Int. J. Human–Computer Studies 197 (2025) 103456



Contents lists available at ScienceDirect

International Journal of Human - Computer Studies

journal homepage: www.elsevier.com/locate/ijhcs



InstaTrust or InstaTrap: How relationships and developmental tasks affect young adults' phishing susceptibility on Instagram

Jennifer Klütsch [a,*], Luise Haehn [a], Annika Kreuder [b,a], Christian Böffel [a], Ulrich Frick [b,1,2], Sabine J. Schlittmeier [a]

[a] Work and Engineering Psychology, RWTH Aachen University, Jägerstraße 17-19, 52066 Aachen, Germany
[b] Research Center, HSD Hochschule Döpfer, Waidmarkt 3 und 9, 50676 Köln, Germany

ARTICLE INFO

Keywords:
Social media phishing
Young adults
Susceptibility
Developmental task
Relationship
Follower

ABSTRACT

Social media phishing attacks are on the rise, with phishers exploiting the social nature of social media and often targeting young adults, the primary user group of most social media platforms. This study examines young adults' susceptibility to social media phishing by integrating a novel developmental perspective. In doing so, it explores the unexamined user-specific susceptibility to phishers who offer developmental opportunities to fulfill age-related developmental tasks. In our experimental online vignette study, 500 young adults between the ages of 16 and 29 years were presented with Instagram chat messages sent by non-followers or followers offering a social, job or partner opportunity to fulfill three selected developmental tasks: (1) belonging to a peer group, (2) entering professional life and (3) being in a committed relationship. For instance, participants received phishing scenarios from supposed followers that introduced them to an upcoming event, an ideal job or partner. Our results indicate that both the relationship with the phisher and, in particular, a social opportunity are predictors of susceptibility. Messages from followers (compared to non-followers) inviting them to an upcoming event and thus offering a social opportunity to fulfill the developmental task of belonging to a peer group (compared to other developmental opportunities) led to the highest susceptibility. Based on our findings, we derive implications for future research and for phishing awareness campaigns for young adults.

1. Introduction

Social media platforms seem almost indispensable, especially for young adults (approx. 16 to 29 years), who are the main users of platforms such as Instagram (Kemp, 2023; Pew Research Center, 2021). However, the high usage and popularity of these platforms come at a high risk of social media fraud with a total of $2.7 billion dollars in reported losses to scams on social media between 2021 to mid-2023 (Federal Trade Commission, 2023). The ease of access, personalization, simplicity of messaging and the trust and familiarity that social media platforms offer make these platforms particularly appealing to phishers (Chung et al., 2021). Within these platforms, phishers typically attack in two stages. Initially, the phisher sends a friend request from a fake account to establish contact with the victim (stage 1). Subsequently, the phisher contacts the victim via a direct message or post, leveraging any available personal information from the victim's profile, when feasible (stage 2) (Vishwanath, 2015a, 2017). In some cases, the phishing attack can be further personalized, when the accounts of known friends are hijacked and used by the phisher to immediately contact their victims. Consequently, phishers can deceive their victims by exploiting social engineering (SE) techniques such as Liking or Social Proof (Parker and Flowerday, 2020; Workman, 2008). For example, in order to obtain sensitive information such as login data, phishers masquerade as someone the user likes such as their followers (utilizing

* Corresponding author at: Work and Engineering Psychology, RWTH Aachen University, Jägerstraße 17-19, 52066 Aachen, Germany.
E-mail addresses: kluetsch@psych.rwth-aachen.de (J. Klütsch), luise.haehn@psych.rwth-aachen.de (L. Haehn), annika.kreuder@psych.rwth-aachen.de (A. Kreuder), boeffel@psych.rwth-aachen.de (C. Böffel), ulrich.frick@uni-wuerzburg.de (U. Frick), sabine.schlittmeier@psych.rwth-aachen.de (S.J. Schlittmeier).
[1] Institute for Clinical Epidemiology and Biometry, Julius-Maximilians-University Würzburg, Josef-Schneider-Str. 2, 97080 Würzburg, Germany.
[2] Ulrich Frick (Prof. Dr.) was a Senior Scientist at the Institute for Clinical Epidemiology and Biometry (IKE-B) at the Julius-Maximilians-University Würzburg. He served as the founding Dean of Psychology, Head of the Research Center, and Senior Scientist at HSD Hochschule Döpfer until 2023. His work spanned a broad portfolio in Public Health, Epidemiology, and Psychology, with a particular focus on risk perception and digital competence, especially among adolescents and young adults. Ulrich Frick sadly passed away during the revision process of this manuscript.

https://doi.org/10.1016/j.ijhcs.2025.103456
Received 4 December 2023; Received in revised form 20 November 2024; Accepted 22 January 2025
Available online 23 January 2025
1071-5819/© 2025 The Authors. Published by Elsevier Ltd. This is an open access article under the CC BY license (http://creativecommons.org/licenses/by/4.0/).

the SE technique of 'Liking') and exploit their tendency to imitate the behavior of relevant others (tapping into the SE technique of 'Social Proof') (Frauenstein and Flowerday, 2020). These attacks can be considered a significant online risk with success rates exceeding those of traditional email phishing (Blancaflor et al., 2021). It is therefore essential to investigate the predictors of users' susceptibility on social media in order to develop user-centered intervention approaches, which can counteract these phishing attacks.

While the majority of research has focused on email phishing (Algarni et al., 2017), there has recently been a growing focus on social media phishing. For example, studies have examined habitual social media use (Vishwanath, 2015b) and social characteristics of phishers, such as their profile picture (Vishwanath, 2015a), as important predictors of susceptibility to social media phishing. However, researchers emphasize, among other things, the need for further research to identify user-specific susceptibilities, particularly to social media phishing (Algarni et al., 2017; Waqas et al., 2023). Given their increased use of most social media platforms (Kemp, 2023; Pew Research Center, 2021), young adults represent a particularly relevant area for future investigation.

Building on developmental research, the present study aims to provide insight into this age group by exploring a user-specific characteristic that has not yet been examined: the desire of young adults to accomplish age-related developmental tasks (Arnett, 2000). As defined by Havighurst (1948), a developmental task is one that arises during a particular stage of life. Its successful completion can contribute to the individual's happiness and future success, whereas its failure can result in unhappiness, disapproval from society, and difficulty in subsequent tasks (Havighurst, 1948). Examples of developmental tasks in young adulthood include, but are not limited to, belonging to a peer group, entering professional life or being in a committed relationship (Arnett, 2000; Seiffge-Krenke, 2015). Related areas of research highlight that young adults' online behavior can be influenced by their desire to accomplish certain developmental tasks, underscoring its importance (Borca et al., 2015; Coyne et al., 2013; Steijn, 2014; Van den Broeck et al., 2015). However, no study has investigated such a developmental perspective in phishing research. Nevertheless, it seems likely that this desire also influences young adults' susceptibility, for example, when phishers impersonate a follower and offer the opportunity to fulfill developmental tasks by introducing young adults to an upcoming event, an ideal job or partner. Using a scenario-based online vignette study, we aim to address this research gap and examine young adults' susceptibility to phishing messages sent by a follower or non-follower (*relationship*) on Instagram offering *developmental opportunities* to fulfill developmental tasks. The resulting research question is as follows:

How is young adults' susceptibility to social media phishing affected by their *relationship* to the phisher and the *developmental opportunity* to fulfill a developmental task offered in a phishing message?

Through answering this research question, we aim to (1) provide empirical evidence on how messages from followers, that offer developmental opportunities for young adults, affect their phishing susceptibility to social media phishing. In addition, we aim to (2) provide user-specific suggestions to counteract such phishing attacks based on our findings.

2. Related work

This section provides an overview of psychological theories about why users fall for social media phishing and related research on social media phishing, young adults and their developmental tasks.

2.1. Information processing in social media phishing

According to information security research (Chou et al., 2021; Frauenstein and Flowerday, 2020; Vishwanath et al., 2018), the tendency of users to fall for phishing messages depends on the way users cognitively process these messages. Based on the **H**euristic-**S**ystematic **M**odel (HSM; Chaiken, 1980; Eagly and Chaiken, 1993)), two types of cognitive processes can be distinguished: (1) *heuristic processing*, where messages are processed quickly, without much effort and based on simple rules of thumb (heuristics), and (2) *systematic processing*, where they are processed thoughtfully and analytically. It is assumed that users who process information heuristically rely on certain cues of a message and show limited attention to other cues, whereas users who process information systematically carefully consider all message cues (Chou et al., 2021; Vishwanath et al., 2018).

The **S**uspicion, **C**ognition, and **A**utomaticity **M**odel (SCAM), developed by Vishwanath et al. (2018), builds on the HSM perspective. It states that users with low *cyber risk beliefs* (e.g., due to messages from trustworthy senders) are highly susceptible to phishing because they may rely on *heuristic* rather than *systematic processing*. Such *heuristic processing* may reduce users' attention to malicious cues and, thus, reduce their suspicion of phishing messages. In addition to these two cognitive processes, the SCAM assumes *automaticity* in behavior to reduce suspicion. Automatic behavior through habits, such as ritualized checking of messages, may reduce suspicion towards phishing because users interact with phishing messages without processing them. These habits seem to depend on the users' *self-regulation*, known as their ability to control their media use (Vishwanath et al., 2018). Integrating these insights from the SCAM (Vishwanath et al., 2018), users may be more likely to fall for phishing on social media because these platforms are perceived as trusted and familiar environments, which reduces their *cyber-risk beliefs* about messages (Frauenstein and Flowerday, 2020). These reduced *cyber-risk beliefs* then may encourage them to engage in quick and thoughtless *heuristic* rather than *systematic processing* of social media chat messages and reduce their suspicion. In addition, social media is likely associated with habitual and ritualized usage behaviors (*habits*) that reduce suspicion, while these habits seem to depend on how well users can control their social media use (Vishwanath, 2015b; Vishwanath et al., 2018).

2.2. Social engineering in social media phishing

While social media is valued as a trusted and habitually-used environment, its design makes it also inherently conducive to the effectiveness of SE attacks (see Frauenstein and Flowerday (2020), for a review). An SE attack can be defined as an "attack wherein the attacker (s) exploit human vulnerabilities by means of social interaction to breach cyber security" (Wang et al., 2020). These attacks are based on six key principles of persuasion, known as (1) Reciprocation, (2) Commitment and Consistency, (3) Social Proof, (4) Liking, (5) Authority and (6) Scarcity (Cialdini, 2007), and have been shown to increase users' susceptibility to email phishing (Butavicius et al., 2016; Parsons et al., 2019). In social media, these social engineering tactics may become more hazardous, as phishers are able to impersonate a follower or friend through a fake or captured account to persuade the victim that the message is credible (utilizing the SE technique of 'Social Proof') and sent by someone they like (utilizing the SE technique of 'Liking') (Frauenstein and Flowerday, 2020). From a SCAM perspective (Vishwanath et al., 2018), this may reduce users' suspicion as messages from known accounts are perceived as rather harmless (low cyber risks), thus promoting quick, heuristic processing. In addition, users' heuristic processing may be encouraged because social characteristics of a phisher such as the number of likes serve as a heuristic cue (Algarni et al., 2017; Vishwanath, 2015a). Reduced attention might also explain why these persuasive strategies are effective: because users' primary task is to respond to a friend's message or post, protecting their own safety becomes a subordinate task. As a result, their attention towards suspicious cues can be reduced (Montañez et al., 2020). Unexpected events, such as deceptive links, can then be overlooked (Montañez et al., 2020), a phenomenon known as *inattentional blindness* in cognitive psychology (Mack and Rock, 1998; Pfleeger and Caputo, 2012). Hence, phishers

take advantage of social media not only as a trusted and habitually used environment, but also as a medium with a strong social component.

2.3. Research on social media phishing

Prior studies have confirmed the risk associated with the social component of social media. For example, evidence has been found that social characteristics of a phisher, such as the number of followers (Algarni et al., 2017; Vishwanath, 2017), common friends, the profile picture (Vishwanath, 2015a), can influence users' susceptibility to phishing. In this regard, researchers observed that users were more likely to fall for stage 1 (friend requests) and stage 2 (information requests) phishing attacks when the phishers' profile included a picture or had friends in common (Vishwanath, 2015a). Similar results were observed in other studies, with researchers highlighting that the number of followers can increase the perceived authenticity of a phisher's friend request (Vishwanath, 2017) as well as the perceived sincerity of phishing messages (Algarni et al., 2017).

However, despite these social characteristics of a phisher, prior research on email phishing indicates that susceptibility can also be influenced by user-specific characteristics such as personality or age. For example, Frauenstein and Flowerday (2020) examined users' manifestation of certain personality traits to influence susceptibility to email phishing. The researchers discovered that users with high levels of openness or agreeableness were more likely to engage in heuristic processing, which increased their susceptibility to email phishing (Frauenstein and Flowerday, 2020). In addition, researchers have identified age as a user-specific characteristic. In these age-related studies, numerous researchers found that young adults show higher susceptibility to both email and social media phishing compared to older adults. Nevertheless, other age-related studies cannot confirm these effects (Gavett et al., 2017; Tornblad et al., 2021), highlighting additional user-specific characteristics as alternative explanations for age-related susceptibility to phishing (Tornblad et al., 2021). For example, Sheng et al. (2010) found that younger users may be more susceptible to email phishing due to lower levels of education, fewer years of internet experience, less exposure to educational materials, and less aversion to financial risk. In addition, researchers have emphasized that age-related susceptibility is contingent on the specific SE technique employed in phishing messages. For example, SE techniques that invoke the notion of scarcity, such as those that imply limited availability, have been shown to lead to an increased susceptibility to email phishing in this age group (Oliveira et al., 2017). Additionally, Oliveira et al. (2017) suggest that messages related to specific life domains (e.g. legal, ideological) can increase users' susceptibility to phishing. In social media phishing, Algarni et al. (2017) found that younger users are more susceptible on Facebook, while Klütsch et al. (2024) examined that their individual level of Fear of Missing Out (FoMO) may increase their susceptibility to social media phishing. In summary, these findings indicate that user-specific characteristics are of high importance in understanding susceptibility to phishing. However, given that previous research has primarily focused on email phishing, avenues for future research include further investigation of user-specific and message characteristics that influence users' susceptibility to social media phishing in particular (Algarni et al., 2017).

2.4. Young adults as user group

Young adults represent a highly relevant area for future research on social media phishing. On the one hand, young adults are considered the primary user group of social media, placing them at an increased risk of becoming a target of social media phishing (Kemp, 2023; Pew Research Center, 2021). On the other hand, they are considered an important user group due to their increased susceptibility to both email and social media phishing (Algarni et al., 2017; Sheng et al., 2010; Tornblad et al., 2021).

One user-specific characteristic that has not yet been examined and may determine this increased susceptibility in young adults is highlighted by developmental research through developmental tasks (Arnett, 2000). While developmental tasks describe tasks that occur during a particular life stage (Havighurst, 1948), researchers emphasize that this age group strives for a variety of them. Examples of developmental tasks include belonging to a peer group, entering professional life or being in a committed relationship (Arnett, 2000; Seiffge-Krenke, 2015). Given that phishers can target these developmental tasks within their phishing messages, this user-group specific characteristic may predispose young adults to increased phishing susceptibility. For example, when phishers impersonate a friend introducing a young adult to an upcoming event, their dream job or an ideal partner, young adults are presented with a highly relevant opportunity that aligns with their developmental task. As a result, such developmental opportunities within a phishing message may be perceived as highly relevant, thereby directing young adults' attention to their developmental task rather than the suspicious link.

While no study has specifically examined the role of developmental tasks for young adults in phishing, the developmental perspective has been integrated into other areas of research on users' online behavior (Borca et al., 2015; Coyne et al., 2013; Steijn, 2014; Van den Broeck et al., 2015). For example, Steijn (2014) examined that young adults post more frequently on social media to belong to their peer group and control their privacy settings more actively to enter professional life. Young adults' need to belong is therefore of particular research interest, because they have been found to perceive increased Fear of Missing Out (FoMO) (Przybylski et al., 2013; Westin and Chiasson, 2021) and because their online behavior has been found to be strongly influenced by their peer group (Kreuder et al., 2023, 2024; Mendel and Toch, 2017).

3. Present study

In this scenario-based online study, we aim to examine young adults' susceptibility to phishing on Instagram – the most used social media platform among young adults (Kemp, 2023). Susceptibility was assessed with two commonly used and complementary indicators: (1) intended behavior (Frauenstein and Flowerday, 2020) and (2) suspicion (Vishwanath et al., 2018). Intended behavior assessed participants' response to each message categorized as either susceptible (open/share the link or respond to/like the message) or not susceptible (ignore/delete the message) (Frauenstein and Flowerday, 2020). Suspicion assessed the level of uncertainty towards a phishing message and was measured through the suspicion scale (Vishwanath et al., 2018). Here and below, we refer to increased susceptibility as an increase in susceptible responses and a decrease in the level of suspicion.

Our main research goal is to investigate how the *relationship* with a phisher and the *developmental opportunity* offered in a phishing message affect young adults' susceptibility to phishing on social media. The developmental opportunities were selected to fulfill three developmental tasks, often mentioned relevant in related research areas (Borca et al., 2015; Coyne et al., 2013; Steijn, 2014; Van den Broeck et al., 2015): (1) a *social opportunity* to fulfill the developmental task of belonging to a peer group, (2) a *job opportunity* to fulfill the developmental task of entering professional life and (3) a *partner opportunity* to fulfill the developmental task of being in a committed relationship. Based on preliminary research highlighting increased FoMO among young adults (Przybylski et al., 2013; Westin and Chiasson, 2021) and online behaviors that are strongly influenced by their peer group (Kreuder et al., 2023, 2024; Mendel and Toch, 2017), we propose the following:

Hypothesis 1. *Messages from followers will increase susceptibility compared to messages from non-followers.*

Hypothesis 2. *Messages addressing social opportunities to fulfill the*

developmental task of belonging to a peer group will increase susceptibility compared to messages offering other developmental opportunities.

In addition, we exploratively examine the relevance of developmental opportunities through the fulfillment and importance of its related developmental task. We propose the following:

Hypothesis 3. *Messages offering opportunities to fulfill developmental tasks, which are perceived as important and/or not fulfilled, will increase susceptibility compared to messages offering opportunities to fulfill developmental tasks which are perceived as not important and/or fulfilled.*

To gain deeper insight into the sample, we further examine how age, gender or Instagram use affect young adults' susceptibility.

4. Method

The study[3] ($N = 500$) was conducted online using PsychoPy (Peirce et al., 2019), HTML and JavaScript and was hosted by Pavlovia (https://pavlovia.org/). We used vignette scenarios referring to short, carefully constructed descriptions (Atzmüller and Steiner, 2010) of social media phishing situations visualized through images of Instagram chat screens. The scenarios varied for two independent variables in a 2 × 3 study design: (a) the *relationship* to the phisher (follower vs. non-follower) and (b) the *developmental opportunity* offered in the phishing message (social vs. job vs. partner opportunity). As dependent variables, we queried two indicators of young adults' susceptibility: (1) intended behavior (Frauenstein and Flowerday, 2020) and (2) suspicion (Vishwanath et al., 2018). In addition, we exploratively examined the relevance of the messages through the fulfillment and importance of the developmental tasks addressed, operationalizing the **D**evelopmental **T**ask **Q**uestionnaire for **Y**oung **A**dults (DTQ-YA; Seiffge-Krenke, 2001).

4.1. Procedure

Before the experiment started, participants received study information and gave informed consent for participation. Then, participants were asked for socio-demographic information (e.g., age, gender) and their daily use of the internet, social media and messaging services. Afterwards, the vignette scenarios were presented. To investigate young adults' susceptibility towards social media phishing, six message scenarios (see Section 4.2) were presented twice and the participants were queried (1) for intended behavior and, afterwards, (2) for suspicion. We opted to measure participants' intended behaviour before assessing suspicion to mitigate potential carry-over effects of the suspicion questionnaire. After completion of all vignette scenarios, follow-up questionnaires, including users' fulfillment and importance of certain developmental tasks were administered (see Section 4.3). Afterwards, participants were able to give additional feedback for the study. The concluding debriefing included information about the purpose of the research as well as further advice, such as on how to detect phishing online. The study took 30 to 40 min to complete. The study procedure is visualized in Fig. 1.

4.2. Vignette scenarios

We investigated phishing scenarios of self-created Instagram chat depictions, which were visualized as images of fictitious chat screens. All chat depictions are available for download at https://doi.org/10.18154/RWTH-2024-12185. Of research interest were the independent variables *relationship* (non-follower vs. follower) and *developmental opportunity* (social vs. job vs. partner opportunity). For *relationship*, we varied the follower status where messages were received either from followers or non-followers (see Fig. 2).

The *developmental opportunity* was varied through the message text offering a social, job or partner opportunity (see Table 1). In total, a participant received three messages from a follower, which offered a social, job and partner opportunity and three messages from a non-follower, which offered a social, job and partner opportunity. The message text of each developmental opportunity was reformulated once to avoid presenting the same message twice from a follower and a non-follower and to mitigate any single effects of wording (see Table 1).

To avoid carry-over effects from messages from the same sender, we varied the sender for each message scenario with six picture-name sender designs that were gender balanced (see Fig. 3). To avoid systematic effects of sender design, we counterbalanced the six sender designs across the six (2 × 3) message scenarios, resulting in 36 combinations of sender design and message scenario.

We queried two complementary susceptibility indicators: (1) *intended behavior*, and (2) *suspicion*. For *intended behavior*, participants were asked whether they would (1) open the link, (2) send an answer, (3) ignore the message, (4) share the link, (5) delete the message, or (6) like the message (translated and adapted to Instagram from Frauenstein and Flowerday, 2020, see Table 2). Multiple answers were possible. For analysis, responses were categorized as either not susceptible (0), when participants indicated they would ignore/delete the message, or susceptible (1), when participants indicated they would open/share the link or respond to/like the message. Contradictory statements, containing intended behavior which could be categorized as both not susceptible and susceptible (e.g., both ignoring and responding to the message) were excluded from the analysis (1.6 % of responses across 35 participants). *Suspicion* was assessed with a translated and Instagram-adapted 5-item questionnaire (adapted from Chou et al., 2021; Moody et al., 2017; Vishwanath et al., 2018) on a Likert scale from 1 "I do not agree at all" to 6 "I fully agree" (see Table 2). For analysis, the mean of the five-item Likert scale (Cronbach's $\alpha = 0.75–0.92$) was calculated for each scenario in which values ranged from 1 (low suspicion) to 6 (high suspicion).

4.3. Follow-up questionnaires

In the following section, the analyzed follow-up questionnaires are described in more detail. Table 3 presents an overview of all items analyzed in our study.

4.3.1. Developmental task questionnaire for young adults (DTQ-YA)

An extended version of the developmental task questionnaire for young adults by Seiffge-Krenke (2001) was applied. To measure the fulfillment of a developmental task, participants could indicate "I have not reached yet", "I have started" or "I have already reached", whereas for its importance, participants could indicate "not important at all", "somehow important" or "very important" on a three-point scale. In our study, we were interested in three items regarding the fulfillment and/or importance of the developmental tasks that can be fulfilled by a developmental opportunity offered in our phishing messages (see Table 3).

We analyzed fulfillment and/or importance of the developmental tasks through the items on belonging to a peer group, entering professional life and being in a committed relationship of both scales (see Table 3). The developmental tasks were categorized as not fulfilled (0) when participants indicated the addressed developmental task as "not reached yet", whereas they were categorized as fulfilled (1) when participants indicated the addressed developmental task as "started" or "already reached". This coding was used because both starting and reaching (1) a connection to ones' peer group, (2) a professional life, and (3) a committed relationship should reduce the perceived relevance of messages addressing these developmental tasks. Furthermore, the developmental task was categorized as not important (0) or important (1). Developmental tasks were categorized as important (1) when participants indicated the associated item as "somehow important" or "very

[3] The study was part of a large-scale research collection within our state-funded project A-DigiKomp.

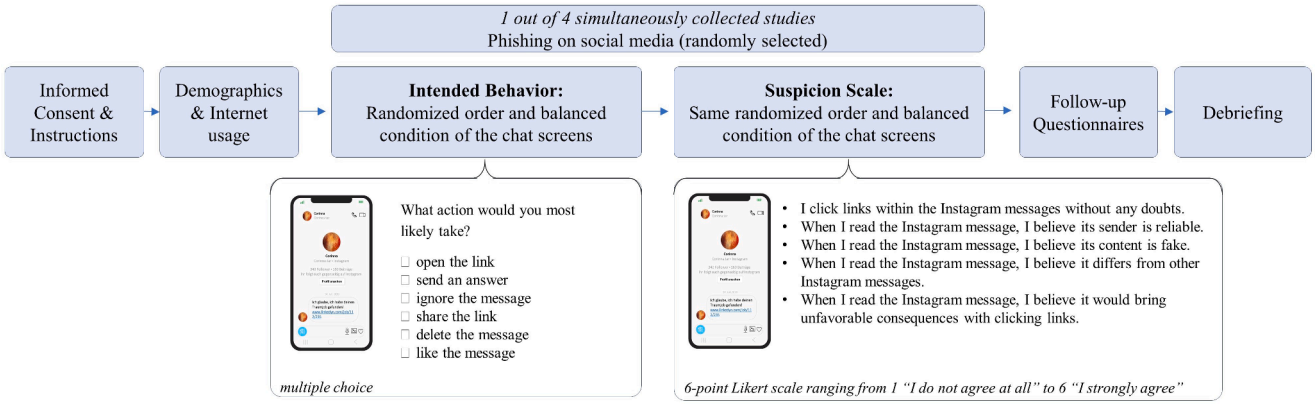


Fig. 1. Study procedure.

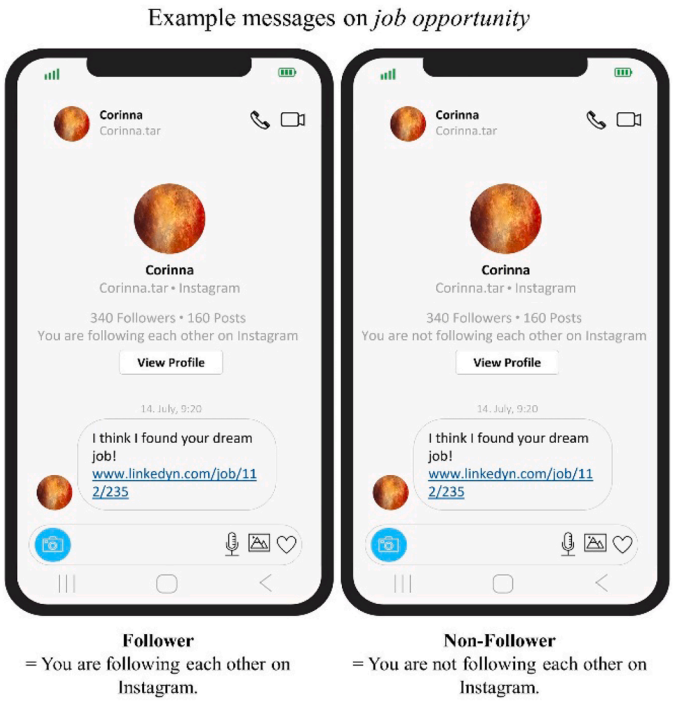


Fig. 2. Examples of messages from followers (= You are following each other on Instagram) and non-followers (= You are not following each other on Instagram) offering a job opportunity to fulfill the developmental task of entering professional life (I think I found your dream job! www.linkedyn.com/job/112/235); translated from German to English.

Table 1
Message scenarios sorted by the *developmental opportunity* (the study used German, in this table message scenarios are translated into English).

Social opportunity…… to fulfill the developmental task of belonging to a peer group.	Job opportunity…… to fulfill the developmental task of entering professional life	Partner opportunity…… to fulfill the developmental task of being in a committed relationship
Look, we have to go there! http://instagram.ru/342/events/	I think I found your dream job! www.linkedyn.com/job/112/235	This is definitely your dream match! http://Iovoo.ru/777_Alex
Will you be there on July 27th? www.eventlm.de/event364872&hs/	This job would definitely suit you. http://stepston.de/job432/form.html	This match would really suit you. www.gotinder.de/account-7213.form-html

important". Otherwise, it was coded as not important (0). In 66.5 % of all phishing scenarios the addressed developmental task was rated as fulfilled and in 91.6 % of all phishing scenarios the addressed developmental task was rated as important.

4.3.3. Additional measures

To ensure attentive participation, two control items were included (see Table 3). Sociodemographic information, duration of internet use, and the type of messenger and social media used were assessed to gain insight into the sample.

4.4. Participants

A total of 500 young adults (398 females, 99 males, 3 with no indication, $M_{Age} = 22.28$ years ($SD_{Age} = 2.56$, $Range_{Age} = 16–29$ years)) met the inclusion criteria and were analyzed. Participants who were older than 29 years or who failed control items were excluded ($N_{excluded} = 53$, 9.6 %). Most participants were students (80 %), followed by apprentices (7.8 %) or employees (7.8 %). In addition, most participants reported A-Levels as their highest educational level (67.8 %). The majority of participants indicated to use the messenger WhatsApp (97.8 %) as well as the social media services Instagram (86.8 %) or YouTube (81.2 %).

Participants were recruited through flyers, university mailing lists, the research platform SurveyCircle, direct requests on social media (e.g. LinkedIn), and at German educational institutions. All participants had the opportunity to win vouchers (1 × 100€, 2 × 50€, 5 × 25€, 15×15€) after completing the study. Students from three German universities received course credits for their participation.

4.4.1. Ethics

The study was designed to comply with established guidelines for human subjects research guidelines and privacy regulations. Participation in the study was voluntary, and participants could withdraw at any time, with the assurance that any data provided up to that point would be deleted. Upon completion of the study, participants were provided with detailed information about the purpose of the study. Data were not stored and analyzed until a participant clicked ''Save data'' after the debriefing. Participants were provided with contact details in the debriefing session to voice any questions or concerns. This research and its sample (16 to 29 years) were approved by the Ethics Committee of HSD Hochschule Döpfer (BEth_20_22, decision of May 19, 2022) and no ethical concerns were raised.

5. Results

The statistics software R (R Core Team, 2022) and RStudio (RStudio Team, 2022, Version: 2022.12.10) were used for analysis. Significance was tested at $\alpha = 0.05$. Within confirmatory regression analyses,

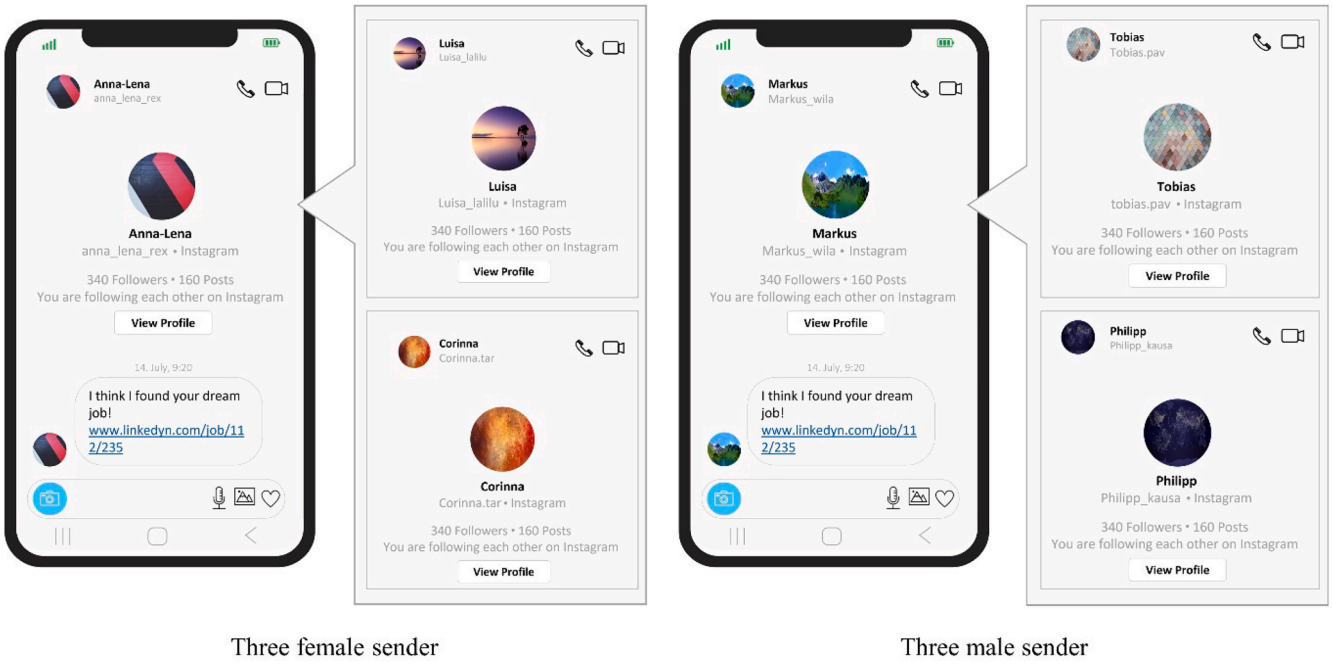


Fig. 3. Examples of the six sender designs for messages offering a job opportunity ("I think I found your dream job! www.linkedyn.com/job/112/235″) and the relationship follower ("You are following each other on Instagram"); translated from German to English.

Table 2
Items of the Instagram-adapted multiple-choice questionnaire for intended behavior and the suspicion scale; translated from German to English.

Measures	Descriptions	Characteristics	Sources
Intended behavior	Multiple choice What action would you most likely take? – open the link – send an answer – ignore the message – share the link – delete the message – like the message	Dependent variable *coded as either not susceptible (0) or susceptible (1)*	adapted from Frauenstein & Flowerday (2020)
Suspicion scale	6-point Likert scale ranging from 1 "I do not agree at all" to 6 "I strongly agree" – I would 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 unfavorable consequences with clicking links.	Dependent variable (Cronbachs' α = 0.75 –0.92) *Item scores were averaged*	adapted from Chou et al. (2021); Moody et al. (2017); Vishwanath et al. (2018)

relationship (follower vs. non-follower) and *developmental opportunities* (social vs. job vs. partner opportunity) as well as their interaction effects were examined. Within the exploratory regression analyses, *developmental task fulfillment* and *importance, age, gender* and *Instagram usage* were examined by adding each as a single predictor to the confirmatory regression equation. All predictors (except for age) were dummy-coded as a 0/1 dichotomized variable, whereas age was grand-mean centered.

5.1. 5.1 Multilevel logistic regression: Intended behavior

The log-odds of intended behavior were modelled using multilevel logistic regression because the dependent variable was dichotomous and because the intra-class-coefficient (ICC) revealed that 38 % of the chances to show a particular intended behavior are explained by between-subject differences. The frequency analysis over all responses indicated that 30.7 % of all responses were categorized as susceptible. Moreover, 336 (67.2 %) participants showed at least one response which was categorized as susceptible.

5.1.1. Confirmatory analysis: Impact of relationship and developmental opportunities on intended behavior

We first conducted a confirmatory analysis using multilevel logistic regression clustered by participants and predicted by relationship, developmental opportunities and their interactions (Table 4). When participants received phishing messages from followers, their intended responses were more likely to be susceptible responses ($\beta = 2.70$, $p < .001$, OR = 14.92, 95% CI [8.80, 25.27]) than when they received the messages from non-followers, confirming the assumed effect of relationship. Further, it was found that developmental opportunities within phishing messages affected intended behavior. The size of the effect depended on the developmental opportunity. When participants received phishing messages offering a social opportunity, they were more likely to show susceptible responses than when they received phishing messages offering a job opportunity ($\beta = 0.58$, $p < .01$, OR = 1.78, 95% CI: [1.18, 2.69]) or partner opportunity ($\beta = 2.19$, $p < .001$, OR = 8.90, 95% CI [5.29, 14.99]). Further, it was shown that when participants received phishing messages offering a job opportunity, they were more likely to show susceptible responses than when they received

Table 3
Items on developmental task fulfillment and importance from the DTQ-YA by Seiffge-Krenke (2001) and control items, translated from German to English.

Measures	Descriptions	Characteristics	Sources
DTQ-YA	Developmental task fulfillment 3-point scale with three response options (1) I have not reached yet, (2) I have started, (3) I have already reached – Have you already started your professional life? – Are you part of a circle of friends or a social group that suits you? – Are you currently in a steady relationship?	Exploratory predictor *coded as either not fulfilled (0) or fulfilled (1)*	Seiffge-Krenke (2001)
	Developmental task importance 3-point scale with three response options (1) not important to me, (2) somewhat important to me, (3) very important to me – Do you wish to enter working life? – Do you wish to become part of a circle of friends or a social group that suits you? – Do you want a steady relationship?	Exploratory predictor *coded as either not important (0) or important (1)*	
Control items	6-point Likert scale ranging from 1 "I do not agree at all" to 6 "I strongly agree" – To make sure you are fully on board, please select "strongly agree" here. 3-point scale with three response options (1) not important to me, (2) somewhat important to me, (3) very important to me – To make sure you are fully engaged, please select " not important to me" here.	Control item *Participants who failed the control items were excluded*	

phishing messages offering a partner opportunity ($\beta = 1.61$, $p < .001$, OR = 5.00, 95% CI [2.94, 8.49]).

Relationship also influenced the effect of the developmental opportunity on intended behavior, as shown within two significant interactions (1) between relationship and social opportunity (vs. job opportunity) ($\beta = 0.63$, $p < .05$, OR = 1.87, 95% CI [1.03, 3.39]) as well as (2) between relationship and job opportunity (vs. partner opportunity) ($\beta = -0.97$, $p < .01$, OR = 0.38 95% CI [0.19, 0.74]). To interpret the interaction effects, the data set was split along the factor levels of relationship (follower vs. non-follower) and multilevel logistic regression analyses were calculated on the split data set (Sommet and Morselli, 2017, 2021). It was shown that the increase in susceptible responses for messages offering a social opportunity compared to job opportunity was larger when the message came from a follower ($\beta = 1.33$, $p < .001$, OR = 3.80, 95% CI [2.49, 5.80]) compared to a non-follower ($\beta = 0.84$, $p < .01$, OR = 2.31, 95% CI [1.28, 4.14]). In contrast, susceptible responses for phishing messages offering a job opportunity compared to a partner opportunity increased more when the message came from a non-follower ($\beta = 2.93$, $p < .001$, OR = 18.82, 95% CI: [5.91, 59.94]) compared to a follower ($\beta = 0.81$, $p < .001$, OR = 2.25, 95% CI: [1.48, 3.42]). The predicted probabilities of the confirmatory analysis are visualized in Fig. 4.

Table 4
Results of the confirmatory model as predicted by relationship (follower vs. non-follower) and developmental opportunity (social vs. job vs. partner opportunity) for intended behavior (DV).

Predictors	Coefficient	Wald χ^2	p	OR	CI_{LL}	CI_{UL}
(Intercept)	−3.98	230.99	< 0.001	0.02	0.01	0.03
Relationship	2.70	100.88	< 0.001	14.92	8.80	25.27
Social opportunity [a]	2.19	67.62	< 0.001	8.90	5.29	14.99
Job opportunity [a]	1.61	35.42	< 0.001	5.00	2.94	8.49
Social opportunity [b]	0.58	7.50	< 0.01	1.78	1.18	2.69
Relationship * Social opportunity [a]	−0.34	1.02	0.31	0.71	0.37	1.38
Relationship * Job opportunity [a]	−0.97	7.95	< 0.01	0.38	0.19	0.74
Relationship * Social opportunity [b]	0.63	4.27	< 0.05	1.87	1.03	3.39
Random Effects						
ICC	0.38					
N_{id}	500					
Observations	2952					
Marginal R^2 / Conditional R^2	0.21 / 0.65					

[a] Confirmatory model with developmental opportunity reference category: partner opportunity, [b] confirmatory model with developmental opportunity reference category: job opportunity.

5.1.2. *Exploratory analysis: impact of developmental task fulfillment and importance, age, gender and Instagram usage on intended behavior*

Contrary to our prediction, we did not find an effect for developmental task fulfillment ($\beta = -0.14$, $p = .36$, OR = 0.87, 95% CI [0.64, 1.18]) or developmental task importance ($\beta = 0.31$, $p = .21$, OR = 1.37, 95% CI [0.83, 2.25]). Effects of age ($\beta = 0.01$, $p = .84$, OR = 1.01, 95% CI [0.93, 1.10]), gender (ß = -0.08, $p = .78$, OR= 0.93, 95% CI [0.54, 1.59]) and Instagram usage ($\beta = 0.49$, $p = .14$, OR = 1.63, 95% CI [0.85, 3.11]) were non-significant and also omitted as predictor for intended behavior.

5.2 *Multilevel linear regression: Suspicion*

As mean values of suspicion can be seen as continuous (Norman, 2010) and the intra-class coefficient (ICC) revealed that 37 % of the variance in suspicion are explained by between-subject differences, suspicion was modelled using multilevel linear regression.

5.2.1 *Confirmatory analysis: Impact of relationship and developmental opportunities on suspicion*

A confirmatory analysis was conducted, clustered by participants predicted by relationship, developmental opportunity and their interactions (Table 5). The analysis confirmed the effect of *relationship* on suspicion. When participants received phishing messages from followers, they were less suspicious ($\beta = -0.79$, 95% CI [−0.92, −0.67], $p < .001$) than when they received them from non-followers. Moreover, the developmental opportunity affected participants' suspicion and the size of this effect varied depending on the developmental opportunity presented. It was found that when participants received phishing messages offering a social opportunity, they were less suspicious than when they received phishing messages offering a job opportunity ($\beta = -0.18$,

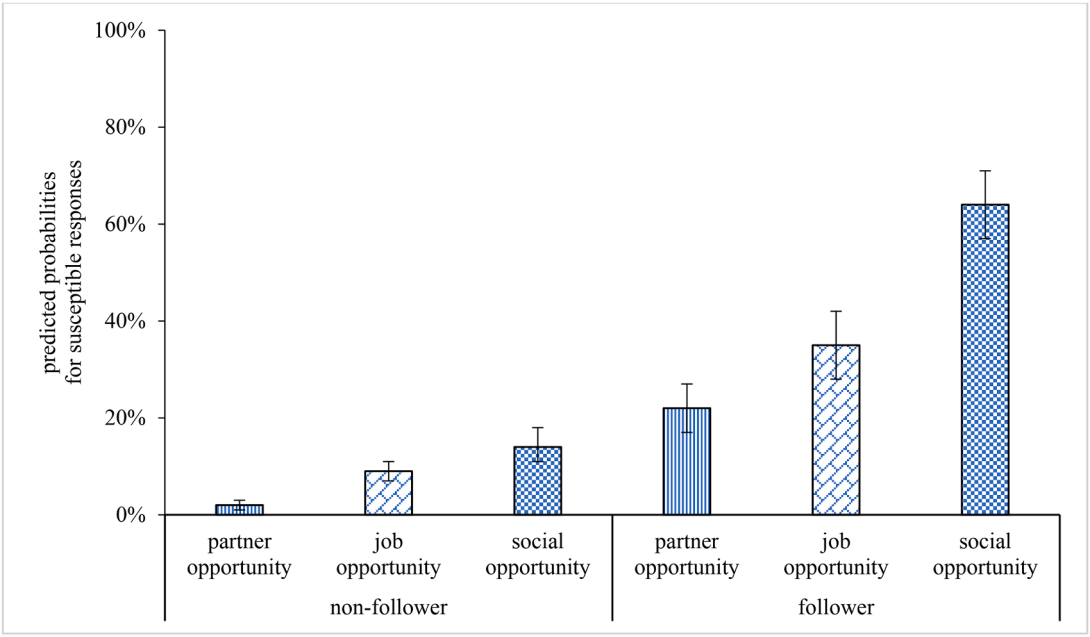


Fig. 4. Predicted probabilities of susceptible responses for developmental opportunity (social, job and partner opportunity) and relationship (non-follower, follower). Error bars indicate the confidence intervals of the predicted probabilities.

Table 5
Results of the confirmatory model predicted by relationship (follower vs. non-follower) and developmental opportunity (social vs. job vs. partner opportunity) for suspicion (DV).

Predictors	Coefficient	*t*-value	*p*	CI
(Intercept)	5.21	90.40	< 0.001	5.10 to 5.32
Relationship [a]	−0.79	−12.22	< 0.001	−0.92 to −0.67
Social opportunity [a]	−0.34	−5.38	< 0.001	−0.46 to −0.22
Job opportunity [a]	−0.16	−2.54	< 0.05	- 0.29 to −0.04
Social opportunity [b]	−0.18	−2.75	< 0.01	−0.30 to −0.05
Relationship * Social opportunity [a]	−0.34	−3.56	< 0.001	−0.53 to −0.15
Relationship * Job opportunity [a]	−0.02	−0.23	0.82	−0.21 to 0.17
Relationship * Social opportunity [b]	−0.32	−3.27	< 0.01	−0.51 to −0.13
Random Effects				
ICC	0.37			
DEFF	2.84			
N_{id}	500			
Observations	3000			
Marginal R^2 / Conditional R^2	0.14/ 0.54			

[a] Confirmatory Model with Developmental Opportunity Reference Category: Partner opportunity, [b] Confirmatory Model with Developmental Opportunity Reference Category: Job opportunity.

95% CI [−0.30, −0.05], $p < .01$) or partner opportunity ($\beta = -0.34$, 95% CI [−0.46, −0.22], $p < .001$). Furthermore, it was shown that when participants received phishing messages offering a job opportunity, they were less suspicious than when they received messages offering a partner opportunity ($\beta = -0.16$, 95% CI [−0.29, −0.04], $p < .05$).

Relationship also influenced the effect of developmental opportunity for the dependent variable suspicion, as shown within two significant interactions (1) between relationship and social opportunity compared to job opportunity ($\beta = -0.32$, 95% CI [−0.51, −0.13], $p < .01$) and (2) between relationship and social opportunity compared to partner opportunity ($\beta = -0.34$, 95% CI [−0.53, −0.15], $p < .001$). The data set was split along the factor levels of relationship (follower vs. non-follower) and multilevel linear regression analyses were calculated on the split data set to interpret the interaction effects (Sommet and Morselli, 2017, 2021). The analyses showed that suspicion for phishing messages offering a social opportunity compared to job opportunity decreased more when the message came from a follower ($\beta = -0.52$, 95% CI [−0.64, −0.41], $p < .001$) compared to a non-follower ($\beta = -0.20$, 95% CI [−0.30, −0.11], $p < .001$). Furthermore, the higher decrease of suspicion for messages from a follower ($\beta = -0.70$, 95% CI [−0.81, −0.59], $p < .001$) compared to a non-follower ($\beta = -0.36$, 95% CI [−0.45, −0.27], $p < .001$) was also found for phishing messages offering a social opportunity compared to partner opportunity. The predicted values of the confirmatory analysis are calculated and visualized in Fig. 5.

5.2.2. Exploratory analysis: impact of developmental task fulfillment and importance, age, gender and Instagram usage on suspicion

Contrary to our prediction, we could not find an impact on suspicion for developmental task fulfillment ($\beta = -0.01$, 95% CI [−0.10, −0.08], $p = .84$) or importance ($\beta = -0.05$, 95% CI [−0.20, 0.10], $p = .51$). Effects of age ($\beta = -0.003$, 95% CI [−0.04, 0.03], $p = .83$), gender ($\beta = 0.02$, 95% CI [−0.18, 0.23], $p = .83$) and Instagram usage ($\beta = -0.08$, 95% CI [−0.32, 0.16], $p = .54$) were also non-significant and did not improve model fit. All examined concomitant predictors were omitted as predictors for suspicion.

6. Discussion

Our online vignette study provides unique insights into young adults' susceptibility to social media phishing integrating a developmental perspective. We investigated whether young adults' susceptibility is affected by their relationship to the phisher and/or the developmental opportunity offered by a phishing message to fulfill three developmental tasks. Additionally, we explored the extent to which participants had accomplished the addressed developmental tasks and the importance they attach to them.

Overall, our results revealed a high level of susceptibility to phishing attempts with approximately two-thirds of our sample exhibiting

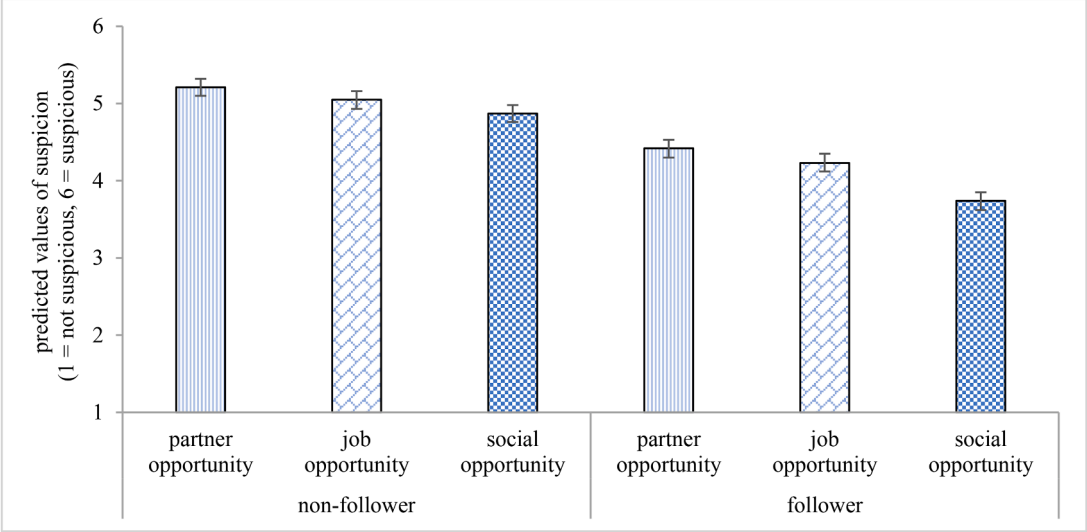


Fig. 5. Predicted values of suspicion for developmental opportunity (social, job and partner opportunity) and relationship (non-follower, follower). Error bars indicate the confidence intervals of the predicted values.

intended behaviors that were classified as susceptible in response to at least one phishing message. Consistent with previous research, we proposed that phishing messages from followers or messages that offer a social opportunity to fulfill the developmental task of belonging to a peer group contribute to this increased susceptibility. Our results support this assumption: first, we found the proposed effect of relationship (Hypothesis 1), indicating increased probabilities to show susceptible responses and less suspicion towards phishing messages if these messages were sent from followers compared to non-followers. Second, these susceptibility indicators seemed to be influenced by the developmental opportunity offered within a phishing message: compared to other developmental opportunities, messages on social opportunities led to the highest probabilities to show susceptible responses and lowest suspicion, confirming Hypothesis 2. In particular, when followers sent a message offering a social opportunity (as opposed to a job or partner opportunity), susceptibility was amplified, with almost two-thirds showing susceptible responses towards such messages and only a medium level of suspicion being shown. Interestingly, these effects occurred even though the phishing links were not hidden behind shortened links and contained evident phishing characteristics such as foreign domains or typographical errors. Similar to the Trojan horse, phishers appear to be able to hide phishing links behind their identity as a follower, in order to obtain sensitive data from their victims.

These findings are consistent with previous research on young adults emphasizing an increased influence of the peer group among this age group (Kreuder et al., 2023, 2024; Mendel and Toch, 2017). Moreover, these findings are consistent with existing phishing research, which highlights an increased susceptibility to social characteristics within the social context of social media (Algarni et al., 2017; Vishwanath, 2015a, 2017). As with the observed effects in previous phishing research, effects of relationship could be explained by increased heuristic processing, where the follower status may be perceived as a heuristic cue to the authenticity of the received phishing message (Vishwanath, 2015b) or where such messages from followers may be perceived as rather harmless (low perceived cyber risks) (Frauenstein and Flowerday, 2020; Vishwanath et al., 2018). Similarly, the findings could be explained by the high importance of the developmental task of belonging to a peer group. Given the high susceptibility to messages that provide social opportunities to fulfill this developmental task, it appears that interacting with social opportunities and/or followers may be perceived as highly relevant to maintaining the relationship with the supposed follower. As a result, these messages may also be processed quickly and heuristically leading to increased susceptibility. An additional explanation for young adults' increased susceptibility to these messages may be attributed to the fact that such messages have the potential to induce FoMO about a rewarding experience with a follower. For example, not responding to messages from followers and/or messages that offer a social opportunity (e.g., "Look, we have to go there!") may lead young adults to a feeling of missing out on these rewarding social experiences, pressuring users to click on the message link. Similar effects were found in current literature, where participants felt pressured to participate in social media despite their privacy concerns to avoid missing out (Westin and Chiasson, 2021) and where phishing messages from known senders induced the feeling of missing out on certain events (Klütsch et al., 2024). However, it should be noted that this effect should depend on the perceived cyber risks. Unlike privacy decisions in which participants indicate pressure to use social media despite their privacy concerns, higher perceived cyber risks should increase suspicion towards these message (Vishwanath et al., 2018).

These potential differences in perceived FoMO in response to specific messages may also explain the observed differences in susceptibility between phishing messages from followers and non-followers offering a social compared to a job opportunity. Messages from followers that invite to an upcoming event and offer a social opportunity might be perceived as more important as they increase FoMO on the upcoming event compared to similar messages from non-followers. Conversely, messages from followers and non-followers that offer a job opportunity might be perceived equally important.

In addition to our hypothesis, our study showed that young adults fall more likely for phishing messages offering a job compared to a partner opportunity, particularly when phishing messages were sent by non-followers (compared to followers). This finding underscores the importance of job opportunities for young adults and is consistent with previous research showing that young adults' transition into professional life is associated with changes in their online privacy settings on social networks (Steijn, 2014). In light of the increased differences in susceptibility between job and partner opportunities sent from non-followers, the perceived likelihood of receiving certain messages from certain senders can serve as an explanation. Job opportunities might be perceived as less personal and more broadly targeted as recruiters can reach out through various channels. Consequently, young adults may consider job opportunities from both followers and non-followers as likely. Conversely, partner opportunities can be seen as highly personal and context-specific. Hence, such messages from

non-followers may appear suspicious and less likely.

Finally, we examined the extent to which participants had accomplished the addressed developmental tasks and the importance they attach to them. Contrary to hypothesis 3, we did not find differences in phishing susceptibility when developmental tasks were rated as important or not fulfilled. One explanation could be the overall high rating of importance (91.4 %) to the developmental tasks addressed in our study. Another explanation may be the questionnaire and its reduction to a binary format. In the binary format, a developmental task was categorized as fulfilled if participants indicated the task as "started" or "already reached" and as not fulfilled if participants indicated the task as "not reached yet". However, this categorization may not fully capture the complexity of developmental tasks. For example, young adults may pursue a new career path or social group even after starting a job or becoming part of one social group. Consequently, this developmental task could still be relevant to them even though it would be categorized as fulfilled.

6.1. Limitations and future research

Given the exploratory nature of our study, this study has several limitations and implications for future research.

First, even if our research findings could be generalized to platforms such as Facebook, it cannot be ruled out that other platforms may exhibit platform-specific susceptibility predictors. We recommend that future research extend our study to other social media platforms. This is particularly important because we discovered that although developmental tasks were rated as highly important, messages offering social opportunities led to higher susceptibility on the platform Instagram, which is a socially oriented platform, than messages relating to other developmental tasks. Other social media platforms with other use relations, such as the strong relation between LinkedIn and entering professional life as a developmental task, could thus pose different platform-specific risks for the younger user group, and further research is needed to identify these.

Another limitation relates to the demographic scope of this study. First, given the exploratory nature of this study and its developmental focus, we chose to limit comparisons with other age groups. Nevertheless, future research could examine age group comparisons within our research design, potentially examining additional age group-specific developmental tasks to gain a more nuanced understanding of age-related differences. Because social media platforms are used differently across certain age groups (Kemp, 2023), we suggest that future research controls for the familiarity and engagement with the social media platforms studied. Additionally, the notable prevalence of female participants in our sample may limit the generalizability of our findings. Although our exploratory gender analysis did not reveal differences in phishing susceptibility between female and male participants, future research should further explore the role of gender in the emerging field of social media phishing. This is particularly important because several studies have suggested that women are more susceptible to phishing attacks than men, while other studies have found inconsistent or contradictory results (Tornblad et al., 2021).

In addition, the binary format of developmental task fulfillment used in the present study may not capture the complexity of this process. As noted above, participants who report starting a career or joining a social group may still be actively exploring other job or social opportunities to fulfill this developmental task. To address this limitation, future research could incorporate multidimensional scales tailored to specific developmental tasks, such as the *Multidimensional Scale of Perceived Social Support* (Zimet et al., 1988) to assess the need for further supportive social connections. In addition, qualitative data through semi-structured interviews or open-ended questions can complement quantitative data and provide deeper insights into the dynamic processes underlying young adults' developmental processes.

Lastly, it should be noted that our scenario-based approach is constrained by the fact that it measures intended rather than actual behavior. Future research should take advantage of multi-method approaches that combine different research methods such as qualitative interviews, eye-tracking and field studies. For example, future research could integrate eye-tracking techniques to determine whether users pay attention to the follower status or the developmental opportunities rather than phishing links (Alsharnouby et al., 2015). Nevertheless, our scenario-based approach helped us to systematically investigate realistic phishing scenarios. We encourage other researchers to use our scenario-based stimulus material and research framework (https://doi.org/10.18154/RWTH-2024-12185) to investigate open research questions arising from our research. Next research steps could be (a) controlling for confounding variables such as participants' phishing awareness or education and (b) incorporating a baseline scenario to further assess the impact of certain phishing content on phishing susceptibility.

6.2. Practical implications

Beyond our theoretical implications, three key actionable insights for phishing awareness campaigns can be derived from our findings: (1) embrace social media in cybersecurity education, (2) highlight the Trojan horse tactic and (3) tailor anti-phishing education to young adults.

(1) Embrace social media in cybersecurity education:

Our findings highlight the high susceptibility to phishing attacks via social media, especially those emanating from followers or tapping into social opportunities. These findings underscore the need to expand current anti-phishing training to cover social media, driving home the point that these platforms can present cybersecurity threats just like e-mails do.

(2) Highlight the trojan horse tactic:

Phishing training needs to emphasize that phishing attacks can come from seemingly trustworthy accounts, emphasizing that attackers might hijack or spoof a friend's account. Higher awareness of these spoofed messages can raise suspicion towards both the message and the supposed follower.

(3) Tailor anti-phishing education to young adults:

Our results demonstrate that young adults are a susceptible user group, prone to be targeted by phishers who exploit their needs and expectations. As such, anti-phishing education should be customized to this target group and integrated into schools, apprenticeships and universities to effectively reach them. For example, face-to-face training and phishing awareness campaigns could be adapted to group-specific platforms (e.g., Instagram, TikTok) or imparted within serious games.

7. Conclusion

Social media phishing poses a major security risk in our digital age, particularly for young adults as the primary user group of most social media platforms. Our research offers a unique insight into this user group and identifies their increased susceptibility to social media phishing attacks, especially towards those from followers or offering social opportunities. We encourage future research to extend our findings and practitioners to tailor and address the rising trend of social media phishing to the young adult user group.

CRediT authorship contribution statement

Jennifer Klütsch: Writing – review & editing, Writing – original

draft, Visualization, Methodology, Investigation, Formal analysis, Data curation, Conceptualization. **Luise Haehn:** Writing – review & editing, Formal analysis, Data curation. **Annika Kreuder:** Writing – review & editing, Methodology, Investigation, Conceptualization. **Christian Böffel:** Writing – review & editing, Methodology, Conceptualization. **Ulrich Frick:** Writing – review & editing, Supervision, Funding acquisition, Formal analysis, Conceptualization. **Sabine J. Schlittmeier:** Writing – review & editing, Supervision, Conceptualization, Funding acquisition, Methodology.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

The authors thank Nina Wirtz for her support within the literature review and data collection and Jian Pan for his support in study programming.

Funding

This work 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.

Data availability

Data can be retrieved at https://doi.org/10.18154/RWTH-2024-12185.

References

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. Inf. Syst. 26, 661–687. https://doi.org/10.1057/s41303-017-0057-y.

Alsharnouby, M., Alaca, F., Chiasson, S., 2015. Why phishing still works: user strategies for combating phishing attacks. Int. J. Hum.-Comput. Stud. 82, 69–82. https://doi.org/10.1016/j.ijhcs.2015.05.005.

Arnett, J.J., 2000. Emerging adulthood: a theory of development from the late teens through the twenties. Am. Psychol. 55, 469–480. https://doi.org/10.1037//0003-066X.55.5.469.

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

Blancaflor, E.B., Alfonso, A.B., Banganay, K.N.U., Dela Cruz, G.A.B., Fernandez, K.E., Santos, S.A.M., 2021. Let's go phishing: a phishing awareness campaign using smishing, email phishing, and social media phishing tools. In: Proceedings of the 11th Annual International Conference on Industrial Engineering and Operations Management. Singapore, pp. 6473–6482.

Borca, G., Bina, M., Keller, P.S., Gilbert, L.R., Begotti, T., 2015. Internet use and developmental tasks: adolescents' point of view. Comput. Hum. Behav. 52, 49–58. https://doi.org/10.1016/j.chb.2015.05.029.

Butavicius, M., Parsons, K., Pattinson, M., McCormac, A., 2016. Breaching the human firewall: social engineering in phishing and spear-phishing emails. In: Australasian Conference on Information Systems (ACIS) 2015 Proceedings. Adelaide, Australia. https://doi.org/10.48550/arXiv.1606.00887.

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

Chou, F.K.-Y., Chen, A.P.-S., Lo, V.C.-L., 2021. Mindless response or mindful interpretation: examining the effect of message influence on phishing susceptibility. Sustain. 13, 1651. https://doi.org/10.3390/su13041651.

Chung, J., Koay, J.-Z., Leau, Y.-B., 2021. A review on social media phishing: factors and countermeasures. In: Anbar, M., Abdullah, N., Manickam, S. (Eds.), Advances in Cyber Security, Communications in Computer and Information Science. Presented at the International Conference on Advances in Cyber Security. Springer Singapore, Singapore, pp. 657–673. https://doi.org/10.1007/978-981-33-6835-4_43.

Cialdini, R.B., 2007. Influence: The Psychology of Persuasion. HarperCollins Publishers, New York.

Coyne, S.M., Padilla-Walker, L.M., Howard, E., 2013. Emerging in a digital world: a decade review of media use, effects, and gratifications in emerging adulthood. Emerg. Adulthood 1, 125–137. https://doi.org/10.1177/2167696813479782.

Eagly, A.H., Chaiken, S., 1993. The Psychology of Attitudes. Harcourt Brace Jovanovich College Publishers.

Federal Trade Commission, 2023. Social media: a golden goose for scammers. https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2023/10/social-media-golden-goose-scammers (assessed 15 November 2024).

Frauenstein, E.D., Flowerday, S., 2020. Susceptibility to phishing on social network sites: a personality information processing model. Comput. Secur. 94, 101862. https://doi.org/10.1016/j.cose.2020.101862.

Gavett, B.E., Zhao, R., John, S.E., Bussell, C.A., Roberts, J.R., Yue, C., 2017. Phishing suspiciousness in older and younger adults: the role of executive functioning. PLoS. One 12, e0171620. https://doi.org/10.1371/journal.pone.0171620.

Havighurst, R.J., 1948. Developmental Tasks and Education. The University of Chicago Press.

Kemp, S., 2023. Digital 2023: global overview report, Global Digital Reports. Data Reportal and we are social and meltwater. https://datareportal.com/reports/digital-2023-global-overview-report (assessed 15 November 2024).

Klütsch, J., Schwab, J., Böffel, C., Zimmermann, V., Schlittmeier, S.J., 2024. Friend or phisher: how known senders and fear of missing out affect young adults' phishing susceptibility on social media. Humanit. Soc. Sci. Commun. 11, 1145. https://doi.org/10.1057/s41599-024-03412-8.

Kreuder, A., Frick, U., Rakoczy, K., Schlittmeier, S.J., 2024. Digital competence in adolescents and young adults: a critical analysis of concomitant variables, methodologies and intervention strategies. Humanit. Soc. Sci. Commun. 11, 48. https://doi.org/10.1057/s41599-023-02501-4.

Kreuder, A., Haehn, L., Klütsch, J., Schlittmeier, S.J., Frick, U., 2023. Cookies? I don't even know what that is. Online Focus Groups On adolescents' Experience and Behavior in the Digital space. Presented at the MuC '23: Mensch und Computer 2023. Association for Computing Machinery, Rapperswil Switzerland, pp. 498–502. https://doi.org/10.1145/3603555.3608570.

Mack, A., Rock, I., 1998. Inattentional blindness: perception without attention. In: Wright, R.D. (Ed.), Visual Attention. Oxford University Press, pp. 55–76.

Mendel, T., Toch, E., 2017. Susceptibility to social influence of privacy behaviors: peer versus authoritative sources. In: Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing. Presented at the CSCW '17: Computer Supported Cooperative Work and Social Computing. Association for Computing Machinery, Portland Oregon USA, pp. 581–593. https://doi.org/10.1145/2998181.2998323.

Montañez, R., Golob, E., Xu, S., 2020. Human cognition through the lens of social engineering cyberattacks. Front. Psychol. 11. https://doi.org/10.3389/fpsyg.2020.01755.

Moody, G.D., Galletta, D.F., Dunn, B.K., 2017. Which phish get caught? An exploratory study of individuals' susceptibility to phishing. Eur. J. Inf. Syst. 26, 564–584. https://doi.org/10.1057/s41303-017-0058-x.

Norman, G., 2010. Likert scales, levels of measurement and the "laws" of statistics. Adv. Health Sci. Educ. 15, 625–632. https://doi.org/10.1007/s10459-010-9222-y.

Oliveira, D., Rocha, H., Yang, H., Ellis, D., Dommaraju, S., Muradoglu, M., Weir, D., Soliman, A., Lin, T., Ebner, N., 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: CHI '17: Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems. Association for Computing Machinery, Denver, Colorado, USA, pp. 6412–6424. https://doi.org/10.1145/3025453.3025831.

Parker, H.J., Flowerday, S.V., 2020. Contributing factors to increased susceptibility to social media phishing attacks. South Afr. J. Inf. Manag. 22, a1176. https://doi.org/10.4102/sajim.v22i1.1176.

Parsons, K., Butavicius, M., Delfabbro, P., Lillie, M., 2019. Predicting susceptibility to social influence in phishing emails. Int. J. Hum.-Comput. Stud. 128, 17–26. https://doi.org/10.1016/j.ijhcs.2019.02.007.

Peirce, J., Gray, J.R., Simpson, S., MacAskill, M., Höchenberger, R., Sogo, H., Kastman, E., Lindeløv, J.K., 2019. PsychoPy2: experiments in behavior made easy. Behav. Res. Methods 51, 195–203. https://doi.org/10.3758/s13428-018-01193-y.

Pew Research Center, 2021. Social media fact sheet. https://www.pewresearch.org/internet/fact-sheet/social-media/(accessed 15 November 2024).

Pfleeger, S.L., Caputo, D.D., 2012. Leveraging behavioral science to mitigate cyber security risk. Comput. Secur. 31, 597–611. https://doi.org/10.1016/j.cose.2011.12.010.

Przybylski, A.K., Murayama, K., DeHaan, C.R., Gladwell, V., 2013. Motivational, emotional, and behavioral correlates of fear of missing out. Comput. Hum. Behav. 29, 1841–1848. https://doi.org/10.1016/j.chb.2013.02.014.

R Core Team, 2022. R: a language and environment for statistical computing [software]. R Foundation for Statistical Computing. https://www.R-project.org.

RStudio Team, 2022. RStudio: integrated development for R (Version 2022.12.10) [software]. RStudio, PBC. http://www.rstudio.com/.

Seiffge-Krenke, I., 2015. Experiencing the transition to adulthood in Germany. In: Žukauskienė, R. (Ed.), Emerging Adulthood in a European Context. Psychology Press, pp. 79–93.

Seiffge-Krenke, I., 2001. Developmental task questionnaire for young adults (DTQ-YA). Unpublished Manuscript. Department of Psychology, University of, Mainz, Germany.

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L.F., Downs, J., 2010. Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. In: Proceedings of the SIGCHI Conference on Human Factors in

Computing Systems. Presented at the CHI '10: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. Association for Computing Machinery, pp. 373–382. https://doi.org/10.1145/1753326.1753383.
Sommet, N., Morselli, D., 2021. Keep calm and learn multilevel linear modeling: a three-step procedure using SPSS, Stata, R, and Mplus. Int. Rev. Soc. Psychol. 34, 24. https://doi.org/10.5334/irsp.555.
Sommet, N., Morselli, D., 2017. Keep calm and learn multilevel logistic modeling: a simplified three-step procedure using Stata, R, Mplus, and SPSS. Int. Rev. Soc. Psychol. 30, 203–218. https://doi.org/10.5334/irsp.90.
Steijn, W.M.P., 2014. A developmental perspective regarding the behaviour of adolescents, young adults, and adults on social network sites. Cyberpsychology J. Psychosoc. Res. Cyberspace 8, 5. https://doi.org/10.5817/CP2014-2-5.
Tornblad, M.K., Jones, K.S., Namin, A.S., Choi, J., 2021. Characteristics that predict phishing susceptibility: a review. Proc. Hum. Factors Ergon. Soc. Annu. Meet. 65, 938–942. https://doi.org/10.1177/1071181321651330.
Van den Broeck, E., Poels, K., Walrave, M., 2015. Older and wiser? Facebook use, privacy concern, and privacy protection in the life stages of emerging, young, and middle adulthood. Soc. Media Soc 1. https://doi.org/10.1177/2056305115616149.
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., 2015a. Diffusion of deception in social media: social contagion effects and its antecedents. Inf. Syst. Front. 17, 1353–1367. https://doi.org/10.1007/s10796-014-9509-2.
Vishwanath, A., 2015b. Habitual Facebook use and its impact on getting deceived on social media. J. Comput.-Mediat. Commun. 20, 83–98. https://doi.org/10.1111/jcc4.12100.
Vishwanath, A., Harrison, B., Ng, Y.J., 2018. Suspicion, cognition, and automaticity model of phishing susceptibility. Commun. Res. 45, 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., Malik, I., 2023. Enhancing cybersecurity: the crucial role of self-regulation, information processing, and financial knowledge in combating phishing attacks. Sage Open. 13. 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: Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems. Presented at the CHI '21: CHI Conference on Human Factors in Computing Systems. Association for Computing Machinery, Yokohama Japan, 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. Inf. Sci. Technol. 59, 662–674. https://doi.org/10.1002/asi.20779.
Zimet, G.D., Dahlem, N.W., Zimet, S.G., Farley, G.K., 1988. The multidimensional scale of perceived social support. J. Pers. Assess. 52 (1), 30–41. https://doi.org/10.1207/s15327752jpa5201_2.