Humanities & Social Sciences Communications

ARTICLE

https://doi.org/10.1057/s41599-024-03412-8 OPEN

Friend or phisher: how known senders and fear of missing out affect young adults' phishing susceptibility on social media

Jennifer Klütsch [1✉], Jasmin Schwab [1,2], Christian Böffel [1], Verena Zimmermann [3] & Sabine J. Schlittmeier [1]

Phishers exploit the social nature of social media, thereby targeting young adults, who are highly susceptible to phishing. This study focuses on two under-researched factors influencing young adults' susceptibility to social media phishing: the user's relation to the message sender and Fear of Missing Out (FoMO). In an online vignette study, 193 young adults were presented with Instagram chat messages from either known or unknown senders, accompanied by varying consequences for not clicking. These ranged from missing an event with no other user (no consequences) to missing an event with one (low) or several other users (high consequences). The analysis focused on intended behaviour and suspicion, while also capturing young adults' situational fear of missing out on the scenario-based event with the message sender (State FoMO) and their individual Trait FoMO. The results highlight that the user-sender relation is a strong predictor of phishing susceptibility and a crucial contributor to State FoMO. Furthermore, young adults who are high in Trait FoMO exhibited lower suspicion towards phishing attempts. These findings are discussed along with methodological considerations. In addition, strategies to mitigate the identified vulnerabilities are suggested, focusing on areas where social media phishing is most likely to affect young adults.

[1] Work and Engineering Psychology, RWTH Aachen University, Aachen, Germany. [2] Institute for the Protection of Terrestrial Infrastructures, Digital Twins for Infrastructures, German Aerospace Center, Cologne, Germany. [3] Security, Privacy and Society, ETH Zurich, Zurich, Switzerland. ✉email: kluetsch@psych.rwth-aachen.de

Introduction

Phishing continues to be a major online cyber threat, with average total costs of more than $4.6 million in 2021 (IBM Security, 2021) and, in recent years, record numbers from more than 4.7 million phishing attacks (Anti-Phishing Working Group, 2022). Phishers try to gain access to sensitive information, such as login credentials or credit card details, commonly by sending fake emails with social engineering (SE) techniques in which 'the attacker(s) exploit human vulnerabilities by means of social interaction' (Wang et al., 2020). For instance, phishers pretend to be the victims' financial institutions through instigating authority, or they invoke social proof by pretending to be colleagues and friends (Frauenstein and Flowerday, 2020; Workman, 2008).

While email is still the most common attack vector, phishers increasingly make use of alternative channels, such as social media (James, 2023; Lourenço and Marinos, 2020). In social media phishing -also known as social or social network phishing (Frauenstein and Flowerday, 2020)-, phishers mostly attack in two stages (Vishwanath, 2017): within the first stage, they send their victim a friend request to gain access to their profile information. In the second stage, they contact their victim, often through personalised chat messages, to gain access to sensitive information. During both stages, phishers exploit the social nature of social media, for example, through using (profile) pictures and liking their victims' posts (Vishwanath, 2017). Thus, phishers can easily pretend to be friends and exploit the human tendency to mimic the behaviour of relevant others (Frauenstein and Flowerday, 2020). Moreover, the increasing use of social media with 4.85 billion users worldwide (Kemp, 2023) and improved chat messages through generative artificial intelligence (AI) (Lourenço and Marinos, 2020) make social media phishing even more threatening. Although initial research investigates predictors of susceptibility to social media phishing, such as habitual use (Vishwanath, 2015b) or certain sender characteristics (e.g., profile picture) (Algarni et al., 2017; Vishwanath, 2017), phishing research (Algarni et al., 2017) as well as interventions (Franz et al., 2021) have mostly addressed email phishing so far. Yet, to establish user-centered interventions countering this novel and harmful phishing trend, research needs to better understand the user-specific characteristics that contribute to their susceptibility towards social media phishing (Waqas et al., 2023; Yan et al., 2018).

We aim to provide deeper insight into these by investigating the impact of the user's relation to the message sender and an often observed phenomenon in social media: Fear of Missing Out (FoMO) (Tandon et al., 2021). FoMO refers to 'a pervasive apprehension that others might be having rewarding experiences from which one is absent' (p. 1841) (Przybylski et al., 2013). Researchers often measure FoMO as a trait and the extent to which an individual in general fears missing out on social events, particularly when friends are attending (Bowman and Clark-Gordon, 2019; Przybylski et al., 2013). These individual differences in Trait FoMO were found to shape the users' online behaviour, such as participating in social media despite his/her privacy concerns (Westin and Chiasson, 2021) or intending to buy recommended products from influencers (Dinh and Lee, 2022). However, its impact on social media phishing has been neglected so far, even though the social characteristics of social media are often exploited by attackers. For example, phishers who invite their victims to an event or other rewarding experience as a supposed friend, particularly through fake or hijacked accounts, could increasingly exploit users with high levels of Trait FoMO. Beyond that, such messages from phishers could trigger a situational FoMO on these rewarding experiences when not clicking. Such situational FoMO, triggered through a specific event that a user feels FoMO about, is known as State FoMO in the literature (Maxwell et al., 2022). Therefore, Trait and State FoMO could be exploited by phishers and lead users to quick heuristic decision processes, in which message cues such as a suspicious link are simply not considered (Frauenstein and Flowerday, 2020; Zhuo et al., 2023).

Young adults (approx. 16−25 years old, Devitt et al. (2009)) appear to be the most vulnerable user group to these attacks due to three major characteristics: First, young adults are more likely to be targeted because of their increased use of most social media platforms, particularly Instagram (Kemp, 2023). Second, young adults are more susceptible to phishing attacks via email and social media than older age groups (Parker and Flowerday, 2020; Sheng et al., 2010; Tornblad et al., 2010) and third, young adults feel increased Trait FoMO compared to older age groups (Przybylski et al., 2013). All of these characteristics make them an easy and more likely target of social media phishing, whose user-specific vulnerabilities are still largely unknown (Oliveira et al., 2017).

To address this research gap, we investigated young adults' susceptibility towards (a) known and unknown senders (user-sender relation), (b) State FoMO through consequences of missing out on a specific rewarding experience when not clicking and (c) their individual level of Trait FoMO, with the following research questions (RQ):

- **RQ1:** How is young adults' susceptibility to social media phishing affected by the *user-sender relation* and the *consequences of not clicking*?
- **RQ2:** How is young adults' susceptibility to social media phishing related to individual differences in *Trait FoMO*?

Background and related work

This section provides an overview of why users fall for phishing on social media and related previous research. It then explains our hypothesis and the methods applied.

Cognitive approaches in phishing. The Suspicion, Cognition, and Automaticity Model (SCAM) (Vishwanath et al., 2018) and the underlying Heuristic Systematic Model (Chaiken, 1980; Eagly and Chaiken, 1993) highlight users' cognitive processing as crucial to understand why users fall for phishing. Herein, two types of cognitive processing are distinguished: (1) heuristic processing, in which individuals base their decisions on salient cues and simple rules of thumb, and (2) systematic processing, in which all cues in a message are carefully considered (Vishwanath et al., 2018). According to SCAM (Vishwanath et al., 2018), a user's processing, be it heuristic or systematic, depends on their perceived cyber risks when receiving the phishing email or chat message. If the perceived cyber risks are low, the user is more likely to engage in heuristic processing. As a consequence, such heuristic processing could lead to overlooking obvious phishing cues, such as a suspicious link, and increase susceptibility to phishing attacks (Vishwanath et al., 2018).

Social characteristics in social media phishing. Integrating these insights, one might fall for social media phishing as the social sender characteristics of social media (e.g., profile pictures) reduce the perceived cyber risks and trigger heuristic instead of systematic processing (Frauenstein and Flowerday, 2020; Vishwanath, 2015a). For instance, when a user receives a chat message from a phisher with a friendly and real profile picture, the profile picture could serve as a cue for the phishers authenticity (Vishwanath, 2015a). Based on this authenticity cue, the

user could perceive reduced risks associated with the phisher and react quickly without considering all cues to the chat message (heuristic processing) (Vishwanath et al., 2018).

Initial research underscores social sender characteristics as a strong predictor for susceptibility to social media phishing. For instance, Vishwanath (2015a) found that the number of friends as well as the phisher's profile picture increased users' susceptibility towards friend requests and their likelihood to fall for phishing in personalised chat messages. According to the researchers, these two sender characteristics could increase heuristic processing through authenticity and social proof (Vishwanath, 2015a). Similarly, in a large-scale study, Algarni et al. (2017) found that the number of friends, real names, common friends, the number of posts, as well as common beliefs strongly affected the perceived sincerity of phishers and with that, the susceptibility to phishing attacks. These findings provide strong indications that social sender characteristics affect one's susceptibility to social media phishing. Specifically, hijacked accounts from actual friends may pose a significant risk, as phishers can exploit these relationships with their victims. However, there has been limited research on phishing messages from user-related senders, such as actual friends. One Facebook study ($N = 20$) shows first evidence that the relation with the message sender (e.g., close friend or partner) seems to be an important predictor of susceptibility to social media phishing (Seng et al., 2019). Yet, it remains to be answered whether this effect can be confirmed for larger samples and across social media channels, such as younger adults' most used social media platform Instagram (Kemp, 2023). This further includes different susceptibility indicators such as users' suspicion, a commonly used measurement of deception detection (Vishwanath et al., 2018). However, understanding user-specific vulnerabilities is crucial for developing effective countermeasures against social media phishing. Therefore, investigating these social sender characteristics within vulnerable user groups such as young adults (Parker and Flowerday, 2020; Sheng et al., 2010; Tornblad et al., 2010) is relevant.

We aim to gain insight into the *user-sender relation* by examining young adults' susceptibility both to known and unknown senders. To address current research gaps, we investigated the susceptibility of 193 young adults on Instagram -the most commonly used platform of young adults (Kemp, 2023)- with two complimentary susceptibility indicators: First, we assessed users' *intended behaviour* through either susceptible (open/share the link or respond to/like the message) or non-susceptible responses (ignore/delete the message) as suggested by Frauenstein and Flowerday (2020). Second, we queried their level of *suspicion* through the suspicion scale (Chou et al., 2021; Vishwanath et al., 2018). In line with previous research on social sender characteristics (Algarni et al., 2017; Seng et al., 2019; Vishwanath, 2015a), it is proposed that: **Hypothesis 1:** *Phishing messages from known senders increase young adults' susceptibility compared to phishing messages from unknown senders*. As we measured two indicators of susceptibility, it is referred here and below to increased susceptibility as an increase in susceptible responses and a decrease in the level of suspicion.

Young adults and Fear of Missing Out (FoMO). Existing literature on FoMO refers to it in two ways: Trait FoMO and State FoMO (Holte, 2023; Maxwell et al., 2022). Trait FoMO is characterised by the 'desire to stay continually connected with what others are doing' (Przybylski et al., 2013). It refers to a user's general FoMO on rewarding experiences. On the contrary, State FoMO is triggered by a specific event or situation and refers to a user's current FoMO on a rewarding experience (Holte, 2023; Maxwell et al., 2022). Trait FoMO has been examined in various online contexts, and individual differences in Trait FoMO were found to contribute to social media (over-)use (Przybylski et al., 2013; Tugtekin et al., 2020) and excessive Instagram use (van der Schyff et al., 2022), making users high in Trait FoMO more likely to be victims of social media phishing. In addition, Trait FoMO was found to influence users' privacy decisions. For example, it was found to elicit pressure in users to engage in social media despite their privacy concerns (Westin and Chiasson, 2021) and to disclose more information on social media services such as Instagram (van der Schyff and Flowerday, 2023). Furthermore, research shows that higher Trait FoMO is connected to increased online risk-taking, such as password sharing, among younger users (12 to 18 years old) (Popovac and Hadlington, 2020) and reduced information security awareness among employees (Hadlington et al., 2020). These findings suggest that Trait FoMO may also be a critical predictor of susceptibility, particularly for younger adults who tend to experience higher levels of Trait FoMO (Przybylski et al., 2013).

State FoMO, on the other hand, has not yet been extensively studied (Holte, 2023; Maxwell et al., 2022). However, preliminary research suggests that State FoMO is similarly associated with online behaviour, such as problematic social media use, as Trait FoMO (Holte, 2023). Therefore, State FoMO may also be an important predictor of susceptibility. Similar to phishing emails that exploit the fear of losing something important such as a course registration (Goel et al., 2017), phishers who invite users to a supposed event may exploit State FoMO by implying that not clicking will result in the consequence of missing out on the event. This urge to join in could then trigger users' heuristic processing, increasing their susceptibility to phishing (Goel et al., 2017). This can be particularly threatening when users perceive low cyber risks, such as when they receive messages from hijacked accounts of actual friends (see SCAM, Vishwanath et al. (2018)).

Therefore, we investigate FoMO as a susceptibility predictor in two ways: (1) by assessing individual differences in Trait FoMO on the FoMO scale (Przybylski et al., 2013) and (2) by examining situational differences in State FoMO through different consequences of not clicking on chat messages inviting to an event. According to research on online risk taking (Popovac and Hadlington, 2020; van der Schyff and Flowerday, 2023; Westin and Chiasson, 2021), we proposed: **Hypothesis 2:** *Young adults with high compared to low Trait FoMO are more susceptible to social media phishing*. As not clicking is connected to consequences such as missing out on a specific event with others, messages implying such consequences of not clicking may induce State FoMO. Therefore, we proposed increased susceptibility for *low/high* compared to *no* consequences of not clicking (3.1) and for *high* compared to *low* consequences of not clicking (3.2) through increased feelings of *State FoMO*: **Hypothesis 3.1** *Phishing messages indicating low/high compared to no consequences of not clicking increase young adults' susceptibility*. **Hypothesis 3.2** *Phishing messages indicating high compared to low consequences of not clicking also increase young adults' susceptibility*. Our evaluation of these hypotheses aims to provide three major contributions: (a) Empirical evidence on how the user-sender relation, situational differences in State FoMO and individual differences in Trait FoMO shape phishing susceptibility in social media for the younger age group, (b) Methodological implications of studying social media phishing and (c) Suggestions such as unobtrusive interventions or notifications (e.g., nudges) to address young adults' susceptibility online.

Methodology

In an experimental online vignette study, participants were asked to imagine being in a certain scenario and to react to different Instagram chat screens that contained varying social media messages and (potential) phishing links. The study was conducted

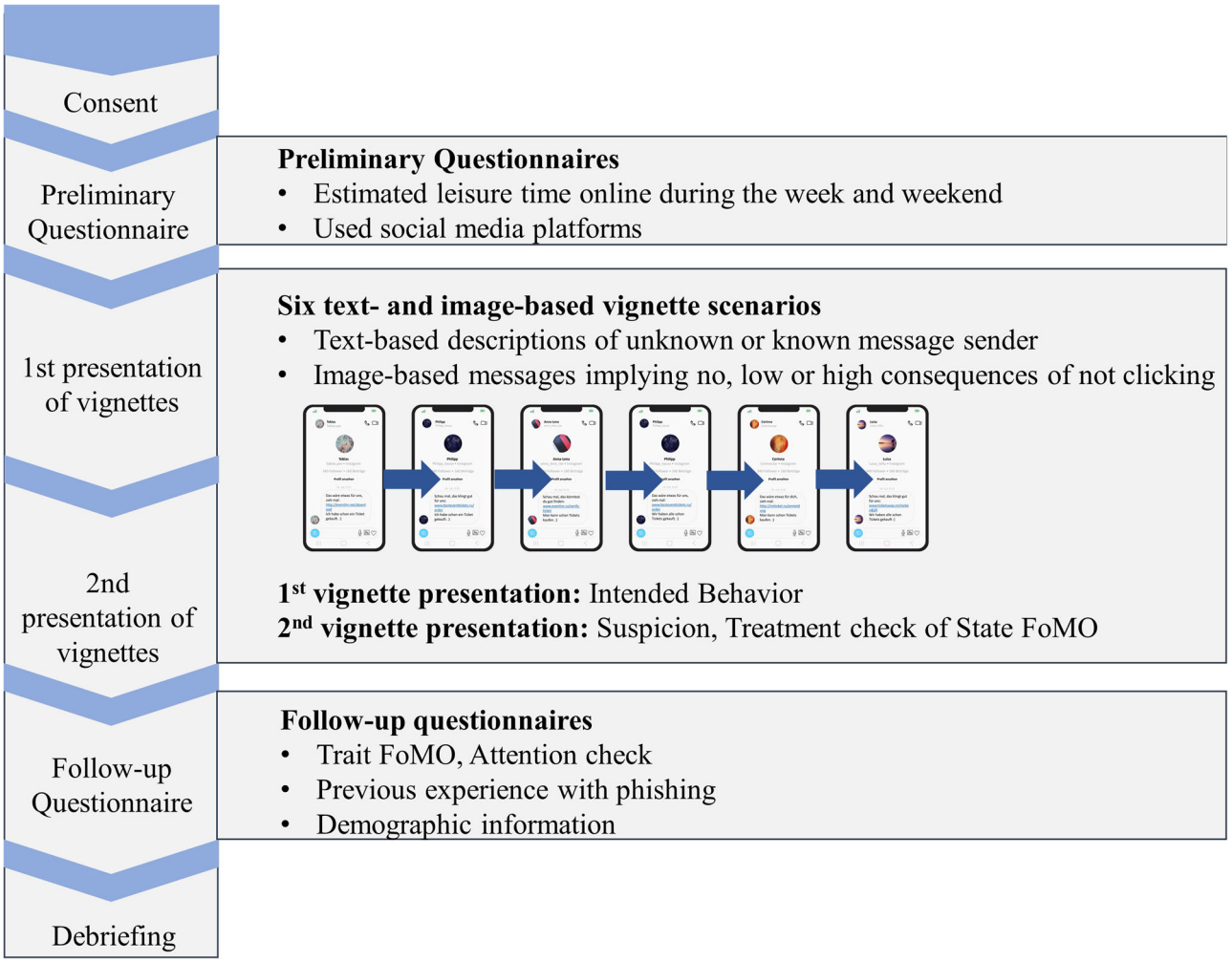

Fig. 1 Study procedure. The figure shows the procedure sequence in the following order: (1) consent; (2) preliminary questionnaires: internet and social media use; (3) first presentation of vignettes for intended behaviour; (4) second presentation of vignettes for suspicion and treatment check; (5) follow-up questionnaires: Trait FoMO, attention check, phishing experience, demographics; (6) debriefing.

online using the software tool Pavlovia[1] and designed with the *user-sender relation* (unknown vs. known) and the *consequences of not clicking* (no vs. low vs. high) as independent within-participant factors. In other words, participants received messages from known and unknown senders with no, low or high consequences of not clicking. The latter ranged from missing an event with no other user (no) to missing an event with one (low) or several other users (high). As dependent variables, two indicators of susceptibility were measured: (1) Intended behaviour and (2) Suspicion.

Procedure. Approximately 10−15 minutes were required to complete the study. Before the study started, each participant gave informed consent. Afterwards, participants were queried about their estimated amount of leisure time spent online and the social media platforms they use. Further instructions on the vignette task followed. The vignette task contained six text- and image-based vignette scenarios. The six vignette scenarios were presented twice: first, querying intended behaviour and, afterwards, querying the suspicion scale as well as a treatment check on State FoMO. After completion of all vignette scenarios, participants' Trait FoMO was queried on the FoMO scale (Przybylski et al., 2013). Then, social media phishing was explained in more detail, and previous experience with phishing via email, Instagram and other social media services was queried. Thereafter, participants were asked to provide demographics. Lastly, debriefing information detailing the study aim and assumptions was presented, and participants were able to save their data. The procedure is visualised in Fig. 1.

Vignettes. This study utilised so-called vignette scenarios, including short-text and -image scenarios of direct chat messages on Instagram. While it should be noted that this methodology does not capture the complexity of real-life situations due to its focus on specific scenarios and cannot be fully generalised to actual behaviour, the scenarios allowed us to systematically investigate our study objective in more realistic scenarios than traditional questionnaire items (Atzmüller and Steiner, 2010). For a detailed reflection on the limitations of this study, see Section *Limitations and implications for future work*. The vignette scenarios were systematically varied for two short-text scenarios describing the sender as either unknown or known (see Table 1) and chat messages describing no, low, or high consequences for not clicking the link (see Table 2).

As *user-sender relation* (known vs. unknown) and *consequences of not clicking* (no vs. low vs. high) were varied within participants, we created two gender-neutral message formulations to avoid presenting the same message twice from unknown and known senders. Similarly, this study contained six picture-name- and gender-balanced senders with one phishing link each (see

Fig. 2) to avoid carry-over effects through phishing messages from the same sender or link. This resulted in three messages from male and three messages from female senders with six phishing links, which were counterbalanced across the conditions. Phishing links were based on a pilot study ($N = 21$) in which 18 fictitious and self-created phishing links were rated for their phishing detection difficulty on a scale from 1 'It is easy for me' to 3 'It is difficult for me'. Moreover, participants were asked for the criteria on which they rated the links and their previous phishing experience. Based on the pilot study, six phishing links of medium difficulty ($M = 1.52$ to 2.24) were selected. An overview of the resulting sender-link designs is shown in Fig. 2.

Susceptibility indicators: intended behaviour and suspicion. Two indicators of susceptibility were queried: (1) intended behaviour and (2) suspicion. First, participants were asked how they would react to the Instagram message to assess intended behaviour (translated and adapted to Instagram from Frauenstein and Flowerday (2020), see Table 3). Similar to Frauenstein and Flowerday (2020), responses were categorised as (a) either non-susceptible when participants indicated to ignore/delete the message or (b) susceptible when participants indicated to open/share the link or respond to/like the message for analysis. As multiple answers were possible, contradictory statements, containing intended behaviour that could be categorised as non-susceptible and susceptible (e.g., ignoring and responding to the message at the same time) were excluded from the analysis (1.1% of all responses).

Second, we queried a translated and Instagram-adapted version of the suspicion scale (Chou et al., 2021; Vishwanath et al., 2018). The scale included five items such as 'I click links within the Instagram message without any doubts.' (see Table 3) on a Likert scale from 1 'I do not agree at all' to 6 'I fully agree'. For analysis, the mean of the suspicion scale (Cronbach's $\alpha = 0.82-0.97$) was calculated for each vignette scenario. Mean values range from 1, indicating no suspicion, to 6, indicating high suspicion.

Treatment check: state FoMO. As a treatment check, we queried participants' State FoMO for each message scenario on a Likert scale item ranging from 1 'I do not agree at all' to 6 'I fully agree' (see Table 3) at the end of the suspicion scale.

Table 1 Translated text-based scenarios for the relation to the message sender.

Relation to message sender	Short text scenario
Unknown	You notice that the sender of this message is unknown to you and that you have never exchanged messages on Instagram (e.g., direct messaging, liking, or sharing posts).
Known	You notice that the sender of this message is known to you and that you have exchanged messages several times on Instagram (e.g., direct messages, liking or sharing).

Questionnaires

Preliminary questionnaires

Average time online and social media use: In the preliminary questionnaire, participants were asked about their estimated leisure time online for a typical day during the week and on weekends in hours, as well as which social media platforms they use.

Follow-up questionnaires

Trait FoMO: To identify individual differences in Trait FoMO, we assessed the 10-item Trait FoMO scale by Przybylski et al. (2013) on a Likert scale from 1 'Not at all true' to 5 'Absolutely true' (see Table 3). The scale examines the extent to which someone in general fears missing out on social events, particularly when friends are attending (Bowman and Clark-Gordon, 2019; Przybylski et al., 2013), and demonstrates high internal consistency (Cronbach's $\alpha = 0.82$ (Przybylski et al., 2013), see also Bowman and Clark-Gordon (2019) for further information on reliability). For analysis, participants were split in two groups along the mean: when participants' mean score was below the sample mean ($M < 3.15$), they were categorised as having a low Trait FoMO score (48.7% of all participants) indicating low Trait FoMO, whereas when participants' mean score was higher than or equal to the average mean ($M > 3.15$), they were categorised as having a high Trait FoMO score (51.3% of all participants), indicating high Trait FoMO.

Attention check: As an attention check, participants were instructed to select 'Not at all true' on one item in addition to the FoMO scale. This was rated on a Likert scale from 1 'Not at all true' to 5 'Absolutely true'.

Previous experience with phishing: Previous experience with phishing via email, Instagram, or other social media services was queried with the response options 'yes', 'no' and 'I do not know'. To avoid conceptual ambiguities, participants received a definition of the term 'phishing' (see Table 3).

Demographic information: Lastly, participants' demographic information (age, gender, educational degree, occupation) was queried.

Table 2 Translated message scenarios, sorted by the level of consequences of not clicking.

Level	Consequence of not clicking	Message content
No	No consequences of missing out on an event others are interested in and doing	Look, you could find this nice: [Link] You can already buy tickets : *or* This might suit you, see: [Link] You can already buy tickets :
Low	Consequence of missing out on an event one other person is interested in and doing	Look, this sounds nice for us: [Link] I already bought a ticket : *or* This might suit us, see: [Link] I already bought a ticket :
High	Consequence of missing out on an event several other persons are interested in and doing	Look, this sounds nice for us: [Link] All of us already bought a ticket : *or* This might suit us, see: [Link] All of us already bought a ticket :

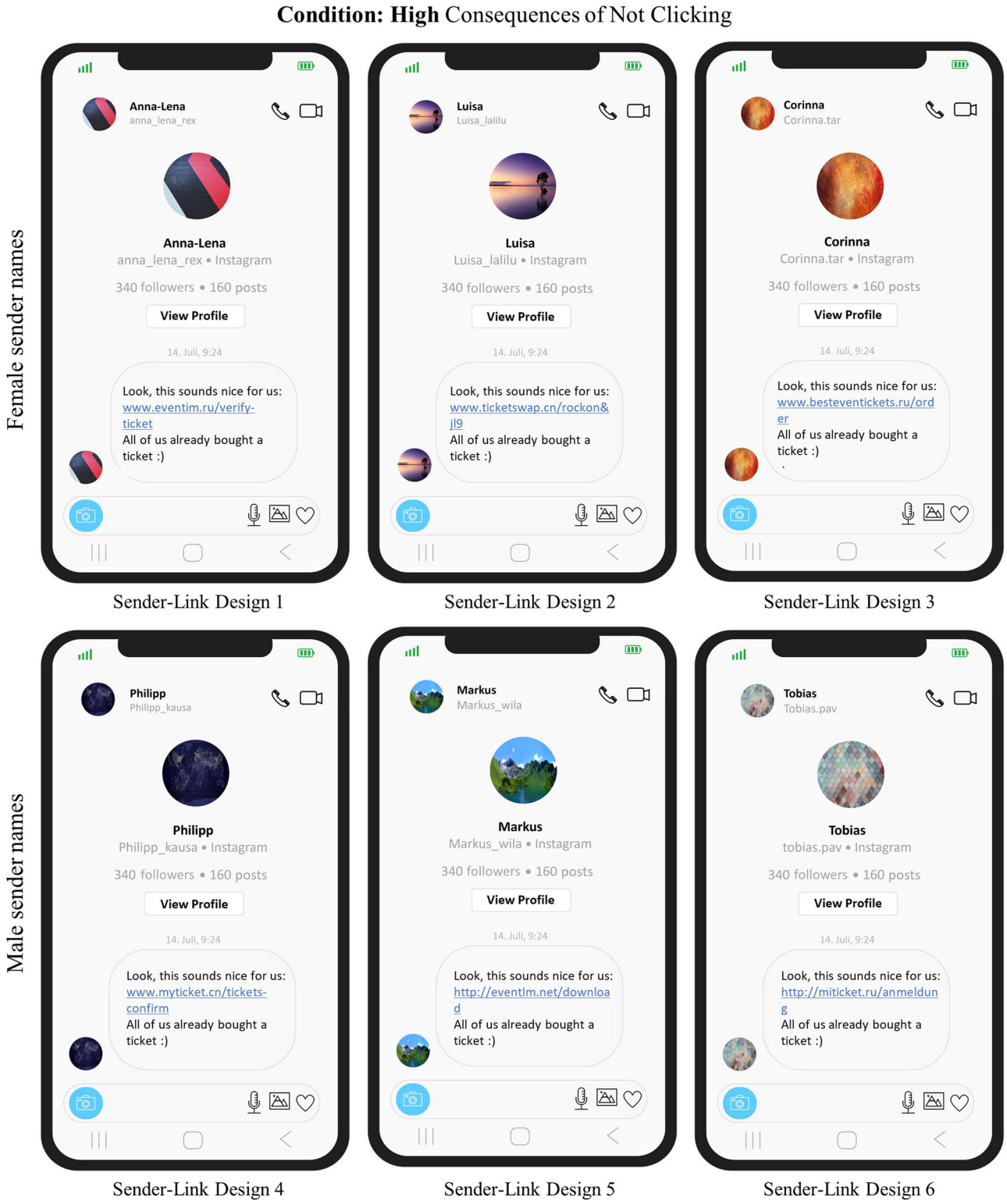

Fig. 2 Translated examples of the picture-name and gender-balanced sender-link designs with six phishing links for high consequences of missing out. Note: The figure shows six fictitious Instagram chat screens with the following sender-link combinations: (1) Anna-Lena (female), www.eventim.ru/verify-ticket, (2) Luisa (female): www.ticketswap.cn/rockon&jl9, (3) Corinna (female): www.besteventickets.ru/order, (4) Philipp (male): www.myticket.cn/tickets-confirm, (5) Markus (male): http://eventim.net/download, (6) Tobias (male): http://miticket.ru/anmeldung.

Participants. A total of $N = 206$ people participated in our study. Participants older than 25 years, who were outside our examined age range, or participants who failed the attention check were excluded ($N_{excluded} = 13$). Data from a total of $N = 193$ young adults (120 females, 73 males) were analysed. Participants were between 16 and 25 years and on average 21 years old ($M = 20.99$, $SD = 2.83$). Further information on the participants' demographics can be found in Table 4. Participants were recruited via email, social media, research platforms, and direct inquiries to schools and universities. Participation was voluntary, and

Table 3 List of items queried on intended behaviour, suspicion, treatment check, FoMO scale and attention check.

Questionnaire	Items	Sources
Intended behaviour *Multiple choice*	What action would you most likely take? • open the link • send an answer • share the link • like the message • ignore the message • delete the message	translated and adapted to Instagram from Frauenstein and Flowerday (2020)
Suspicion *Likert scale*	• I click links within the Instagram message without any doubts. • When I read the Instagram message, I believe its sender is reliable. • When I read the Instagram message, I believe its content is fake. • When I read the Instagram message, I believe it differs from other Instagram messages. • When I read the Instagram message, I believe it would bring unfavourable consequences of clicking links.	translated and adapted to Instagram from Vishwanath et al. (2018) and Chou et al. (2021)
Treatment Check *Likert scale*	• When I ignore or delete the Instagram message, I fear missing out on rewarding experiences with the message sender.	
FoMO Scale *Likert Scale*	• I fear others have more rewarding experiences than me. • I fear my friends have more rewarding experiences than me. • I get worried when I find out my friends are having fun without me. • I get anxious when I don't know what my friends are up to. • It is important that I understand my friends 'in jokes.' • Sometimes, I wonder if I spend too much time keeping up with what is going on. • It bothers me when I miss an opportunity to meet up with friends. • When I have a good time, it is important for me to share the details online (e.g., updating status). • When I miss out on a planned get-together, it bothers me. • When I go on holiday, I continue to keep tabs on what my friends are doing.	translated from Przybylski et al. (2013)
Attention Check *Likert Scale*	• Please select 'Not at all true'.	
Previous Experience with Phishing *single-choice*	In a phishing attack, the attacker attempts to obtain the victim's sensitive data, e.g., user account login data. For this purpose, fake links pointing to fake websites are often used. Phishing attacks are playing an increasingly important role in today's world and pose a great threat to the victim. I have previous experience of dealing with phishing messages. • Email • Instagram • Other social media services	

students from RWTH Aachen University could receive course credits for participation.

Results

The analyses were conducted with the software R (R Core Team, 2019) and RStudio (RStudio Team (2022), Version 2022.12.0), particularly the lme4 package (Bates et al., 2015). The log-odds of *intended behaviour* were modelled using multilevel (mixed-effect) logistic regression, as *intended behaviour* was measured as a dichotomous variable (susceptible vs. non-susceptible). Additionally, given the use of a repeated-measures design, the measurements were nested within the participants, necessitating a multilevel structure. For the dependent variable *suspicion*, multilevel (mixed-effect) linear regression was calculated because *suspicion* can be considered a continuous variable. Additionally, the multilevel structure was required because the intra-class-coefficient (ICC) indicated that the variances in suspicion was partially (32%) explained by between-subject differences. The repeated-measures design was utilised with a multilevel structure for both analyses. For logistic and linear regression analyses, assumptions were checked and fulfilled.

Within our analyses, one multilevel logistic and linear confirmatory regression analysis with both within-subject factors (*user-sender relation*, *consequences of not clicking*) and their interaction terms was calculated. Afterwards, the exploratory regression analyses were calculated, in which we added questionnaire-based predictors as a single predictor to the confirmatory regression equation. These predictors were *Trait FoMO* (low vs. high), *previous phishing experience* via email, on Instagram, or on other social media services (no vs. previous experience), and *gender* (male vs. female). Further, the interaction term of *user-sender relation* and *Trait FoMO* was investigated. All predictors were dummy-coded. Statistical significance was tested at $\alpha = 0.05$.

Confirmatory multilevel logistic regression: influences of user-sender relation and consequences of not clicking on intended behaviour. Within our confirmatory analysis of intended behaviour, we found the proposed effect of *user-sender relation*: When participants received phishing messages from known senders, they were more likely ($\beta = 15.18$, $p < .001$, $OR = 3.90e+06$, 95 % CI: [4.98e + 05, 3.05e + 07]) to show susceptible responses than

when they received phishing messages from unknown senders. Interestingly, the effect of sender was much larger than expected, with a 100 % predicted probability to show susceptible responses (open/share the link or respond to/like the message) when phishing links were received from known compared to unknown senders. Contrary to *hypotheses 3.1* and *3.2*, we did not find the proposed effect for *consequences of not clicking*: Participants were not more likely to show susceptible responses when phishing messages implied low compared to no consequences ($\beta = 0.31$, $p = 0.67$, $OR = 1.36$, 95 % CI: [0.34, 5.49]) or high compared to no consequences ($\beta = 0.01$, $p = 0.99$, $OR = 1.01$, 95 % CI: [0.23, 4.36]). Furthermore, they were not more likely to show susceptible responses when phishing messages implied high compared to low consequences ($\beta = -0.30$, $p = 0.69$, $OR = 0.74$, 95 % CI: [0.18, 3.12]). In addition, no significant interactions between *user-sender relation* and *consequences of not clicking* were found. Thus, the effect of *user-sender relation* does not seem to be affected by the *consequences of not clicking* ($p \geq 0.50$, see Table 5). Table 5 summarises the results of the confirmatory multilevel logistic regression.

Table 4 Participants demographics for the online study.

Demographic categories	*N* = 193
Leisure time online	Median 3 h on a typical week day Median 4 h on a typical weekend day
Used Social Media Platforms	92.7% Instagram users 59.6% YouTube users 55.4% Snapchat users 42.5% Facebook users 33.7% TikTok users
Educational degree	43.5% A-Level 25.9% University degree 16.6% Secondary school diploma 7.3% Non-degree 6.2% Others 0.5% No answer
Occupation	54.9% University student 14.5% School student 14.5% Employee 10.9% Apprenticeship 5.2% Others
Email phishing	73.6% experienced phishing
Instagram phishing	48.2% experienced phishing
Other social media phishing	31.6% experienced phishing

Frequencies: intended behaviour. The frequencies over all responses indicated that 41.1% of all responses were susceptible. Moreover, 160 (82.9%) participants showed at least one response which was categorised as susceptible. To gain in-depth insight into the large effects of *user-sender relation* (see Figure Table 5), frequencies for susceptible and non-susceptible responses were calculated for both unknown and known senders (see Table 6). Within our sample, a relative frequency of 6.6 % ($N = 31$) showed susceptible responses to unknown senders, whereas 93.4 % ($N = 440$) showed susceptible responses to known senders over all susceptible responses ($N = 471$). Further, splitting the coded non-susceptible and susceptible responses into the six given response options, the frequency table indicates *responding to the message* ($N = 295$) and *opening the link* ($N = 257$) as the most frequently selected options for susceptible responses. *Ignoring the message* ($N = 359$) was the most frequent option for non-susceptible responses.

Exploratory multilevel logistic regression: other influences on intended behaviour. We did not find a significant difference in intended behaviour between individuals with low and high levels

Table 6 Frequency table of the coded (non)-susceptible responses and the response options (multiple answers possible) by user-sender relation (unknown, known sender).

		unknown sender	known sender
non-susceptible responses		544	132
susceptible responses		31	440
responses split into response options			
non-susceptible	ignore the message	359	102
	delete the message	272	39
susceptible	open the link	6	257
	share the link	0	11
	respond to the message	14	295
	like the message	11	133

Table 5 Results of the confirmatory multilevel logistic model for intended behaviour (DV) as predicted by user-sender relation (unknown, known sender) and consequences of not clicking (no, low, high).

Predictors	Coefficient	Wald chi^2	*p*	*OR*	CI_{LL}	CI_{UL}
(Intercept)	−8.48	140.33	<0.001	0.00	0.00	0.00
Known sender[a]	15.18	208.83	<0.001	3.90e + 06	4.98e + 05	3.05e + 07
Low consequences[b]	0.31	0.19	0.67	1.36	0.34	5.49
High consequences[b]	0.01	0.00	0.99	1.01	0.23	4.36
High consequences[c]	−0.30	0.16	0.69	0.74	0.18	3.12
Known Sender[a]*Low consequences[b]	0.59	0.47	0.50	1.80	0.34	9.69
Known Sender[a]*High consequences[b]	0.35	0.16	0.69	1.42	0.26	7.81
Known Sender[a]*High consequences[c]	−0.24	0.08	0.78	0.79	0.14	4.31
Random Effects						
ICC	0.06					
N_{id}	193					
Observations	1147					
Marginal R^2	0.39					
Conditional R^2	0.98					

[a]Reference: Unknown sender.
[b]Reference: No consequences.
[c]Reference: Low consequences.

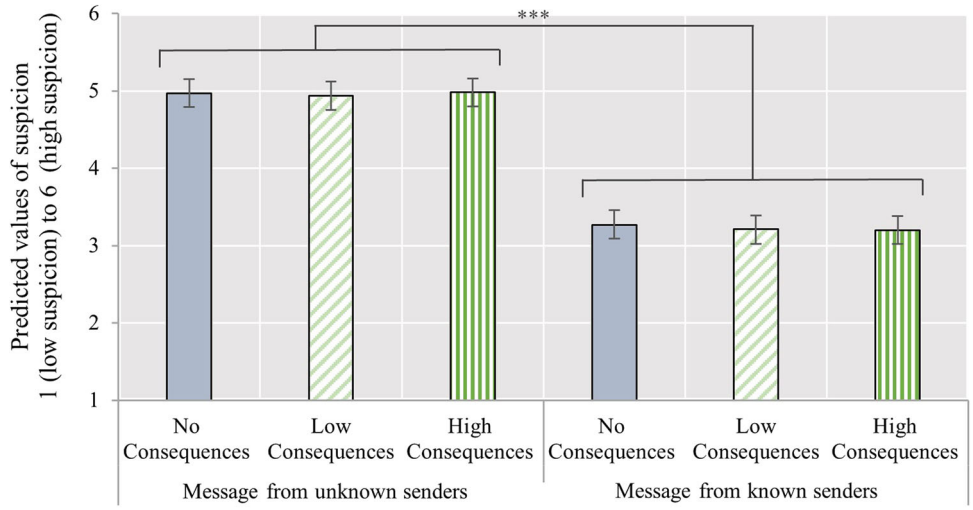

Fig. 3 Predicted values of suspicion from 1 (low suspicion) to 6 (high suspicion) divided into no, low, and high consequences of not clicking for unknown and known message sender. Error bars indicate the confidence intervals of the predicted values.

of Trait FoMO ($\beta = 1.04$, $p = 0.17$, $OR = 2.82$, 95 % CI: [0.64, 12.39]). However, an interaction between *user-sender relation* and *Trait FoMO* ($\beta = 3.11$, $p < 0.05$, $OR = 22.43$, 95 % CI: [1.49, 338.13]), which significantly improved model fit ($p < 0.05$), was examined. In line with Sommet and Davide (2017), the data was split between participants (1) with low and (2) high Trait FoMO scores. Two multilevel logistic regression analyses were calculated on the split data sets. The split-data analysis revealed that the chances for susceptible responses towards known compared to unknown senders sharply increased when participants indicated high ($\beta = 19.27$, $p < 0.001$, $OR = 2.33e+08$, 95 % CI: [2.91e + 06, 1.87e + 10]) compared to low Trait FoMO scores ($\beta = 9.03$, $p < 0.001$, $OR = 8.36e+03$, 95 % CI: [5.19e + 02, 1.35e + 05]). The effects of gender ($\beta = 0.30$, $p = 0.68$, $OR = 1.35$, 95 % CI: [0.32, 5.58]) and previous phishing experience via email ($\beta = -0.36$, $p = 0.68$, $OR = 0.70$, 95 % CI: [0.13, 3.79]), Instagram ($\beta = 0.09$, $p = 0.90$, $OR = 1.09$, 95 % CI: [0.26, 4.62]) and other social media platforms ($\beta = -0.11$, $p = 0.89$, $OR = 0.90$, 95 % CI: [0.20, 4.09]) were non-significant, indicating no effect on users' intended behaviour.

Confirmatory multilevel linear regression: influence of sender and consequences of not clicking on suspicion. Our results confirmed the proposed effect of *user-sender relation* on users' suspicion (see Fig. 3): When participants received phishing messages from known senders, they showed less suspicion ($\beta = -1.70$, 95 % CI: [−1.88, −1.53], $p < 0.001$) than when phishing messages were received from unknown senders. However, similar to the effects on intended behaviour, the proposed effect for *consequences of not clicking* on young adults' suspicion was not found. Suspicion did not significantly differ in low compared to no consequences ($\beta = -0.04$, 95 % CI: [−0.21, 0.14], $p = 0.69$) nor in high compared to no consequences ($\beta = 0.01$, 95 % CI: [−0.16, 0.18], $p = 0.93$). Similarly, suspicion did not differ between high compared to low consequences ($\beta = 0.04$, 95 % CI: [0.13, 0.21], $p = 0.63$). In addition, no significant interactions between *user-sender relation* and *consequences of not clicking* were found ($p \geq 0.52$). Table 7 summarizes the results of the confirmatory multilevel linear regression.

Exploratory multilevel linear regression: other exploratory influences on suspicion. As proposed in *Hypothesis 2*, we observed the effect of *Trait FoMO* on suspicion: Participants with high Trait FoMO scores reported lower suspicion towards phishing messages compared to those with low Trait FoMO scores ($\beta = -0.90$, 95 % CI: [−1.16, −0.64], $p < 0.001$, see Fig. 4). Interestingly, the analysis also revealed a significant interaction effect between *user-sender relation* and *Trait FoMO* ($\beta = -0.48$, 95 % CI: [−0.67, −0.28], $p < 0.001$). The data were split between (1) low and (2) high Trait FoMO scores, in which two multilevel linear regression analyses were calculated on the split data sets (Sommet and Davide, 2021). The split data analysis revealed that suspicion for known compared to unknown senders sharply decreased when participants indicated high Trait FoMO scores ($\beta = -1.94$, 95 % CI: [−2.16, −1.71], $p < 0.001$) compared to low Trait FoMO scores ($\beta = -1.46$, 95 % CI: [−1.71, −1.20], $p < 0.001$).

In addition, we found that *previous phishing experience* via email ($\beta = 0.58$, 95 % CI: [0.22, 0.93], $p < 0.01$) and other social

Table 7 Results of the confirmatory multilevel linear model for suspicion (DV) predicted by user-sender relation (unknown, known sender) and consequences of not clicking (no, low, high).

Predictors	Coefficient	*t*-value	*p*	CI_{LL}	CI_{UL}
(Intercept)	4.97	53.65	<0.001	4.79	5.15
Known sender[a]	−1.70	−19.58	<0.001	−1.88	−1.53
Low consequences[b]	−0.04	−0.41	0.69	−0.21	0.14
High consequences[b]	0.01	−0.08	0.93	−0.16	0.18
High consequences[c]	0.04	0.49	0.63	0.13	0.21
Known sender[a]*Low consequences[b]	−0.03	−0.24	0.81	−0.27	0.21
Known sender[a]*High consequences[b]	−0.08	−0.64	0.52	−0.32	0.16
Known sender[a]*High consequences[c]	−0.05	−0.40	0.69	−0.29	0.19
Random Effects					
ICC	0.32				
DEFF	2.62				
N_{id}	193				
Observations	1147				
Marginal R^2/ Conditional R^2	0.32/0.70				

[a]Reference: Unknown sender.
[b]Reference: No consequences.
[c]Reference: Low consequences.

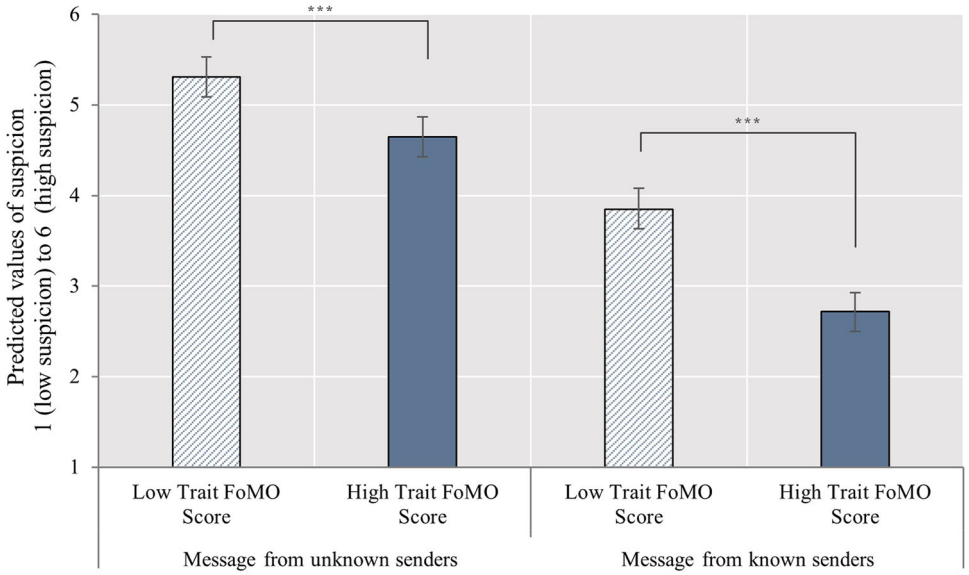

Fig. 4 Predicted values of suspicion from 1 (low suspicion) to 6 (high suspicion) divided into low and high Trait FoMO score and unknown and known message sender. Error bars indicate the confidence intervals of the predicted values.

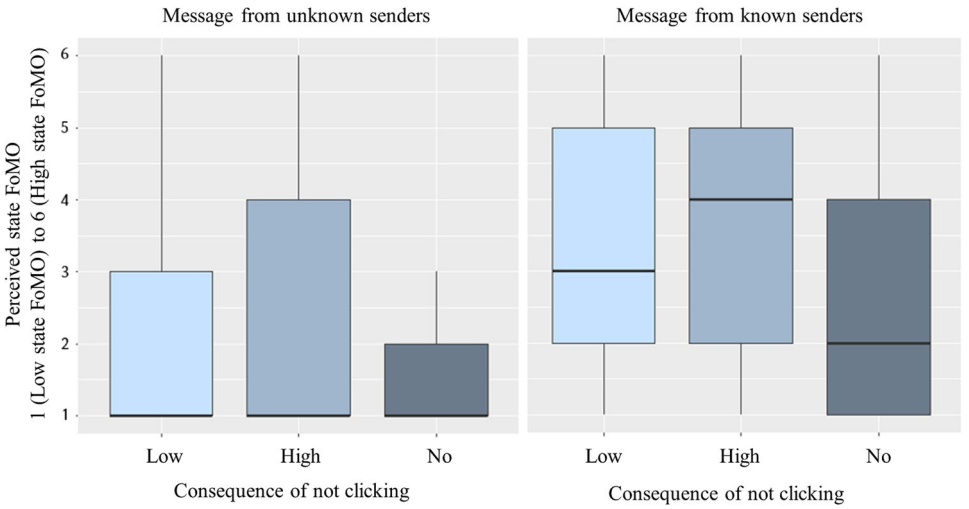

Fig. 5 Boxplots for State FoMO. The boxplots range from 1 (low state FoMO) to 6 (high state FoMO) and are divided into no, low and high consequences of not clicking on phishing messages received from unknown or known message senders.

media platforms than Instagram ($\beta = 0.35$, 95 % CI: [0.02, 0.68], $p < 0.05$) significantly increased participants' suspicion towards phishing messages compared to no previous experience. Surprisingly, compared to no previous experience, for *previous phishing experience* with Instagram only a marginal significant increase in suspicion was found ($\beta = 0.30$, 95 % CI: [−0.02, 0.62], $p = 0.07$). Lastly, *gender* was analysed as a predictor for suspicion. Our analysis revealed no effects of *gender* on users' suspicion ($\beta = -0.10$, 95 % CI: [−0.40, 0.20], $p = 0.52$).

Treatment check. As a treatment check, we examined whether *consequences of not clicking* (no vs. low vs. high) increased *State FoMO* in the message scenarios. As the item for *State FoMO* was not normally distributed, two non-parametric Friedman tests with an α-level of 0.05 comparing no, low, and high *consequences of not clicking* for (1) known and (2) unknown senders were calculated. For messages from known senders, the Friedman test indicated significant differences (χ^2 (2) = 57.13, $p < 0.001$, w = 0.15) in *State FoMO*: Post hoc tests revealed that participants perceived higher State FoMO for low (difference = 60.00) and high (*difference* = 108.00) compared to no *consequences of not clicking*. Moreover, participants perceived significantly higher State FoMO for high (*difference* = 48.00) compared to low *consequences of not clicking* (*critical difference* = 47.03). For messages from unknown senders, the Friedman test also indicated significant differences (χ^2 (2) = 34.53, $p < 0.001$, w = 0.09) in *State FoMO*. However, participants only perceived significantly higher State FoMO in high (*difference* = 71.00) compared to no *consequences*. On the contrary, State FoMO did not differ in low compared to high (*difference* = 35.50) nor in low compared to no (*difference* = 35.50) *consequences of not clicking* (*critical difference* = 47.03). Figure 5 shows that State FoMO is increased for known senders (Median = 2 to 4) compared to unknown senders (Median = 0).

Discussion

To develop effective countermeasures against phishing attacks on social media, understanding how the senders' social characteristics

and message content influence young adults' susceptibility is crucial. This study represents a first step in this direction, examining (1) the impact of the users' relation to the message sender, (2) the implied consequences of not clicking that induce State FoMO in phishing messages, and (3) the effect of users' Trait FoMO on their phishing susceptibility to such attacks on social media.

As first research indicates sender characteristics (e.g., profile picture) and the user-sender relation (e.g., close friend) to increase users' susceptibility towards social media phishing (Algarni et al., 2017; Seng et al., 2019; Vishwanath, 2015a), we assumed comparable effects for young adults on Instagram. Therefore, *hypothesis 1* proposed that phishing messages from known senders increase young adults' susceptibility compared to unknown senders. Our findings aligned with our expectations, yet they surpassed the anticipated effect size, underscoring the user-sender relation as a key predictor of susceptibility. A substantial majority of participants (93.4%) exhibited susceptible responses, such as answering the message or opening the link, when phishing messages were received from known senders. Compared to unknown senders, a predicted probability of 100% to show susceptible responses and sharply decreased suspicion towards known senders was revealed. In addition, we examined Trait FoMO, which has not been previously examined as a predictor for susceptibility on Instagram. However, it has been examined to affect online behaviour such as social media (over-) use (Przybylski et al., 2013; Tugtekin et al., 2020) or online risk-taking in younger users (Popovac and Hadlington, 2020). In *hypothesis 2* we therefore proposed that high Trait FoMO increases susceptibility to social media phishing compared to low Trait FoMO. Our results partially confirmed our hypothesis: although young adults with high compared to low Trait FoMO scores were not more likely to show susceptible responses, evidence was found that high Trait FoMO scores decrease young adults' suspicion towards phishing. Additionally, our results indicated that high Trait FoMO exacerbate the impact of user-sender relation: Young adults high in Trait FoMO showed more likely susceptible responses and decreased suspicion towards known compared to unknown senders than young adults low in Trait FoMO. As preliminary research indicated that State FoMO is similarly associated with online risk behaviour, as Trait FoMO (Holte, 2023), we investigated the consequences of not clicking within phishing messages as predictor for phishing susceptibility and assessed whether these can induce feelings of State FoMO in our participants. We proposed that phishing messages, implying low or high consequences of not clicking, increase susceptibility compared to no consequences of not clicking (*hypothesis 3.1*). Additionally, we assumed that phishing messages, implying high consequences of not clicking, increase susceptibility compared to low consequences of not clicking (*hypothesis 3.2*). However, other than expected, neither more likely susceptible responses nor less suspicion were found between no, low, and high consequences of not clicking. The treatment check therefore indicated that State FoMO seems to depend on the relation with the message sender, in which the proposed gradation of State FoMO was solely shown when messages were received from known senders. Lastly, exploratory analysis revealed that young adults' suspicion increased when they had previous experience with phishing via email or other social media services than Instagram. However, differences in gender did not seem to affect young adults intended behaviour or suspicion towards social media phishing.

As our study showed a much stronger effect of the user-sender relation for young adults on Instagram than previous studies for users on Facebook (Seng et al., 2019) or for other social sender characteristics (Algarni et al., 2017; Vishwanath, 2015a), it remains open to question why such an enhanced effect was found. One explanation could lay in the younger-aged sample: First, the effects of user-sender relation could be amplified for young adults, as they are found to be more susceptible to phishing in general (Frauenstein and Flowerday, 2020; Sheng et al., 2010; Tornblad et al., 2010). Second, the effects could be further increased as our younger sample showed increased Trait FoMO scores ($M_{ourstudy} = 3.15$) compared to previous studies such as from Przybylski and co-authors ($M_{YoungAdults} = 2.37$, Przybylski et al. (2013)).

Although our results indicated that users perceived higher State FoMO as intended for the different levels of consequences of not clicking (no < low < high), at least for known senders, the expected effects for the consequences of not clicking were not found. In other words, neither more likely susceptible responses nor less suspicion for high versus low versus no consequences of not clicking were found. One explanation could be that the user-sender relation is considered first in the decision process. As mentioned above, if the sender is perceived as trustworthy and authentic, low perceived cyber risks or heuristic processing could be triggered. However, if the sender is perceived untrustworthy and inauthentic, high perceived cyber risk and more systematic processing could be activated (see SCAM, Vishwanath et al. (2018)). In both cases, the chat message content and, thus, the consequences of not clicking could become less relevant for the decision process because the sender served as the initial criterion for trust and authenticity of the message.

Lastly, our results suggest that particularly young adults with high Trait FoMO and no previous phishing experience are vulnerable to social media phishing, as both indicators decreased users' suspicion. Herein, high Trait FoMO seems crucial, as it was associated with increased susceptibility towards known compared to unknown senders. These findings underscore that Trait FoMO can easily be exploited through phishers, especially when they impersonate a follower or friend. Coupled with the high susceptibility to our phishing messages - where 82.9 % of young adults showed susceptible responses to at least one phishing message -, counteracting social media phishing becomes highly relevant.

Counteracting social media phishing. Therefore, we suggest three intervention approaches: (1) Phishing awareness campaigns to raise awareness for cyber risks on social media, (2) Security nudges in social media chat messages to interrupt heuristic processing and (3) Emotional awareness campaigns to counteract high feelings of Trait FoMO. These three intervention approaches have been tested in current human-computer interaction (HCI) research, among others, to counteract vulnerabilities to email phishing. Therefore, they could be applicable to counteract the vulnerabilities related to social media phishing identified in our research.

As a first step, phishing awareness campaigns and training, commonly applied in email phishing (Franz et al., 2021), should be implemented and customised to the social characteristics exploited by phishers on social media platforms such as Instagram. These campaigns could then increase awareness of the cyber risks of social media and reduce the high susceptibility identified in our findings.

However, since campaigns and training alone may lead to decreased awareness over time (Franz et al., 2021), we propose security nudges in chat messages as an intervention approach to reach young adults where phishing affects them. Nudges, after Thaler and Sunstein (Thaler and Sunstein, 2009), can be described as small interface tweaks that guide users in the desired direction without limiting the existing choice set, i.e., none of the choices are made significantly more costly or prohibited. In

cybersecurity research, nudges have already been trialled to nudge towards the secure direction in the context of secure password creation (Zimmermann and Renaud, 2021; Zimmermann et al., 2023), secure Wi-Fi choices (Turland et al., 2015), cookie consent banners (Gerber et al., 2023), and also phishing (Franz et al., 2021). Phishing-related examples include the highlighting of domains (Lin et al., 2011) and interventions, leveraging social influences (Nicholson et al 2017) or using fear appeals (Schuetz et al., 2020). From an ethical standpoint and building on previous work by Hansen and Jespersen (Hansen and Jespersen, 2013), transparent nudges, such as reminders on the consequences of a particular behaviour (Caraban et al., 2019), targeting systematic processing were deemed most favourable. Related work could show that these nudges, while transparent, were still effective (Kroese et al., 2016; Zimmermann and Renaud, 2021; Zimmermann et al., 2023) and even have the potential to interrupt heuristic processes (Acquisti et al., 2017; Gerber et al., 2023). As social sender characteristics and the user-sender relation seem to trigger such heuristic processing (Frauenstein and Flowerday, 2020; Vishwanath, 2015a), interrupting these processes through transparent nudges could be highly beneficial in counteracting social media phishing. Herein, it appears crucial to place the nudge closely to the message and the actual decision taken. This is because even a single extra click could represent too much effort to take when pursuing other main tasks (Zimmermann and Renaud, 2021), such as reacting to social media messages. Future work could therefore examine non-intrusive nudges embedded directly into the social media chat interface (e.g., a visual warning) to reduce phishing susceptibility. As a result, this could interrupt heuristic processing and increase suspicion towards the message sender so that the message is checked in more detail.

Lastly, our findings highlight that high Trait FoMO reduced young adults' suspicion and amplified the impact of user-sender relation. Thus, supporting young adults in their emotion regulation may be another approach to counteract social media phishing. Herein, the effectiveness of user-centred emotion awareness campaigns, as suggested by Chen et al. (2022), could be investigated. Considering our findings, such campaigns could be not only promising to improve emotional well-being (Chen et al., 2022) but also to reduce phishing susceptibility.

Limitations and implications for future work. Our study has limitations that lead to methodological implications and suggestions for future work.

First, through the strong effects of the user-sender relation, particularly shown through intended behaviour, we cannot fully clarify the extent to which other potential susceptibility predictors, such as implied consequences of not clicking in phishing messages, affect susceptibility. Therefore, it might be helpful to preserve a lower user-sender relation in future research, for instance, when capturing other susceptibility indicators (e.g., scarcity). For instance, future studies could investigate the consequences of not clicking or other susceptibility indicators, such as scarcity, implied in messages within typical two-stage phishing attacks. These attacks often utilise social sender characteristics like profile pictures and friend counts, especially in fake accounts rather than in hijacked ones.

Second, this study used experimental online vignette survey methodology to systematically investigate the effects of the user-sender relation and the consequences of not clicking in more realistic scenarios than traditional questionnaire items (Atzmüller and Steiner, 2010). The integration of complementary indicators of susceptibility helped us draw conclusions about actual behaviour. Nevertheless, our experimental design cannot be fully extrapolated to actual behaviour because it focuses on specific and reduced scenarios, which do not fully capture the complexity of real-life situations. We therefore recommend gaining insights through qualitative data approaches such as online ethnography, e.g., through online observations or interviews with young adults on Instagram (Skågeby, 2011) to increase external validity in future research. In addition, we recommend investigating real phishing attacks on social media, e.g., by impersonating a phisher (Vishwanath, 2015b). However, conducting such real-life field studies poses ethical challenges, e.g., regarding privacy or informed consent (Munteanu et al., 2021), which need to be carefully addressed.

Lastly, even though we did not find an effect of gender on young adults' susceptibility to social media phishing, gender or other demographics (e.g., education, social media usage time) could be examined in the understudied area of social media phishing for young adults and other age groups in future research. This is particularly important because previous studies on email phishing have shown contradictory results across different demographic variables (e.g., gender or education, Tornblad et al. (2010)).

Conclusion

Our study expands previous social media phishing research. Our results provide unique empirical insights that highlight the user-sender relation as a crucial contributor to young adults' phishing susceptibility and their State FoMO when ignoring or deleting messages. High Trait FoMO, referring to a users' general FoMO on rewarding experiences (Holte, 2023; Maxwell et al., 2022), was found to reduce young adults' suspicion and to amplify the impact of the user-sender relation on young adults' susceptibility. For future research, we recommend maintaining a low user-sender relation to explore other potential predictors of susceptibility. In addition, we suggest combining complementary susceptibility indicators, such as suspicion and intended behaviour, as well as conducting real-life field studies to gain more insight into *why* users fall for phishing. To develop countermeasures against social media phishing, we suggest investigating the effectiveness of non-intrusive nudges, such as visual warnings.

Data availability

The data sets analysed during the current study are available on https://doi.org/10.18154/RWTH-2024-00509.

Received: 16 January 2024; Accepted: 25 June 2024;
Published online: 20 September 2024

Note

1 https://pavlovia.org/

References

Acquisti A, Adjerid I, Balebako R (2017) Nudges for privacy and security: understanding and assisting users' choices online. ACM Comput Surv 50(3):1–41. https://doi.org/10.1145/3054926

Algarni A, Xu Y, Chan T (2017) An empirical study on the susceptibility to social engineering in social networking sites: the case of facebook. Eur J Inform Syst 26(6):661–687. https://doi.org/10.1057/s41303-017-0057-y

American Psychological Association Ethical principles of psychologists and code of conduct. https://www.apa.org/ethics/code (2017)

Anti-Phishing Working Group Phishing activity trends report 4th qarter 2022. Tech. rep., Anti-Phishing Working Group (2022)

Atzmüller C, Steiner PM (2010) Experimental vignette studies in survey research. Methodology 6(3):128–138. https://doi.org/10.1027/1614-2241/a000014

Bates D, Mächler M, Bolker B (2015) Fitting linear mixed-effects models using lme4. J Stat Softw 67(1):1–48. https://doi.org/10.18637/jss.v067.i01

Bowman ND, Clark-Gordon CV (2019) Fear of missing out scale, Routledge, New York, NY, United States, pp 265–267. https://doi.org/10.4324/9780203730188-29

Caraban A, Karapanos E, Gonçalves D et al. (2019) 23 ways to nudge: a review of technology-mediated nudging in human-computer interaction. In: CHI' 19: Proceedings of the 2019 CHI Conference on Human factors in Computing systems. Association for Computing Machinery, New York, NY, United States, CHI, pp 1–15, https://doi.org/10.1145/3290605.3300733

Chaiken S (1980) Heuristic versus systematic information processing and the use of source versus message cues in persuasion. J Person Soc Psychol 39(5):752–766. https://doi.org/10.1037/0022-3514.39.5.752

Chen SC, Chang YH, Huang JH. et al. (2022) Exploring the effect of emotion awareness intervention on reducing fomo. In: CHI EA '22: Extended Abstracts of the 2022 CHI Conference on Human Factors in Computing Systems. Association for Computing Machinery, New York, NY, USA, CHI EA, pp 1–7, https://doi.org/10.1145/3491101.3519839

Chou FKY, Chen APS, Lo VCL (2021) Mindless response or mindful interpretation: examining the effect of message influence on phishing susceptibility. Sustainability 13(4):1–18. https://doi.org/10.3390/su13041651

Devitt K, Knighton L, Lowe K (2009) Young adults today: key data on 16-25 year-olds, transitions, disadvantage and crime. Young People in Focus (YPF), The Transition to Adulthood Alliance (T2A), Report, Young People in Focus Ltd, Brighton, p 14, https://pure.port.ac.uk/ws/portalfiles/portal/1587567/Young_People_in_Focus_Young_Adults_Today_2009.pdf

Dinh TCT, Lee Y (2022) "i want to be as trendy as influencers"–how "fear of missing out" leads to buying intention for products endorsed by social media influencers. J Res Interact Mark 16(3):346–364. https://doi.org/10.1108/JRIM-04-2021-0127

Eagly AH, Chaiken S (1993) The psychology of attitudes. Harcourt Brace Jovanovich College Publishers, San Diego, CA, United States

Franz A, Zimmermann V, Albrecht G et al. (2012) 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, Berkeley, CA, United States, SOUPS, pp 339–358, https://doi.org/10.26083/tuprints-00020675

Frauenstein ED, Flowerday S (2020) Susceptibility to phishing on social network sites: A personality information processing model. Computers & Security 94:1–18. https://doi.org/10.1016/j.cose.2020.101862

Gerber N, Stöver A, Peschke J et al. (2023) Don't accept all and continue: exploring nudges for more deliberate interaction with tracking consent notices. ACM Transactions on Computer-Human Interaction pp 1–32. https://doi.org/10.1145/3617363

Goel S, Williams K, Dincelli E (2017) Got phished? internet security and human vulnerability. J Assoc Inform Syst 18(1):22–44. https://doi.org/10.17705/1jais.00447

Hadlington L, Binder J, Stanulewicz N (2020) Fear of missing out predicts employee information security awareness above personality traits, age, and gender. Cyberpsychol Behav Soc Netw 23(7):459–464. https://doi.org/10.1089/cyber.2019.0703

Hansen PG, Jespersen AM (2013) Nudge and the manipulation of choice: a framework for the responsible use of the nudge approach to behaviour change in public policy. Eur J Risk Regul 4(1):3–28. https://doi.org/10.1017/S1867299X00002762

Holte AJ (2023) The state fear of missing out inventory: development and validation. Telemat Inform Rep 10:100055. https://doi.org/10.1016/j.teler.2023.100055, https://www.sciencedirect.com/science/article/pii/S2772503023000154

IBM Security Cost of a data breach report 2021. Tech. rep., Ponemon Institute and IBM Security

James, N (2023) 81 phishing attack statistics 2023: The ultimate insight. https://www.getastra.com/blog/security-audit/phishing-attack-statistics/

Kemp, S (2023) Digital 2023: Global overview report. Tech. rep., Data Reportal and We Are Social and Meltwater

Kroese FM, Marchiori DR, De Ridder DT (2016) Nudging healthy food choices: a field experiment at the train station. J Public Health 38(2):e133–e137. https://doi.org/10.1093/pubmed/fdv096

Lin E, Greenberg S, Trotter E et al. (2011) Does domain highlighting help people identify phishing sites? In: CHI'11: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. Association for Computing Machinery, New York, NY, United States, CHI, pp 2075–2084, https://doi.org/10.1145/1978942.1979244

Lourenço MB, Marinos L (2020) Enisa threat landscape 2019/2020 - the year in review. Tech. rep., European Union Agency for Cybersecurity, Attiki, Greece, https://doi.org/10.2824/552242

Maxwell LC, Tefertiller A, Morris D (2022) The nature of fomo: trait and state fear-of-missing-out and their relationships to entertainment television consumption. Atlantic J Commun 30(5):522–534. https://doi.org/10.1080/15456870.2021.1979977

Munteanu C, Waycott J, McNaney R (2021) Dealing with ethical challenges in hci fieldwork. In: Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems. Association for Computing Machinery, New York, NY, United States, CHI EA, pp 1–3, https://doi.org/10.1145/3411763.3445006

Nicholson J, Coventry L, Briggs P (2017) Can we fight social engineering attacks by social means? assessing social salience as a means to improve phish detection. In: Proceedings of the Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017). USENIX Association, Berkeley, CA, USA, SOUPS, pp 285–298

Oliveira D, Rocha H, Yang H et al. (2017) Dissecting spear phishing emails for older vs young adults: on the interplay of weapons of influence and life domains in predicting susceptibility to phishing. In: Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems. Association for Computing Machinery, New York, NY, USA, CHI, p 6412−6424, https://doi.org/10.1145/3025453.3025831

Parker HJ, Flowerday SV (2020) Contributing factors to increased susceptibility to social media phishing attacks. South Afr J Inform Manag 22(1):1–10. https://doi.org/10.4102/sajim.v22i1.1176

Popovac M, Hadlington L (2020) Exploring the role of egocentrism and fear of missing out on online risk behaviours among adolescents in south africa. Int J Adolesc Youth 25(1):276–291. https://doi.org/10.1080/02673843.2019.1617171

Przybylski AK, Murayama K, DeHaan CR (2013) Motivational, emotional, and behavioral correlates of fear of missing out. Comput Hum Behav 29(4):1841–1848. https://doi.org/10.1016/j.chb.2013.02.014

R Core Team (2019) The r project for statistical computing. https://www.R-project.org/

RStudio Team (2022) Rstudio: Integrated development for r. https://posit.co/download/rstudio-desktop/

Schuetz SW, Benjamin Lowry PB, Pienta DA (2020) The effectiveness of abstract versus concrete fear appeals in information security. J Manag Inform Syst 37(3):723–757. https://doi.org/10.1080/07421222.2020.1790187

Seng S, Kocabas H, Al-Ameen MN et al. (2019) Poster: Understanding user's decision to interact with potential phishing posts on facebook using a vignette study. In: CCS'19: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security. Association for Computing Machinery, New York, NY, United States, CCS, p 2617-2619, https://doi.org/10.1145/3319535.3363270

Sheng S, Holbrook M, Kumaraguru P et al. (2010) Who falls for phish? a demographic analysis of phishing susceptibility and effectiveness of interventions. In: Proceedings of the ACM conference on human factors in computing systems. ACM, New York, NY, USA, pp 373–382,https://doi.org/10.1145/1753326.1753383

Skågeby J (2011) Online ethnographic methods: towards a qualitative understanding of virtual community practices. In: Handbook of research on methods and techniques for studying virtual communities: Paradigms and phenomena. IGI Global, Hershey, PA, United States, p 410–428, https://doi.org/10.4018/978-1-60960-040-2.ch025

Sommet N, Davide M (2017) Keep calm and learn multilevel logistic modeling: A simplified three-step procedure using stata, r, mplus, and spss. Int Rev Soc Psychol 30(1):203–218. https://doi.org/10.5334/irsp.90

Sommet N, Davide M (2021) Keep calm and learn multilevel linear modeling: A three-step procedure using spss, stata, r, and mplus. Int Rev Soc Psychol 34(1):1–19. https://doi.org/10.5334/irsp.555

Tandon A, Dhir A, Almugren I (2021) Fear of missing out (fomo) among social media users: a systematic literature review, synthesis and framework for future research. Internet Res 31(3):782–821. https://doi.org/10.1108/INTR-11-2019-0455

Thaler RH, Sunstein CR (2009) Nudge: improving decisions about health, wealth, and happiness. Penguin Books, London, UK

Tornblad MK, Jones KS, Namin AS et al. (2010) Characteristics that predict phishing susceptibility: A review. In: CHI '10: Proceedings of the SIGCHI Cconference on Human Factors in Computing Ssystems. Association for Computing Machinery, New York, NY, United States, CHI, pp 373–382, https://doi.org/10.1145/1753326.1753383

Tugtekin U, Tugtekin EB, Kurt AA (2020) Associations between fear of missing out, problematic smartphone use, and social networking services fatigue among young adults. Social Media Soc 6(4):1–17. https://doi.org/10.1177/2056305120963760

Turland J, Coventry L, Jeske D et al. (2015) Nudging towards security: Developing an application for wireless network selection for android phones. In: British HCI' 15: Proceedings of the 2015 British HCI conference. Association for Computing Machinery, New York, NY, United States, British HCI, pp 193–201, https://doi.org/10.1145/2783446.2783588

van der Schyff K, Flowerday S(2023) The mediating role of perceived risks and benefits when self-disclosing: a study of social media trust and fomo Comput Security 126:103071. https://doi.org/10.1016/j.cose.2022.103071

van der Schyff K, Renaud K, Townes JP(2022) Investigating the mediating effects of phubbing on self-presentation and fomo within the context of excessive

instagram use Cogent Psychol 9(1):2062879. https://doi.org/10.1080/23311908.2022.2062879
Vishwanath A (2015b) Habitual facebook use and its impact on getting deceived on social media. J Comput Mediated Commun 20(1):83–98. https://doi.org/10.1111/jcc4.12100
Vishwanath A (2015a) Diffusion of deception in social media: Social contagion effects and its antecedents. Inform Syst Front 17:1353–1367. https://doi.org/10.1007/s10796-014-9509-2
Vishwanath A (2017) Getting phished on social media. Decis Support Syst 103:70–81. https://doi.org/10.1016/j.dss.2017.09.004
Vishwanath A, Harrison B, Ng YJ (2018) Suspicion, cognition, and automaticity model of phishing susceptibility. Commun Res 45(8):1146–1166. https://doi.org/10.1177/0093650215627483
Wang Z, Sun L, Zhu H (2020) Defining social engineering in cybersecurity. IEEE Access 8:85094–85115. https://doi.org/10.1109/ACCESS.2020.2992807
Waqas M, Hania A, Yahya F (2023) Enhancing cybersecurity: The crucial role of self-regulation, information processing, and financial knowledge in combating phishing attacks. SAGE Open 13(4):21582440231217720. https://doi.org/10.1177/21582440231217720
Westin F, Chiasson, S (2021) "it's so difficult to sever that connection": The role of fomo in users' reluctant privacy behaviours. In: CHI '21: Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems. Association for Computing Machinery, New York, NY, United States, CHI, pp 1–15, https://doi.org/10.1145/3411764.3445104
Workman M (2008) Wisecrackers: a theory-grounded investigation of phishing and pretext social engineering threats to information security. J Am Soc Inform Sci Technol 59(4):662–674. https://doi.org/10.1002/asi.20779
Yan Z, Robertson T, Yan R (2018) Finding the weakest links in the weakest link: How well do undergraduate students make cybersecurity judgment? Comput Human Behav 84:375–382. https://doi.org/10.1016/j.chb.2018.02.019
Zhuo S, Biddle R, Koh YS (2023) Sok: Human-centered phishing susceptibility. ACM Transact Privacy Security 26(3):1–27. https://doi.org/10.1145/3575797
Zimmermann V, Renaud K (2021) The nudge puzzle: matching nudge interventions to cybersecurity decisions. ACM Transact Comput Human Interact 28(1):1–45. https://doi.org/10.1145/3429888
Zimmermann V, Marky K, Renaud K (2023) Hybrid password meters for more secure passwords–a comprehensive study of password meters including nudges and password information. Behav Inform Technol 42(6):700–743. https://doi.org/10.1080/0144929X.2022.2042384

Acknowledgements

The contribution of JK and CB was supported by the Federal Ministry of Education and Research (Bundesministerium für Bildung und Forschung, BMBF) within the funded project "Adaptively promoting digital competence and sovereignty of adolescents through micro games" [A-DigiKomp: Digitale Kompetenz und Souveränität Adoleszenter durch Micro Games adaptiv fördern"; grant number: 16SV8541]. The funders had no role in the study design, data collection and analysis, decision to publish, or preparation of the manuscript.

Author contributions

JK, CB and JS designed the study. JK and JS performed the study. JK, JS, CB, VZ and SJS analysed and interpreted the data. JK wrote the initial draft of the paper. JS, CB, VZ and SJS critically revised the manuscript. All authors have contributed to, read, and approved the final version of the manuscript.

Funding

Open Access funding enabled and organized by Projekt DEAL.

Competing interests

The authors declare no competing interests.

Ethical Approval

The study was designed to comply with established guidelines for research involving humans (American Psychological Association, 2017) and the EU General Data Protection Regulation (EU-GDPR). Approval was obtained from the ethics committee of HSD Hochschule Döpfer (BEth_20_22, decision of May 19, 2022), with no ethical concerns raised.

Informed consent

All participants gave informed consent for their participation, for adhering to the privacy declaration, and for their data being published in anonymised and aggregated form in a data repository. To avoid bias in the responses, the study aim was more vaguely phrased as gaining insight into users' reactions to different Instagram messages. In the follow-up questionnaire, participants then received detailed information on the study aims.

Additional information

Correspondence and requests for materials should be addressed to Jennifer Klütsch.

Reprints and permission information is available at http://www.nature.com/reprints

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.