Awareness of security and privacy settings in video conferencing apps among faculty during the COVID-19 pandemic

Ali Alammary [Equal first author, 1] , **Moneer Alshaikh** [2] , **Ahmad R Pratama** [Corresp. Equal first author, 3]

[1] College of Computing and Informatics, Saudi Electronic University, Riyadh, Saudi Arabia

[2] Department of Cybersecurity, College of Computer Science and Engineering, The University of Jeddah, Jeddah, Saudi Arabia

[3] Department of Informatics, Universitas Islam Indonesia, Sleman, DI Yogyakarta, Indonesia

Corresponding Author: Ahmad R Pratama
Email address: ahmad.rafie@uii.ac.id

COVID-19 has forced many schools and universities worldwide, including Saudi Arabia, to move from traditional face-to-face learning to online learning. Most online learning activities involve the use of video conferencing apps to facilitate synchronous learning sessions. While some faculty members were not accustomed to using video conferencing apps, they had no other choice than to jump on board regardless of their readiness, one of which involved security and privacy awareness. On the other hand, video conferencing apps users face a number of security and privacy threats and vulnerabilities, many of which rely on human factors to be exploited. In this study, we used survey data from 307 faculty members at 43 Saudi Arabian universities to determine the level of awareness among Saudi Arabian faculty regarding security and privacy settings of video conferencing apps and to investigate the factors associated with it. We analyzed the data using the Knowledge-Attitudes-Behaviors (KAB) model and the Partial Least Squares Structural Equation Modeling (PLS-SEM) method. We found that the average awareness score of video conferencing apps' security and privacy settings falls into the "Poor" category, which is not surprising considering that many faculty members only started using this new technology on a daily basis because of the pandemic. Further analysis showed that perceived security, familiarity with the app, and digital literacy of faculty members are significantly associated with higher awareness. Privacy concerns are significantly associated with higher awareness only among STEM faculty members, while attitudes toward ICT for teaching and research are negatively associated with such awareness among senior faculty members with more than ten years of experience. This study lays the foundation for future research and user education on the security and privacy settings of video conferencing applications.

1 Awareness of security and privacy settings in video
2 conferencing apps among faculty during the COVID-
3 19 pandemic

5 Ali Alammary[1*], Moneer Alshaikh [2], Ahmad R. Pratama[3*]

7 [1] College of Computing and Informatics, Saudi Electronic University, Riyadh, Saudi Arabia
8 [2] Department of Cybersecurity, College of Computer Science and Engineering, The University of
9 Jeddah, Jeddah, Saudi Arabia
10 [3] Department of Informatics, Universitas Islam Indonesia, Sleman, DI Yogyakarta, Indonesia

12 [*] Equal first author

14 Corresponding Author: Ahmad R. Pratama
15 Jl. Kaliurang Km 14,5, Sleman, DI Yogyakarta, 55584, Indonesia
16 Email address: ahmad.rafie@uii.ac.id

18 Abstract

19 COVID-19 has forced many schools and universities worldwide, including Saudi Arabia, to
20 move from traditional face-to-face learning to online learning. Most online learning activities
21 involve the use of video conferencing apps to facilitate synchronous learning sessions. While
22 some faculty members were not accustomed to using video conferencing apps, they had no other
23 choice than to jump on board regardless of their readiness, one of which involved security and
24 privacy awareness. On the other hand, video conferencing apps users face a number of security
25 and privacy threats and vulnerabilities, many of which rely on human factors to be exploited. In
26 this study, we used survey data from 307 faculty members at 43 Saudi Arabian universities to
27 determine the level of awareness among Saudi Arabian faculty regarding security and privacy
28 settings of video conferencing apps and to investigate the factors associated with it. We analyzed
29 the data using the Knowledge-Attitudes-Behaviors (KAB) model and the Partial Least Squares
30 Structural Equation Modeling (PLS-SEM) method. We found that the average awareness score
31 of video conferencing apps' security and privacy settings falls into the "Poor" category, which is
32 not surprising considering that many faculty members only started using this new technology on
33 a daily basis because of the pandemic. Further analysis showed that perceived security,
34 familiarity with the app, and digital literacy of faculty members are significantly associated with
35 higher awareness. Privacy concerns are significantly associated with higher awareness only
36 among STEM faculty members, while attitudes toward ICT for teaching and research are
37 negatively associated with such awareness among senior faculty members with more than ten
38 years of experience. This study lays the foundation for future research and user education on the
39 security and privacy settings of video conferencing applications.

Introduction

41 During COVID-19 pandemic, video conferencing apps have gained popularity as the most viable
42 way to facilitate business processes during work-from-home or learning-from-home strategies.
43 According to a cross-country study (Pratama 2017), there is an intriguing bidirectional
44 relationship between ICT adoption and education indicators, and video conferencing apps are no
45 exception. In many educational institutions, including those in Saudi Arabia, they have become
46 the most popular tool for supporting online learning (Alshehri et al. 2020). Due to their unique
47 characteristics, they are ideal for use in teaching and learning (Alammary, Carbone, and Sheard
48 2016). They enable instructors to set up online synchronous classes that can be recorded and
49 accessed at a later time, either for those who want to review the class again or for those who
50 missed a class. Using personal computers, laptops, or even mobile phones, students can attend
51 these online classes from anywhere (Camilleri and Camilleri 2021).
52
53 Even prior to the COVID-19 pandemic, a variety of video conferencing applications were
54 available. Many other video conferencing apps, such as Google Meet, Microsoft Teams, and
55 Blackboard Collaborate Ultra, also saw an increase in downloads and usage as a result of the
56 COVID-19 pandemic (Trueman 2020). The vast majority of universities in Saudi Arabia use
57 Blackboard Collaborate Ultra because the Ministry of Education (MOE) has designated the
58 Blackboard platform as the official e-learning platform (Iffat Rahmatullah 2021). Prior to the
59 COVID-19 pandemic, the majority of Saudi Arabian faculty were unfamiliar with Blackboard
60 Collaborate Ultra; however, they had no choice but to adopt it regardless of their level of
61 preparedness (Ali Alammary, Alshaikh, and Alhogail 2021).
62
63 On the other hand, the shift from traditional face-to-face to online learning that occurred during
64 the pandemic has raised numerous cybersecurity and protection of individual and organizational
65 information resource concerns (Almaiah, Al-Khasawneh, and Althunibat 2020). Several
66 cybersecurity and privacy threats and vulnerabilities plague users of video conferencing apps,
67 including the exposure of user data, unwanted and disruptive intrusions, the spread of malware,
68 and the hijacking of host machines through remote control tools (Joshi and Singh 2017). Recent
69 security reports indicate that the number of cyberattacks against numerous organizations,
70 including universities, has increased significantly (Hakak et al. 2020; Lallie et al. 2021). Many
71 cybersecurity incidents are caused by employees who disregard security policies due to their
72 initial lack of security awareness (Hina and Dominic 2016). Due to their role as instructors, who
73 must frequently administer and host online classes on their own, faculty members become the
74 primary actors in higher education. As a result, assessing their knowledge of security and privacy
75 settings when using video conferencing apps is crucial for ensuring that everyone's online
76 learning experience is as secure and private as possible.
77
78 This is the first study to use a national survey to assess the security and privacy awareness of
79 Saudi Arabian faculty members regarding the use of Blackboard Collaborate Ultra as the primary

80 video conferencing app during the COVID-19 pandemic. The specific objectives of this study are
81 to 1) comprehend and investigate the factors associated with the Saudi Arabian faculty's level of
82 security and privacy awareness regarding the use of video conferencing apps, particularly
83 Blackboard Collaborate Ultra, which is the most widely used video conferencing app in this
84 country for teaching and research purposes during and possibly beyond the COVID-19
85 pandemic, and 2) assist universities, particularly in Saudi Arabia, in improving their security
86 policies.
87
88 **Online learning in Saudi Arabian universities during the COVID-19 pandemic**
89 In 2005, the Saudi National E-learning Center (NELC) was established. In Saudi Arabia, NELC
90 is in charge of establishing governance frameworks and regulations for e-learning and online
91 learning. NELC plays a significant role in enhancing the online learning experience in
92 universities and promoting effective online learning practices (A. Y. Alqahtani and Rajkhan
93 2020). In addition, the center develops policies and procedures for the delivery and
94 administration of online learning programs. The policies stipulate the technologies that
95 universities must implement and the level of support they must provide for their faculty and
96 students. Policies also include standards and practices for creating online learning environments
97 that are accessible (National eLearning Center 2021).
98
99 NELC has provided universities with guidelines that specify e-learning infrastructure including
100 hardware (e.g., servers, storage, and networking), e-learning solutions (e.g., learning
101 management systems and video conferencing apps), establishing dedicated deanships to manage
102 e-learning matters, providing training and awareness programs, and other e-learning and online
103 learning initiatives (Malik et al. 2018). As a result of NELC's efforts and investment in e-
104 learning, universities in Saudi Arabia have a sufficient online learning infrastructure (Thorpe and
105 Alsuwayed 2019). During the COVID-19 pandemic, other researchers discovered that the IT
106 infrastructure in Saudi Arabian universities successfully supported the transition from face-to-
107 face to online learning (A. Y. Alqahtani and Rajkhan 2020). However, the maturity level of the
108 university played a significant role in its ability to overcome obstacles and implement e-learning
109 solutions before the pandemic.
110
111 Research indicates that faculty and students in Saudi Arabia have overwhelmingly positive
112 attitudes towards e-learning (Hoq 2020). Others have discovered that Saudi Arabian students
113 prefer e-learning due to its adaptability and enhanced communication with their teachers and
114 peers. However, the same study revealed that students viewed online instruction as less
115 advantageous than traditional face-to-face instruction (El-Sayed Ebaid 2020). While students'
116 attitudes toward e-learning are partially influenced by their prior experience and readiness for
117 online learning (N. Alqahtani, Innab, and Bahari 2021), numerous other factors, including
118 gender, course level, and quality of online learning approaches, also play a role (Vadakalu
119 Elumalai et al. 2020).
120

121 In the midst of the COVID-19 pandemic, which has presented significant challenges to societies,
122 Saudi Arabia, along with numerous other nations, has attempted to adapt to the impending crisis.
123 During the COVID-19 pandemic, Saudi Arabian universities took a number of steps to
124 accommodate the decision to adopt online learning, as education was one of the sectors most
125 severely impacted by the pandemic. To support and facilitate the transition to e-learning and
126 online learning, the Ministry of Education (MOE) of Saudi Arabia has provided all universities
127 with e-learning solutions licenses, including Blackboard Learning Management System (LMS)
128 and its video conferencing app, Blackboard Collaborate Ultra (Ministry of Education 2021). In
129 addition to providing free internet access to students across the nation, the Ministry of Education
130 increased bandwidth to accommodate the high demand for internet connections. In collaboration
131 with charitable organizations, the Ministry of Education has also provided laptops and training to
132 deserving students (A. Y. Alqahtani and Rajkhan 2020).
133
134 As of May 2020, the MOE reports that approximately 1.6 million students have taken more than
135 4 million online exams at 43 private and public universities. Over 58,179 faculty members
136 participated in this transition by delivering lectures, administering exams, and holding online
137 discussions, averaging 1.5 million online classes per week (Ministry of Education 2021).
138 UNESCO has lauded Saudi Arabia's efforts to pursue successful transitions to online learning to
139 facilitate the education of over six million students in schools and universities during the
140 COVID-19 pandemic (Vadakalu Elumalai et al. 2020). For these transitions to be successful, it is
141 essential that faculty members serving as frontline instructors are able to provide students with
142 the best online learning experience possible. This includes ensuring that their awareness level is
143 sufficient to keep online learning activities secure and private for all parties.
144
145 **Theoretical framework**
146 In 2006, Kruger and Kearney developed the KAB model, a prototype for assessing information
147 security awareness, which consists of three different dimensions (i.e., knowledge, attitudes, and
148 behaviors) (Kruger and Kearney 2006). Each dimension is measured by a series of multiple-
149 choice questions with either correct or incorrect answers for all three dimensions, as well as a
150 "Don't know" option for the "knowledge" and "attitudes" dimensions only. Since then, this KAB
151 model has been widely adopted as a tool for evaluating information security awareness
152 (McCormac et al. 2017; Onumo, Ullah-Awan, and Cullen 2021).
153
154 In addition, based on our literature review, we identified a number of individual factors that are
155 associated with security and privacy awareness. We identified five specific factors to include in
156 this study: attitudes toward information and communication technology (ICT) for teaching and
157 research, digital literacy, privacy concerns, perceived security awareness, and familiarity with
158 the video conferencing app platform.
159
160 *Perceived Security Policy Awareness and Privacy Concerns*

161 There is a large body of literature on people's concerns about how their private information is
162 shared when they use information technology products and services (Petronio and Child 2020),
163 as well as on how they perceive themselves to have the security awareness to protect them
164 (Bulgurcu, Cavusoglu, and Benbasat 2010; Li et al. 2019). According to these studies, perceived
165 security policy awareness and privacy concerns result in more cautious decisions regarding the
166 use of information technology-related goods and services. Consequently, we anticipate the same
167 for the video conferencing applications investigated in this study. The first two hypotheses in this
168 study are therefore:
169
170   H1: Faculty with a higher level of perceived security policy awareness have a higher
171   level of awareness of video conferencing apps' security and privacy settings.
172
173   H2: Faculty with a higher level of privacy concerns have a higher level of awareness of
174   video conferencing apps' security and privacy settings.
175

176 *Attitudes toward ICT for Teaching & Research and Digital Literacy*
177 Indisputable is the contribution of ICT to the improvement of education. However, it is no secret
178 that not all faculty share the same attitudes toward the use of ICT for teaching and research,
179 either because of their lack of experience, which may translate into lower levels of digital
180 literacy (Cavas et al. 2009), or because of their personal preferences (Bauwens et al. 2020).
181 Taking these findings into account, we hypothesize that:
182
183   H3: Faculty with more positive attitudes toward ICT for teaching and research have a
184   higher level of awareness of video conferencing apps' security and privacy settings.
185
186   H4: Faculty with a higher level of digital literacy have a higher level of awareness of
187   video conferencing apps' security and privacy settings.
188

189 *Familiarity with the App*
190 In the wake of the global adoption of distance learning in response to the COVID-19 pandemic,
191 numerous institutions use a variety of video conferencing apps. Each app may have its own user
192 interface and minor features, despite the fact that the majority of video conferencing apps will
193 have the same major features. Consequently, we hypothesize that:
194
195   H5: Faculty who are more familiar with the video conferencing app in use have a higher
196   level of awareness of video conferencing apps' security and privacy settings.
197

198 Based on all the aforementioned hypotheses, the conceptual model awareness in video
199 conferencing apps' security and privacy settings in this study is depicted in Figure 1.
200

Materials & Methods

Target Population

There are 29 public universities and 14 private universities in Saudi Arabia (Ministry of Education 2020). Due to the spread of the COVID-19 pandemic, the Saudi government has suspended face-to-face instruction in all of these universities as of the middle of the spring 2020 semester. The Ministry of Education demanded that universities move all courses online utilizing the available e-learning solutions. Online education will continue for the following three semesters. This study's target population consisted of professors from any Saudi Arabian university who were teaching during the study period. Included in this category are teaching assistants, lecturers, assistant professors, associate professors, and full professors. According to the Ministry of Education's most recent report, published in 2020, there were approximately 71,000 faculty teaching in Saudi Arabian universities (Ministry of Education 2021). Universities in Saudi Arabia typically provide their faculty with computers, assign them email addresses, and require them to regularly check their emails. Consequently, it can be stated that the entire population of interest to this study was theoretically accessible.

Measures

There are five latent exogenous variables in this study (i.e., attitudes toward ICT for teaching and research, digital literacy, perceived privacy concerns, perceived security awareness, and familiarity with Blackboard Collaborate Ultra). As summarized in Table 1, we created, adopted, or adapted items from other studies for all five. In addition, three other observed variables (i.e., knowledge, attitudes, and behaviors) will be merged into a single composite score to answer the first research question and will be treated as a latent endogenous variable (i.e., awareness of security and privacy settings on Blackboard Collaborate Ultra) to answer the second research question.

Perceived Security Policy Awareness

We adopted the scales from (Bulgurcu, Cavusoglu, and Benbasat 2010) to measure perceived security policy awareness among the faculty in this study. We omitted the first three out of six items in the original scales because they measured security awareness in general, as opposed to awareness of security policy within an organization, which was the focus of the last three items that we kept. The scales were measured on a 5-point Likert scale.

Privacy Concerns

We adopted the scales from (Malhotra, Kim, and Agarwal 2004) to measure privacy concerns among the faculty in this study. Specifically, we selected only the two most pertinent items from three to four original items for each of the control, awareness of practice, and collection dimensions to make it six, as opposed to ten items in total. The scales were measured on a 5-point Likert scale.

241 *Attitudes toward ICT for teaching and research*
242 We adapted the scales from (Ng 2012) to measure the attitudes of the faculty in this study toward
243 using ICT for teaching and research. Specifically, we merged the teaching and research
244 components into a single item, reducing the total number of items from eight to four. The scales
245 were measured on a 5-point Likert scale.
246
247 *Digital Literacy*
248 We adopted the scales from (Ng 2012) to measure digital literacy of the faculty in this study. In
249 particular, we eliminated three of the original six items for the technical dimensions while
250 retaining both items for the cognitive and social-emotional dimensions, reducing the total
251 number of items from nine to six. The scales were measured on a 5-point Likert scale.
252
253 *Familiarity with Blackboard Collaborate Ultra*
254 We developed three items to measure the faculty' familiarity with Blackboard Collaborate Ultra.
255 On a 5-point Likert scale, the first two questions assessed respondents' familiarity with and
256 frequency of use of Blackboard Collaborate Ultra, while the last questioned whether or not they
257 had read the terms of service.
258
259 *Awareness of Security and Privacy Settings on Blackboard Collaborate Ultra*
260 We developed five questions about Blackboard Collaborate Ultra to assess our participants'
261 knowledge, attitudes, and behaviors regarding Blackboard Collaborate Ultra's security and
262 privacy settings. The first three questions contain side-by-side images of the app's default and
263 altered security and privacy settings. We asked respondents to indicate which one was the default
264 (i.e., knowledge), which one they preferred (i.e., attitudes), and which one they primarily utilized
265 (i.e., behaviors). For the final two questions, we presented them with two hypothetical scenarios
266 involving security and privacy incidents and asked them to describe the available options and the
267 actions they would take in each scenario. For each response, we assigned a score of 0 for any
268 incorrect answer for the knowledge dimension or the worst option for the attitudes and behavior
269 dimensions, a score of 5 for "Don't know" or a partially correct response, and a score of 10 for
270 the correct answer or the most secure option. The complete questions are available in Appendix
271 1.
272
273 **Data collection**
274 In preparation for the data collection phase, a research ethics application was submitted to the
275 University of Jeddah ethics committee, which granted this study an ethics approval number (UJ-
276 REC-021). We collected the data by distributing a series of questionnaires using the online
277 survey software Qualtrics. On the survey's landing page, we provided an explanation of the
278 study's purpose. In addition to being informed of the length of time required to complete the
279 survey, participants were asked for their permission to participate. They were informed that

280 participation is voluntary and that they may opt out or withdraw at any time. To eliminate the
281 possibility of bias, no gifts or incentives of any kind were promised to the participants.
282
283 The questionnaire contained three sections. The first objective was to collect participant
284 demographic information, including gender, age, level of education, academic fields, academic
285 rank, teaching experience, and university name. This component served as a control variable for
286 the analysis.
287
288 The second section consisted of Likert-type questions with five levels for participants to indicate
289 their attitudes toward ICT, their digital literacy, their perceived privacy concerns, their perceived
290 privacy awareness, and their familiarity with Blackboard Collaborate Ultra. This section was
291 used to measure the model's exogenous variables.
292
293 In the third section, we measured the actual security and privacy awareness score of each
294 participant, which represented their awareness of security and privacy settings on Blackboard
295 Collaborate Ultra and served as the endogenous variable in our model. Four scenarios were
296 included. Each scenario included: a) two screenshots captured from Blackboard Collaborate
297 Ultra either during a running session or from the settings window; and b) several questions
298 designed to assess the knowledge, attitudes, and behaviors of each participant regarding some
299 important security and privacy settings in Blackboard Collaborate Ultra, as well as potential
300 security and privacy issues that may arise while using the application.
301
302 The objective of the first scenario was to assess participants' awareness of the risks associated
303 with guest access. The second scenario involved the activation of vital permissions, such as
304 media file sharing and whiteboard access. The third scenario involved private chat rooms that
305 could be abused to disseminate harmful and inappropriate content. The final scenario was
306 intended to assess participants' knowledge of what to do when malicious links are posted in chat.
307
308 Before we began collecting data, we conducted a pilot study to confirm the content validity of
309 the survey items, evaluate their difficulty, and obtain rough estimates of the time required to
310 complete the survey. Validity was evaluated based on its content and appearance. Validity of
311 content can help "establish an instrument's credibility, accuracy, relevance, and breadth of
312 domain knowledge." Face validity, on the other hand, examines survey items for "ease of use,
313 clarity, and readability" (Burton and Mazerolle 2011). Twelve faculty members from multiple
314 universities in Saudi Arabia were invited to participate in the pilot study. The pilot survey was
315 created as an online survey using Qualtrics survey software. Participants were given a blank text
316 field to comment on the item's relevance and clarity. In addition, they were required to indicate
317 whether a revision was necessary for the item. Participants were encouraged to provide a
318 revision for the item if one was suggested. All participant feedback was analyzed, and a few
319 survey questions were modified to reflect the suggested alterations. Several items were rewritten

320   to improve their relevance or clarity. Others were eliminated due to irrelevance or duplication. In
321   addition, items were added to measure certain missing aspects.

322

323   The survey was then distributed to faculty members at Saudi Arabia's 43 public and private
324   universities. To reach a representative sample, invitations were emailed, and the survey link was
325   shared on the four most popular social media platforms in Saudi Arabia: WhatsApp, LinkedIn,
326   Telegram, and Twitter. On these platforms, the objective was to reach as many academic
327   communities as possible. The responses were gathered between October and November of 2021.
328   Around 470 responses were received, and 307 were determined to be complete and valid. The
329   vast majority of responses that were eliminated were incomplete, but there were also a small
330   number of participants who refused to participate in the survey.

331

332   **Data analysis**
333   To determine the actual level of security and privacy awareness on video conferencing apps
334   among Saudi Arabian faculty in this study, we calculated a composite score with a 3:2:5 weight
335   as suggested by Kruger and Kearney for each of knowledge, attitudes, and behaviors variable
336   based on the responses to the third survey part (Kruger and Kearney 2006). The final security
337   and privacy awareness score for each participant was then normalized to a range between 0 and
338   100. According to Kruger and Kearney's classification, a score below 60 is categorized as
339   "Poor," a score of 80 or higher is categorized as "Good," and a score in between is categorized as
340   "Average" (Kruger and Kearney 2006).

341

342   We employed the Partial Least Squares Structural Equation Modeling (PLS-SEM) technique
343   with the "plssem" package in STATA 15 to identify factors associated with the awareness of
344   video conferencing apps' security and privacy settings (Venturini and Mehmetoglu 2019). PLS-
345   SEM is a widely employed structural equation modeling approach that permits the estimation of
346   complex relationships between latent variables in path models. It is especially useful for the
347   exploration and development of theory, as well as when prediction is the primary purpose of a
348   study, and it performs well with a small sample size (Hair, Howard, and Nitzl 2020). Prior to
349   running the path analysis, we examined the standardized loadings of each measurement item to
350   identify any that should be excluded from the model, and we used the squared interfactor
351   correlation and average variance extracted (AVE) from the path analysis to confirm discriminant
352   validity. To address the issue of endogeneity, we employed the control variable strategy by
353   conducting multiple multigroup comparison analyses across all demographic variables (Hult et
354   al. 2018). The complete code and data set can be found in our GitHub repository.

355

356   # Results
357   ## Participant Demographic Information
358   The demographic information of all participants in this study is summarized in Table 2. In terms
359   of gender (50.81% male vs. 49.19% female), academic fields (46.91% STEM vs. 53.09% non-

360   STEM), and position, the sample is quite balanced (57.33% tenured vs 42.67% non-tenured).
361   The majority of participants are under 45 years old (80.7%), hold a PhD (60.5%), and have at
362   least ten years of academic experience (63.84%).
363

364   **Awareness of Video Conferencing Apps' Security and Privacy Settings**
365   Figure 2 depicts the distribution of the composite score for awareness of the security and privacy
366   settings of video conferencing applications. According to Kruger and Kearney's classification,
367   the overall score for all participants in this study (M = 44.27, SD = 16.06) falls into the "Poor"
368   level of awareness (Kruger and Kearney 2006).
369

370   **Factors Associated with Awareness of Security and Privacy Settings**
371   Several measurement items in our model, all from the exogenous variables, were found to have a
372   low standardized loading score, and thus had to be eliminated (Hair et al. 2012). After multiple
373   iterations of this validity test for the measurement model, 17 items with standard loading scores
374   exceeding 0.800 are retained. Table 3 provides a summary of the summary statistics for all
375   remaining measurement items and the results of their validity tests. Importantly, as summarized
376   in Table 4, the AVE scores for each latent variable are greater than the squared interfactor
377   correlation scores, confirming that the model's discriminant validity has been met (Hair, Howard,
378   and Nitzl 2020; Venturini and Mehmetoglu 2019).
379

380   The results from PLS-SEM demonstrated a very high average R^2 value of 0.91, indicating a
381   substantial coefficient of determination (Hair, Ringle, and Sarstedt 2011), as well as a relative
382   goodness-of-fit (GoF) value of 0.99, which meets the rule of thumb (Henseler and Sarstedt 2013;
383   Vinzi, Trinchera, and Amato 2010). In addition, the path analysis demonstrated that all five
384   hypothesized relationships are statistically significant. One unexpected result is the negative
385   correlation between attitudes toward ICT for teaching and learning and awareness of the security
386   and privacy settings of video conferencing applications. Our subsequent multigroup comparison
387   analysis revealed that, with the exception of two demographic factors, the results are quite
388   consistent across the board. First, the structural effect of privacy concerns on the awareness of
389   the security and privacy settings of video conferencing apps is significant only for STEM faculty
390   and not for non-STEM faculty. Second, the negative structural effect of attitudes toward ICT for
391   teaching and learning on awareness of the security and privacy settings of video conferencing
392   apps is significant only for those with more than ten years of academic experience and not for
393   those with less.
394

395   Based on the findings, Figure 3 illustrates the final model of the awareness of video conferencing
396   apps' security and privacy settings among Saudi Arabian faculty in this study, while Table 5
397   summarizes the model's hypothesis tests results.
398

Discussion

399

400 This study investigates Saudi Arabian faculty's awareness of security and privacy settings of

401 video conferencing apps, especially Blackboard Ultra that they use to teach during the COVID-

402 19 pandemic. One of the study's key findings is that, in general, faculty in Saudi Arabia still

403 have poor security and privacy awareness on video conferencing apps. This may be

404 understandable considering that most of them only got into this new technology on a daily basis

405 because of the pandemic (Ali Alammary, Alshaikh, and Alhogail 2021). As evidenced by earlier

406 studies, the use of Blackboard and subsequentially Blackboard Collaborate Ultra in Saudi Arabia

407 was relatively low prior to the pandmic (Al Meajel and Sharadgah 2018; Tawalbeh 2017). This

408 finding is consistent with a previous study's conclusion that general awareness of cybersecurity

409 practices in Saudi Arabia is still below the desired level (Ali Alammary, Alshaikh, and Alhogail

410 2021). Therefore, additional efforts must be made to raise awareness by implementing multiple

411 strategies, not only to raise awareness but also to establish a cybersecurity culture (Alshaikh

412 2020). Establishing support groups called "cyber champions" to raise academic privacy

413 awareness and influence faculty behavior toward adopting cybersecurity practices is an example

414 of a proposed strategy to build a cybersecurity culture. Multiple studies have found that using

415 support groups and peers to modify cybersecurity behavior is an effective method (Alshaikh and

416 Adamson 2021; Cram et al. 2019; Guo et al. 2011). Universities could employ this strategy to

417 educate their academic community about the significance of maximizing the security and privacy

418 settings within video conferencing apps.

419

420 The effect of perceived security policy awareness on awareness of security and privacy settings

421 in video conferencing apps is the strongest among the five latent exogenous variables examined

422 in this study. This particular discovery is not unexpected. Despite the fact that this is not always

423 the case (Tariq, Brynielsson, and Artman 2014), a higher perceived level of security awareness

424 typically results in enhanced security and privacy practices (Lebek et al. 2014; Pratama and

425 Firmansyah 2021; Hwang et al. 2021). Therefore, it is only natural that faculty with a greater

426 understanding of their organization's security policies will be more willing to invest time in

427 learning the security and privacy settings for any app they use, including video conferencing

428 apps.

429

430 Familiarity with the video conferencing app itself was discovered to have the second largest

431 positive effect on awareness of the security and privacy settings of the app. Given the abundance

432 of available applications, each with its own features and configurations, familiarity with the app

433 in use is crucial, as predicted when developing a new construct for this variable. Consequently,

434 those unfamiliar with the video conferencing app in use may be unaware of all available security

435 and privacy settings. This finding is also consistent with findings from other studies regarding

436 familiarity with concepts, technical terms, or security-related systems that can aid in increasing

437 individuals' security awareness (Schmidt et al. 2008; Zwilling et al. 2022). Fortunately, this is a

438 relatively straightforward issue to address, for example with adequate technical support to
439 educate faculty on the subject.
440
441 Digital literacy was found to have a moderately positive impact on the awareness of security and
442 privacy settings in video conferencing applications. Individuals with a higher level of digital
443 literacy are able to independently navigate all security and privacy settings, according to a
444 straightforward explanation. As a result, individuals with a higher level of digital literacy tend to
445 have a heightened security and privacy awareness, which is consistent with the findings of a
446 number of previous studies (Sasvári, Nemeslaki, and Rauch 2015; Nemeslaki and Sasvari 2015;
447 Cranfield et al. 2020).
448
449 Privacy concerns were identified as the fourth exogenous variable positively influencing the
450 awareness of security and privacy settings in video conferencing applications. This result is
451 consistent with the extensive literature on the relationship between privacy concerns and security
452 awareness in general (Chung et al. 2021; Siponen 2001). Unlike the previous three exogenous
453 variables, however, this variable has a significant positive effect only on STEM faculty. In other
454 words, the effect is essentially nonexistent among faculty members in the social sciences, arts,
455 humanities, health, and medical sciences. This result could be explained by the increased
456 familiarity of STEM faculty members with ICT in general, including its benefits and risks.
457 According to a separate study, STEM faculty were more aware of cybersecurity threats like
458 phishing than non-STEM faculty (Diaz, Sherman, and Joshi 2020). Consequently, they are more
459 aware of the security and privacy settings of all applications, including video conferencing apps,
460 than their non-STEM counterparts.
461
462 Unlike the other factors, attitudes toward ICT for teaching and research were found to have a
463 negative impact on video conferencing app users' awareness of security and privacy settings. The
464 fact that this finding is significant only among participants with more than ten years of teaching
465 experience may provide insight into an intriguing story. The senior faculty appear to be
466 accustomed to whatever ICT solutions they utilized prior to the COVID-19 pandemic, which
467 were probably not video conferencing applications. Having to learn something new in order to
468 perform a task they are already very familiar with may be preventing them from fully utilizing
469 this new technology, particularly in terms of its security and privacy settings. After all, resistance
470 to change, whether among individuals in general (Audia and Brion 2007), or among faculty in
471 particular (McCrickerd 2012; Tallvid 2016) is not something new. The good news is that despite
472 being statistically significant, this variable has the smallest effect of all exogenous variables in
473 this model. As a result, focusing on the other variables that have a positive effect may be enough
474 to compensate for it.
475
476 Other than academic field and teaching experience, no statistically significant differences in age,
477 gender, educational attainment, or tenure-track status were observed. On the one hand, this

478   suggests that the endogeneity issue is largely addressed in this model, which strengthens the
479   reliability of the findings. On the other hand, the relatively similar scores across demographic
480   groups can be viewed as a positive development. It indicates equality in terms of security and
481   privacy awareness among Saudi Arabian faculty, as is also the case in some countries
482   (Hadlington, Binder, and Stanulewicz 2020; Pratama, Firmansyah, and Rahma 2022), whereas
483   some other countries continue to demonstrate inequality (McCormac et al. 2017; Zwilling et al.
484   2022).
485

Conclusions

487   In this study, we used the Knowledge-Attitude-Behavior (KAB) model to determine the actual
488   security and privacy awareness of faculty in Saudi Arabia regarding Blackboard Collaborate
489   Ultra, the most widely used video conferencing app in the country, in terms of video
490   conferencing apps. We discovered that the average score falls into the "Poor" category (mean =
491   44.27, SD = 16.06), which is not surprising considering that many of them only use this new
492   technology on a daily basis because of the pandemic.
493

494   In addition, based on the results of the subsequent PLS-SEM analysis, we found that all five
495   latent variables in our model have significant relationships with Saudi Arabian faculty members'
496   awareness of the security and privacy settings of video conferencing apps. In particular,
497   perceived security policy awareness has the greatest impact, followed by familiarity with the
498   video conferencing app's platform and digital literacy. Moreover, perceived privacy concerns are
499   only significant among STEM faculty, and surprisingly, attitudes toward the use of ICT for
500   teaching have a significant, albeit small, negative impact on senior faculty with more than ten
501   years of teaching experience.
502

503   This study lays the groundwork for future research and interventions that aim to increase user
504   awareness of security and privacy concerns when using video conferencing apps for educational
505   and research purposes. Given the rapid adoption of video conferencing apps as a result of
506   distance learning in response to the COVID-19 pandemic, it is becoming increasingly important
507   to address this issue. Blackboard Collaborate Ultra, despite being the most applicable in the
508   Saudi Arabian context, is not one of the most widely used video conferencing applications in the
509   world. There are alternative applications such as Zoom, Google Meet, Microsoft Teams, Skype,
510   and VooV Meeting among others. There may be some technical differences in their security and
511   privacy settings, so some of the findings of this study may not necessarily be applicable to the
512   other apps, despite the fact that their primary functions are typically identical. Therefore, we
513   recommend that similar research be conducted in other regions of the world to account for
514   cultural and technical differences that may make users of video conferencing apps less aware of
515   their security and privacy settings.
516

Acknowledgements

518 We would like to thank Dr. Firman M. Firmansyah for his contributions to the research design,
519 specifically for suggesting and reviewing the adequacy of our use of psychometric scales in
520 developing the questionnaire for this study, as well as for copy editing the final manuscript.
521

References

523 Al Meajel, Talal Mohammad, and Talha Abdullah Sharadgah. 2018. "Barriers to Using the
524   Blackboard System in Teaching and Learning: Faculty Perceptions." *Technology*
525   *Knowledge and Learning* 23 (2): 351–66. https://doi.org/10.1007/s10758-017-9323-2.
526 Alammary, Ali, Moneer Alshaikh, and Areej Alhogail. 2021. "The Impact of the COVID-19
527   Pandemic on the Adoption of e-Learning among Academics in Saudi Arabia." *Behaviour*
528   *& Information Technology*, September, 1–23.
529   https://doi.org/10.1080/0144929x.2021.1973106.
530 Alammary, Ali, Angela Carbone, and And Judy Sheard. 2016. "Blended Learning in Higher
531   Education: Delivery Methods Selection." In *Twenty-Fourth European Conference on*
532   *Information Systems (ECIS 2016)*. İstanbul,Turkey.
533 Almaiah, Mohammed Amin, Ahmad Al-Khasawneh, and Ahmad Althunibat. 2020. "Exploring
534   the Critical Challenges and Factors Influencing the E-Learning System Usage during
535   COVID-19 Pandemic." *Education and Information Technologies* 25 (6): 5261–80.
536   https://doi.org/10.1007/s10639-020-10219-y.
537 Alqahtani, Ammar Y., and Albraa A. Rajkhan. 2020. "E-Learning Critical Success Factors
538   during the COVID-19 Pandemic: A Comprehensive Analysis of E-Learning Managerial
539   Perspectives." *Education Sciences* 10 (9): 216. https://doi.org/10.3390/educsci10090216.
540 Alqahtani, Naji, Adnan Innab, and Ghareeb Bahari. 2021. "Virtual Education during COVID-19:
541   Exploring Factors Associated with E-Learning Satisfaction among Saudi Nursing
542   Students." *Nurse Educator* 46 (2): E18–22.
543   https://doi.org/10.1097/NNE.0000000000000954.
544 Alshaikh, Moneer. 2020. "Developing Cybersecurity Culture to Influence Employee Behavior: A
545   Practice Perspective." *Computers & Security* 98 (102003): 102003.
546   https://doi.org/10.1016/j.cose.2020.102003.
547 Alshaikh, Moneer, and Blair Adamson. 2021. "From Awareness to Influence: Toward a Model
548   for Improving Employees' Security Behaviour." *Personal and Ubiquitous Computing* 25
549   (5): 829–41. https://doi.org/10.1007/s00779-021-01551-2.
550 Alshehri, Yasser Ali, Najwa Mordhah, Sameer Alsibiani, Samir Alsobhi, and Noha Alnazzawi.
551   2020. "How the Regular Teaching Converted to Fully Online Teaching in Saudi Arabia
552   during the Coronavirus COVID-19." *Creative Education* 11 (07): 985–96.
553   https://doi.org/10.4236/ce.2020.117071.
554 Audia, Pino G., and Sebastien Brion. 2007. "Reluctant to Change: Self-Enhancing Responses to
555   Diverging Performance Measures." *Organizational Behavior and Human Decision*
556   *Processes* 102 (2): 255–69. https://doi.org/10.1016/j.obhdp.2006.01.007.
557 Bauwens, Robin, Jolien Muylaert, Els Clarysse, Mieke Audenaert, and Adelien Decramer. 2020.
558   "Teachers' Acceptance and Use of Digital Learning Environments after Hours:
559   Implications for Work-Life Balance and the Role of Integration Preference." *Computers*
560   *in Human Behavior* 112 (106479): 106479. https://doi.org/10.1016/j.chb.2020.106479.
561 Bulgurcu, Burcu, Hasan Cavusoglu, and Izak Benbasat. 2010. "Information Security Policy
562   Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security

563   Awareness." *The Mississippi Quarterly* 34 (3): 523–48.
564   https://doi.org/10.2307/25750690.
565 Burton, Laura J., and Stephanie M. Mazerolle. 2011. "Survey Instrument Validity Part I:
566   Principles of Survey Instrument Development and Validation in Athletic Training
567   Education Research." *Athletic Training Education Journal* 6 (1): 27–35.
568   https://doi.org/10.4085/1947-380x-6.1.27.
569 Camilleri, Mark Anthony, and Adriana Caterina Camilleri. 2021. "The Acceptance of Learning
570   Management Systems and Video Conferencing Technologies: Lessons Learned from
571   COVID-19." *Technology Knowledge and Learning*, August.
572   https://doi.org/10.1007/s10758-021-09561-y.
573 Cavas, Bulent, Pinar Cavas, Bahar Karaoglan, and Tarik Kisla. 2009. "A Study on Science
574   Teachers' Attitudes toward Information and Communications Technologies in
575   Education." *The Turkish Online Journal of Educational Technology* 8 (2).
576   https://eric.ed.gov/?id=ED505935.
577 Chung, Kuo-Cheng, Chun-Hung Chen, Hsueh-Hsuan Tsai, and Ya-Hsueh Chuang. 2021. "Social
578   Media Privacy Management Strategies: A SEM Analysis of User Privacy Behaviors."
579   *Computer Communications* 174 (June): 122–30.
580   https://doi.org/10.1016/j.comcom.2021.04.012.
581 Cram, W. Alec, Bentley University, John D'Arcy, Jeffrey G. Proudfoot, University of Delaware,
582   and Bentley University. 2019. "Seeing the Forest and the Trees: A Meta-Analysis of the
583   Antecedents to Information Security Policy Compliance." *MIS Quarterly: Management
584   Information Systems* 43 (2): 525–54. https://doi.org/10.25300/misq/2019/15117.
585 Cranfield, Desireé Joy, Isabella M. Venter, Rénette J. Blignaut, and Karen Renaud. 2020.
586   "Smartphone Security Awareness, Perceptions and Practices: A Welsh Higher Education
587   Case Study." In *INTED2020 Proceedings*. IATED.
588   https://doi.org/10.21125/inted.2020.0891.
589 Diaz, Alejandra, Alan T. Sherman, and Anupam Joshi. 2020. "Phishing in an Academic
590   Community: A Study of User Susceptibility and Behavior." *Cryptologia* 44 (1): 53–67.
591   https://doi.org/10.1080/01611194.2019.1623343.
592 El-Sayed Ebaid, Ibrahim. 2020. "Accounting Students' Perceptions on e-Learning during the
593   Covid- 19 Pandemic: Preliminary Evidence from Saudi Arabia." *Journal of Management
594   and Business Education* 3 (3): 236–49. https://doi.org/10.35564/jmbe.2020.0015.
595 Guo, Ken H., Yufei Yuan, Norman P. Archer, and Catherine E. Connelly. 2011. "Understanding
596   Nonmalicious Security Violations in the Workplace: A Composite Behavior Model."
597   *Journal of Management Information Systems : JMIS* 28 (2): 203–36.
598   https://doi.org/10.2753/mis0742-1222280208.
599 Hadlington, Lee, Jens Binder, and Natalia Stanulewicz. 2020. "Fear of Missing Out Predicts
600   Employee Information Security Awareness above Personality Traits, Age, and Gender."
601   *Cyberpsychology, Behavior and Social Networking* 23 (7): 459–64.
602   https://doi.org/10.1089/cyber.2019.0703.
603 Hair, Joe F., Matt C. Howard, and Christian Nitzl. 2020. "Assessing Measurement Model
604   Quality in PLS-SEM Using Confirmatory Composite Analysis." *Journal of Business
605   Research* 109 (March): 101–10. https://doi.org/10.1016/j.jbusres.2019.11.069.
606 Hair, Joe F., Christian M. Ringle, and Marko Sarstedt. 2011. "PLS-SEM: Indeed a Silver Bullet."
607   *The Journal of Marketing Theory and Practice* 19 (2): 139–52.
608   https://doi.org/10.2753/mtp1069-6679190202.

609 Hair, Joe F., Marko Sarstedt, Christian M. Ringle, and Jeannette A. Mena. 2012. "An
610   Assessment of the Use of Partial Least Squares Structural Equation Modeling in
611   Marketing Research." *Journal of the Academy of Marketing Science* 40 (3): 414–33.
612   https://doi.org/10.1007/s11747-011-0261-6.
613 Hakak, Saqib, Wazir Zada Khan, Muhammad Imran, Kim-Kwang Raymond Choo, and
614   Muhammad Shoaib. 2020. "Have You Been a Victim of COVID-19-Related Cyber
615   Incidents? Survey, Taxonomy, and Mitigation Strategies." *IEEE Access: Practical*
616   *Innovations, Open Solutions* 8 (June): 124134–44.
617   https://doi.org/10.1109/ACCESS.2020.3006172.
618 Henseler, Jörg, and Marko Sarstedt. 2013. "Goodness-of-Fit Indices for Partial Least Squares
619   Path Modeling." *Computational Statistics* 28 (2): 565–80.
620   https://doi.org/10.1007/s00180-012-0317-1.
621 Hina, Sadaf, and Dhanapal Durai Dominic. 2016. "Information Security Policies: Investigation
622   of Compliance in Universities." In *2016 3rd International Conference on Computer and*
623   *Information Sciences (ICCOINS)*, 564–69. IEEE.
624   https://doi.org/10.1109/iccoins.2016.7783277.
625 Hoq, Mohammad Ziaul. 2020. "E-Learning during the Period of Pandemic (COVID-19) in the
626   Kingdom of Saudi Arabia: An Empirical Study." *American Journal of Educational*
627   *Research* 8 (7): 457–64. https://doi.org/10.12691/education-8-7-2.
628 Hult, G. Tomas M., Joseph F. Hair Jr, Dorian Proksch, Marko Sarstedt, Andreas Pinkwart, and
629   Christian M. Ringle. 2018. "Addressing Endogeneity in International Marketing
630   Applications of Partial Least Squares Structural Equation Modeling." *Journal of*
631   *International Marketing* 26 (3): 1–21. https://doi.org/10.1509/jim.17.0151.
632 Hwang, Inho, Robin Wakefield, Sanghyun Kim, and Taeha Kim. 2021. "Security Awareness:
633   The First Step in Information Security Compliance Behavior." *Journal of Computer*
634   *Information Systems* 61 (4): 345–56. https://doi.org/10.1080/08874417.2019.1650676.
635 Iffat Rahmatullah, Shadma. 2021. "Blackboard as Online Learning Management System in Saudi
636   Context: Challenges and Prospects." *SSRN Electronic Journal*.
637   https://doi.org/10.2139/ssrn.3874035.
638 Joshi, Chanchala, and Umesh Kumar Singh. 2017. "Information Security Risks Management
639   Framework – A Step towards Mitigating Security Risks in University Network." *Journal*
640   *of Information Security and Applications* 35 (August): 128–37.
641   https://doi.org/10.1016/j.jisa.2017.06.006.
642 Kruger, H. A., and W. D. Kearney. 2006. "A Prototype for Assessing Information Security
643   Awareness." *Computers & Security* 25 (4): 289–96.
644   https://doi.org/10.1016/j.cose.2006.02.008.
645 Lallie, Harjinder Singh, Lynsay A. Shepherd, Jason R. C. Nurse, Arnau Erola, Gregory
646   Epiphaniou, Carsten Maple, and Xavier Bellekens. 2021. "Cyber Security in the Age of
647   COVID-19: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks during the
648   Pandemic." *Computers & Security* 105 (102248): 102248.
649   https://doi.org/10.1016/j.cose.2021.102248.
650 Lebek, Benedikt, Jörg Uffen, Markus Neumann, Bernd Hohler, and Michael H. Breitner. 2014.
651   "Information Security Awareness and Behavior: A Theory-Based Literature Review."
652   *Management Research Review* 37 (12): 1049–92. https://doi.org/10.1108/mrr-04-2013-
653   0085.

654 Li, Ling, Wu He, Li Xu, Ivan Ash, Mohd Anwar, and Xiaohong Yuan. 2019. "Investigating the
655   Impact of Cybersecurity Policy Awareness on Employees' Cybersecurity Behavior."
656   *International Journal of Information Management* 45 (April): 13–24.
657   https://doi.org/10.1016/j.ijinfomgt.2018.10.017.
658 Malhotra, Naresh K., Sung S. Kim, and James Agarwal. 2004. "Internet Users' Information
659   Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model." *Information
660   Systems Research* 15 (4): 336–55. https://doi.org/10.1287/isre.1040.0032.
661 Malik, Hafiz Abid Mehmood, Faiza Abid, R. Kalaicelvi, and Zeeshan Bhatti. 2018. "Challenges
662   of Computer Science and IT in Teaching-Learning in Saudi Arabia." *Sukkur IBA Journal
663   of Computing and Mathematical Sciences* 2 (1): 29–35.
664   https://doi.org/10.30537/sjcms.v2i1.71.
665 McCormac, Agata, Tara Zwaans, Kathryn Parsons, Dragana Calic, Marcus Butavicius, and
666   Malcolm Pattinson. 2017. "Individual Differences and Information Security Awareness."
667   *Computers in Human Behavior* 69 (April): 151–56.
668   https://doi.org/10.1016/j.chb.2016.11.065.
669 McCrickerd, Jennifer. 2012. "Understanding and Reducing Faculty Reluctance to Improve
670   Teaching." *College Teaching* 60 (2): 56–64.
671   https://doi.org/10.1080/87567555.2011.633287.
672 Ministry of Education. 2020. "University Education." Ministry of Education Website. November
673   17, 2020. https://moe.gov.sa/en/education/highereducation/pages/default.aspx.
674 ———. 2021. "Data and Statistics." Ministry of Education Website. December 21, 2021.
675   https://www.moe.gov.sa/en/knowledgecenter/dataandstats/Pages/infoandstats.aspx.
676 National eLearning Center. 2021. "E-Learning Standards for Higher Education." National
677   ELearning Center Website. April 26, 2021. https://nelc.gov.sa/ar/node/230.
678 Nemeslaki, A., and P. Sasvari. 2015. "Empirical Analysis of Information Security Awareness in
679   the Business and Public Sectors of Hungary." In *Central and Eastern European EDem
680   and EGov Days 2015. Time for a European Internet?*, 405–18. Wien: Österreichische
681   Computer-Gesellschaft.
682 Ng, Wan. 2012. "Can We Teach Digital Natives Digital Literacy?" *Computers & Education* 59
683   (3): 1065–78. https://doi.org/10.1016/j.compedu.2012.04.016.
684 Onumo, Aristotle, Irfan Ullah-Awan, and Andrea Cullen. 2021. "Assessing the Moderating
685   Effect of Security Technologies on Employees Compliance with Cybersecurity Control
686   Procedures." *ACM Transactions on Management Information Systems* 12 (2): 1–29.
687   https://doi.org/10.1145/3424282.
688 Petronio, Sandra, and Jeffrey T. Child. 2020. "Conceptualization and Operationalization: Utility
689   of Communication Privacy Management Theory." *Current Opinion in Psychology* 31
690   (February): 76–82. https://doi.org/10.1016/j.copsyc.2019.08.009.
691 Pratama, Ahmad R. 2017. "Cross-Country Analysis of ICT and Education Indicators: An
692   Exploratory Study." In *IOP Conference Series: Materials Science and Engineering*,
693   185:012006. IOP Publishing. https://doi.org/10.1088/1757-899X/185/1/012006.
694 Pratama, Ahmad R., and Firman M. Firmansyah. 2021. "Until You Have Something to Lose!
695   Loss Aversion and Two-Factor Authentication Adoption." *Applied Computing and
696   Informatics*, April. https://doi.org/10.1108/aci-12-2020-0156.
697 Pratama, Ahmad R., Firman M. Firmansyah, and Fayruz Rahma. 2022. "Security Awareness of
698   Single Sign-on Account in the Academic Community: The Roles of Demographics,

699   Privacy Concerns, and Big-Five Personality." *PeerJ Computer Science* 8 (March): e918.
700   https://doi.org/10.7717/peerj-cs.918.

701 Sasvári, Péter, András Nemeslaki, and Wolf Rauch. 2015. "Old Monarchy in the New
702   Cyberspace: Empirical Examination of Information Security Awareness among Austrian
703   and Hungarian Enterprises." *Academic and Applied Research in Military and Public* 14
704   (1): 63–78. https://doi.org/10.32565/aarms.2015.1.6.

705 Schmidt, Mark B., Allen C. Johnston, Kirk P. Arnett, Jim Q. Chen, and Suichen Li. 2008. "A
706   Cross-Cultural Comparison of U.s. and Chinese Computer Security Awareness." *Journal*
707   *of Global Information Management* 16 (2): 91–103.
708   https://doi.org/10.4018/jgim.2008040106.

709 Siponen, M. T. 2001. "Five Dimensions of Information Security Awareness." *SIGCAS Comput.*
710   *Soc* 31 (2): 24–29.

711 Tallvid, Martin. 2016. "Understanding Teachers' Reluctance to the Pedagogical Use of ICT in
712   the 1:1 Classroom." *Education and Information Technologies* 21 (3): 503–19.
713   https://doi.org/10.1007/s10639-014-9335-7.

714 Tariq, Muhammad Adnan, Joel Brynielsson, and Henrik Artman. 2014. "The Security
715   Awareness Paradox: A Case Study." In *2014 IEEE/ACM International Conference on*
716   *Advances in Social Networks Analysis and Mining (ASONAM 2014)*. IEEE.
717   https://doi.org/10.1109/asonam.2014.6921663.

718 Tawalbeh, Thaer Issa. 2017. "EFL Instructors' Perceptions of Blackboard Learning Management
719   System (LMS) at University Level." *English Language Teaching* 11 (1): 1.
720   https://doi.org/10.5539/elt.v11n1p1.

721 Thorpe, Stephen J., and Hassan M. Alsuwayed. 2019. "Saudi Academic Perceptions of E-
722   Learning Systems." *International Journal of Learning Technology* 14 (3): 251.
723   https://doi.org/10.1504/ijlt.2019.105710.

724 Trueman, Charlotte. 2020. "Pandemic Leads to Surge in Video Conferencing App Downloads."
725   Computerworld. April 3, 2020.
726   https://www.computerworld.com/article/3535800/pandemic-leads-to-surge-in-video-
727   conferencing-app-downloads.html.

728 Vadakalu Elumalai, Kesavan, Jayendira P Sankar, Kalaichelvi, Jeena Ann John, Nidhi Menon,
729   Mufleh Salem M Alqahtani, and May Abdulaziz Abumelha. 2020. "Factors Affecting the
730   Quality of E-Learning during the COVID-19 Pandemic from the Perspective of Higher
731   Education Students." *Journal of Information Technology Education Research* 19: 731–
732   53. https://doi.org/10.28945/4628.

733 Venturini, Sergio, and Mehmet Mehmetoglu. 2019. "Plssem: A Stata Package for Structural
734   Equation Modeling with Partial Least Squares." *Journal of Statistical Software* 88
735   (March): 1–35. https://doi.org/10.18637/jss.v088.i08.

736 Vinzi, Vincenzo Esposito, Laura Trinchera, and Silvano Amato. 2010. "PLS Path Modeling:
737   From Foundations to Recent Developments and Open Issues for Model Assessment and
738   Improvement." In *Handbook of Partial Least Squares*, 47–82. Berlin, Heidelberg:
739   Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-540-32827-8_3.

740 Zwilling, Moti, Galit Klien, Dušan Lesjak, Łukasz Wiechetek, Fatih Cetin, and Hamdullah Nejat
741   Basim. 2022. "Cyber Security Awareness, Knowledge and Behavior: A Comparative
742   Study." *Journal of Computer Information Systems* 62 (1): 82–97.
743   https://doi.org/10.1080/08874417.2020.1712269.

Figure 1

Conceptual model of video conferencing security and privacy settings awareness in this study

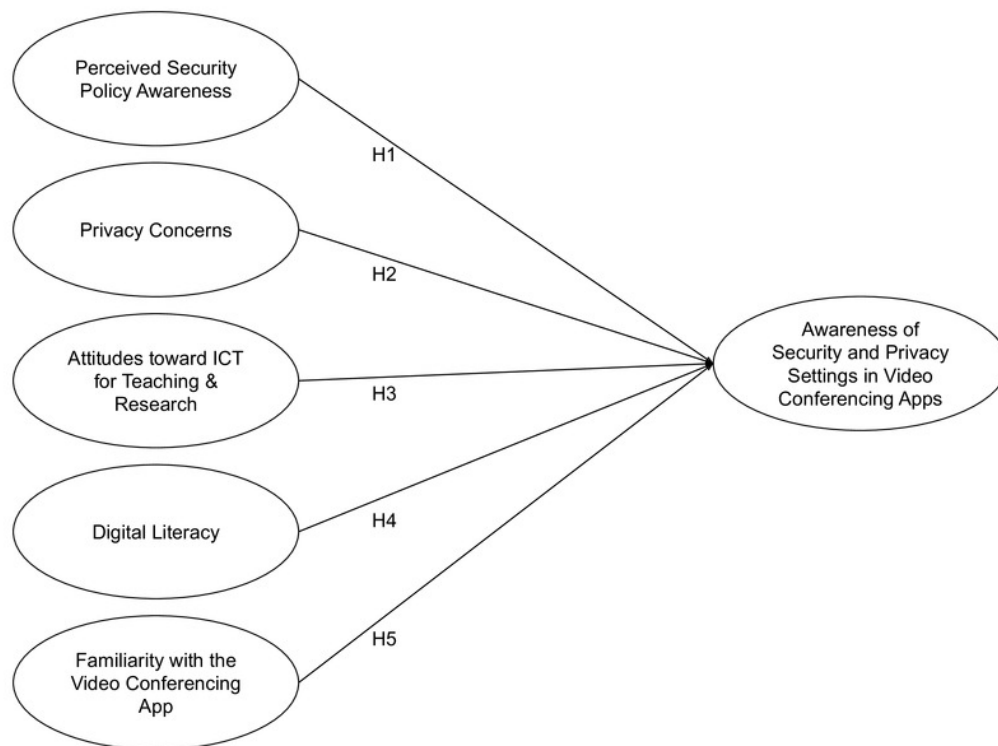



Figure 2

Density plot of the video conferencing apps security and privacy settings awareness score among all participants

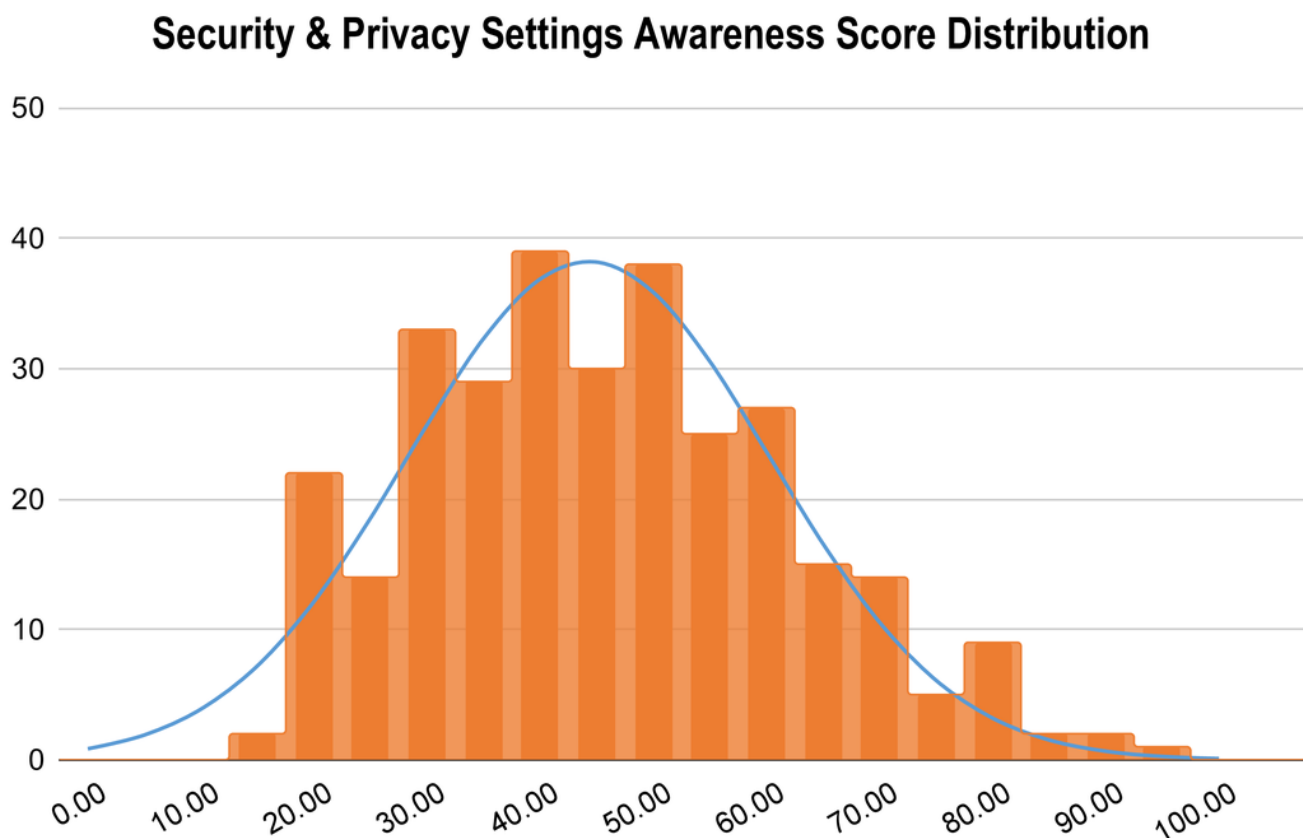
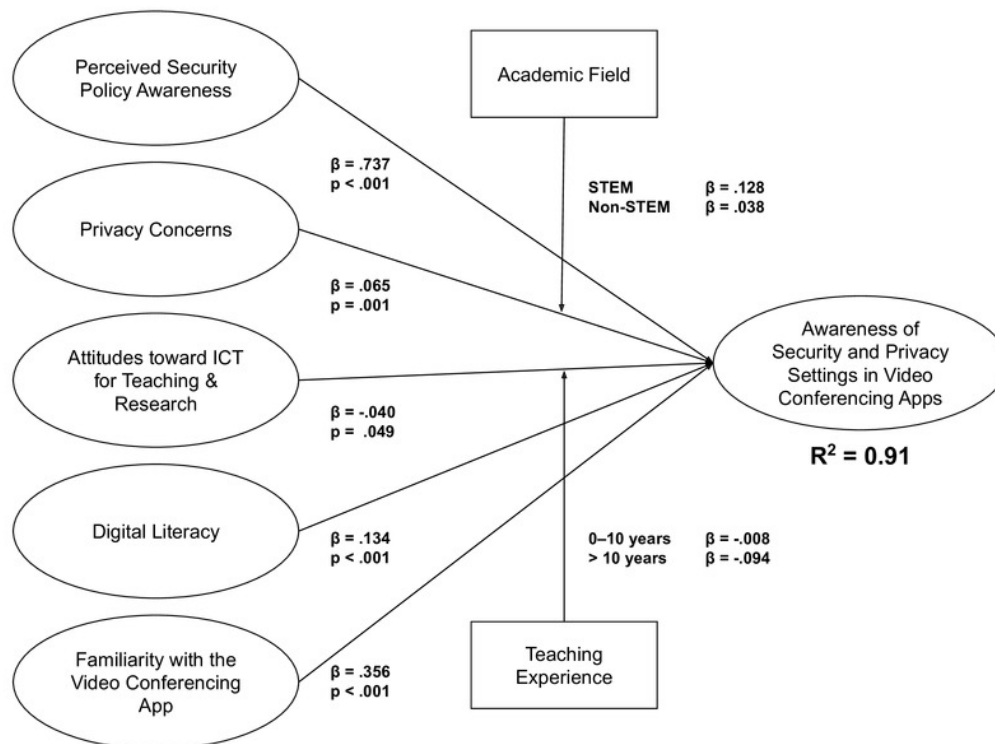



Figure 3

Final model of video conferencing security and privacy settings awareness in this study

Research instruments for all latent independent variables

1   Table 1. Research Instruments for all Latent Exogenous Variables

Variables	Measurement Items	Code	Source
Perceived Security Policy Awareness	I know the rules and regulations prescribed by the security policy of my university.	psa1	(Bulgurcu et al., 2010)
	I understand the rules and regulations prescribed by the security policy of my university.	psa2	
	I know my responsibilities as prescribed in the security policy to enhance the information security of my university.	psa3	
Privacy Concerns	User online privacy is really a matter of users' right to exercise control and autonomy over decisions about how their information is collected, used, and shared.	pc1	(Malhotra et al., 2004)
	I believe that online privacy is invaded when control is lost or unwillingly reduced as a result of a marketing transaction.	pc2	
	Companies seeking information online should disclose the way the data are collected, processed, and used.	pc3	
	It is very important to me that I am aware and knowledgeable about how my personal information will be used.	pc4	
	When online companies ask me for personal information, I sometimes think twice before providing it.	pc5	
	I'm concerned that online companies are collecting too much personal information about me.	pc6	
Attitudes toward ICT for Teaching & Research	I like using ICT for teaching or conducting research	att1	(Ng, 2012)
	ICT makes teaching or conducting research more interesting	att2	
	I am more motivated to teach or to conduct research with ICT	att3	
	There is a lot of potential in the use of mobile technologies (e.g., smartphones, tablets) for teaching and research	att4	
Digital Literacy	I know how to solve my own technical problems.	dl1	(Ng, 2012)
	I can learn new technologies easily.	dl2	
	I know about a lot of different technologies.	dl3	
	I am confident with my search and evaluate skills in regard to obtaining information from the Web	dl4	

	I am familiar with issues related to web-based activities e.g., cyber safety, search issues, plagiarism	dl5	
	ICT enables me to collaborate better with their peers on project work and other learning activities	dl6	
	I frequently obtain help with my university work from my friends over the Internet e.g., through email, social media, or Videoconference	dl7	
Familiarity	How familiar are you with Blackboard Collaborate Ultra?	fam1	Developed by the authors
	How much do you use Blackboard Collaborate Ultra?	fam2	
	Have you read the terms & agreements of Blackboard Collaborate Ultra?	fam3	

Demographic information of participants

1   Table 2. Respondent Demographic Information

Variable	Categories	Freq	%
Gender	Male	156	50.81%
	Female	151	49.19%
Age	<35	87	28.34%
	35-44	161	52.44%
	45-54	52	16.94%
	55-64	7	2.28%
Education	Bachelor's degree	9	2.93%
	Master's degree	112	36.48%
	PhD degree	186	60.59%
Rank	Teaching assistant (Nontenured)	23	7.49%
	Lecturer (Nontenured)	108	35.18%
	Assistant Professor (Tenured)	135	43.97%
	Associate Professor (Tenured)	33	10.75%
	Full Professor (Tenured)	8	2.61%
Experience	< 3 years	50	16.29%
	3 to 9 years	146	47.56%
	10 to 24 years	97	31.60%
	25 +	14	4.56%
Academic Fields	Arts, Humanities and Social Sciences	118	38.44%
	Science, Engineering and Technology	144	46.91%
	Medical and Health Sciences	45	14.66%

Summary statistics and validity tests of the measurement model

1   Table 3. Summary statistics and validity tests of the measurement model

Variables	Measurement Items	Mean	SD	Standardized Loading (Initial)	Standardized Loading (Final)	Cronbach	DG	rho_A
Perceived Security Policy Awareness	pspa1	3.48	1.07	0.949	0.949	0.947	0.966	0.948
	pspa2	3.47	1.07	0.970	0.970			
	pspa3	3.61	1.06	0.934	0.934			
Privacy Concerns	pc1*	4.21	0.86	0.680	-	-	-	-
	pc2	4.30	0.80	0.728	0.846	0.772	0.866	0.790
	pc3	4.53	0.73	0.714	0.802			
	pc4	4.66	0.63	0.767	0.831			
	pc5 *	4.45	0.81	0.690	-	-	-	-
	pc6 *	4.28	0.87	0.663	-	-	-	-
Attitudes toward Using ICT for Teaching & Research	att1	4.42	0.82	0.878	0.892	0.884	0.928	0.891
	att2	4.26	0.87	0.884	0.902			
	att3	4.19	0.90	0.886	0.907			
	att4 *	4.18	0.93	0.699	-	-	-	-
Digital Literacy	dl1 *	3.85	0.92	0.671	-	-	-	-
	dl2	4.21	0.77	0.783	0.823	0.787	0.875	0.796
	dl3	3.90	0.87	0.809	0.863			
	dl4 *	4.22	0.82	0.757	-	-	-	-
	dl5	3.98	0.86	0.771	0.823			
	dl6 *	4.26	0.79	0.765	-	-	-	-
	dl7 *	3.99	0.96	0.438	-	-	-	-
Familiarity with Blackboard	fam1	3.87	1.18	0.857	0.914	0.741	0.884	0.764
	fam2	4.25	1.19	0.790	0.865			

Collaborate Ultra	fam3 *	2.32	1.51	0.542	-	-	-	-
Awareness of	k	3.74	0.80	0.937	0.937	0.913	0.945	0.918
Security and	a	3.82	0.77	0.942	0.942			
Privacy Settings	b	2.79	0.69	0.889	0.889			

Discriminant validity

Note: diagonal elements are average variance extracted (AVE), off-diagonal elements are squared interfactor correlation

1   Table 4. Discriminant validity

Variable	PSPA	PC	Att	DL	Fam	AoSPS
PSPA	**0.905**					
PC	0.026	**0.683**				
Att	0.065	0.077	**0.810**			
DL	0.218	0.077	0.219	**0.700**		
Fam	0.034	0.008	0.012	0.069	**0.792**	
AoSPS	0.750	0.058	0.072	0.326	0.280	**0.852**

2   Note: diagonal elements are average variance extracted (AVE), off-diagonal elements are
3   squared interfactor correlation

Hypothesis test results

final

1 Table 5. Hypothesis test results

Hypothesis	Relationship	Result
H1	PSPA → Awareness	Significantly positive effect
H2	PC → Awareness	Significantly positive effect, moderated by academic fields
H3	Att → Awareness	Significantly negative effect, moderated by teaching experience
H4	DL → Awareness	Significantly positive effect
H5	Fam → Awareness	Significantly positive effect