Information Systems and e-Business Management (2023) 21:123–158
https://doi.org/10.1007/s10257-022-00575-2

ORIGINAL ARTICLE

Moving beyond cyber security awareness and training to engendering security knowledge sharing

Saad Alahmari[1] · Karen Renaud[2] · Inah Omoronyia[3]

Received: 5 December 2021 / Revised: 1 September 2022 / Accepted: 19 September 2022 /
Published online: 12 October 2022

Abstract

Employees play a critical role in improving workplace cyber security, which builds on widespread security knowledge and expertise. To maximise knowledge levels, organisations run awareness and training course. Yet, they should also encourage and facilitate *Security Knowledge Sharing* (SKS). To facilitate such sharing, we used a bespoke App which deploys a game to deliver security training and to encourage sharing based on the *Transactive Memory System* (TMS) theory. An empirical study was conducted within a Saudi Arabian Fortune 100 organisation to test the impact of the app on employee knowledge. The app demonstrated efficacy in enhancing organisational security awareness and knowledge. The results highlight the potential of TMS in improving overall security knowledge in organisations.

Keywords Self-determination theory (SDT) · Transactive memory system (TMS) · Cyber security awareness (CSA) · Security knowledge · Information security awareness (ISA)

✉ Saad Alahmari
Saad.alahmari@nbu.edu.sa

Karen Renaud
karen.renaud@strath.ac.uk

Inah Omoronyia
Inah.Omoronyia@glasgow.ac.uk

[1] Applied College, Northern Border University, Arar, Saudi Arabia

[2] Department of Computer and Information Sciences, University of Strathclyde, Glasgow, UK

[3] School of Computing Science, University of Glasgow, Glasgow, UK

1 Introduction

Organisations cannot secure their information and systems without the active involvement of their employees. They are essential in bolstering organisational cyber security (Ahmed et al. 2014). In essence, employees need to know what to do, and how to do it, Hence they have to possess the required knowledge and skills (know-how) to play their part in maintaining cyber security. While awareness drives and training are undeniably valuable and essential, such drives are not sufficient. Of particular interest in this paper is cyber security knowledge sharing (SKS). Knowledge sharing, of all types, improves the organisation as a whole and engenders trust between employees (Dang and Nkhoma 2017). The knowledge held by an organisation's employees is its most important asset (Wegner 1987). If cyber security knowledge is shared, it can potentially prevent security breaches (Dixon 2000) and help to reinforce the importance of cyber security (Rahim et al. 2015). The efficacy of deliberate engendering of informal SKS between employees should be investigated in terms of its potential to improve overall organisational cyber security (Mermoud et al. 2018).

The biggest SKS challenge lies in understanding the key factors which make it successful (Ortiz et al. 2017; Kim and Lee 2006). A previous study explored a number of different theories designed to mitigate the SKS challenge (Al Ahmari et al. 2018) and others focus on individual-focused aspects rather than the social aspects of SKS (Safa et al. 2018; Safa and Von Solms 2016; Bulgurcu et al. 2010; Abawajy 2014; Bada et al. 2019) These approaches neglect the impact of factors facilitating and motivating knowledge exchange within organisations and generally do not address social aspects influences on cyber security activities. We would be helpful for organisations to know how to promote cyber security knowledge sharing (Al Ahmari et al. 2018; Abawajy 2014). As such, the research questions are:

RQ1: Can organisational security knowledge sharing (SKS) be modelled using *Transactive Memory System* (TMS) Theory?

RQ2: Can individual SKS be encouraged by satisfying employees' self-determination needs?

Section 2 reviews the background literature on SKS. Section 4 then lays out our research methodology which we engaged in to answer the two research questions. Section 5 reports the results, Section 6 returns to the research questions and then Sect. 7 discusses the findings and reflects on their implications. Section 8 concludes.

2 Related research

As business dependence on internet technologies increases, so does the likelihood of security breaches. Employees play a crucial role in enhancing cyber security (Ahmed et al. 2014). Their understanding of the cyber security risks and knowledge of mitigations can positively influence organisational cyber security behaviours (Becerra-Fernandez and Sabherwal 2014). The term ‘security is critical’ is one that all employees should be familiar with. Due to the rapid integration of internet technology into modern businesses, employees play a critical role in bolstering organisational systems’ cyber security.

An essential prerequisite for making such secure behaviour possible is for employees to know *what* they should do (knowledge), and *how* to do it (skills). However, in addition to that, a powerful additional way to increase and enhance cyber security knowledge is to encourage and facilitate SKS within organisations (Mermoud et al. 2018).

SKS, of all types, facilitates trust between employees (Dang and Nkhoma 2017; Politis 2003). Of particular interest in this paper is cyber SKS, which improves cyber security awareness (Dixon 2000). Organisations should therefore facilitate and engender SKS to make the knowledge accessible to all of those who need it and ultimately to enhance cyber security.

2.1 Cyber security awareness (CSA)

CSA can be described as “*a state where users in an organisation are aware of ideally committed to their security mission*” P.31, (Siponen 2000). According to Abawajy (2014), CSA may be described as users’ understanding of the critical nature of cyber security best practice. Employees, in general, have varying degrees of security knowledge. Several studies argue that employees’ CSA is among the most significant elements for achieving the objectives of cyber security in organisations (Siponen 2000; Bauer and Bernroider 2017; D’Arcy et al. 2009).

CSA offers significant insights into how to enhance employees’ awareness of security policies to mitigate risk (Siponen 2000; Vance and Siponen 2012). There have been multiple approaches to increasing employees’ awareness through traditional training programmes (Killmeyer 2006). According to Thomson and von Solms, programmes are most commonly delivered via presentations, workshops, and multimedia packages, email reminders and screen savers (Siponen 2000). Moreover, Bauer and Bernroider (2017) implemented an action programme to raise CSA associated with phishing, password security and clear screen policies. Consequently, Puhakainen and Siponen (2010) argued that there are two requirements to ensure a security training programme is effective. The *first* must provide theoretical clarification of why and who the programme works for. The *second* requirement, the theory, must deliver guidelines for how effective training is to be delivered in the workplace (Puhakainen and Siponen 2010). Bada et al. (2019) agreed that considering how employees perceive risks is key to building awareness.

Enhancing employees’ technology expertise is a significant precursor of CSA (Haeussinger and Kranz 2013). Information knowledge refers to understanding the fundamental information technology applications used in daily business, such as computers, email systems, and the internet. The level of general IT knowledge of employees positively affects their CSA (Haeussinger and Kranz 2013). Employees who are more knowledgeable about cyber security and information technology will be more aware of cyber security issues (Khando et al. 2021). Thus, organisations are recommended to improve their employees' IT skills to avoid them from engaging in unintentional non-secure behaviour. Mejias confirmed this, stating that the constructs of technical expertise, organisational influence, and attacker assessment all had significant connections with CSA (Mejias 2012). Intriguingly, corporate influence and attacker evaluation were associated with CSA more strongly than technical knowledge (Mejias 2012).

People can gain security knowledge from training programmes (Bauer and Bernroider 2017; Killmeyer 2006; Thomson and von Solms 1998), from personal experience (Dang-Pham et al. 2017) or from other employees in the workplace (He and Johnson 2017). However, approaches of this type of carry with them a variety of well-known limitations, such as the difficulty in determining the effectiveness of such training (He and Johnson 2017).

One mechanism for improving CSA is for employees to transfer security-related knowledge to other employees (Siponen 2000). Organisations should implement suitable incentive schemes to foster employee cooperation and promote sharing, it is claimed. Several studies examined the impact of SKS processes and discovered that a well-developed cooperative theory enables effective information sharing, knowledge application, and informal SKS (Choi et al. 2010; Davison et al. 2013). In the following sections, we will discuss information SKS and its role in general terms.

2.2 Cyber security knowledge sharing (SKS)

Knowledge is gained when meaning is added to information. People can gain knowledge from others in their environment (Feledi et al. 2013) or from personal experience (Feledi and Fenz 2012). In the cyber security context, people can gain information from training drives, but are more likely to gain the knowledge they need from other employees in the workplace Alahmari et al. (2019). The cyber security field is characterised by it fluidity, emergent threats and, specifically, the fact that security behaviours have to evolve accordingly.

Zhang (2018) confirms that knowledge expires in this field, and needs to be renewed constantly. Moreover, Junger et al. (2017) showed that warnings, by themselves, do not necessarily make that much of a difference to susceptibility to social-engineering attacks. Gcaza and von Solms (2017) finds that cultivating a cyber security culture, which implies that SKS has become *de rigueur*, is the best approach for addressing human-related cyber security vulnerabilities.

SKS implies collaboration i.e., working together to achieve an objective. Safa et al. (2017) identified cyber security collaboration as a powerful and efficient approach to reducing the risks associated with managing cyber security. In particular, the goal is to facilitate SKS (Safa et al. 2017; Chen et al. 2014). While several studies have explored the organisational and individual aspects to enhance CSA (Tsohou et al. 2015), limited studies into collaboration have been conducted in the cyber security field into the organisational context.

2.3 Theory of transactive memory system (TMS)

TMS has been described as "*a set of individual memory systems in combination with the communication that takes place between individuals*" (Wegner 1987). TMS determines the specific division of cognitive labour within a group of people, as a means to facilitate encoding, storage, and retrieval of knowledge pertaining to various domains. When a TMS is being utilised, each group member is aware of "who knows what, and who knows who knows what" (Choi et al. 2010). Simply put, the characteristics of a TMS mean that three crucial qualities, common to other types of socially shared cognition, are present – i.e., differentiated knowledge; processes of transactive encoding, storage and retrieval; and the dynamic nature of TMS functions (Lewis and Herndon 2011). Thus, an alternative and more suitable approach might involve a shift of focus away from repositories towards processes (Jackson and Klobas 2008).

Liang et al. (1995) described three aspects of TMS:

(1) Specialisation is the term used to describe the degree of differentiation of the knowledge held by team members (Liang et al. 1995). Specialisation reduces the cognitive burden on community participants by allowing each to focus on his or her own area of expertise. It urges members to prioritise information integration through different domains in order to maximise team knowledge use (Lewis 2003). Moreover, differentiated group knowledge results in specialisation within the team, resulting from the team's knowledge duties being divided. While expertise variety is a feature of the original team composition, specialisation occurs when team members collaborate and relates to task-specific knowledge obligations. Expertise diversity is different from the knowledge specialisation components of TMS structures in that it represents the breadth of each team member's abilities, knowledge, and training before their collaboration (Cronin and Weingart 2007).

(2) Coordination describes the efficiency of the team in terms of knowledge processing while working together to enhance the coordination of information within teams (Ali et al. 2019). Moreover, coordination is a team process that entails the coordination, behaviour patterns, and skills among team members in order to achieve shared objectives (Rico et al. 2008). Zhong et al. (2012) confirmed that improved coordination and collaboration would increase task performance.

(3) Credibility is the way in which individual team members perceive the reliability of the knowledge held by the other members of the team (Kotlarsky et al. 2015; Liang et al. 1995). As Lewis asserts, these three variables "reflect transactive memory itself, as well as the cooperative processes illustrative of transactive memory use" (Lewis 2003; Wang et al. 2018). Davison et al. (2013) argue that TMS facilitates SKS, leading to improved team creative performance via team creative efficacy. Our premise is that organisations should facilitate and engender SKS by removing the challenges that prevent SKS, i.e., "specialisation, credibility and coordination" (Kotlarsky et al. 2015). The aim is to make security knowledge accessible to all of those who need it and ultimately to improve security awareness across the organisation. Our first qualitative study delivered insights about which factors impact SKS, and we are able to align these factors to the core tenets of TMS theory.

2.4 Motivating sharing

Motivation refers to an innate need shared by all humans to seek novelty and challenges, expand, and exercise their skills, and explore and discover (Ryan and Deci 2000). Regarding the area's significance, there are several academic fields in which reward management may be theorised, for example, economics (Perkins and Jones 2020), password manager adoption (Alkaldi and Renaud 2019), and information security policy compliance (Alzahrani et al. 2018). This effect results from motivation's essential role in assisting in the understanding of employee performance and reward. Indeed, the basis is one of psychology's oldest ideas, and we depend on established theories to help us understand how it manifests in the workplace (Ambrose and Kulik 1999). Thus, examining a theory of human motivation seems to be an appropriate way to to encourage SKS.

The core of Self-Determination Theory (SDT) is that individuals may be motivated to perform certain behaviours both extrinsically and intrinsically. Deci, a social psychologist, and Ryan, a clinical psychologist, pioneered the creation of SDT, a theory of human motivation and development that elucidates the fundamental principles underpinning sustained motivation (Deci and Ryan 2010). According to DeCharms (1972) and Deci and Ryan (2010), intrinsic motivation works by motivating an individual through their own natural interest in activities that are new or challenging. With intrinsic motivation, there is no need for the individual to be rewarded for their behaviour (Deci and Ryan 2010; Arachchilage 2016). In fact, there is a natural desire to learn; people have an innate wish to master something, learn something new through interest, or to explore, and this is the driver to pursue mastery throughout life (Deci and Ryan 2010; Arachchilage 2016).

The core of SDT is that individuals may be motivated to perform certain behaviours (Wang and Hou 2015; Ryan and Deci 2000). In SDT, three key human needs must be met: autonomy, competence, and connectedness (Ryan and Deci 2002). Studies have shown that when these three core needs are satisfied, individuals are more likely to take part in and exhibit better performance on an activity (Roca and Gagné 2008; Alahmari et al. 2019).

(1) Autonomy refers to when individuals act in their own interests and ideals; the feeling of having choice over behaviour (Baard et al. 2004); and feeling like the initiator of one's own activities. There is a need for autonomy, which is a person's wish to organise their own actions (Ryan and Deci 2000). According to Deci et al. (1994), autonomy support is when a person in a position of power considers the viewpoint of others, recognises their emotions, and gives relevant information, reasoning, and opportunities for choice.

(2) Competence is the knowledge of how to engage effectively with one's surroundings and the conviction that one can affect significant outcomes (Baard et al. 2004), and the need for a sense of competence, which is when a person desires self-efficacy (Ryan and Deci 2000). According to Deci and Ryan, individuals with a desire to engage successfully with the environment feel competent in generating desired results, and in order to avoid undesirable occurrences, competence is needed (Ryan and Deci 2002).

The need for **(3) relatedness** encompasses creating a sense of mutual respect and dependence (Baard et al. 2004), and the need for relatedness, i.e., a person's wish for the support and feelings of connection with others around them (Rocha Flores et al. 2014). Deci and Ryan asserted that relatedness entails a feeling of belonging or a sense of connection to a particular social environment (Ryan and Deci 2002).

As a consequence, the study adopted the SDT as an intrinsic motivation to change human behaviour. To apply SDT to empirical research, the idea was to implement education games that use gamification elements while applying SDT dimensions to the gamification elements.

2.5 Summary

Previous research in social network and technical systems has indicated that various reward system indicators can have a significant positive effect on SKS (Gagné 2009; Wickramasinghe and Widyaratne 2012). Conversely, other studies have revealed the negative impacts of reward systems (Cabrera and Cabrera 2005). Such tactics focus on short-term motivation, yet SKS ought to be seen as a long-term solution to low levels of security awareness.

Our literature review revealed that cyber security investigations generally use a specific limited number of theories, such as the Theory of Planned Behaviour and Theory of Reasoned Action (Lebek et al. 2014). There have also been other approaches to improving security awareness. These have generally been based on individualistic models (considering an individual in isolation), but our proposal is to use a more collaborative model to improve security awareness (Bulgurcu et al. 2010; Safa et al. 2018; Safa and Von Solms 2016).

Individual-focused models have more to do with predicting factors leading to security-related behaviours than with factors that lead to security-related SKS within organisations. Recent studies show that conventional social engineering and cyber security training approaches often lack actual exposure for employees (Olusegun and Ithnin 2013; Aldawood and Skinner 2019). These techniques do not expose employees to real-world situations in the way that contemporary training methods do. Employees are educated about the assault via traditional methods, but they may fail to identify it when confronted with the actual attack. These conventional techniques alone are insufficient to foster a culture of security among employees (Olusegun and Ithnin 2013; Aldawood and Skinner 2019).

We thus consider using the lens offered by TMS in order to understand and encourage SKS. TMS has been used in other contexts to model SKS between employees (Lehner and Maier 2000). Moreover, researchers in information retrieval have adopted the individual experience directory of TMS to gain access to the data usage of IT-based expertise information (Yuan et al. 2007). Thus, this study selected the TMS to model the dissemination of security knowledge in organisations. Choi et al. (2010) argued that SKS activities have features that support specific communication and collaboration practices to facilitate team-related TMS. Yet TMS only describes existing SKS within organisations; our interest is also in encouraging such sharing. We thus propose incorporating the core tenets of SDT into our model as well, in order to enhance SKS. Furthermore, Tsohou et al. (2015) confirmed that there are limited studies examining security awareness at both levels (organisational and individual level) in terms of having effective cyber security awareness programmes . Moreover, it is claimed that organisations should implement suitable incentive schemes to foster employee cooperation and promote sharing (Choi et al. 2010). Several studies examined the impact of TMS on knowledge processes and discovered that a well-developed TMS enables effective information sharing, knowledge application, and informal SKS (Choi et al. 2010; Davison et al. 2013). According to Vance et al. (2012) prior work in an organisational setting has focused on employees' compliance with security procedures.

3 Application design & development

3.1 Design

To test our intervention, we needed to create an app to facilitate knowledge sharing, incorporating the relevant aspects of SDT to encourage sharing. To encourage engagement with the app, we harness an educational game, widely recognised as a powerful teaching tool with the potential to result in an "instructional revolution" (Cone et al. 2007; Arachchilage 2016; Cone et al. 2007). Security games (SGs) give employees the opportunity to enjoy learning and to collaborate, as the games comprise a form of intrinsic motivation (Alzahrani and Johnson 2019; Hart et al. 2020; Aladawy et al. 2018).

3.2 Implementation

The instrument was created with the goal of allowing learners to learn and share their knowledge on the basis of the SKS model, as seen in Fig. 1. (Alahmari et al. 2020) . As a result, the learner was given as much influence over and interaction with the learning process as possible by constant input on the information transfer process (Alahmari et al. 2019). Moreover, the structuring and presentation of the instrument around critical aspects of baseline security expertise enabled them to address the challenges and validate the security knowledge. The SKS model was used to build the instrument components in line with the cooperation model established in provides work. The instrument, named STOW SYS, reflected the primary objective of the study (Alahmari et al. 2019).

When developing the instrument, the study considered previous work in terms of how it tackled challenges and how the SKS model could be implemented to mitigate those challenges (Al Ahmari et al. 2018). Further, what security knowledge issues should the employees be informed of, and how should these topics be presented? To achieve these goals, we adapted e-learning scenarios to encourage reflection and discovery among employees that involve multiple-choice questions delivered through a virtual connection (Chen et al. 2014; Dixon et al. 2019). The

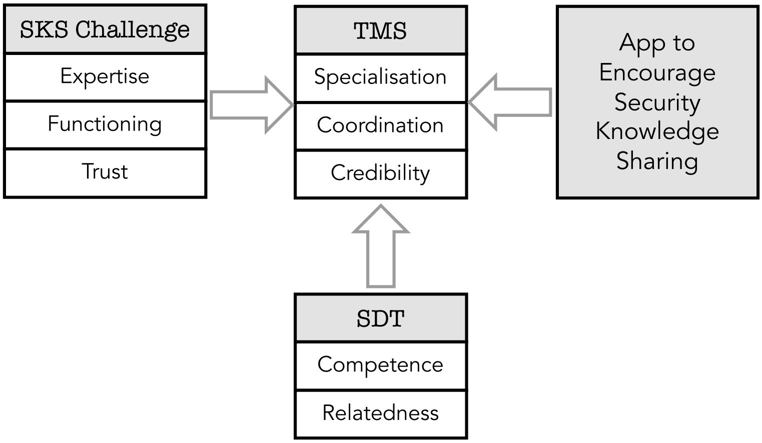


Fig. 1 The proposed research model

scenarios are based on the Global cyber security policy, as well as basic human mistakes (in the real world) (Tsohou et al. 2015).

Many instructional concept models are available for use in developing effective e-learning in the workplace. Each researcher employs a unique approach, which varies based on the current aim and participants (Garrison 2011). The ADDIE model is the most traditional model for instructional design, and all others are based on it. The model's name is an acronym of the five phases that are involved in the process: Analyse, Design, Development, Implementation, and Evaluation (Battou et al. 2016), as shown in Fig. 2.

3.3 The STOW game overview and rules

The STOW is a security game presented as a mobile app (e-learning scenarios to encourage reflection and discovery by employees), which includes multiple-choice questions. The scenarios are based on the Global Information Security Policy and commonly made human errors. STOW is designed to be played by employees working together under the guidance of the IT department, who will control the game. Several features were included in the game to assist employees in interacting with each other. For example, we gave them scenarios to think about, and the correct answers were ranked based on their expertise. The experts could share their knowledge by adding their personal motivation for choosing a particular answer via the "Check Your Answer" button. The "Add a New Answer" button could be used if they were not satisfied with the current 'best' answer. The STOW system allowed employees to look at the newly posted answer. They could evaluate it and post a response. Moreover, the STOW provided a "The Best Answer" button based on the employees' evaluations and by the IT department, who validated it. The flow of the game is as shown in Fig. 3.

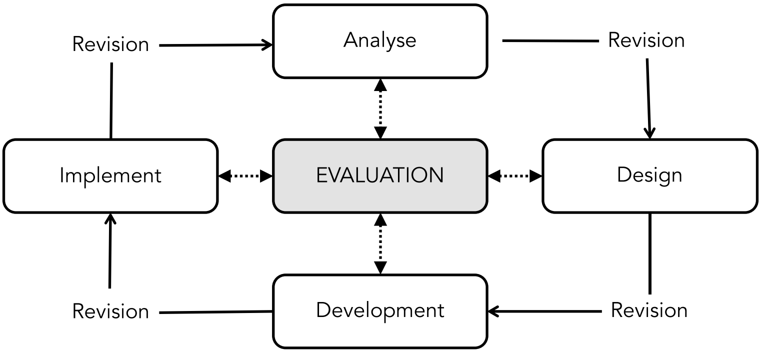


Fig. 2 The five processes of the ADDIE model

Appropriate competition dynamics will help persuade employees to become more engaged in their assignments which were developed using the SKS model, as shown in Fig. 11.

3.3.1 Interface design

This section details the STOW as it was applied to the employees during the experiment as seen in Fig. 4 .After registering for STOW, employees received a pre-assessment evaluation. Following this, they began the game and then wrote their nickname or email to match pre- and post-assessment with the STOW players.

Several features were included in the game to assist employees with interactions, including 'Check your Answer' and 'Evaluate'. Moreover, to authenticate the response, STOW allowed employees to evaluate it in the manner agreed upon by the SKS model. By pushing the same button, the best response is shown to the staff. Additionally, the information technology department developed a tag that verified the best response and awarded the best response badge (Figs. 5 and 6).

4 Study methodology

In order to determine the impact of the intervention, we need to collect sufficient data. Data generation, according to Oates (2005), is the "*method of producing analytical data or facts, which may be quantitative or qualitative*". During the exploratory case analysis, three data generation approaches were used, which are outlined in Table 1. Within the application, participants were allocated to either the control or experimental group, the latter interacting with the intervention.

The study was conducted to whether the effects of satisfaction of SDT needs mitigate SKS challenges between the intervention and control groups. After the study was approved by the FIMS ethics committee of the University of Glasgow, 300 employees at a large organization in Saudi Arabia were invited to participate in the study (in two different campuses and cities). One hundred

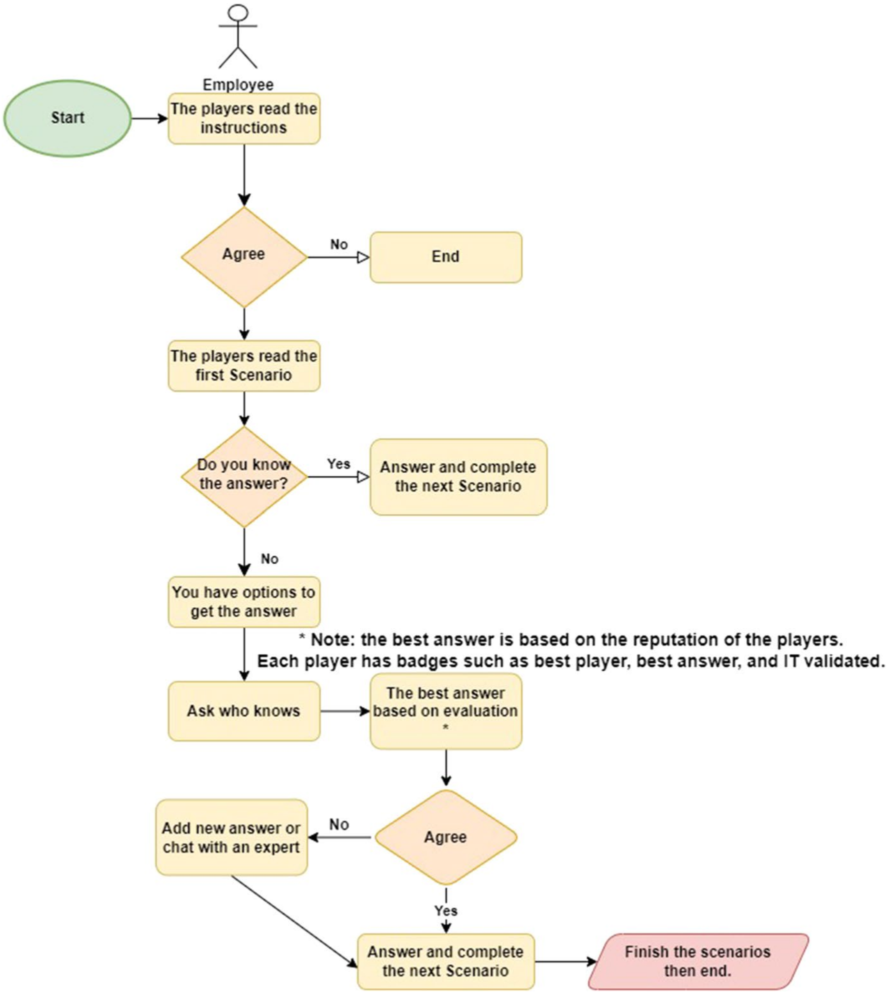

Employee
Start
The players read the instructions
Agree
No
End
The players read the first Scenario
Do you know the answer?
Yes
Answer and complete the next Scenario
No
You have options to get the answer
* Note: the best answer is based on the reputation of the players.
Each player has badges such as best player, best answer, and IT validated.
Ask who knows
The best answer based on evaluation *
Add new answer or chat with an expert
No
Agree
Yes
Answer and complete the next Scenario
Finish the scenarios then end.

Fig. 3 The flow of the game

and twenty-eight (43%)employees agreed to participate in the study and were allocated to one of two conditions: experimental (A) in (n = 64) and control (B) (n = 64). The study groups were not randomly allocated: our goal was to reduce the chance that the control group might learn about the intervention from the other two groups. As a result, participants were divided into groups based on their buildings' geographic isolation to ensure that we reduced cross contamination.

For pre- and post-testing, we adopted the scaleproposed by Kruger and Kearney (2006) to measure CSA, which can quantify the level of awareness as shown in Table 14.

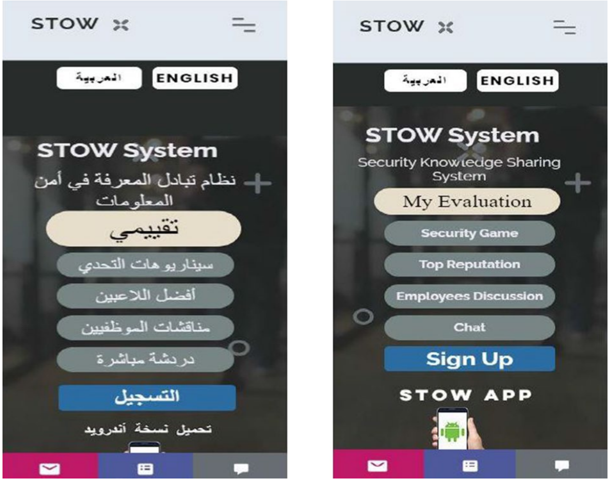
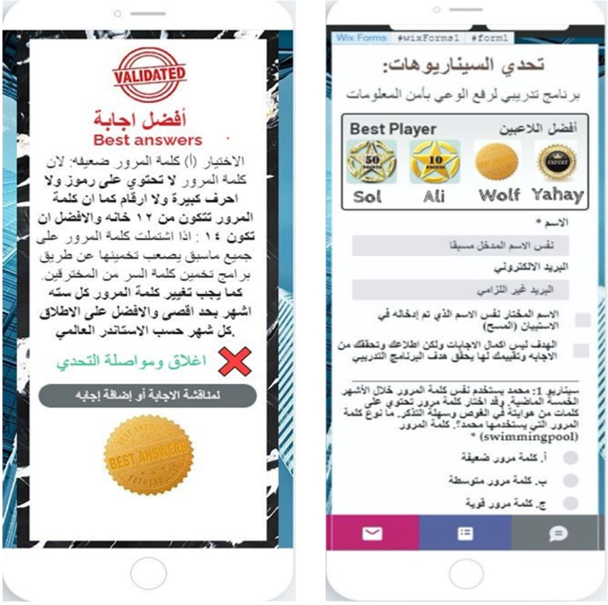


Fig. 4 Home screen



أفضل اجابة
Best answers

الاختيار (أ) كلمة المرور ضعيفه: لان كلمة المرور لا تحتوي على رموز ولا احرف كبيرة ولا ارقام كما ان كلمة المرور تتكون من ١٢ خانه والافضل ان تكون ١٤ : اذا اشتملت كلمة المرور على جميع ماسبق يصعب تخمينها عن طريق برامج تخمين كلمة السر من المخترقين. كما يجب تغيير كلمة المرور كل سته اشهر بحد اقصى والافضل على الاطلاق كل شهر حسب الاستاندر العالمي.

اغلاق ومواصلة التحدي

لمناقشة الاجابة أو إضافة إجابه

Wix Forms #wixForms1 #form1

تحدي السيناريوهات:

برنامج تدريبي لرفع الوعي بأمن المعلومات

Best Player أفضل اللاعبين

Sol Ali Wolf Yahay

الاسم *

نفس الاسم المدخل مسبقا

البريد الالكتروني

البريد غير اللزامي

□ الاسم المختار نفس الاسم الذي تم إدخاله في الاستبيان (المسح)

□ الهدف ليس اكمال الاجابات ولكن اطلاعك وتحققك من الاجابه وتقييمك لها يحقق هدف البرنامج التدريبي

سيناريو 1: محمد يستخدم نفس كلمة المرور خلال الأشهر الخمسة الماضية. وقد اختار كلمة مرور تحتوي على كلمات من هوايتة في الغوص وسهلة التذكر. ما نوع كلمة المرور التي يستخدمها محمد؟. كلمة المرور (swimmingpool) *

○ أ. كلمة مرور ضعيفة

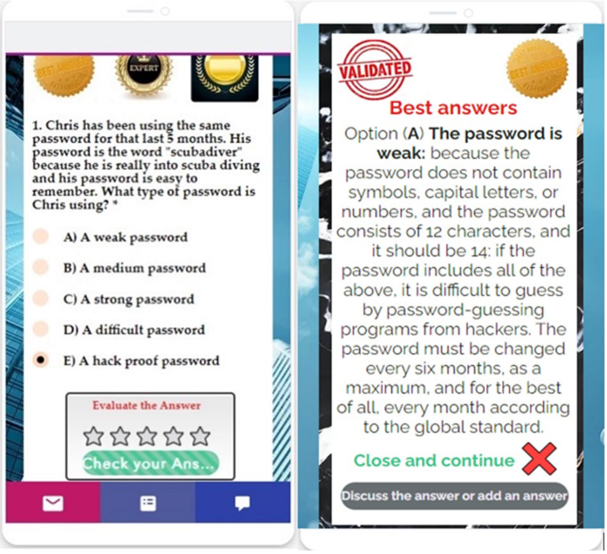
○ ب. كلمة مرور متوسطة

○ ج. كلمة مرور قوية

Fig. 5 Steps to validate the best answer (AR)

4.1 Study procedure

Step 1: Obtain consent after providing full information.
Step 2: Pre-test to assess baseline security knowledge.
Step 3: Depending on the individual's assigned condition:



1. Chris has been using the same password for that last 5 months. His password is the word "scubadiver" because he is really into scuba diving and his password is easy to remember. What type of password is Chris using? *

○ A) A weak password

○ B) A medium password

○ C) A strong password

○ D) A difficult password

● E) A hack proof password

Best answers

Option (A) **The password is weak:** because the password does not contain symbols, capital letters, or numbers, and the password consists of 12 characters, and it should be 14: if the password includes all of the above, it is difficult to guess by password-guessing programs from hackers. The password must be changed every six months, as a maximum, and for the best of all, every month according to the global standard.

Fig. 6 STOW evaluate and check your answer (translate Fig. 4 into English)

Table 1 Data generation methods

Generation method	Description
Survey (Questionnaire)	This included two sections: quantitative survey questions and qualitative open questions. Surveys are a method whereby a researcher poses a set of predetermined questions to an entire group, or sample, of people to assist in the planning of a more oriented, in-depth analysis that may involve time-consuming approaches such as in-depth interviews or field studies. In this scenario, a survey may assist a researcher in determining persons or locations from which to obtain additional details, and defining and measuring concepts.
Documents	The document that existed prior to the study was the report of the incidents from the IT Dept. The document explicitly created for the benefit of the research mission was the pre-assessment to measure the user awareness in this organization. In addition, documents were obtained from the app, which recorded players' interactions during the game, such as how long each player spent in the games and how many players completed all the scenarios. Also, players scores before and after playing the game, best STOW players during the game and STOW's panel control (including Players registered, Players who completed the game, Player Interaction and Answers evaluated)
Observation	Observing and paying attention to what individuals actually do over what they say they do Goodwin et al. (2006). Furthermore, the extra time spent observing provides information that may not have been obtained through the Survey and Documents approaches Moriarty (2011). The observations were recorded using the Qualitative Results section of Questions 19–24, which measured knowledge sharing both before and after STOW's deployment.

Group A – Experimental group: Employees were given a pre-questionnaire (Cyber Security Assessment). They were then given the game application which provided users with knowledge about how their security awareness can be improved (two-week intervention). Following this, participants were given a post-questionnaire (Cyber Security Assessment).

Group B – Control group Participants in this group were given a pre- and post-test (Cyber Security Assessment) with no intervention to maximise SKS, as seen in Fig. 7.

Step 4: Experimental group use the STOW app.
Step 5: Post-test to assess post intervention/post delay security knowledge.

4.2 Participants

hree hundred employees at a large organization in Saudi Arabia were invited to participate in the study. Participants were allocated to one of two study groups: experimental (A) (n = 64) and control (B) (n = 64). Study groups were not randomly allocated to ensure that we reduced cross-contamination. Participants who completed the steps are presented in Table 8, with participant statistics shown in Table 12.

4.3 Analysis

As indicated in the Data Collection Procedure section, the data for this stage came from a survey (questionnaire) which was measured the improvement in Security Awareness levels pre-and post-intervention, documents, and observations.

Quantitative data, taken from the pre- and post-intervention measurements were compared to see whether the intervention had made any changes to the employees' security knowledge. Quantitative data analysis was the first phase, which included information taken from a questionnaire which was collected pre- and post-assessment. First of all, normality tests were performed on the data prior to running the

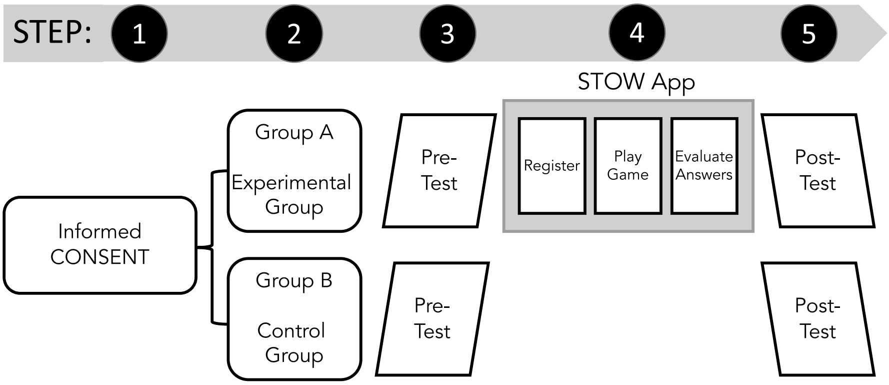


Fig. 7 Assessment and game flow

Table 2 Tests of normality

	Kolmogorov Smirnov			Shapiro Wilk		
	Statistic	Df	*P*-value	Statistic	Df	*P*-value
Intervention	0.152	39	0.023	0.930	39	0.017
Control	.081	40	0.200	0.976	40	0.552*

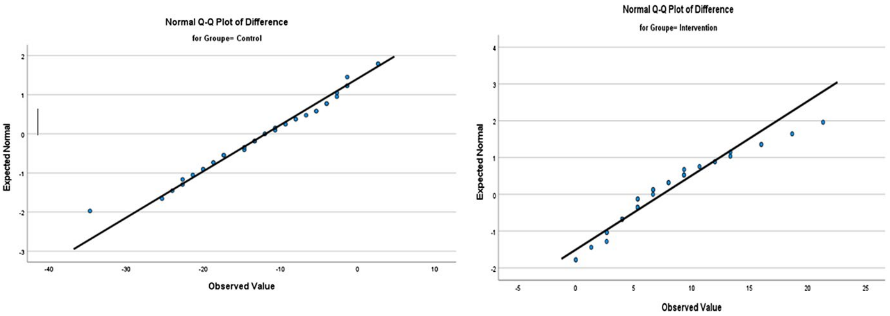


Fig. 8 Visual inspection of normal Q-Q plots of control group

analysis. To fulfil normality requirements, the research tested outliers in the intervention and control groups (Tabachnick et al. 2007). Engagement scores were normally distributed for the control and intervention groups, as seen in Table 2. The control group was assessed using Shapiro-Wilk's test (p= 0.552< .05) as shown in Table 2. This group was also assessed by visual inspection of normal Q-Q plots, as shown in Fig. 8. Thus, as the p-value is larger than 0.05, we assume a normal distribution.

The intervention group was as assessed by Shapiro-Wilk's test (p= 0.017 < .05) as shown in Table 2. Additionally, the participants were assessed by visual inspection of normal Q-Q plots, as shown in Fig. 8. Therefore, if the p-value is smaller than 0.05, we do not assume a normal distribution, as seen in Table 2.

The control group was dispersed normally, whereas the intervention group was not. Thus, non-parametric tests were used in the statistical analysis (Diggle et al. 2000; Luengo et al. 2009).

The Wilcoxon signed-rank test was used within groups to determine the median difference between pre and post-intervention (Gibbons and Chakraborti 2020). A between-group design was used in the Mann-Whitney U test to determine differences between the two groups on a continuous or ordinal dependent variable (Dinneen and Blakesley 1973).

The analysis analysed the qualitative data from three experimental steps:

Step 2: *Pre-assessment test:*The pre-assessment test score was used to determine the players' cyber security awareness before the game, as well as to measure SKS during work before STOW.

Step 3: *During the game:* we followed the requirements of the factors which we have addressed in the SKS model in the document. The document included the employees' scores before, after, and during the game. Also included are interactions during the game, such as contributions to the knowledge repository, evaluation of the players' answers, and lower players before and after the game.

Step 4: *Post-assessment test:* Following the game, the post-assessment test score was utilised to establish the players' level of cyber security awareness, as well as to determine whether the STOW improved knowledge exchange during the workday after use.

5 Results

5.1 Scenario and questionnaire component validity

Validity was measured using a content validity expert panel consisting of two faculty members and six doctoral students experienced in quantitative analysis and quantitative research. The techniques established content validity for all scenarios (both formative and reflective) via a literature study (Gefen and Straub 2005). Our target in this experiment was to improve the delivery of training in cyber security awareness. To put this theory to the test, scenarios and questionnaires focused on password management, email usage, and general questions about incidents that occurred during the workday. For several reasons, both the recommendations in the Literature Review and the Data Breach Investigations Report confirmed that the most common causes of security breaches in many organisations were password management and email use (Ahmed et al. 2019; Hadlington 2021). Due to the short duration of the experiment, it was not possible to cover all aspects of cyber security awareness. Additionally, concentrating on specific elements aids in testing the research hypothesis and obtaining an answer.

After we implemented and empirically tested the application, the research question could be addressed. The results are divided into two sections: quantitative and qualitative.

5.2 Quantitative results

Step 3A: Experimental Group A: To determine whether the intervention increased employees' level of cyber security awareness, a Wilcoxon signed-rank test revealed a statistically significant increase in employees' security knowledge for the intervention group participants: $z = -5.35$, $p = 0.00$, with a large effect size ($r = 0.72$) as seen in the descriptive statistics (Table 3) and Wilcoxon signed-rank test (Table 4). Participants' pre-test and post-test scores are presented in Fig. 9.

Step 3B: Control Group B: There was no significant increase in the employees' level of cyber security awareness: $z = -5.31$, $p = 0.00$, with a large effect size ($r = 0.71$), as seen the descriptive statistics (Table 5) and Wilcoxon signed-rank test (Table 6). Participants' pre-test and post-test scores are presented in Fig. 10.

Table 3 Descriptive statistics: group A

Group A	N	Mean	Std. deviation	Minimum	Maximum
Pre-test	39	78.57	8.1	48	90.7
Post-test	39	86.02	6.75	64	96

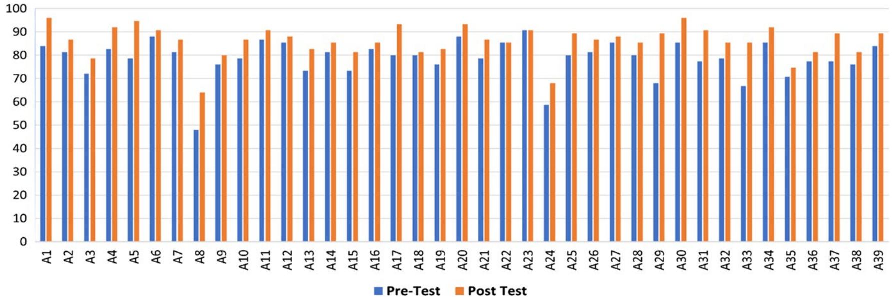


Fig. 9 Intervention group A

Table 4 Wilcoxon signed ranks test: group A

	Ranks			value		
	Negative ranks	Positive ranks	Ties	Total	Z-value	*P*-value
Pre-test – Post-test	0	37	2	39	−5.35	0.00

Table 5 Descriptive statistics: group B

Group A	N	Mean	Std. deviation	Minimum	Maximum
Pre-test	40	79.1	8.2	53.3	94.6
Post-test	40	67.2	9.6	41.3	93.3

Table 6 Wilcoxon signed ranks test: group B

	Ranks			value		
	Negative ranks	Positive ranks	Ties	Total	Z-value	*P*-value
Pre-test – Post-test	38	2	0	40	−5.35	0.00

Comparison Between and Within Groups: There were no statistically significant differences in pre-test scores for security knowledge. The mean rank was 39.76 in Group A, while Group B was 40.24, illustrating no significant difference between control and intervention.

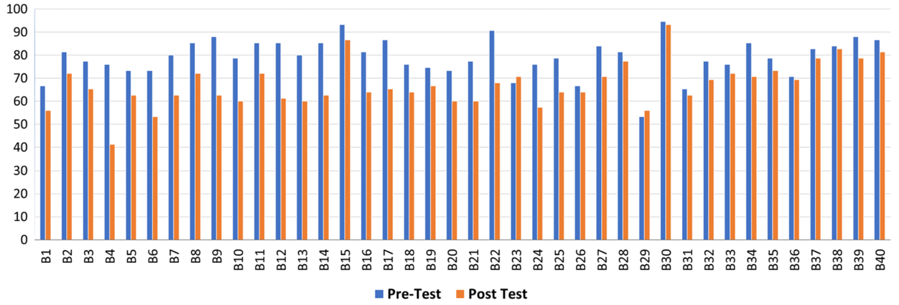


Fig. 10 Control group B

Table 7 Mann-Whitney test - ranks

Test	Group	N	Mean rank	Sum of ranks
Pre-test	Intervention A	39	39.76	1550.5
	Control B	40	40.24	1609.5
Post test	Intervention A	39	57.23	2232
	Control B	40	23.2	928

The intervention group significantly improved their knowledge (mean rank = 57.23) after the intervention. The control group demonstrated no significant differences between pre-test and post-test scores in security knowledge (mean rank = 23.2), as seen in Table 7. Unexpectedly, the control group result in the post-test was lower than the pre-test, most likely due to the fact that they did not know the answers and therefore did not spend much time answering the questions. The results were z = -6.59, p = 0.00, with a large effect size (r = 0.56). The decrease in group B's scores was caused the participants disengaging and not caring about their scores the second time around. We noted that the average time taken to complete the pre-questionnaire was 10–12 minutes, whereas the post-questionnaire took 4–6 minutes on average. The pre- and post-scores were equal for only two players (B29 and B23). To find a scientific explanation, we looked at the data and the time spent taking the test. It became clear that B23 spent ten minutes completing the pre test, while spending 7 minutes on the post test. B29 spent 8 minutes doing the pre test, doing the post test in 10 minutes. Hence, these players spent the same amount of time doing the test. One of the biggest acknowledged problems with cyber security training is waning engagement and growing indifference. STOW improved engagement – and the control group's disengagement confirms this tendence as well as STOW's ability to counteract this tendency. The mean for both tests can be seen in Fig. 11.

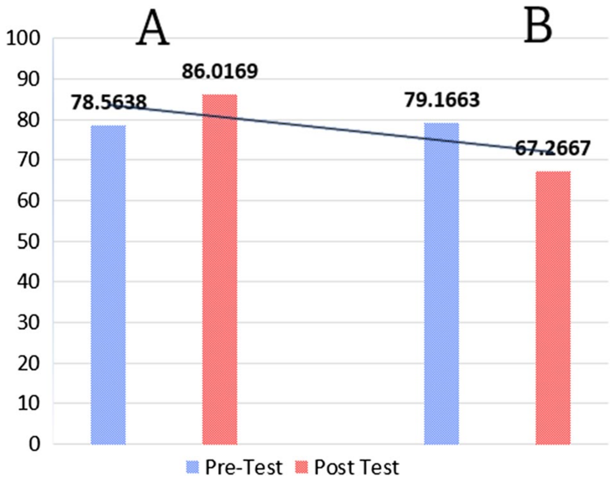


Fig. 11 Mean of the average score A and B

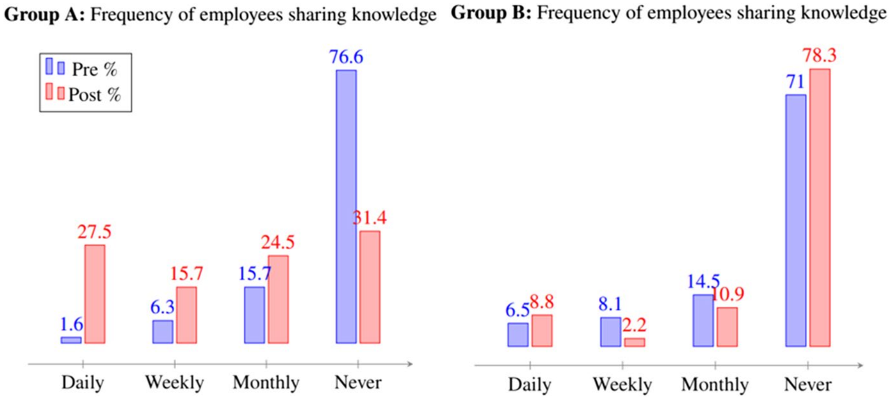


Fig. 12 Frequency of employees sharing knowledge

5.3 Qualitative results

Step 2: pre-assessment test: Prior to the game, we evaluated each player's level of cyber security knowledge. As shown in Fig. 13, the players' awareness levels were a good 21%, an average 16%, and a poor 3%. We also counted how many times employees shared their information before using the STOW system. As shown in Fig. 12, the employees were 2% daily, 6% weekly, 16% monthly, and 76% never.

Step 3A: during the game: Many players were registered on the STOW SYS as the record was confirmed from the file that tracked the players during the game. Forty players completed the steps of the games until they have completed all rounds of the games. One of the main goals of the STOW was to encourage employees to interact with one another during the game. Consequently, 39 out of 40 employees

Table 8 STOW's panel control

Players registered	Players completed game	Player interaction	Answer evaluated
52	40	39	372

Table 9 Best STOW players during the game

Best player	Assessment test	Measurement	Reward
A17	93.33%	Expert	Expert User, 3 Best Answers and Second-best player
A1	96%	Expert	Expert User, 1 Best Answer and First best player
A31	90.66%	Expert	Expert User, 1 Best Answer and Third best player

interacted with STOW and shared their knowledge with others. They evaluated 372 answers in order to evaluate the knowledge added by the employees and to obtain the correct answer, as seen in Table 8.

Best players based on contributions and evaluated answers: To track players and award them tags based on their expertise, the STOW offered them numerous tags, such as "Expert User", based on their performance on the pre-assessment test. Furthermore, employee evaluation was used to find the best replies. Finally, based on the tags, the best three players were identified and validated by the IT department, who supplied the best response (Table 9).

Lower players before and after the game: The experiment focused on lower-level players both before and after the game, with the findings reported by four employees who had improved their game knowledge. The first employee, B8, scored 48% in the pre-assessment, which was poor. After he used the STOW, completed all of the scenarios, and interacted with others to evaluate the best answers, he improved his score to 64% in the post-assessment, which is average. Employee B24 scored 58%, which was also low, but he improved to 68% after following all of the game instructions. The third user scored 66%, which is considered poor after scoring 85% in the first one. This user completed all of the scenarios but did not select the best answer because experts had recommended some of them. During the game, he also interacted with many other players. The last user, B29, scored 68% in the pre-assessment. After the interaction with the STOW, he completed all of the scenarios, but he also did not select the best answer because experts had recommended some of them. He also interacted with many other players during the game, and he improved to 85%, as shown in Table 10.

Step 5: post-assessment test: After the game, each player's level of cyber security knowledge was evaluated. As shown in Fig. 13, players' awareness levels were good at 90% rather than 54%, an average 10% instead of 41%, and a poor 0% instead of 5%. Additionally, there was an increase in the frequency with which employees shared knowledge following the implementation of STOW. Following the game, we found that employees increased their daily sharing by 28% rather than 2%, their weekly sharing by 15% rather than 6%, their monthly sharing by

Table 10 Lower scoring players before and after the game

Lower player	Before (%)	During	After (%)
A8	48	All scenarios completed and best answers evaluated	64
A24	58	All scenarios completed and best answers evaluated	68
A33	66	All scenarios completed but best answer not chosen as experts recommended some answers. Interacted with other players during the game	85
A29	68	All scenarios completed, best answers evaluated, and user interacted with other players during the game	89

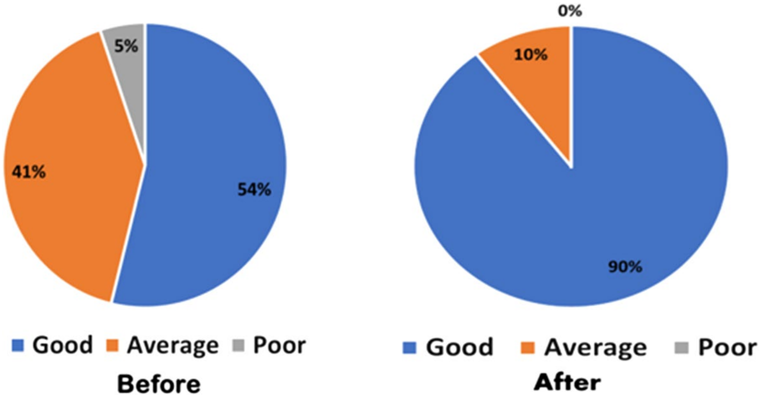


Fig. 13 Group A: player awareness levels

35% rather than 16%, and never sharing reduced to 31% from 76%. In contrast, as seen in Fig. 12, the control group did not improve.

6 Returning to the research questions

6.1 Contribution

The main experimental contribution of our study lies in extending TMS and SDT theory beyond the delivery of CSA training (Hamari et al. 2014), which tends to create an 'objectivist' view of the collaborative model (Safa et al. 2017).

RQ1: Can organisational security knowledge sharing (SKS) be modelled using *Transactive Memory System* (TMS) Theory?

Organisational shared knowledge was modeled using TMS during this investigation. The success of the intervention, especially in terms of increased SKS, suggests that this theory was indeed appropriate given that the SDT need satifaction was specifically targeted to enhance TMS constituents.

RQ2: Can individual SKS be encouraged by satisfying employees' self-determination needs?

The findings from the experiment indicate that the experimental group, which met SDT needs, developed a superior knowledge of assessing and responding to security incidents, as compared to the control group. Their CSA improved (See Fig. 11), and their SKS increased (See Fig. 12).

6.2 In summary

This study extends the knowledge on how to deliver security training by exploring the positive effects of including autonomy as intrinsic motivation and relatedness into training (STOW). Both encouraged the employees to complete the training without any external influence, which led to enhancing the employees' security knowledge.

Along with obtaining additional data, new findings explored the positive relationship between autonomy as intrinsic motivation and relatedness, which has not been investigated before

7 Reflection

This research was carried out to determine whether SKS could be increased if we used SDT need satisfaction to enhance the three constituent parts of TMS. Some researchers have speculated that the connection between motivation and SKS at work is an important issue, but the data on the topic are contradictory (Heilmann et al. 2013; Sáiz-Pardo et al. 2021). According to Choi et al. (2010), no empirical research has explicitly examined the impact of information technology in the enhancement of TMS.

We conducted an empirical investigation where half of participants received an intervention to satisfy SDT needs, with the transitive impact on TMS, while the control group did not. During the experiment, we consulted three sources which, together with supporting quotations from participants, make up the application's observations. The three sources were: (1) interaction and facilitating learning, (2) self-efficacy and encouraging others, and (3) the impact of enjoyment on learning (Alahmari et al. 2020).

(1) Interaction and Facilitating Learning: Interaction and facilitating learning are essential factors required to develop an understanding of interaction among employees and understanding what needs must be met in the system (Alahmari et al. 2020, 2019). The study included interaction within the app to satisfy the relatedness of the SKS model (Alahmari et al. 2019). As mentioned in the literature review, relatedness is the need for connection, i.e., a person's wish for support and feelings of connection with others around them (Roca and Gagné 2008). This is a type of intrinsic motivation which encourages humans to change their behaviour by being self-motivated (Roca and Gagné 2008). It connects employees via the app. Furthermore, the study satisfies the facilitated coordination requirements in our model, which was included in the app. As previously stated in the review of the literature, coordination describes the efficiency of the team in terms of knowledge processing while working together (Kotlarsky et al. 2015; Lewis and Herndon 2011).

The majority of the previous studies investigated a specific strategy for increasing employees' security knowledge based on an individual theory (Alahmari et al. 2020; Sailer et al. 2017; Safa et al. 2018; Safa and Von Solms 2016). In particular, the individual approach considers a person in isolation (Alahmari et al. 2019). However, according to our findings, coordination and relatedness can make a difference in changing employees' attention and interaction during training. These results match those observed in earlier studies using the SKS model that established a relationship between those factors (Alahmari et al. 2019, 2020). Empirical research has also confirmed such a link (Alahmari et al. 2019). with participants noting that knowledge repositories help to resolve recurring problems and enable employees to obtain solutions to problems from sources other than IT staff. This conveys the significance of those factors in managing knowledge and connecting employees via the app, especially when working from home during the COVID-19 pandemic. Additionally, the app's recording revealed the actions that occurred during the game, as seen in Table 8, in which the employees interacted with one another in order to answer all the scenarios. This finding is consistent with (Tortorella et al. 2021)), whose results demonstrate the critical nature of organisational learning practices via TMS and individual behaviour when individuals are not in their usual work environment – for instance, during a pandemic.

(2) Self-Efficacy and Encouraging Others: Self-efficacy is an important factor in instilling trust in employees as well as validating their knowledge during SKS (Hsu et al. 2007). Credibility, specialisation at the organisational level, and individual competence were the elements adopted to achieve the self-efficacy factor in our app. As stated in the existing literature, Credibility is the way in which individual team members perceive the reliability of the knowledge held by the other members of the team. Specialisation is the term used to describe the degree of differentiation of the knowledge held by team members (Kotlarsky et al. 2015; Lewis and Herndon 2011). Moreover, competence is the need for a sense of competence, which is when a person desires self-efficacy, which shows the ability of the person to do something. Competence is one of the intrinsic motivations that can cause changes in the behaviour of humans.

To date, only a few studies on the effect of TMS on motivation have been conducted (Alahmari et al. 2020; David et al. 2020; Sáiz-Pardo et al. 2021). The SKS model adopted competence as an intrinsic motivation in order to demonstrate the ability of employees through the elements of our intervention (Ryan and Deci 2000). This study produced results which corroborate the findings of a great deal of the previous work on competence related to an individual's sense of self-efficacy. When feelings of competence are experienced during a particular action as a result of evaluation and feedback, intrinsic motivation increases (Ryan and Deci 2000; Dixon et al. 2019). Positive performance feedback has been demonstrated to increase intrinsic motivation in previous research. Furthermore, recent evidence confirms that user feedback and evaluation can positively influence behavioural intentions to engage in secure behaviours (Dixon et al. 2019; Zhang et al. 2019). Moreover, the result of reinforcing a person's competence in terms of computer-based activities was a rise in their confidence in their aptitude in this area (Menard et al. 2017). Credibility and specialisation define the extent to which team members trust that the relevant task expertise of another team member is correct and accurate (Lewis 2003).

The current study's findings support our theoretical model, which was implemented in the STOW (Alahmari et al. 2020). The STOW created a feature that converted the challenge scenarios' elements into points and badges. Additionally, a leader board was created, which was crucial in building confidence in employees regarding their ability to choose the correct answer during the game (Dixon et al. 2019; Ryan and Deci 2000). Likewise, the best answer tag was the means used to evaluate employees during the game (Dixon et al. 2019; Zhang et al. 2019). Our findings report that employees' confidence improves when they have a sense of self-efficacy. As a result, we strive to maximise SKS within our organisations. The majority of participants expressed confidence in their ability to find the correct answer based on STOW. Comments from the participants supported this, mentioning how well the app facilitated communication among employees, and that the validity of the data was verifiable through the badges given to experts, further cementing their trust in the credibility of the information available. Moreover, employees appreciated the way in which the app enabled the exchange and preservation of knowledge, giving the opportunity for collaborative training and knowledge sharing.

(3) The Impact of Enjoyment on Learning: The impact of intrinsic motivation through autonomy was significant. Autonomy is defined as a person's desire to self-organise his or her own actions in order to as if they have control over what they do. The fact that STOW was a game provided an intrinsic motivation (Alzahrani et al. 2018) by giving players complete control over their actions. Because of their enjoyment of the game, the majority completed their tasks, as shown in Table 8. Most previous studies have overlooked intrinsic motivational elements, which refer to doing something purely for the sake of intrinsic interest or enjoyment (Alzahrani and Johnson 2019; Son 2011). Moreover, some participants shared their experiences with the STOW, commenting that not only was it fun and facilitated communication, but also did not take them too long to complete the tasks.

Finally, as Alkaldi and Renaud Alkaldi and Renaud (2019) confirmed, enjoyment plays a vital role in achieving behavioural change. Moreover, a satisfactory SDT is effective at encouraging such compliance in organisations Alzahrani and Johnson (2019). Our study confirmed the positive impact of perceived autonomy, such as changing security training to gamification that includes features mentioned in the previous sections (Alahmari et al. 2020). According to Rigby and Ryan (2011), if a game is designed using meaningful stories, avatars, and teammates, a shared goal is introduced, and this leads to perceptions of relevance. Feelings of social relatedness were induced (Sailer et al. 2017). An important aspect of gamification is that players are provided with specific feedback that serves to induce feelings of competence in their performance. There is thus an expectation that leader boards, badges, and performance charts will induce these feelings of competence in our users (Sailer et al. 2017). Consequently, these features enable employees to develop social bonds, allowing them to cooperate. Designing appropriate competition dynamics will help persuade employees to be more engaged in cyber security (Sailer et al. 2017; Rigby and Ryan 2011).

Summary: STOW significantly improved employee security knowledge (as measured by a post-assessment test) in comparison to who did not receive the training. In addition, the intervention participants demonstrated attitude changes related to both positive and negative outcomes. Participants who completed the STOW game demonstrated significantly higher self-efficacy perceptions than those who did not receive the training. Finally, the results revealed that employees who received STOW training perceived and interacted with the game in a more positive light than employees who did not interact with the game.

The intervention group worked through a number of scenarios and debriefings that included a range of different types of learning methods, including active learning, cooperative learning, and expert evaluation. Deliberate practice and feedback have been found to enhance trust and validate knowledge (Zhang et al. 2019).

Overall, our study revealed that the intervention group participants, who received training, had superior knowledge in assessing and responding to security incidents compared to the control group. Moreover, due to the lack of studies confirming the association, the study eliminated autonomy and relatedness. However, a limited study conducted in a security context confirmed that autonomy positively affects human behaviour changes. According to recently published policy compliance research, satisfying SDT successfully encourages such compliance in organisations (Alzahrani and Johnson 2019; Alzahrani et al. 2018). Alkaldi and Renaud (2019) confirmed the critical effect of applying autonomy to security tool adoption decisions. The new findings explored the positive relationship between autonomy as intrinsic motivation and relatedness, which previous research did not investigate.

7.1 Research limitations

We did not randomly assign participants to experimental conditions, which is contrary to usual practice in this kind of experiment. We did this to ensure that we reduced the possibility of cross-contamination, but we have to acknowledge the possibility that the two differently located groups had different security cultures. Given that they both worked for the same organisation this is unlikely, but not impossible.

The number of participants is relatively small, although the numbers were large enough to support statistical analysis. It is always difficult to get participants when there is a requirement to install an app and to engage with the app for more than a few minutes. If funding can be secured to pay participants in subsequent studies, it is possible that more participants could be recruited, and the study re-run to confirm our findings.

A pre and post-survey instrument were developed to measure the impact of information security knowledge sharing. The pre and post-surveys are identical and include a total of 24 questions. The post-questionnaire was in random order after two weeks. However, the main point of the randomising was not to change the meaning of the questionnaire but to reduce the chance of someone remembering the pre-questionnaire. The results of group B (in the case of the control group) should return the same results, but we noted that the decrease caused the participants not to care about their score the second time around. After noting that the average time taken to complete the pre-questionnaire was 10–12 minutes, we noticed that the post-questionnaire took 4–6 minutes."

7.2 Research implications

This study was concerned with the fundamentals of TMS for different teams, where team members benefit from the successful utilisation and coordination of various expertise. The findings have provided insights into why expertise variety may stimulate TMS (Cronin and Weingart 2007). Thus, the findings shed light on why expertise variety has the potential to both boost and harm TMS. The SKS model has deduced this issue using a combination of motivation and collaboration theory. For instance, employees can find expertise (specialisation) through feedback and evaluation via the STOW system (competence). Future work may consider these findings to adapt e-learning among employees or students.

Recent studies show that conventional social engineering and cyber security training approaches often lack actual exposure for employees (Aldawood and Skinner 2019; Olusegun and Ithnin 2013). These techniques do not expose employees to real-world situations in the way that contemporary training methods do. Employees are educated about the assault via traditional methods, but they may fail to identify it when confronted with the actual attack. These conventional techniques alone are insufficient to foster a culture of security among employees (Aldawood and Skinner 2019; Olusegun and Ithnin 2013).

Additionally, expanding the cycle of the SKS model to incorporate additional iterations of awareness sessions and a greater number of assessment tests may be a future extension of this study. Due to the fact that awareness gains in SKS are time and location dependent, extended studies will examine the importance of the two dynamic factors (TMS and SDT) in the SKS model, which may be expanded upon in future studies.

7.3 Practical implications

IT practitioners must change their organisational culture to foster an attitude toward cyber security rules that views them as a necessary evil rather than a hindrance to workers performing their jobs. The training plan should be changed to consider individual and organisational factors to deliver practical training to the employees.

Cyber security has become an organised process as more and more companies recognise its importance. One of the most difficult aspects of managing an information system is implementing appropriate security measures. Various studies have shown the critical importance of protecting valuable information, and one critical element that must be addressed is cyber security awareness. CSA is about ensuring that all employees of the cyber security function understand their role and are aware of the rules and regulations they must follow.

The majority of CSA training is developed using the traditional method, which does not accurately reflect reality in organisations. The evidence of this is that the employees attended training, but they could not defend themselves when they encountered a security breach. This study utilised a unique technique based on real-world scenarios to educate employees about security risks. Any subsequent study must take these findings into account and construct the CSA based on real-world settings. IT practitioners must consider the findings to create interactive training capable of changing employee behaviour.

Organisations would benefit if IT practitioners and security experts would change their organisational culture to foster security knowledge sharing. At the moment, there is often a regrettable view of information security rules being a necessary evil and a hindrance to workers performing their jobs. The training plan should be changed to consider individual and organisational factors to deliver practical training to the employees. In this context, the study provides practical implications for system designers and developers who seek to improve cyber security within organisations via a collaborative model. Moreover, the study encourages employees to engage in prosocial behaviour through educational security games. The interaction impact on procedural and conceptual knowledge may be achoeved via the deployment of educational games, web-based training materials, contextual training, and embedded training to enhance users' capacity to detect and avoid phishing assaults and other security incidents.

8 Conclusion

This study proposed a SKS model that aims to improve how employees are made aware of cyber security risks. The empirical study shows that it can help enhance security knowledge and deliver training by adopting the cooperation model. Based on the study findings, ignoring the difficulties inherent in social engineering training and CSA programmes may end in victimisation. Security training that is provided effectively is considered the first line of protection against security attacks. The IT department must consider the effective delivery of CSA. If an employee is not updated on the current security risk fraud methods, attackers may obtain access to the organisation's information systems via an open door. The STOW's objective is to offer an interactive and user-friendly approach to enhance employees' cybersecurity knowledge. The system utilises several strategies to ensure that employees acquire necessary expertise at the appropriate time: a set of interactive scenarios that need the adoption of cybersecurity threats to address one or more actual security concerns. This strategy ensures that employees are kept up to date with potential risks and damage due to security incidents.

Appendix

See Tables 11, 12, 13, 14.

Table 11 Game design elements

Game dynamics	Related game elements	Description
Challenge scenarios	Points, and badges	Competence is an important component of intrinsic motivation and plays a key role in Credibility via Evaluation, as seen in Fig. 6
Leader board	Badges	Relatedness: Employees can trust co-workers based on the leader board, as seen in Fig. 5
Best answer	Reuse and Retrieve	Competence: Choosing the best answer based on employees' personal opinion, as seen in Fig. 5
Chat and ask who knows	Tracking improvement	Employees The plan of the study was changed after Coronavirus to be online – the data will help to analyse improvements
Badges	Badges	Competence: Employees can collect badges that visually show their achievements, as shown in left Fig. 5

Table 12 Participants' characteristics of the first experiment

Categories	Sub-categories control group A	# (n = 40)
Gender	Female	9
	Male	31
Age	20–30	4
	31–40	27
	41–50	6
	Over 51	3
Education	High school or below	5
	Bachelor degree	26
	Master degree	6
	PhD	3
Categories	**Sub-categories Intervention Group B**	**# (n = 39)**
Gender	Female	12
	Male	27
Age	20-30	3
	31–40	27
	41–50	5
	Over 51	3
Education	High school or below	6
	Bachelor degree	19
	Master degree	7
	PhD	7

Table 13 Summary of cybersecurity games :approaches, their key findings and underlying theories

Study	Approaches	Key findings	Theory base
Aladawy et al. (2018)	Empirical research	The researchers developed a serious game that teaches individuals how to defend themselves against social engineering by using social psychology's defensive mechanisms. Empirical assessment of the game indicates that it is capable of entertainingly raising awareness of social engineering	Social Psychology
Hart et al. (2020)	Empirical research	This article presents Riskio, a tabletop game aimed at increasing cybersecurity awareness among non-technical employees in organisations. Riskio creates an active learning environment in which users gain information about cybersecurity assaults and defences by taking on both attacker and defender of fictional organisation's vital assets. Evaluation revealed that Riskio might help raise players' awareness of cyber security concepts.	The design of the game is based on the principles of constructivism learning theory (Riskio App)
Ghazvini and Shukur (2018)	Empirical research	The aim to improve CSA in the healthcare sector. The game covers various subjects, including phishing, online use, harmful programming, and password security. Employees found the game to be engaging and enjoyed playing it. The assessment indicates that employees' CSA levels rose significantly as a result of playing the game. Additionally, employees demonstrated a desire to engage in CSA training due to their enjoyment of the game	Serious games, based on learning theory (Info Secure App)

Table 13 (continued)

Study	Approaches	Key findings	Theory base
Gjertsen et al. (2017)	Empirical research	Investigated the possibility of using gamification mechanics to improve motivation and learning results in this setting via SDT. Based on interviews with security experts and a workshop with ordinary workers at two companies, the researchers created an interactive CSA prototype application. The findings showed that gamification has promise for application in SAT training, particularly in regions where existing CSA initiatives are ineffective. Additionally, the researchers highlighted the lack of high-quality studies on the actual impacts of gamification at the moment.	Self-Determination Theory
Tsohou et al. (2015)	Action research	According to Tsohou et al. (2015) the training and practices for cyber security awareness programs focus on the content and procedures of the programs, without considering how the employees interact with the program in order to make security-related right decisions	Theory of planned behaviour and Triandis model
Alotaibi et al. (2018)	Action research	The paper discusses the design of two mobile games being created to raise awareness about cybersecurity. Two critical elements of cybersecurity are included in the games created in this study: strong password generation and virus prevention. Both the Password Protector and Malware Guardian games are well-designed, with an emphasis on usability. The pre-and post-study survey analysis for both games revealed substantial increases in the participants' knowledge of password and malware awareness	Password Game Prototype

Table 13 (continued)

Study	Approaches	Key findings	Theory base
Safa et al. (2017)	Theoretical research model	Identified cyber security collaboration as a powerful, efficient approach to reducing the risks to cyber security. Moreover, the researchers confirmed that limited studies have been conducted collaboratively in the cyber security field within organisations	Theory of planned behaviour and Triandis model

Table 14 Awareness level measurement

Awareness	Measurement	Actions
Good	80–100	Satisfactory: badges as an expert user and can be group leader
Average	60–79	Minor– action potentially required
Poor	59 and less	Unsatisfactory: need improve

Acknowledgements The authors extend their appreciation to the Northern Border University, the Deputyship for Research & Innovation, Ministry of Education in Saudi Arabia for funding this research work through the Project No. IF_2020_NBU_303.

References

Abawajy J (2014) User preference of cyber security awareness delivery methods. Behav & Info Technol 33:237–248

Ahmed G, Ragsdell G, Olphert W (2014) Knowledge sharing and information security: a paradox? In: 15th european conference on knowledge management (ECKM 2014), Polytechnic Institute of Santarém Portugal. pp. 1083–1090

Ahmed M, Kambam HR, Liu Y, Uddin MN (2019) Impact of human factors in cloud data breach. In: International conference on intelligent and interactive systems and applications, Springer. pp. 568–577

Al Ahmari S, Renaud K, Omoronyia I (2018) A systematic review of information security knowledge-sharing research. In: Proceedings of the twelfth international symposium on human aspects of information security & assurance (HAISA 2018), p. 101

Aladawy D, Beckers K, Pape S (2018) Persuaded: fighting social engineering attacks with a serious game. In: International conference on trust and privacy in digital business, Springer. pp. 103–118

Alahmari S, Renaud K, Omoronyia I (2019) A model for describing and maximising security knowledge sharing to enhance security awareness. In: European, mediterranean and middle eastern conference on information systems, Springer. pp. 376–390

Alahmari S, Renaud K, Omoronyia I (2020) Implement a model for describing and maximising security knowledge sharing. In: 2020 15th international conference for internet technology and secured transactions (ICITST), IEEE. pp. 1–4

Aldawood H, Skinner G (2019) Reviewing cyber security social engineering training and awareness programs-pitfalls and ongoing issues. Fut Intern 11:73

Ali A, Wang H, Khan AN (2019) Mechanism to enhance team creative performance through social media: a transactive memory system approach. Comp Human Behav 91:115–126

Alkaldi N, Renaud K (2019) Encouraging password manager adoption by meeting adopter self-determination needs. In: Proceedings of the 52nd Hawai'i international conference on system sciences. January, Maui

Alotaibi F, Furnell S, Stengel I, Papadaki M (2018) Design and evaluation of mobile games for enhancing cyber security awareness. J Intern Technol Secur Trans 6:569–578

Alzahrani A, Johnson C (2019) Autonomy motivators, serious games and intention toward ISP compliance. Int J Seri Game 6:67–85

Alzahrani A, Johnson C, Altamimi S (2018) Information security policy compliance: investigating the role of intrinsic motivation towards policy compliance in the organisation. In: 2018 4th International conference on information management (ICIM), IEEE. pp. 125–132

Ambrose ML, Kulik CT (1999) Old friends, new faces: motivation research in the 1990s. J Manag 25:231–292

Arachchilage, NAG (2016) Serious games for cyber security education. arXiv preprint arXiv:1610.09511

Baard PP, Deci EL, Ryan RM (2004) Intrinsic need satisfaction: a motivational basis of performance and weil-being in two work settings. J Appl Soci Psychol 34:2045–2068

Bada M, Sasse AM, Nurse JR (2019) Cyber security awareness campaigns: why do they fail to change behaviour? arXiv preprint arXiv:1901.02672

Battou A, Baz O, Mammass D (2016) Learning design approaches for designing virtual learning environments. Commun Appl Electr 5:31–37

Bauer S, Bernroider EW (2017) From information security awareness to reasoned compliant action: analyzing information security policy compliance in a large banking organization. ACM SIGMIS Database: the DATABASE Adv Info Sys 48:44–68

Becerra-Fernandez I, Sabherwal R (2014) Knowledge management: systems and processes. Routledge

Bulgurcu B, Cavusoglu H, Benbasat I (2010) Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS Quart 34:523–548

Cabrera EF, Cabrera A (2005) Fostering knowledge sharing through people management practices. Int J Human Res Manag 16:720–735

Chen YH, Lin TP, Yen DC (2014) How to facilitate inter-organizational knowledge sharing: the impact of trust. Info Manag 51:568–578

Choi SY, Lee H, Yoo Y (2010) The impact of information technology and transactive memory systems on knowledge sharing, application, and team performance: a field study. MIS Quart 34:855–870

Cone BD, Irvine CE, Thompson MF, Nguyen TD (2007) A video game for cyber security training and awareness. Comput Secur 26:63–72

Cronin MA, Weingart LR (2007) Representational gaps, information processing, and conflict in functionally diverse teams. Acad Manag Rev 32:761–773

Dang D, Nkhoma M (2017) Effects of team collaboration on sharing information security advice: insights from network analysis. Info Resour Manag J (IRMJ) 30:1–15

Dang-Pham D, Pittayachawan S, Bruno V (2017) Why employees share information security advice? exploring the contributing factors and structural patterns of security advice sharing in the workplace. Comp Human Behav 67:196–206

D'Arcy J, Hovav A, Galletta D (2009) User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. Info Sys Res 20:79–98

David EM, Johnson LU, Meng CY, Lopez TN (2020) Stronger together: conditional indirect effect of servant leadership on transactive memory systems. J Leaders & Organiz Stud. https://doi.org/10.1177/1548051820969137

Davison RM, Ou CX, Martinsons MG (2013) Information technology to support informal knowledge sharing. Info Sys J 23:89–109

DeCharms R (1972) Personal causation training in the schools 1. J Appl Soci Psychol 2:95–113

Deci EL, Eghrari H, Patrick BC, Leone DR (1994) Facilitating internalization: the self-determination theory perspective. J Personal 62:119–142

Deci EL, Ryan RM (2010) Intrinsic motivation. The Corsini Encyclopedia of Psychology, 1–2

Diggle PJ, Mateu J, Clough HE (2000) A comparison between parametric and non-parametric approaches to the analysis of replicated spatial point patterns. Adv Appl Probabil 32:331–343

Dinneen L, Blakesley B (1973) Algorithm as 62: a generator for the sampling distribution of the mann-whitney u statistic. J Royal Stat Soci Series C (Appl Stat) 22:269–273

Dixon M, Gamagedara Arachchilage NA, Nicholson J (2019) Engaging users with educational games: The case of phishing. In: Extended abstracts of the 2019 CHI conference on human factors in computing systems, pp. 1–6

Dixon NM (2000) Common knowledge: how companies thrive by sharing what they know. Harvard Business School Press, Brighton

Feledi D, Fenz S (2012) Challenges of web-based information security knowledge sharing. In: 2012 seventh international conference on availability, reliability and security, IEEE. pp. 514–521

Feledi D, Fenz S, Lechner L (2013) Toward web-based information security knowledge sharing. Infor Secur Tech Report 17:199–209

Gagné M (2009) A model of knowledge-sharing motivation. Human Resource Management: published in Cooperation with the School of Business Administration, The University of Michigan and in alliance with the Society of Human Resources Management 48:571–589

Garrison DR (2011) E-learning in the 21st century: a framework for research and practice. Routledge, New York

Gcaza N, von Solms R (2017) Cybersecurity culture: An ill-defined problem. In: IFIP World conference on information security education, Springer. pp. 98–109

Gefen D, Straub D (2005) A practical guide to factorial validity using pls-graph: tutorial and annotated example. Commun Associat Info Sys 16:5

Ghazvini A, Shukur Z (2018) A Serious game for healthcare industry: information security awareness training program for hospital universiti kebangsaan Malaysia. Int J Adv Comp Sci Appl 9:236–245

Gibbons JD, Chakraborti S (2020) Nonparametric statistical inference. CRC Press, Cambridge

Gjertsen, E.G.B., Gjære EA, Bartnes M, Flores WR (2017) Gamification of information security awareness and training. In: ICISSP, pp. 59–70

Goodwin D, Mays N, Pope C (2006) Ethical issues: qualitative research in health care, 3rd edn. Wiley, Hoboken

Hadlington L (2021) The "human factor" in cybersecurity: Exploring the accidental insider. In: Research anthology on artificial intelligence applications in security. IGI Global, pp. 1960–1977

Haeussinger F, Kranz J (2013) Understanding the antecedents of information security awareness-an empirical study. In: Proceedings of the nineteenth americas conference on information systems, Chicago, Illinois

Hamari J, Koivisto J, Sarsa H (2014) Does gamification work? A literature review of empirical studies on gamification. In: 2014 47th Hawaii international conference on system sciences, pp. 3025–3034

Hart S, Margheri A, Paci F, Sassone V (2020) Riskio: a serious game for cyber security awareness and education. Comp Secur 95:101827

He Y, Johnson C (2017) Challenges of information security incident learning: an industrial case study in a chinese healthcare organization. Info Health Social Care 42:393–408

Heilmann SG, Bartczak SE, Hobbs SE, Leach SE (2013) Assessing influences on perceived training transfer: If I only knew then what I need to know now. J Bus Educat Leadership 4:34

Hsu MH, Ju TL, Yen CH, Chang CM (2007) Knowledge sharing behavior in virtual communities: the relationship between trust, self-efficacy and outcome expectations. Int J Human-Comp Stud 65:153–169

Jackson P, Klobas J (2008) The organization as a transactive memory system. In: Becoming Virtual. Springer, pp. 111–133

Junger M, Montoya L, Overink FJ (2017) Priming and warnings are not effective to prevent social engineering attacks. Comp Human Behav 66:75–87

Khando K, Gao S, Islam SM, Salman A (2021) Enhancing employees information security awareness in private and public organisations: a systematic literature review. Comp Secur. https://doi.org/10.1016/j.cose.2021.102267

Killmeyer J (2006) Information security architecture: an integrated approach to security in the organization. CRC Press, Cambridge

Kim S, Lee H (2006) The impact of organizational context and information technology on employee knowledge-sharing capabilities. Public Administr Rev 66:370–385

Kotlarsky J, van den Hooff B, Houtman L (2015) Are we on the same page? knowledge boundaries and transactive memory system development in cross-functional teams. Commun Res 42:319–344

Kruger HA, Kearney WD (2006) A prototype for assessing information security awareness. Comp Secur 25:289–296

Lebek B, Uffen J, Neumann M, Hohler B, Breitner HM (2014) Information security awareness and behavior: a theory-based literature review. Manag Res Rev 37:1049–1092

Lehner F, Maier RK (2000) How can organizational memory theories contribute to organizational memory systems? Info Sys Front 2:277–298

Lewis K (2003) Measuring transactive memory systems in the field: scale development and validation. J Appl Psychol 88:587–604

Lewis K, Herndon B (2011) Transactive memory systems: current issues and future research directions. Organiz Sci 22:1254–1265

Liang DW, Moreland R, Argote L (1995) Group versus individual training and group performance: the mediating role of transactive memory. Personal Soc Psychol Bull 21:384–393

Luengo J, García S, Herrera F (2009) A study on the use of statistical tests for experimentation with neural networks: Analysis of parametric test conditions and non-parametric tests. Expert Sys Appl 36:7798–7808

Mejias RJ (2012) An integrative model of information security awareness for assessing information systems security risk. In: 2012 45th Hawai'i international conference on system sciences, IEEE. pp. 3258–3267

Menard P, Bott GJ, Crossler RE (2017) User motivations in protecting information security: Protection motivation theory versus self-determination theory. J Manag Info Sys 34:1203–1230

Mermoud A, Keupp M, Huguenin K, Palmié, M., David DP (2018) Incentives for human agents to share security information: a model and an empirical test. In: 17th workshop on the economics of information security (WEIS), pp. 1–22

Moriarty J (2011) Qualitative methods overview. National Institute for Health Research School for Social Care, London

Oates BJ (2005) Resear Info Sys Comp. Sage, London

Olusegun OJ, Ithnin NB (2013) People are the answer to security: establishing a sustainable information security awareness training (ISAT) program in organization. arXiv preprint arXiv:1309.0188

Ortiz J, Chang SH, Chih WH, Wang CH (2017) The contradiction between self-protection and self-presentation on knowledge sharing behavior. Comp Human Behav 76:406–416

Perkins SJ, Jones S (2020) Reward management: alternatives, consequences and contexts. Kogan Page Publishers, London

Politis JD (2003) The connection between trust and knowledge management: what are its implications for team performance. J Knowl Manag 7:55–66

Puhakainen P, Siponen M (2010) Improving employees' compliance through information systems security training: an action research study. MIS Quart 34:757–778

Rahim NHA, Hamid S, Mat Kiah ML, Shamshirband S, Furnell S (2015) A systematic review of approaches to assessing cybersecurity awareness. Kybernetes 44:606–622

Rico R, Sánchez-Manzanares M, Gil F, Gibson C (2008) Team implicit coordination processes: a team knowledge-based approach. Acad Manag Rev 33:163–184

Rigby S, Ryan RM (2011) Glued to games: how video games draw us in and hold us spellbound: how video games draw us in and hold us spellbound. Greenwood Publishing Group, Santa Barbara

Roca JC, Gagné M (2008) Understanding e-learning continuance intention in the workplace: a self-determination theory perspective. Comp Human Behav 24:1585–1604

Rocha Flores W, Holm H, Svensson G, Ericsson G (2014) Using phishing experiments and scenario-based surveys to understand security behaviours in practice. Info Manag & Comp Secur 22:393–406

Ryan RM, Deci EL (2000) Self-determination theory and the facilitation of intrinsic motivation, social development and well-being. Am Psychol 55:68

Ryan RM, Deci EL (2002) Overview of self-determination theory: an organismic dialectical perspective. Handbk Self-Determ Res 2:3–33

Safa NS, Maple C, Watson T, Furnell S (2017) Information security collaboration formation in organisations. IET Info Secur 12:238–245

Safa NS, Maple C, Watson T, Von Solms R (2018) Motivation and opportunity based model to reduce information security insider threats in organisations. J Info Secur Appl 40:247–257

Safa NS, Von Solms R (2016) An information security knowledge sharing model in organizations. Comp Human Behav 57:442–451

Sailer M, Hense JU, Mayr SK, Mandl H (2017) How gamification motivates: an experimental study of the effects of specific game design elements on psychological need satisfaction. Comp Human Behav 69:371–380

Sáiz-Pardo M, Domínguez MCH, Molina LM (2021) Transactive memory systems mediation role in the relationship between motivation and internal knowledge transfers in a military environment. J Knowl Manag 25:2396–2419. https://doi.org/10.1108/JKM-10-2020-0777

Siponen MT (2000) A conceptual foundation for organizational information security awareness. Info Manag Comp Secur 8:31–41

Son JY (2011) Out of fear or desire? toward a better understanding of employees' motivation to follow is security policies. Info Manag 48:296–302

Tabachnick BG, Fidell LS, Ullman JB (2007) Using multivariate statistics, vol 5. Pearson, Boston, MA

Thomson ME, von Solms R (1998) Information security awareness: educating your users effectively. Info Manag Comp Secur 6:167–173

Tortorella G, Narayanamurthy G, Staines J (2021) Covid-19 implications on the relationship between organizational learning and performance. Knowl Manag Res & Pract 19:1–14

Tsohou A, Karyda M, Kokolakis S, Kiountouzis E (2015) Managing the introduction of information security awareness programmes in organisations. Eur J Info Sys 24:38–58

Vance A, Siponen M, Pahnila S (2012) Motivating is security compliance: insights from habit and protection motivation theory. Info Manag 49:190–198

Vance A, Siponen MT (2012) Is security policy violations: a rational choice perspective. J Organiz User Comp (JOEUC) 24:21–41

Wang WT, Hou YP (2015) Motivations of employees' knowledge sharing behaviors: a self-determination perspective. Info Organiz 25:1–26

Wang Y, Huang Q, Davison RM, Yang F (2018) Effect of transactive memory systems on team performance mediated by knowledge transfer. Int J Info Manag 41:65–79

Wegner DM (1987) Transactive memory: A contemporary analysis of the group mind. In: Theories of Group Behavior. Springer, pp. 185–208

Wickramasinghe V, Widyaratne R (2012) Effects of interpersonal trust, team leader support, rewards and knowledge sharing mechanisms on knowledge sharing in project teams. Vine 42:214–236

Yuan YC, Fulk J, Monge PR (2007) Access to information in connective and communal transactive memory systems. Commun Res 34:131–155

Zhang T (2018) Knowledge expiration in security awareness training. In: Annual ADFSL conference on digital forensics, security and law, pp. 197–212

Zhang T, Wang WYC, Techatassanasoontorn AA (2019) User's feedback contribution to enhance professional online community: a motivational process. VINE J Info Knowl Manag Sys. https://doi.org/10.1108/VJIKMS-11-2018-0108

Zhong X, Huang Q, Davison RM, Yang X, Chen H (2012) Empowering teams through social network ties. Int J Info Manag 32:209–220

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