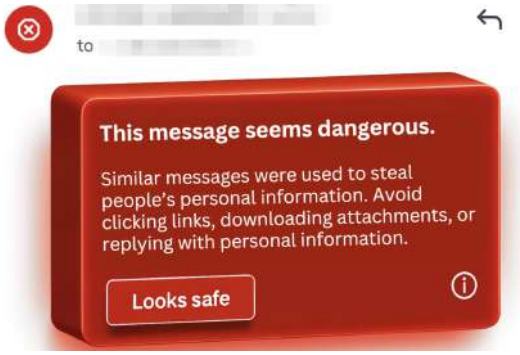

Fig. 3: 3D phishing warning

senders or pretexts used in the email to render more persuasive conditions under which the user might be more inclined to follow through with the email's request for login or opening an attachment.

C. Countering Suspicious Emails in VR

The warning banners we evaluated, and are currently available to the users of Gmail, are effectively two-dimensional superimposed images when displaying the email header and body. The availability of a third dimension in VR offers an opportunity to explore designs of suspicious email warnings that make use of the space as well as the multimodal nature of immersiveness. Based on our participants' recommendations and the nascent work on usable security warnings for immersive interactions, we offer a couple of proposals, we intend to implement and evaluate with VR users in our follow up work: (i) a 3D warning banner with an integrated auditory feedback; and (ii) a 2D warning banner with glow and scale up, per the affordances proposed in [26]. The first one is shown in Figure 3 (for demonstration, we used the phishing email banner). We envision any banner warning to materialize as a three-dimensional box (other shapes are possible) that, instead of a "pop-up" action, slides out as an extension in space to draw the user's attention (directions and spatial positions are subject to configuration). Users here would have the option to allow 3D banners only, or pair them with a particular warning sound (e.g., a beep, alert, or a tone) [72] or a custom speech as a warning (for example, *warning, this email needs attention*). This design, per our participants' suggestions, could well be customized to replace the banners with simple 3D indicators or tooltips incorporating the standard warning signage (e.g., check marks, exclamation marks, stop signs, etc.) that are shown to work in the context of avoiding suspicious emails [25].

The second design proposal is shown in Figure 4. The two-dimensional rendition of the email display is retained here for the sake of minimizing distraction in a productivity-oriented multitasking environment, and instead, the warning is conveyed through a red encircling glow, shown to effectively alert users on potential deception in VR [26]. An optional implementation of this approach is to position a suspicious email in VR at a different distance from regular emails.

One option is to scale it up and place it closer to the focal point of the user to implicitly draw their attention away from other concurrent tasks, though coming with the trade-off of interrupted immersion on the account of more mindful deception evaluation. If the immersion warrants, then an opposite configuration is also possible where the glow is retained, but the email itself is scaled down and positioned farther from the focal point, but with a ratio to nevertheless allow for noticeability on the user side [73].

Both of the proposed designs come with slightly *slower-than-the-usual sensitivity* and *affordance precision (towards focused previews)* for opening the suspicious emails' URLs and attachments compared to emails deemed safe as a deliberate episodic friction shielding from the VR-specific 'misclicking' susceptibility identified in our study. This is an open design choice that allows for incorporating various gestures in addition (or replacing) the usual clicking or tapping, in a VR specific email client, so users are 'nudged' to interact in varying ways with different types of emails (e.g., a tossing mail gesture for spam, tearing a paper mail, hand zooming for a link preview).

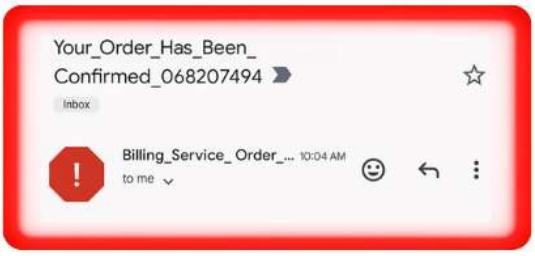

Fig. 4: Red glow phishing warning

D. Limitations

The use of a realistic scenario imposes several limitations pertaining to our study, coming from the sample size, the VR headset chosen, Gmail as an email provider, and the format of the warnings, all of which prevent the generalization of the results. Our participants were university students, and we see this as an expected limitation imposed on any empirical VR research, at least for the time being, due to the need to manage expensive VR headsets, especially for mild deception and observational studies like ours that demand close proximity of the researchers for the purpose of safeguarding and prevention of harm. Students also may also be more proficient with VR technology and may be more aware of the risks of phishing emails than the average user. The time and space of participation were also a limitation, as we used a shared collaborative space. The use of this controlled space with a researcher present has the potential to introduce an observer effect and influence the participants' behavior. The research setup might have primed our participants, but it was a necessary compromise to introduce and test a methodology adapted to the immersiveness of the VR environments. The use of Gmail as an email provider created limitations because we cannot fully generalize our results to other email platforms. A structural limitation is the choice of using the participants' spam folders instead of their inboxes. We were not permitted by our IRB to phish, spam, or tamper with Gmail's filtering rules due to greater than minimal risk to them. Another limitation comes from the choice of the *false positive* emails we used. Similarly, a limitation comes from the choice of spam emails our participants arbitrarily selected in our study.

VI. Conclusion

To the best of our knowledge, this study is the first to empirically investigate user interaction with suspicious emails in VR. Using an innovative methodological approach that allows for results with high ecological validity (i.e., users evaluated suspicious emails sent to their *own* email address, and in their *own* inboxes), we found that the immersive interaction itself is conducive to deception susceptibility for suspicious emails that users might otherwise avoid on a smartphone or computer. In our study, 20 Apple Vision Pro users and 20 Meta Quest 3 users sorted their *own* Gmail spam folders via a VR headset. While our participants utilized the warning banners, they felt they needed improvements to be fully transferable in an immersive context. Participants also experienced unique VR-related interaction perception manipulations, which although unintended, led three of them to fall for our test suspicious email by clicking a link or opening an attachment. We operationalized this evidence to offer a comprehensive take on the deceptive patterns associated with VR that could be utilized for immersive social engineering. Using the feedback from our participants' interactions, we offer several design recommendations for dedicated VR-based suspicious email warnings specifically tailored to counter immersive phishing and spamming threats.

References

[1] S. Stephenson, B. Pal, S. Fan, E. Fernandes, Y. Zhao, and R. Chatterjee, "SoK: Authentication in augmented and virtual reality," in *2022 IEEE Symposium on Security and Privacy (SP)*, 2022, pp. 267–284. [Online]. Available: https://doi.org/10.1109/SP46214.2022.9833742

[2] G. Freeman, D. Acena, N. J. McNeese, and K. Schulenberg, "Working together apart through embodiment: Engaging in everyday collaborative activities in social virtual reality," *Proceedings of the ACM on Human-Computer Interaction*, vol. 6, no. GROUP, Jan 2022. [Online]. Available: https://doi.org/10.1145/3492836

[3] Y. Fu, Y. Hu, and V. Sundstedt, "A systematic literature review of virtual, augmented, and mixed reality game applications in healthcare," *ACM Transactions on Computing for Healthcare (HEALTH)*, vol. 3, no. 2, Mar 2022. [Online]. Available: https://doi.org/10.1145/3472303

[4] T. Drey, P. Albus, S. der Kinderen, M. Milo, T. Segschneider, L. Chanzab, M. Rietzler, T. Seufert, and E. Rukzio, "Towards collaborative learning in virtual reality: A comparison of co-located symmetric and asymmetric pair-learning," in *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, ser. CHI '22. New York, NY, USA: Association for Computing Machinery, 2022. [Online]. Available: https://doi.org/10.1145/3491102.3517641

[5] A. Ward, S. Avula, H.-F. Cheng, S. M. Sarwar, V. Murdock, and E. Agichtein, "Searching for products in virtual reality: Understanding the impact of context and result presentation on user experience," in *Proceedings of the 46th International ACM SIGIR Conference on Research and Development in Information Retrieval*, ser. SIGIR '23. New York, NY, USA: Association for Computing Machinery, 2023, pp. 2359–2363. [Online]. Available: https://doi.org/10.1145/3539618.3592057

[6] Atopia, "Who's really using VR these days? Six data-driven insights into today's VR user demographic," Oct 2023. [Online]. Available: https://medium.com/@annabell_37704/whos-really-using-vr-these-days-six-data-driven-insights-into-today-s-vr-user-demographic-422372a75c8c

[7] D. Frankel, "While more than half of Americans are interested in Apple's $3,500 Vision Pro, 76% say they have no intention of buying one," Apr 2024. [Online]. Available: https://www.yahoo.com/tech/while-more-half-americans-interested-161909011.html

[8] M. Gonzalez-Franco and A. Colaco, "Guidelines for productivity in virtual reality," *Interactions*, vol. 31, no. 3, pp. 46–53, May 2024. [Online]. Available: https://doi.org/10.1145/3658407

[9] Apple, "Apple Vision Pro." [Online]. Available: https://www.apple.com/apple-vision-pro/

[10] S. Hayden, "Facebook lays out the future of work and productivity on Quest," Sep 2020. [Online]. Available: https://www.roadtovr.com/facebook-future-work-productivity-quest-2/

[11] J. Hart, "I tried working a full day wearing Apple's Vision Pro. It's the ultimate WFH device." [Online]. Available: https://www.businessinsider.com/using-apple-vision-pro-for-the-day-productivity-2024-2

[12] S. Axon, "I worked exclusively in vision pro for a week-here's how it went," Mar 2024. [Online]. Available: https://arstechnica.com/gadgets/2024/03/i-worked-exclusively-in-vision-pro-for-a-week-heres-how-it-went/

[13] M. Miller, "I used the Apple Vision Pro for my 8-hour work day, and it left me wanting more," Feb 2024. [Online]. Available: https://www.zdnet.com/article/i-used-the-apple-vision-pro-for-my-8-hour-work-day-and-it-left-me-wanting-more/

[14] R. Cheng, N. Wu, M. Varvello, E. Chai, S. Chen, and B. Han, "A first look at immersive telepresence on Apple Vision Pro," *Proceedings of the 2024 ACM on Internet Measurement Conference*, pp. 555–562, Nov 2024.

[15] K. Makortoff, "No more FOMO: Top firms turn to VR to liven up meetings," Feb 2021. [Online]. Available: https://www.theguardian.com/business/2021/feb/20/no-more-fomo-top-firms-turn-to-vr-to-liven-up-meetings

[16] M. Mcgill, A. Kehoe, E. Freeman, and S. Brewster, "Expanding the bounds of seated virtual workspaces," *ACM Transactions on Computer-Human Interaction (TOCHI)*, vol. 27, no. 3, May 2020. [Online]. Available: https://doi.org/10.1145/3380959

[17] P. Burda, L. Allodi, and N. Zannone, "Cognition in social engineering empirical research: A systematic literature review," *ACM Transactions on Computer-Human Interaction*, vol. 31, no. 2, Jan 2024. [Online]. Available: https://doi.org/10.1145/3635149

[18] D. Lain, K. Kostiainen, and S. Čapkun, "Phishing in organizations: Findings from a large-scale and long-term study," in *2022 IEEE Symposium on Security and Privacy (SP)*, 2022, pp. 842–859.

[19] V. Distler, "The influence of context on response to spear-phishing attacks: An in-situ deception study," in *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, ser. CHI '23. New York, NY, USA: Association for Computing Machinery, 2023. [Online]. Available: https://doi.org/10.1145/3544548.3581170

[20] V. Krauß, P. Saeghe, A. Boden, M. Khamis, M. McGill, J. Gugenheimer, and M. Nebeling, "What makes XR dark? Examining emerging dark patterns in augmented and virtual reality through expert co-design," *ACM Transactions on Computer-Human Interaction*, vol. 31, no. 3, Aug 2024. [Online]. Available: https://doi.org/10.1145/3660340

[21] H. Hadan, L. Choong, L. Zhang-Kennedy, and L. E. Nacke, "Deceived by immersion: A systematic analysis of deceptive design in extended reality," *ACM Compututing Surveys*, vol. 56, no. 10, May 2024. [Online]. Available: https://doi.org/10.1145/3659945

[22] A. H. Mhaidli and F. Schaub, "Identifying manipulative advertising techniques in XR through scenario construction," in *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, ser. CHI '21. New York, NY, USA: Association for Computing Machinery, 2021. [Online]. Available: https://doi.org/10.1145/3411764.3445253

[23] H. Lee, J. Lee, D. Kim, S. Jana, I. Shin, and S. Son, "AdCube: WebVR ad fraud and practical confinement of Third-Party ads," in *30th USENIX Security Symposium (USENIX Security 21)*. USENIX Association, Aug 2021, pp. 2543–2560. [Online]. Available: https://www.usenix.org/conference/usenixsecurity21/presentation/lee-hyunjoo

[24] J. Petelka, Y. Zou, and F. Schaub, "Put your warning where your link is: Improving and evaluating email phishing warnings," in *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, ser. CHI '19. New York, NY, USA: Association for Computing Machinery, 2019, pp. 1–15. [Online]. Available: https://doi.org/10.1145/3290605.3300748

[25] M. Volkamer, K. Renaud, B. Reinheimer, and A. Kunz, "User experiences of torpedo: Tooltip-powered phishing email detection," *Computers & Security*, vol. 71, pp. 100–113, 2017.

[26] A. Mengascini, R. Weil, A. Walle, J. Steimle, and G. Pellegrino, "Exploring the design space for security warnings in immersive environments," in *2025 IEEE 10th European Symposium on Security and Privacy (EuroS&P)*, 2025, pp. 227–250.

[27] B. Liu, V. S. Simhadri, and X. Zhang, "Hunting insecure UI properties in extended reality," in *Proceedings of the Twenty-Sixth International Symposium on Theory, Algorithmic Foundations, and Protocol Design for Mobile Networks and Mobile Computing*, ser. MobiHoc '25. New York, NY, USA: Association for Computing Machinery, 2025, pp. 462–467. [Online]. Available: https://doi.org/10.1145/3704413.3765301

[28] E. Kablo, Y. Last, P. A. Cabarcos, and M. Volkamer, "The (un)suitability of passwords and password managers in virtual reality," 2025. [Online]. Available: https://arxiv.org/abs/2503.18550

[29] V. Paneva, V. Winterhalter, F. Augustinowski, and F. Alt, "User understanding of privacy permissions in mobile augmented reality: Perceptions and misconceptions," *Proceedings of the ACM on Human-Computer Interaction*, vol. 9, no. 5, Sep 2025. [Online]. Available: https://doi.org/10.1145/3743738

[30] E. Kablo, M. Kleber, and P. A. Cabarcos, "PrivaCI in VR: Exploring perceptions and acceptability of data sharing in virtual reality through contextual integrity," in *34th USENIX Security Symposium (USENIX Security 25)*, 2025, pp. 1531–1548.

[31] F. Roesner, T. Kohno, and D. Molnar, "Security and privacy for augmented reality systems," *Communications of the ACM*, vol. 57, no. 4, pp. 88–96, Apr 2014. [Online]. Available: https://doi.org/10.1145/2580723.2580730

[32] C. M. Gray, Y. Kou, B. Battles, J. Hoggatt, and A. L. Toombs, "The dark (patterns) side of ux design," in *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, ser. CHI '18. New York, NY, USA: Association for Computing Machinery, 2018, pp. 1–14. [Online]. Available: https://doi.org/10.1145/3173574.3174108

[33] W.-J. Tseng, E. Bonnail, M. McGill, M. Khamis, E. Lecolinet, S. Huron, and J. Gugenheimer, "The dark side of perceptual manipulations in virtual reality," in *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, ser. CHI '22. New York, NY, USA: Association for Computing Machinery, 2022. [Online]. Available: https://doi.org/10.1145/3491102.3517728

[34] R. Düzgün, N. Noah, P. Mayer, S. Das, and M. Volkamer, "SoK: A systematic literature review of knowledge-based authentication on augmented reality head-mounted displays," in *Proceedings of the 17th International Conference on Availability, Reliability and Security*, ser. ARES '22. New York, NY, USA: Association for Computing Machinery, 2022. [Online]. Available: https://doi.org/10.1145/3538969.3539011

[35] A. A. Arafat, Z. Guo, and A. Awad, "VR-Spy: A side-channel attack on virtual key-logging in VR headsets," in *2021 IEEE Virtual Reality and 3D User Interfaces*, 2021, pp. 564–572.

[36] S. R. K. Gopal, D. Shukla, J. D. Wheelock, and N. Saxena, "Hidden reality: Caution, your hand gesture inputs in the immersive virtual world are visible to all!" in *32nd USENIX Security Symposium (USENIX Security 23)*. Anaheim, CA, USA: USENIX Association, Aug 2023, pp. 859–876. [Online]. Available: https://www.usenix.org/conference/usenixsecurity23/presentation/gopal

[37] H. Khalili, A. Chen, T. Papaiakovou, T. Jacques, H.-J. Chien, C. Liu, A. Ding, A. Hass, S. Zonouz, and N. Sehatbakhsh, "Virtual keymysteries unveiled: Detecting keystrokes in VR with external side-channels," in *2024 IEEE Security and Privacy Workshops (SPW)*, 2024, pp. 260–266.

[38] S. Luo, A. Nguyen, H. Farooq, K. Sun, and Z. Yan, "Eavesdropping on controller acoustic emanation for keystroke inference attack in virtual reality," in *The Network and Distributed System Security Symposium (NDSS)*, 2024.

[39] C. Slocum, Y. Zhang, N. Abu-Ghazaleh, and J. Chen, "Going through the motions: AR/VR keylogging from user head motions," in *32nd USENIX Security Symposium (USENIX Security 23)*. Anaheim, CA, USA: USENIX Association, Aug 2023, pp. 159–174. [Online]. Available: https://www.usenix.org/conference/usenixsecurity23/presentation/slocum

[40] H. Wang, Z. Zhan, H. Shan, S. Dai, M. Panoff, and S. Wang, "GAZEploit: Remote keystroke inference attack by gaze estimation

from avatar views in VR/MR devices," in *Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '24. New York, NY, USA: Association for Computing Machinery, 2024, pp. 1731–1745. [Online]. Available: https://doi.org/10.1145/3658644.3690285

[41] Z. Yang, C. Y. Li, A. Bhalla, B. Y. Zhao, and H. Zheng, "Inception attacks: Immersive hijacking in virtual reality systems," *arXiv preprint arXiv:2403.05721*, 2024.

[42] Verizon, "Data Breach Investigations Report 2023," 2023. [Online]. Available: https://www.verizon.com/business/resources/Tabb/reports/2023-data-breach-investigations-report-dbir.pdf

[43] R. Pourmohamad, S. Wirsz, A. Oest, T. Bao, Y. Shoshitaishvili, R. Wang, A. Doupé, and R. A. Bazzi, "Deep dive into client-side anti-phishing: A longitudinal study bridging academia and industry," in *Proceedings of the 19th ACM Asia Conference on Computer and Communications Security*, ser. ASIA CCS '24. New York, NY, USA: Association for Computing Machinery, 2024, pp. 638–653. [Online]. Available: https://doi.org/10.1145/3634737.3657027

[44] A. Franz, V. Zimmermann, G. Albrecht, K. Hartwig, C. Reuter, A. Benlian, and J. Vogt, "SoK: Still plenty of phish in the sea — A taxonomy of User-Oriented phishing interventions and avenues for future research," in *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*. USENIX Association, Aug 2021, pp. 339–358. [Online]. Available: https://www.usenix.org/conference/soups2021/presentation/franz

[45] Google, "Advanced phishing and malware protection," 2023. [Online]. Available: https://support.google.com/a/answer/9157861?hl=en

[46] Microsoft, "Overview of the junk email filter," 2023. [Online]. Available: https://support.microsoft.com/en-us/office/overview-of-the-junk-email-filter-5ae3ea8e-cf41-4fa0-b02a-3b96e21de089

[47] "Fighting phishing with smarter protections." [Online]. Available: https://blog.google/technology/safety-security/fighting-phishing-smarter-protections/

[48] M. F. Veit, O. Wiese, F. L. Ballreich, M. Volkamer, D. Engels, and P. Mayer, "SoK: The past decade of user deception in emails and today's email clients'susceptibility to phishing techniques," *Computers & Security*, vol. 150, pp. 3449–3464, 2025.

[49] R. Wash, "How experts detect phishing scam emails," *Proceedings of the ACM on Human-Computer Interaction*, vol. 4, no. CSCW2, Oct 2020. [Online]. Available: https://doi.org/10.1145/3415231

[50] M. Mossano, O. Kulyk, B. M. Berens, E. M. Häußler, and M. Volkamer, "Influence of URL formatting on users' phishing URL detection," in *Proceedings of the 2023 European Symposium on Usable Security*, ser. EuroUSEC '23. New York, NY, USA: Association for Computing Machinery, 2023, pp. 318–333. [Online]. Available: https://doi.org/10.1145/3617072.3617111

[51] A. Kanaoka and T. Isohara, "Enhancing smishing detection in AR environments: Cross-device solutions for seamless reality," in *2024 IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops (VRW)*, 2024, pp. 565–572.

[52] P. Jansen and F. Fischbach, "The social engineer: An immersive virtual reality educational game to raise social engineering awareness," in *Extended Abstracts of the 2020 Annual Symposium on Computer-Human Interaction in Play*, ser. CHI PLAY '20. New York, NY, USA: Association for Computing Machinery, 2020, pp. 59–63. [Online]. Available: https://doi.org/10.1145/3383668.3419917

[53] S. Bakker, "Immersive virtual reality and cybersecurity: Combatting social engineering in a healthcare context," July 2024. [Online]. Available: http://essay.utwente.nl/100811/

[54] F. Sharevski and A. Zeidieh, "Assessing suspicious emails with banner warnings among blind and Low-Vision users in realistic settings," in *33rd USENIX Security Symposium (USENIX Security 24)*. Philadelphia, PA, USA: USENIX Association, Aug 2024, pp. 2083–2100. [Online]. Available: https://www.usenix.org/conference/usenixsecurity24/presentation/sharevski

[55] OpenPhish, "OpenPhish database." [Online]. Available: https://openphish.com/phishing_database.html

[56] M. S. Wogalter, V. C. Conzola, and T. L. Smith-Jackson, "Research-based guidelines for warning design and evaluation," *Applied Ergonomics*, vol. 33, no. 3, pp. 219–230, 2002. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0003687002000091

[57] S. Vigderman, "Virtual reality awareness and adoption report," Jan 2024. [Online]. Available: https://www.security.org/digital-security/virtual-reality-annual-report/

[58] Cybersecurity and Infrastrucure Security Agency (CISA), "Avoiding social engineering and phishing attacks," 2021. [Online]. Available: https://www.cisa.gov/news-events/news/avoiding-social-engineering-and-phishing-attacks

[59] V. Braun and V. Clarke, *Thematic Analysis: A Practical Guide*. SAGE Publications, 2021.

[60] K. Malterud, V. D. Siersma, and A. D. Guassora, "Sample size in qualitative interview studies: Guided by information power," *Qualitative Health Research*, vol. 26, no. 13, pp. 1753–1760, Jan 2015.

[61] L. J. Camp, "Mental models of privacy and security," *IEEE Technology and Society Magazine*, vol. 28, no. 3, pp. 37–46, 2009.

[62] A. Khurana, M. Glueck, and P. K. Chilana, "Do I just tap my headset? How novice users discover gestural interactions with consumer augmented reality applications," *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, vol. 7, no. 4, Jan 2024. [Online]. Available: https://doi.org/10.1145/3631451

[63] T. Kojic, M. Vergari, M. Warsinke, D. Ali, S. Möller, and J.-N. Voigt-Antons, "Multimodal user experience in extended reality: Exploring hand tracking, voice, and passthrough interactions," in *Proceedings of the 17th International Workshop on IMmersive Mixed and Virtual Environment Systems*, ser. MMVE '25. New York, NY, USA: Association for Computing Machinery, 2025, pp. 8–14. [Online]. Available: https://doi.org/10.1145/3712677.3720459

[64] J. Wentzel, F. Anderson, G. Fitzmaurice, T. Grossman, and D. Vogel, "SwitchSpace: Understanding context-aware peeking between VR and desktop interfaces," in *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems*, ser. CHI '24. New York, NY, USA: Association for Computing Machinery, 2024. [Online]. Available: https://doi.org/10.1145/3613904.3642358

[65] C. Glennon, "Use of virtual reality to distract from pain and anxiety," vol. 45, no. 4, pp. 545–552, 2018. [Online]. Available: https://pubmed.ncbi.nlm.nih.gov/29947355/

[66] J. Petelka, B. Berens, C. Sugatan, M. Volkamer, and F. Schaub, "Restricting the link: Effects of focused attention and time delay on phishing warning effectiveness," in *2025 IEEE Symposium on Security and Privacy (SP)*. Los Alamitos, CA, USA: IEEE Computer Society, May 2025, pp. 7–7. [Online]. Available: https://doi.ieeecomputersociety.org/10.1109/SP61157.2025.00007

[67] G. Stivala and G. Pellegrino, "Deceptive previews: A study of the link preview trustworthiness in social platforms," *The Network and Distributed System Security Symposium (NDSS)*, 2020.

[68] Anti Phishing Working Group (APWG), "Phishing activity trends reports: 2025 Q2," 2025. [Online]. Available: https://www.apwg.org/trendreports

[69] M. Weinz, N. Zannone, L. Allodi, and G. Apruzzese, "The impact of emerging phishing threats: Assessing quishing and LLM-generated phishing emails against organizations," in *Proceedings of the 20th ACM Asia Conference on Computer and Communications Security*, ser. ASIA CCS '25. New York, NY, USA: Association for Computing Machinery, 2025, pp. 1550–1566. [Online]. Available: https://doi.org/10.1145/3708821.3736195

[70] M. Kowalewski, L. Lassak, M. Dürmuth, and T. Schnitzler, "Scanned and scammed: Insecurity by ObsQRity measuring user susceptibility and awareness of QR code-based attacks," in *34th USENIX Security Symposium (USENIX Security 25)*, 2025, pp. 1415–1434.

[71] A. Wang, P. Gopalkrishnan, Y. Wang, C. W. Fletcher, H. Shacham, D. Kohlbrenner, and R. Paccagnella, "Pixnapping: Bringing pixel stealing out of the stone age," in *Proceedings of the 2025 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '25. New York, NY, USA: Association for Computing Machinery, 2025, pp. 3266–3280. [Online]. Available: https://doi.org/10.1145/3719027.3765093

[72] D. Jain, S. Junuzovic, E. Ofek, M. Sinclair, J. Porter, C. Yoon, S. Machanavajhala, and M. Ringel Morris, "A taxonomy of sounds in virtual reality," in *Proceedings of the 2021 ACM Designing Interactive Systems Conference*, ser. DIS '21. New York, NY, USA: Association for Computing Machinery, 2021, pp. 160–170. [Online]. Available: https://doi.org/10.1145/3461778.3462106

[73] D. Medeiros, R. d. Anjos, N. Pantidi, K. Huang, M. Sousa, C. Anslow, and J. Jorge, "Promoting reality awareness in virtual reality through proxemics," in *2021 IEEE Virtual Reality and 3D User Interfaces (VR)*, 2021, pp. 21–30.

[74] L. Buck and R. McDonnell, "Security and privacy in the metaverse: The threat of the digital human," *Proceedings of the 1st Workshop on*

APPENDIX A
STUDY STIMULI

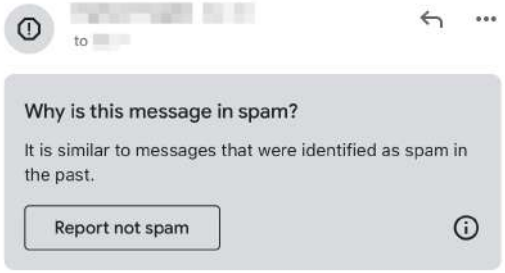

Fig. 5: Spam warning banner

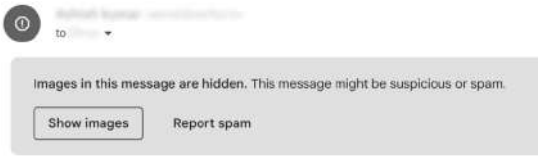

Fig. 6: Hidden images warning banner

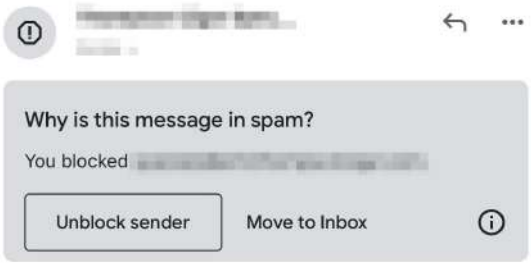

Fig. 7: Block sender warning banner

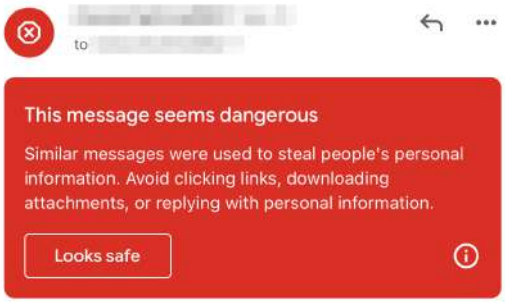

Fig. 8: Phishing warning banner

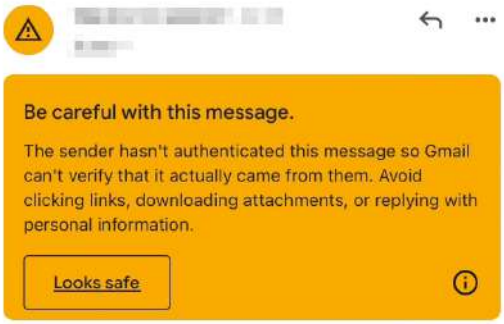

Fig. 9: Report phishing warning banner

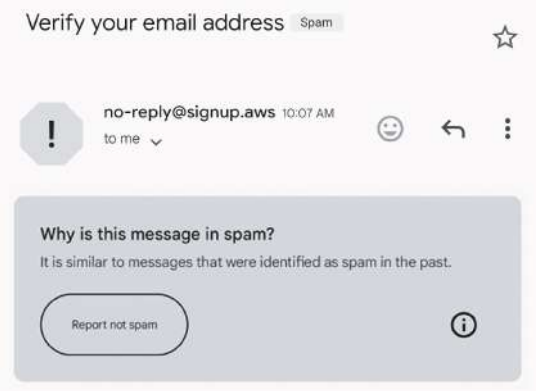

Fig. 10: The *false positive* AWS sign-up email

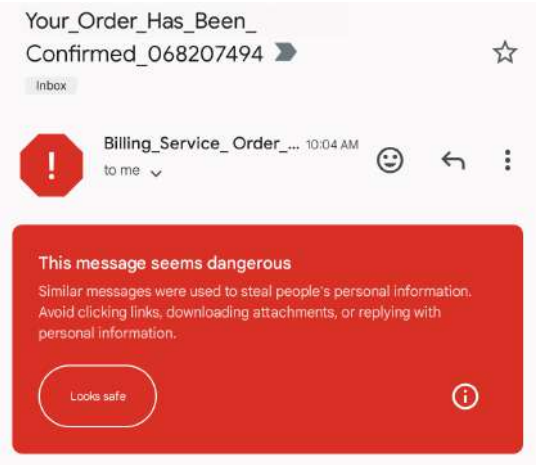

Fig. 11: The *false positive* invoice attached email

APPENDIX B
RECRUITMENT EMAIL

From: Researcher's Email
Subject: Research Study Participation
To: Potential Participant

Hello,

My name is [redacted], a professor at [redacted]. I am conducting a research study about the experiences with email sorting through Virtual Reality (VR) headsets.

The purpose of the research is to learn more about how people utilizing virtual reality headsets to interact with emails general. I am recruiting only volunteers for this research study and you can participate on your own volition. You are eligible to participate if you are 18 years or above old, you are from United States, you are able to understand and converse in English language, are able to use a VR headset, and you are actively using emails as a mode of communication.

I will ask you several open-ended questions and collect some personal information about you such as age, gender, ethnicity/race, education, computer, and VR headset proficiency. If there is a question you do not want to answer, you may ask us to skip it. Your information will be kept confidential and stored in a secured computer under password protection and with encrypted files. The data will be kept de-identified. The participation will take about 30 minutes. You will receive an extra credit for a successful participation in a class of your choice (selected in [redacted] during the sign-up). You must have an email client and internet connection on your phone. You must be able to understand and converse in English.

If you are interested in participating, please respond directly to this email expressing your interest in the study and your familiarity with virtual reality headsets. My email is [redacted] and my cell phone number is [redacted]. Once I have ascertained your eligibility, we will agree for a timeslot for your IN-PERSON participation in the [redacted]

Thank you for your time.

APPENDIX C
INTERVIEW SCRIPT

Announcement

This interview is being audio-recorded for research purposes. You may stop the recording at any time. Do you consent to being audio-recorded? Recording starts now.

Questions and Tasks

1) Which statement best describes your level of experience with virtual reality headsets?
   - I have tried one out, but never operated it alone.
   - I have used a headset for gaming.
   - I have used a headset for functions outside of gaming (ask for types of tasks performed).
2) What device do you prefer to read your emails on?
   - Phone (ask for make and OS)
   - Desktop/Laptop (ask for make and OS)
   - Tablet (ask for make and OS)
   - VR Headset (ask for make and OS)
3) Can you please check your spam or junk folder. Can you please go over the most recent few emails – one by one – you have received in this folder.
4) Carefully open each of these emails and just review the contents. We would like to ask some questions about this particular experience:
   1.1 Have you noticed anything unusual about these emails? Please specify in as many details as you can.
   1.2 Have you noticed any warnings, notifications, or labels about these emails? Please specify in as many details as you can.
   1.3 How do you usually review and decide what to do with these emails?
   1.4 How do these warnings, notifications, or labels affect your opinion about the safety of the email they were substantiated to (e.g. email phishing or not, spam or not, scam or not)?

   Note: A baseline of "suspicious" and "safe" (legitimate) is established, based on the participant's interpretation of what they think is suspicious (or safe). In case this interpretation differs from the definition of phishing/spam suspiciousness/legitimacy provided by CISA (https://www.cisa.gov/news-events/news/avoiding-social-engineering-and-phishing-attacks), a brief explanation of "suspicious" and/or "safe" (legitimate) is provided. This is done as such to minimize the probability of priming participants for the subsequent tasks.

   1.5 What cues do you usually use to assess the legitimacy of emails?
   1.6 How often do you see suspicious emails in your inbox?
   1.7 How often do you see legitimate emails in your spam folder?
5) What is your opinion on how your email provider handles suspicious emails?
6) Have you received any phishing, spam, scam or dangerous email training?
7) Have you ever been a victim of a successful phishing, spam, or a email scam campaign? If you are comfortable with, please share your experiences with this event(s). [What lessons you have learn from here and how this episode affected your way of dealing with emails after-

wards]

8) Have you seen any other types of phishing, spam, scam campaigns delivered over other types of communication than email (e.g. SMS, social media, Discord)?
9) What would you recommend about how these email warnings, notifications, labels should be made to work for individuals utilizing virtual reality headsets?
10) Anything else you want to add on this topic or your experience with warnings about emails?
11) Demographic Questions
    a) How old are you?
    b) What race/ethnicity do you identify as?
    c) What is your gender?

APPENDIX D
CODEBOOK

A. Reflection

1) **Banner Message Received** Codes pertaining to the warnings and indicators the participant observed on their spam emails.
   - **Why is This in Spam** The participant expressed their spam emails contained a warning indicating that the email was spam and they had to opportunity to report that the email was not spam
   - **Images are Hidden** The participant expressed their email contained a warning that the images are hidden for their safety
   - **Dangerous Email** The participants expressed that their spam email contained a warning that the email or attachment was potentially dangerous
   - **Unblock Sender** The participants expressed that their spam email contained a warning that the sender had previously been blocked
   - **No Warning** The participant expressed that their emails did not have any warning message
2) **Cues** Codes pertaining to the cues noticed by the participant during their experience with the emails in their spam folder.
   - **Warning** The participant expressed their spam emails contained a warning indicating that the email was spam or phishing
   - **Unknown Sender** The participant expressed that the email was from an unknown sender
   - **Context** The participant expressed that the email was unsolicited or inapplicable
   - **Attachment** The participant expressed that there was an attachment that did not fit with the content of the email
   - **Formatting** The participant expressed that the email contained characters or grammar inconsistent with their expectations for an email in English
   - **Images** The participant expressed that the images did not load properly or were missing
3) **Action** Codes pertaining to the actions taken by the participant during their experience with the emails in their spam folder.
   - **Leave** The participant indicated they would leave the email in their spam folder and ignore it
   - **Investigate** The participant indicated that they would further investigate the elements of the email to determine if it is legitimate
   - **Delete** The participant indicated they would delete the email
   - **Report** The participant indicated that they would report the email as spam
   - **Unsubscribe** The participant indicated they would use the unsubscribe option within the email to prevent future emails
   - **Block** The participant indicated they would block the sender

B. Email Assessment, Training, Past Experience

1) **Dealing with Unsolicited Emails** Codes pertaining to cues, criteria or rules of thumb used to determine a legitimacy of an email.
   - **Grammatical Cues** The participant expressed that they relied on cues such as grammatical inconsistencies, typos, misspellings, out-of-order symbols
   - **Logical Cues** The participant expressed that they relied on logical cues such as the improbability of an email request
   - **Elements in the Email** The participant expressed that they relied on cues in the email structure such as the subject, email sender, timestamp, and body without attachments
2) **Email Provider Sorting** Codes Pertaining to the participant's opinion of how well their email provider is sorting their emails based on if they are spam or not.
   - **Spam Going to Inbox** The participant reported that they had spam emails coming to their inbox frequently
   - **Important Emails Going to Spam** The participant reported that they had an experience where an important email (job, school, requested materials, one-time password) went to their spam

C. Usability and Improvements

1) **Email Usability Improvements** Codes pertaining to banner warning improvements

- **Severity/Risk Level Indicators** The participant recommends for the banner warnings to include severity/risk level indicators to better discriminate between various levels of threats and risk exposures based on the email type
- **Color Coding** The participant recommends for the banner warnings to be color coded to allow for better discrimination between various levels of threats and risk exposures based on the email type
- **Pop-up** The participant expressed that a warning be implemented as a pop-up that must be accepted before a suspicious link or attachment is opened
- **Message Content** The participant expressed that the content of the warning message could be more descriptive
- **Algorithm Control** The participant expressed that users should have a more active role in what is determined to be spam and the warnings received

2) **VR Usability** Codes pertaining to the ability to detect phishing and spam using a VR headset.
   - **Misclicks** The participant expressed that it is too easy to click on phishing links or attachments
   - **Distractions** The participant noted that there were too many distractions that they wouldn't give the task the same level of focus
3) **VR Usability Improvements** Codes pertaining to suggestions to improve user's abilities to detect spam and phishing when checking emails using a VR headset.
   - **Screen Takeover** The participant expressed that the email browser/app should take over the full screen to reduce distractions
   - **Navigation** The participant expressed that the navigation should be different when doing productivity tasks instead of gaming

APPENDIX E
DEBRIEFING

Thank you for participating in our research on how users who are utilizing virtual reality headsets experience and utilize email warnings. This study aimed to examine whether people pay attention to warnings as a cue before they proceed to the website or not. So far, no research exists on how users are experiencing and utilizing emails warnings while utilizing virtual reality headsets. This is why we asked you to select and examine one email from your spam folder.

It was necessary for the researchers to withhold this information from you regarding the purpose of the study to ensure that your actions and answers to questions accurately reflected your cybersecurity hygiene, perceptions, and beliefs. Your participation in the study is important in helping researchers identify the best ways to address the accessibility of the warnings assigned by the email provided to the emails in the spam folder. Since we did not collect any personal information, we would not able to remove your entry from the data bank of our research interviews enforced once you leave the research site.

The final results of this study will be published in a peer-reviewed journal. Your results will not be available individually and your participation will remain confidential. We do not keep, record, or collect any personal credentials. If you have any additional inquiries please contact [redacted]. If you have questions about your rights as a research subject, you may contact [redacted] in the Office of Research Services at [redacted] or via email at [redacted]. You may also contact [redacted] Office of Research Services if your questions, concerns, or complaints are not being answered by the research team, you cannot reach the research team, or you want to talk to someone besides the research team.

APPENDIX F
DECEPTIVE PATTERNS THEMES AND SUBTHEMES

TABLE VIII: Deceptive Patterns Themes and Subthemes

Themes/Subthemes	Presence	Description
Adverse Effects of User Experience		
Present	●	The use of a VR headset as a productivity tool is intended to enhance user experience, yet participants found that it introduces new barriers that reduce their ability to detect and address phishing emails.
Inferred	◐	Malicious emails have the potential to exploit the heightened realism of VR environments, making phishing attempts more convincing as products, branding, and logos appear more lifelike [22].
Exacerbated User Manipulation		
Obscuring reality, disguising risks	◐	Determining whether an email is malicious can require cross-checking information, yet VR may limit access to external devices and create layered interface elements that could prevent users from hovering over URLs or clearly seeing security banners [22].
Data fuels privacy risks and manipulation	◐	Checking email within a VR environment may expose behavioral data such as hand-gesture inputs, that a phishing attempt could potentially exploit to gather more detailed user information [36].
Interaction insecurity increases manipulation risk	●	Participants identified that current VR technology is not well equipped to handle email and phishing scenarios, noting that the lack of a purpose-built VR email application creates vulnerabilities that allow phishing emails to bypass user defenses.
Ergonomic vulnerabilities amplify manipulation	◐	Physical, cognitive, perceptual, and interaction ergonomic vulnerabilities, such as fatigue from sustained headset wear, divided attention, spatial distraction, imprecise hand or gaze tracking, and hypersensitive selection mechanisms can negatively affect users' decision-making processes and thus create exploitable conditions. Using VR for productivity may lead to prolonged headset use, potentially increasing the number of phishing-related decisions users must make each day and contributing to repeated exposure and attention fatigue [22].
User Perception Tricking		
Perception hacking	◐	Participants reported imprecise clicking and frequent mis-selections in VR, indicating that email review may be especially vulnerable to clickjacking or cursorjacking that causes users to select unintended options [23].
Imbalancing options	◐	VR navigation and input challenges may make certain options within a phishing email appear easier to select or require less effort, potentially steering users toward harmful actions [20].
Psychological Manipulation		
Hyperpersonalization	◐	The personalized nature of VR experiences could make phishing emails appear more tailored to the user, potentially reducing their ability to identify unsolicited or suspicious messages [74].