The Walls Have Ears: Gauging Security Awareness in a Home Workspace

Gokul Jayakrishnan
TCS Research
Tata Consultancy Services Ltd.
gokul.cj@tcs.com

Vijayanand Banahatti
TCS Research
Tata Consultancy Services Ltd.
vijayanand.banahatti@tcs.com

Sachin Lodha
TCS Research
Tata Consultancy Services Ltd.
sachin.lodha@tcs.com

***Abstract*— The pandemic changed the global enterprise working model. Work from home became the norm and so did the associated security risks. The new workspace posed new dangers such as insecure network and lack of organizational supervisions at home. Failing to adhere to strict security practices in the comfort of home could result in the leakage of confidential information. So, employees' security awareness plays a major role in this new setting. In this paper, we present 'Secure Workspace', a serious game set in a simulated home workspace, that we used to gauge the awareness levels of enterprise employees on secure practices. Our game was well received and played by over 36,000 participants. Based on the participants' performance, we present insights on their awareness, and an advisory to help reduce the number of security violations while working from home.**

I. Introduction

The number of employees who worked from home had doubled to 38% [1] in the UK alone, just one month after the Work from Home (WFH) policies came into effect. In the US, this increased to 44% post COVID-19, as compared to 17% before the pandemic [2]. A Gartner survey [3] revealed that 70% of the survey respondents wished to continue WFH even after the pandemic ended. WFH has raised new challenges when it comes to security compliance. A study by Furnell et al. [4] reports that about 75% of businesses they studied do not have explicit written rules for cybersecurity while WFH. The World Health Organization (WHO) reports that there has been a five-fold increase in the cybersecurity attacks during the pandemic [5]. As Schneck suggests [6], a WFH scenario where office comes to the living room has less support for phone calls or video conferences or protection of proprietary information. While there is an increasing body of literature on the cybersecurity risks during WFH [7, 8, 9, 10, 11, 12], little exists in the domain of employees' actions and how these actions might affect security during such a scenario. A simple routine such as attending a conference call could also lead to leakage of confidential data if it is done carelessly, for example, while standing on the balcony of an apartment with potential listeners in the adjoining apartments. User awareness is one step that could reduce such unforeseen security risks.

To gauge the cybersecurity preparedness of an organization's (name redacted) employees and to make them aware of various secure practices while working from home, we decided to test employees' awareness and provide an enterprise training on security best practices. Our research questions were to (RQ1) measure how the enterprise employees perform in identifying various security violations during WFH and (RQ2) identify the areas where they need more awareness building. While measuring the participants' awareness levels, we wanted to eliminate any possibilities of having a response bias or social desirability bias [13] in their responses. Hence, we avoided questionnaire-based training method. As a result, we developed "Secure Workspace", a simulation-based serious game, aimed at providing an interactive experience on security dos and don'ts during WFH, while simultaneously enabling us to gauge their contextual knowledge on the same.

The game was played by 36,390 participants over a period of two weeks. In this paper, we detail the game mechanics and discuss the insights gathered from the analysis of participants' gameplay data. Following are the contributions of this study: (1) We measure the enterprise participants' understanding of various security-related scenarios during WFH, (2) we analyze their responses and rank the areas where they pay the least (or most) attention, and (3) we discuss the implications and insights for enterprises to reduce security risks during WFH.

II. Background and Related Work

A. Cybersecurity Risks during Work from Home

Prior studies have pointed out various cybersecurity risks such as hacking, phishing, financial frauds, malwares, physical security, leakage of personal and confidential information associated with WFH [4, 10, 11,12]. Considering security risks during WFH, a report by Furnell et al. [4] and the UK Cybersecurity Breaches Survey (CSBS) 2020 [14] state that only a quarter to a third of businesses (in the UK) claim to have addressed 'home working and user awareness' [4].

Symposium on Usable Security and Privacy (USEC) 2023
27 February 2023, San Diego, CA, USA
ISBN 1-891562-91-6
https://dx.doi.org/10.14722/usec.2023.231868
www.ndss-symposium.org, https://www.usablesecurity.net/USEC/

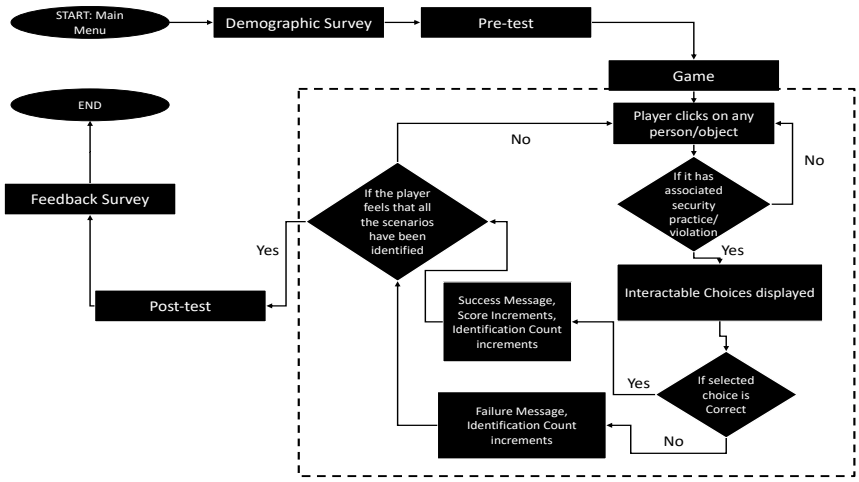

Fig. 1. Game Flow of Secure Workspace

Cybersecurity threat mitigation methods such as the use of Virtual Private Networks (VPN), multi-factor authentication (MFA), employing anti-malware and anti-virus programs, and tightening the organization's security policies [12] help in alleviating cyberattacks to a certain extent. However, all the firewalls and security measures implemented in the devices will be useless if an unauthorized person were to gain physical access to the device [15] or get near the devices and/or confidential information. Physical security of home office [12] includes practical approaches of protecting the work devices. Several guidelines were presented by security firms on how to ensure physical security during WFH [16, 17, 18, 19]. However, the users' actions also play an important role in the extent of security of their work devices.

B. Security Awareness Using Serious Games

While users are often considered the weakest link in security [12], equipping them with the required knowledge of cybersecurity and privacy is a measure that could help in combating security risks [20]. A review of the existing literature on cybersecurity training shows that serious games have shown positive responses in this regard. 'Serious Games' are games with a definite purpose, such as providing awareness, apart from entertainment [21, 22]. Zyda [22] defines 'serious games' as games with specific rules that uses entertainment to further training, education, policies, and strategic communication objectives. Studies show that serious games can be considered as effective educational tools [23, 24].

Serious games such as Anti-phishing Phil [25], What.Hack [26], and Phishy [27] focus on anti-phishing awareness training. CyberCIEGE [28] and Control-Alt-Hack [29] focus on network security and white hat hacking respectively. Passworld [30] and GAP [31] focus on password security awareness. The anti-phishing and password security awareness games had pre-test and post-test methods, and the post-test analysis have reported better user performances as compared to traditional methods of training such as reading documents and slideshows. CyberCIEGE [28] is a security simulation game where the players can purchase and configure workstations and network devices. However, to the best of our knowledge, none of the existing literature offers a study on the general security best practices (cybersecurity and physical security) during a WFH environment. The closest we could find was the 'Spot the Risks' 2D game from teachprivacy.com [32], which consists of an interactive 2D image featuring an office environment. But there were no studies associated with this game. Considering the requirement, we believed a serious game with a simulated environment would enable users to experience the real-life actions and learn from their mistakes in a WFH scenario. Simulation games have been used as pedagogic tools to create experiential learning and are found to be effective as a learning tool [33]. Our work focuses on gauging the participants' understanding on various aspects of security in the home workspace and simultaneously provide training on best practices.

III. Secure Workspace: The Game

A. Game Design and Technology

Secure Workspace was designed and launched in collaboration with the organization's Corporate Security Office (CSO), Human Resource department (HR) and the IT team. We focused on an 'Experiential Learning' method, meaning learning from experience, or learning by doing [34, 35] to improve the learning outcome. The game enables participants to perform actions that they must follow in real life if such scenarios are encountered. The game consists of a simulated work environment that resembles a home workspace.

Considering the requirement of external factors like neighbors in adjacent apartments, we planned the game environment to be an apartment complex instead of an independent house. A report also shows that the most popular resident type is apartments, followed by independent houses [36]. The game also depends on timely feedback to impart

TABLE I. LM-GM MODEL USED IN THE GAME

Learning Mechanics	Game Mechanics	Implementation in the game
Instructional content and Guidance	Game controls and "how to play" instructions	Instructions are provided before gameplay and can be viewed during the game using "Help" option.
Activity/Task/Discovery	Interaction/Movement/ Selection	The 3D interactive virtual WFH environment consists of various security violations that the player must carefully identify.
Motivation/ External Thinking	Relationship with game	The player is provided a WFH environment simulating real-life, and the game environment consists of objects/assets that the player (as an employee of the organization) encounters in real-life.
Feedback	Immediate feedback within game	At the end of each scenario identification, the player gets quick feedback to reflect upon their choice and to understand what needs to be done in such a scenario in real-life.
Instructional content and Guidance	Game controls and "how to play" instructions	Instructions are provided before gameplay and can be viewed during the game using "Help" option.
Activity/Task/Discovery	Interaction/Movement/ Selection	The 3D interactive virtual WFH environment consists of various security violations that the player must carefully identify.

Fig. 2. Secure Workspace Gameplay

conceptual knowledge to the participants. Feedback helps in making the participants understand the concepts and reflect on their learnings [37, 38]. We originally designed a first-person navigation version, where the user can move from one room to another and inspect the elements within the room. The initial tests revealed that the players found the movements to add extra cognitive overload to the experience. We could not test the game in virtual reality (VR) since the employees were working from home, and not everyone has access to VR headsets. So, we developed the game to be played on the company desktop/laptop devices as they constitute majority of the official WFH devices. Since the organization's workforce involve demographic of all age groups (with ages 21 and above), we used a minimal set of controls to make it easy for all, and hence, has a point-and-click [39] mode of interaction with an isometric interface of the gaming environment. Developed using Unity 3D, the game could be played using both the keyboard and the mouse, or just using the mouse alone.

B. *Game Flow*

The game flow (cf. Fig. 1) shows the basic outline of the game. The players should enter their responses to a demographic survey (voluntary and non-mandatory), after which they are presented with a pre-test, which is used to gauge their pre-game knowledge levels. This is followed by the game. A post-test appears after the game, and the flow is concluded with a game feedback survey where we measure the player's engagement and learning levels.

C. *Game Mechanics and Play*

Game mechanics are defined as 'the methods invoked, or the rules followed to interact with the game world' [40, 41]. Learning mechanics involve the patterns of behavior or actions that form the learning activity in the game [41]. To support intrinsic experiential learning, we followed the Learning Mechanics - Game Mechanics (LM-GM) Model [42]. This model allows the users to relate the learning and game mechanics to help maximize learning. Table I shows how Secure Workspace relates the learning and game mechanics. Learning Mechanics that we focused consists of instructional content, activity and tasks, motivation, and feedback [42].

The game play follows the LM-GM model. Fig. 2 shows the events within the game as the player sees them. As soon as the player enters the game, a set of instructions on game controls and "steps to play" are displayed. Once the player carefully reads them, they can proceed to play the game. These instructions are always available to the player using dedicated buttons ("Help", "Controls"). The player can freely navigate the game interface to view the animated characters and objects

(cf. Fig. 2 (a)). Each game character has an associated indicator and when clicked, reveals the information about that character, such as whether they are an organization's employee or a non-employee, along with their relation to the surrounding characters. The player can choose to click on any object that they find to be associated with any insecure/secure practice, for example, a laptop that is kept on the edge of a balcony (cf. Fig. 2 (b)). Immediately after clicking, the player is presented with a set of options that could represent the respective scenario (cf. Fig. 2(c)). Appropriate options will be displayed based on the player's selection to help the player pinpoint the exact scenario (especially in the case where multiple characters appear together). The player should select the most appropriate answer from the choices. The correct answer is immediately displayed as a feedback message (cf. Fig. 2(d)), irrespective of whether the player selected the correct or incorrect option.

Following this, the "Identification count" and "Score" is appropriately updated (cf. Fig. 2 (e)). There are 14 scenarios in the game, with 10 points for each correct identification. We did not disclose this number (14) to the participants because we wanted them to search the whole game environment and identify as many scenarios as they could. Hovering over clickable scenarios would change the cursor to a "magnifying glass" icon indicating that there is a scenario present there. If the player fails the game by providing more than four incorrect responses, there is an option to retry the game level. Within this paper, we mention both 'identifying a scenario' and 'classifying a scenario'. 'Identification' is used when a participant spots the said scenario within the game interface, by the method of inspection. When the spotted scenario is correctly marked as 'secure' or 'insecure', we call it 'classification'. There was no specific order for identifying these scenarios and the players were free to click on any of these as they spot them during navigation within the game.

D. Scenarios Within the Game

The scenarios included the following: (S1) an office laptop, unlocked and unattended on a table, (S2) an employee asking her spouse to check her official email and revert in case of urgency as she has a doctor's appointment (shown with the help of speech bubble), (S3) an employee communicating proprietary information over phone while standing on the balcony, (S4) an employee checking official emails, (S5) an open, filled water bottle kept near laptop, (S6) confidential printouts lying in the open, (S7) a mother working with her infant close by, (S8) a laptop kept at the edge of balcony, at the risk of falling, (S9) a child taking selfie-photos with his parent's official laptop unlocked, behind him, (S10) an employee checking game scores on TV while working, (S11) personal laptop, locked and kept on bed, (S12) an employee running on a treadmill, with open laptop kept on the balcony, (S13) newspapers lying around, and (S14) a child pulling the wires of an official laptop that is left unattended. The 14 scenarios were classified into three categories, namely Unauthorized Disclosure (UD), Physical Protection (PP), and Not a Security Violation (NSV) (Table II). Following sections detail the scenarios in the game based on their respective categories.

TABLE II. SECURITY SCENARIOS CLASSIFIED INTO CATEGORIES

Security Scenarios	Category
S1, S2, S3, S6, S9	Unauthorized Disclosure (UD)
S5, S8, S12, S14	Physical Protection (PP)
S4, S7, S10, S11, S13	Not a security violation (NSV)

1). Unauthorized Disclosure (UD)

Certain scenarios represent situations where an unauthorized data leakage might happen if the user is careless. This includes situations such as an unlocked and unattended laptop with confidential information lying on the table in plain sight (S1), requesting others to check official emails on your behalf, thereby leading to disclosure of information to unintended recipients (S2), communication of proprietary information over phone, standing out in the open, with possibility of neighbors listening to the conversation (S3), unattended confidential printouts lying around (S6), someone taking a photograph in front of another person's official laptop with exposed confidential information (S9). Fig. 3 shows how these scenarios were represented within the game.

Fig. 3. Scenarios depicting Unauthorized Disclosure: (1) S1, (2) S2, (3) S3, (4) S6, (5) S9. To clearly view these scenarios, the players could zoom in and pan within the game's user interface.

2) Physical Protection (PP)

Certain scenarios might not directly lead to leakage of data or confidential information, however, could tamper it indirectly. Physical protection deals with those scenarios whereby a physical intervention can affect the work device and the enclosing data. Scenarios within the game that represented PP include: an open water bottle next to a work device (S5), a laptop kept carelessly at the edge of a balcony, at the risk of falling down (S8), keeping the laptop at a distance while doing physical exercises (S12), and an unattended laptop with a child tampering with the connection wires, possibly leading to a danger for the child and damage to the laptop (S14). Fig. 4 shows these scenarios from the game.

Fig. 4. Scenarios depicting Physical Protection: (1) S5, (2) S8, (3) S12, and (4) S14.

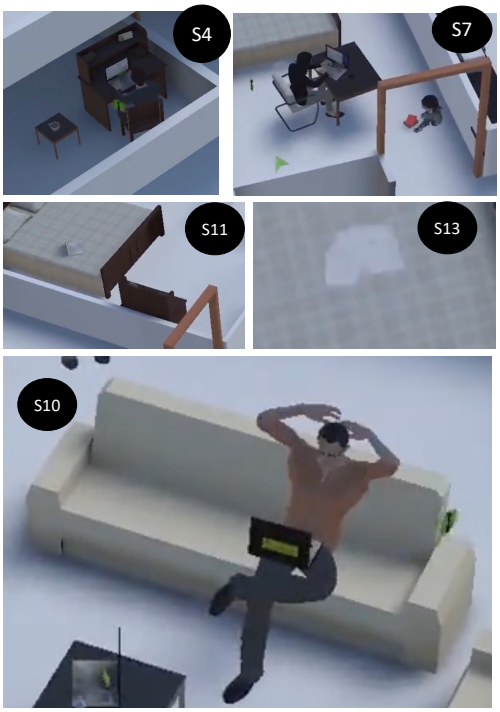

Fig. 5. Scenarios depicting 'Not a Security Violation': (1) S4, (2) S7, (3) S10, (4) S11, and (5) S13.

3) Not a Security Violation (NSV)

Within the game, we had also provided certain scenarios as distractions, as these were not really security violations. However, we measured how the players reacted to these scenarios. These were (Fig. 5): (1) an employee checking official emails (the screen is legible when zoomed in) (S4), (2) a mother working with her infant close by (S7), (3) an employee checking game scores on TV while working (this can be viewed clearly after scrolling and zooming in on the television in front of the person) (S10), (4) personal laptop, locked and kept on bed (this can be identified by the lack of organization's sticker on the laptop, which is mandatory for all office devices) (S11), and (5) newspapers lying around (readable when zoomed in) (S13).

IV. Secure Workspace: The Study

A. Participants

Secure Workspace was launched in an organization with primarily software and information technology (IT)-related workforce. The information on the game launch was communicated to the employees through emails. The web game could be accessed through browsers without the need to install any local game files. The participation was voluntary. The required approvals for the study were granted by the organization's CSO (who also finalized the 14 scenarios used in the game), and Global Privacy Office. The participants were rewarded ($5) using a daily lucky-draw lottery. 36,390 employees from the organization successfully completed the game during the WFH period in December 2020. We gathered the participants' demographic information through a survey. This could also be skipped by providing 'Not Applicable' (NA) as a response. Based on demographic survey responses, the percentages for various categories are as follows: (1) Participants having: Computer Science (CS)/IT background = 44.7%, non-CS/IT background = 43.6%, NA = 11.7%, (2) Participants falling in age-group: 21-30 = 60.8%, 31-40 = 29.5%, 41-50 = 5.0%, Above 50 = 0.9%, Not disclosed = 3.8 %, and (3) Participants based on gender: Female =37.6%, Male = 58.7%, Others = 0.11%, Not disclosed = 3.59%.

B. Materials: The Game and Learning Content

The study material involved the simulation-based serious game with a set of 14 scenarios (*Section III D.),* which consist of the learning content - the dos and don'ts of security within WFH. These scenarios were to test the user's understanding of what constitutes 'secure' and 'insecure', hence some of the scenarios were also categorized as NSVs.

C. Method

We focused on a pre-test and post-test method for measuring learning outcome. A set of five questions, with 'Yes' or 'No' responses, were asked before the game to measure the participants prior-game knowledge on security practices during WFH. A similar set of five questions were asked after the participants played the game. The pre-test and post-test questions (Appendix) were related to the learning content within the game. Each pre-test and post-test question was associated with a Likert-scale [43] rating of 1 to 5 to measure the confidence of the participants while giving the responses. The gameplay responses were also used to measure the participants' understanding of what constitutes 'secure' and 'insecure' practices during WFH. We recorded the following responses of the participants: a) the responses to demographics-related questions, b) responses to the

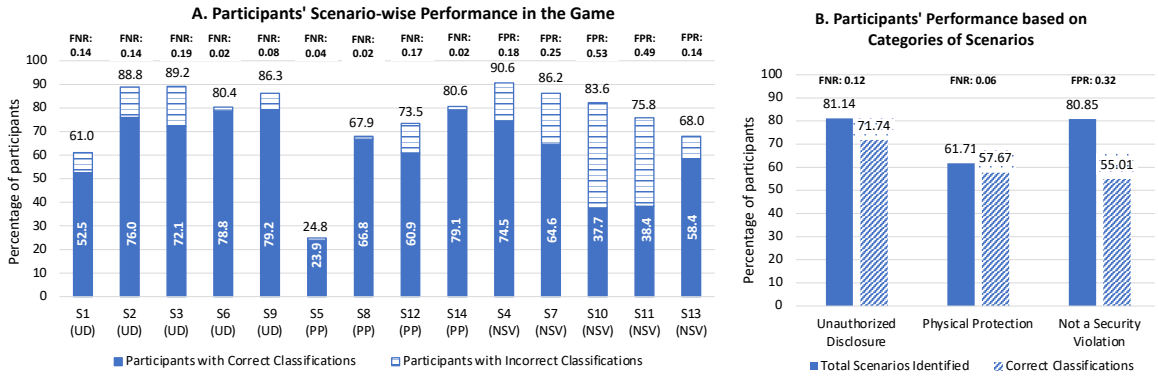

Fig. 6. A. Scenario-wise performance of the participants B. Category-wise performance of the participants

pre-test and post-test questions (five each), c) start and end time of the gameplay, d) scenarios attempted and their order, e) player's classifications, f) time to identify each scenario, g) the score obtained, and h) the feedback survey responses.

D. Data Analysis Measures

Based on the responses to 14 scenarios, we measured False Positive Rate (FPR), False Negative rate (FNR) and overall Correctness (C) in participants' responses using the following formulae:

$$FPR = FP/ (FP + TN) \quad (1)$$

$$FNR = FN/ (FN + TP) \quad (2)$$

$$C = (TP + TN)/ (TP + TN + FP + FN) \quad (3)$$

where FP = False Positive, FN = False Negative, TP = True Positive, and TN = True Negative.

False positive happens when the player identifies a non-security violation as a security violation, and false negative is when they mistake a security violation as a normal scenario. True positive and true negative occurs when the player identifies a security violation and non-security violation appropriately.

V. Results

A. Answering RQ1: How Enterprise Employees Perform in Identifying Security Violations During WFH

Fig. 6(A) shows the distribution of participants' performance in identifying the 14 scenarios. Scenarios S1, S5, S6, S8, S12 and S14 were identified by less than 85% participants, of which the least was for S5 (24.8%). However, considering those who indeed identified them, a higher percentage of participants classified them correctly. For the 36,390 participants, the mean FPR was found to be 0.35 (var = 0.09) and average FNR was 0.11 (var = 0.03), suggesting that the participants had more false classifications for NSV scenarios. Mean Correctness was found to be 0.76 (var = 0.04), which shows there is a near 80% chance that the participants classified the identified scenarios correctly.

Increase in Correctness post gameplay: The mean of the participants' correct answers changed from 4.5 (var=0.72) to 4.75 (var=0.53) after playing the game, and the change is statistically significant (p value <0.001, paired t-test). The participant-wise correctness increased from 90.0% (FNR: 0.1) in the pre-test to 96.4% (FNR: 0.03) in the post-test. The question-wise correctness also increased significantly for post-test (mean FNR = 0.05, mean C = 0.95) as compared to pre-test questions (mean FNR = 0.1, mean C = 0.90), shown in Table III. We saw a similar increase in the confidence ratings as well, with the average confidence rating increasing from 4.73 (pre-test, var = 0.25) to 4.85 (post-test, var = 0.19). To answer RQ1, we have relatively higher pre-test scores denoting higher knowledge levels of participants when it comes to aspects of security in the home workspace. The FNR values have decreased from pre-test to post-test meaning the participants now identify the security violations better. Considering the participants who have relatively lower pre-test scores of 'n' correct answers, where n=0,1,2 (M = 1.9), we found an increase in post-test correctness (M = 3.1). This shows that there has been a positive influence from the game for participants with lesser pre-test knowledge.

Table IV shows the increase in overall correctness (mean) for the post-test questions as compared to the pre-test questions, for all demographics. Considering overall difference, we can see that age-group 21-30 showed a higher increase in the mean of correct answers for the post-test as compared to the pre-test.

TABLE III. Post-test Performance vs. Pre-test Performance for Correct Responses per Question.

Questions	Pre-test	Post-test
	Mean	***Var (Stdev)***[a]
q1	0.85	0.12 (.35)
q2	0.89	0.09 (.30)
q3	0.92	0.06 (.26)
q4	0.90	0.08 (.29)
q5	0.91	0.07 (.28)

[a.] 'Var' denotes variance and 'Stdev' denotes standard deviation of the population.

TABLE IV. PRE-TEST VS. POST-TEST PERFORMANCE BASED ON DEMOGRAPHICS.

Demographics	Pre-test (M1)	Post-test (M2)	Difference (M2-M1) [b]	t-stat	p-value
CS/IT	4.51	4.77	0.26	t(16269) = -42.0	<0.001
Non-CS/IT	4.48	4.74	0.26	t(15856) = -41.1	<0.001
Age					
21-30	4.45	4.73	0.28	t(22133) = -50.9	<0.001
31-40	4.57	4.80	0.23	t(10728) = -31.8	<0.001
41-50	4.67	4.86	0.19	t(1826) = -13.3	<0.001
Above 50	4.69	4.83	0.14	t(327) = -4.6	<0.001
Gender					
Female	4.46	4.73	0.27	t(13698) = -39.6	<0.001
Male	4.53	4.78	0.25	t(21359) = -47.3	<0.001

[b.] 'M1' and 'M2' denote Means (out of five) of correct answers.

B. Answering RQ2: Areas Where the Participants Need More Focus

From Fig. 6(B) we can see that relatively lesser percentage of participants identified and classified physical protection scenarios. There are certain scenarios with high FNR (S3, S12). This needs more care as a higher FNR suggests that the participants categorized the security violations as NSVs. The scenarios that were completely missed by the participants are another major area where more awareness is required, such as S1 (unauthorized disclosure of confidential information on laptop) and S5 (physical security issue with an open water bottle next to laptop). For NSV scenarios S10, S11, and S13, a few participants might have ignored them thinking they are not security violations. Out of the participants who identified them, we can see higher rates of FPR (S10, S11), suggesting that they falsely categorized them as security violations.

C. Other Analysis

In the demographic analysis for the game, we found that the CS/IT background participants (C=81%, FNR: 0.1) showed slightly better correctness percentages to those with no CS/IT background (C=79%, FNR: 0.1). Table V shows that the percentage of participants who correctly responded to scenarios related to 'unauthorized disclosure' was higher than the rest of the categories, for all demographic groups. The performance was almost similar in all age-groups, with the group 21-30 showing a minor increase overall, and for gender, males showed slightly higher performance as compared to females. Considering the game feedback survey data collected from the participants based on 5-point Likert Scale [43], we found 85.1% participants agreeing to game being fun (M=4.24, var=0.62), 88.9% agreeing it to be educational (M = 4.32, var = 0.51), and over 89.5% participants agreed that they learned about various security risks during the WFH after playing the game (M = 4.34, var = 0.50). Regarding the timings, the participants on an average took 9.02 minutes (SD = 3.78 min) for completion from start to end (including the pre-and post-tests), with the least time (mean) taken to identify S6 (31 seconds) and the most time taken for S12 (49 seconds).

TABLE V. THE DEMOGRAPHIC-WISE CORRECTNESS (IN-GAME) FOR THE VARIOUS CATEGORIES (UD, PP, NSV)

Category	UD (Scenarios S1, S2, S3, S6, S9)	PP (Scenarios S5, S8, S12, S14)
CS/IT background	73.19	59.04
Non-CS/IT background	70.21	56.2
Age 21-30	71.79	57.66
Age 31-40	71.45	57.69
Age 41-50	71.41	56.46
Age Above 50	69.09	55.41
Male	71.9	58.08
Female	71.35	56.92

VI. FINDINGS AND DISCUSSION

From *Section V A.* and Fig. 6(A), we can see that for PP scenarios, the percentage of participants who identified is relatively less. The office environment provides a better security and physical infrastructure, with colleagues working for the same organization. However, in a home environment, the situation changes and it becomes more uncontrolled, considering the interference of family members, outsiders, and neighbors who may even work for competitors. This could involuntarily result in physical security-related issues if actions are not performed carefully. Even if technical controls are placed for the work devices, proper training should be provided for the security of physical devices. The analysis resulted in higher FPR for certain scenarios (S10: 0.53, S11: 0.49, cf. Fig. 6(A)), and they were falsely categorized as security violations. This could likely be because they were extra careful regarding these scenarios. Overall, the FNR values reduced for post-test meaning the participants correctly identified the security violations post gameplay.

A. Comparison with Previous Serious Games

Secure Workspace had shown a generally positive outcome among the enterprise employees, with higher post-test correctness and positive player feedback. We find that the overall percentage increase in correctness from pre-test to post-test is relatively small (5.6% increase, from 90% in pre-test to 95.1% in post-test) upon comparison with the previous games for cybersecurity training, such as Anti-phishing Phil [25] (26.08% increase, from 69% in pre-test to 87% in post-test), Phishy [27] (12.25% increase, from 71% in pre-test to 79.7% in post-test), and What.Hack [26] (36.9% increase, from 65% in pre-test to 89% in post-test). Besides, the previous games from literature focus on certain domain-specific aspects of cybersecurity and deal with user training whereas our exploratory study focuses on gauging employees' awareness levels and general preparedness during a WFH

scenario. To the best of our knowledge, we were unable to find studies with games like Secure Workspace in the literature.

B. Implications: Suggestions from the Study

Security measures, especially in an enterprise, cost time and money. Users typically do not want or like them because most of these measures make it inconvenient to get work done. Therefore, it is always critical for any organization to judiciously select and deploy appropriate security measures. A simulated environment-based game like Secure Workspace allows organization to make more informed decisions in this direction. Hence, based on our study, we suggest a few interventions that could help strengthen the existing control measures and reduce security violations.

*a) Auto-system lock***:** Only 52.55% of the participants identified an open and unattended laptop (S1) to be a security violation. Implementing automated count down timer (for just a few seconds) for screen lock could act as a first layer in reducing unintended disclosure of confidential content within work devices to a certain extent, however it also depends on the user and surroundings. Organizations should ensure that the devices have some form of automation to prevent unauthorized device access. Methods to decide if the users (owners) are in front of the device (facial recognition) could be another intervention for device security. This could include keyboard biometrics and even voice recognition techniques.

b) Physical Device Security: For scenarios involving placement of user's laptop (S8, S12), the awareness should be augmented with enterprise practices. One solution is the use of thin clients. The users could log in to their devices from anywhere, but the data resides in a centralized cloud server. Ensuring appropriate data backup facilities will also aid in securing the data on a regular basis.

c) Secure Conversations: For the scenario S3, where a user is communicating confidential information over phone, 30% missed identifying this as a violation. Organizational methods such as mandating use of official and organizational apps for communication and restricting it to office desktop and laptop could reduce unauthorized disclosure of information during communication. Additionally, enhancing organization-provided communication apps that monitor if headphones are connected while making conversations is also a step that could aid this goal. This will be beneficial in WFH scenario as the neighbors could be from competitor organizations, a situation less likely to happen during work from office.

d) Unauthorized Disclosure: Future training methods on enterprise awareness should focus greatly on credential sharing and other forms of disclosure. Every system login and organizational portal logins should be secured with multi-factor authentications. Organizations must implement one-time passwords (OTPs) to avoid users from misusing the passwords. OTPs could also help to ensure that the intended user is logging in.

C. Limitations and Future Work

We had not used a control condition apart from the serious game. Our demographics included the enterprise IT sector crowd, so some level of prior security awareness is expected. One other limitation of our study is fewer number of questions in the pre-test and post-test. We plan to increase the number of questions and categorize them into various levels based on difficulty in the upgraded version of the game. In our future study, we intend to analyze more on how the arrangement of scenarios within the game affects participants' identification process. The future version of the game will also focus on a set of different categories of security threats during WFH. While the current study mainly serves as a tool to identify knowledge levels, our future plan is to develop tools to measure learning improvement due to training. We also plan to test the employee's knowledge retention using a similar exercise to help in improving the existing training. The study provided us an opportunity to explore areas of user-interface, controls, and overall presentation of a game based on real-life WFH environment. Such a training will also benefit from the incorporation of virtual reality and augmented reality by providing more realistic environment for the participants to interact with. Our next item in the agenda is to improve the game to favor a wider demographics of educational backgrounds and to incorporate a better level-based game mechanics to focus on specific sets of security (and non-security) scenarios for both WFH and Work-from-Office situations.

VII. Conclusion

We conducted an exploratory study using a simulation-based serious game Secure Workspace to gauge the awareness of an organization's (name redacted) employees on various aspects of dos and don'ts to be followed while working from home. The participants' responses show that there is an increased need of providing physical security awareness in the current scenario of WFH. To answer our research question RQ1, the enterprise users performed well in correctly identifying majority of the security scenarios. To answer RQ2, we found physical security to have relatively lesser percentage of correct identification. We suggest certain interventions that could help improve the overall security landscape while working from home, such as multifactor authentication, ensuring use of headphones while communicating confidential information, employing device camera-based facial recognition systems, auto-system lock, thin clients, and immersive user awareness methods. The participant feedback suggests that simulated experiences have a positive effect in training the users. While Secure Workspace helped gauge the WFH security awareness levels of enterprise users, we plan to use the results of this study as a starting point to create targeted security training for enterprise demographics.

REFERENCES

[1] 'Coronavirus Polling – 10-13 April 2020'. Ipsos MORI. Accessed Jul 2020. www.ipsos.com/sites/default/ files/ct/news/documents/2020-04/ node-658626-659361.zip.

[2] Mlitz, Kimberly. Remote work frequency before and after COVID-19 in the United States 2020. April 2020. Retrieved July 01, 2021 from https://www.statista.com/statistics/1122987/change-in-remote-work-trends-after-covid-in-usa/

[3] https://www.gartner.com/en/newsroom/press-releases/2021-02-17-gartner-survey-reveals-70--of-customer-service-and-su

[4] Furnell S, Shah JN. Home working and cyber security–an outbreak of unpreparedness? Comput Fraud Secur. 2020;2020(8):6-12.

[5] WHO reports fivefold increase in cyber attacks, urges vigilance. World Health Organization. 2020 Apr 23. URL: https:/ /www.who.int/news-room/detail/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance

[6] Schneck, Phyllis A. "Cybersecurity During COVID-19." IEEE Annals of the History of Computing 18.06 (2020): 4-5.

[7] Lenovo. Technology and the Evolving World of Work. July 2020. Retrieved July 01, 2021 from https://news.lenovo.com/wp-content/uploads/2020/07/Technology-and-the-Evolving-World-of-Work_Lenovo-IDG-Global-Research-Report_FINAL.pdf

[8] '10 steps to cyber security'. National Cyber Security Centre, 17 Nov 2018. Accessed August 18, 2021. https://www.ncsc.gov.uk/news/large-uk-organisation-10-steps-stay-ahead

[9] WHO reports fivefold increase in cyber attacks, urges vigilance. World Health Organization. 2020 Apr 23. URL: https:/ /www.who.int/news-room/detail/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance

[10] Williams, Christina Meilee, Rahul Chaturvedi, and Krishnan Chakravarthy. "Cybersecurity risks in a pandemic." Journal of Medical Internet Research 22.9 (2020): e23692.

[11] Lallie, Harjinder Singh, et al. "Cyber security in the age of covid-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic." Computers & Security 105 (2021): 102248.

[12] Pranggono, Bernardi, and Abdullahi Arabo. "COVID-19 pandemic cybersecurity issues." Internet Technology Letters 4.2 (2021): e247.

[13] Chung, Janne, and Gary S. Monroe. "Exploring social desirability bias." Journal of Business Ethics 44.4 (2003): 291-302.

[14] UK Cyber Security Breaches Survey (CSBS) 2020. Ipsos MORI. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/874693/Technical_annex_-_Cyber_Security_Breaches_Survey_2020.pdf

[15] Physical Security and Why It Is Important. Hutter, David. https://www.sans.org/reading-room/whitepapers/physical/physical-security-important-37120

[16] Arntz,Pieter, MalwareBytes Labs. Security tips for working from home, March 19, 2020.Retrieved July 01, 2021 from https://blog.malwarebytes.com/how-tos-2/2020/03/security-tips-for-working-from-home-wfh/

[17] Kaspersky. Cyber Security Risks: Best Practices for Working from Home and Remotely. Retrieved July 01, 2021 from https://www.kaspersky.com/resource-center/threats/remote-working-how-to-stay-safe

[18] Barry, Rowan, The Physical Security Guide to Working From Home. April 09, 2020, Retrieved July 01, 2021 from https://www.barrybros.com/2020/04/the-physical-security-guide-to-working-from-home/

[19] Violino, Bob, Securing the Work-At-Home Environment, Retrieved July 01, 2021 from https://securityboulevard.com/2020/04/securing-the-work-at-home-environment/

[20] Alotaibi, Faisal, et al. "A review of using gaming technology for cyber-security awareness." Int. J. Inf. Secur. Res.(IJISR) 6.2 (2016): 660-666.

[21] Bellotti, Francesco, et al. "Designing serious games for education: from pedagogical principles to game mechanisms." Proceedings of the 5th European Conference on Games Based Learning. Greece: University of Athens, 2011.

[22] Zyda, Michael. "From visual simulation to virtual reality to games." Computer 38.9 (2005): 25-32.

[23] Anastasiadis, T., Lampropoulos, G., & Siakas, K. (2018). Digital Game-based Learning and Serious Games in Education. International Journal of Advances in Scientific Research and Engineering, 4(12), 139-144.

[24] Bellotti, F., Berta, R., De Gloria, A., D'ursi, A., & Fiore, V. (2013). A serious game model for cultural heritage. Journal on Computing and Cultural Heritage (JOCCH), 5(4), 1-27.

[25] Sheng, Steve, et al. "Anti-phishing phil: the design and evaluation of a game that teaches people not to fall for phish." Proceedings of the 3rd symposium on Usable privacy and security. 2007.

[26] Wen, Zikai Alex, et al. "What. hack: engaging anti-phishing training through a role-playing phishing simulation game." Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems. 2019.

[27] CJ, Gokul, et al. "Phishy-a serious game to train enterprise users on phishing awareness." Proceedings of the 2018 annual symposium on computer-human interaction in play companion extended abstracts. 2018.

[28] Irvine, Cynthia E., Michael F. Thompson, and Ken Allen. "CyberCIEGE: gaming for information assurance." IEEE Security & Privacy 3.3 (2005): 61-64.

[29] Denning, Tamara, et al. "Control-Alt-Hack: the design and evaluation of a card game for computer security awareness and education." Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security. 2013.

[30] Jayakrishnan, Gokul Chettoor, et al. "Passworld: A serious game to promote password awareness and diversity in an enterprise." Sixteenth Symposium on Usable Privacy and Security ({SOUPS} 2020). 2020.

[31] Tupsamudre, Harshal, et al. "GAP: A game for improving awareness about passwords." Joint International Conference on Serious Games. Springer, Cham, 2018.

[32] Privacy and Security Training Games. TeachPrivacy.com. Retrieved on October 14, 2022 from https://teachprivacy.com/privacy-and-security-training-games/

[33] Keys, B. and Wolfe, J. (1990) 'The role of management games and simulations in education and research', Journal of Management, vol. 16, no. 2, pp. 307

[34] Gentry, James W. "What is experiential learning." Guide to business gaming and experiential learning 9 (1990): 20.

[35] Lewis, Linda H., and Carol J. Williams. "Experiential learning: Past and present." New directions for adult and continuing education 1994.62 (1994): 5-16.

[36] The Times of India, Over 50% people live in their own houses in India. Retrieved July 01, 2021 from https://timesofindia.indiatimes.com/business/india-business/over-50-people-live-in-their-own-houses-in-india/articleshow/70586938.cms

[37] Donovan, M. Suzanne, John D. Bransford, and James W. Pellegrino. How people learn: Bridging research and practice. National Academy Press, 2101 Constitution Avenue NW, Lockbox 285, Washington, DC 20055, 1999.

[38] Penuel, B., Roschelle, J., & Cohen, A. L. (1999). Designing learning: Cognitive science principles for the innovative organization. Designing learning: Principles and technologies (SRI paper series). SRI Project, 10099.

[39] Inkpen, Kori, Kellogg S. Booth, and Maria Klawe. "Interaction styles for educational computer environments: A comparison of drag-and-drop vs. point-and-click." Working Draft (1996).

[40] Sicart, Miguel. "Defining game mechanics." Game studies 8.2 (2008): 1-14.

[41] Plass, Jan L., et al. "Learning mechanics and assessment mechanics for games for learning." G4LI White Paper 1 (2011): 2011.

[42] Lim, T., Carvalho, M. B., Bellotti, F., Arnab, S., De Freitas, S., Louchart, S., ... & De Gloria, A. (2015). The LM-GM framework for serious games analysis. Pittsburgh: University of Pittsburgh.

[43] I. Elaine Allen and Christopher A. Seaman. 2007. Likert Scales and Data Analyses. July 2007. Retrieved February 19, 2020 from http://rube.asq.org/quality-progress/2007/07/statistics/likert-scales-and-data-analyses.html

APPENDIX

The questions presented to the participants during the pre-test and post-test are given below:

A. Pre-test Questions

1. Security awareness training is applicable when I work from office. It is not so much relevant while I work from home.
2. Personal data should be accessible only to the rightful owners.
3. For swift response, you may use external instant messaging services to share <organization> information
4. In the WFH scenario, it is advisable to connect devices, other than those allotted by <organization>, to store official data.
5. You can take tea / coffee breaks while you are working from home.

B. Post-test Questions

1. You can share confidential information to family members and to social media.
2. In WFH environment, you may share official information through apps like WhatsApp or through public email.
3. Use headphones during calls to protect privacy confidentiality of <organization> /customer information
4. Always use secure channels for communication, like MS Teams or <redacted>, instead of personal emails.
5. You can share laptops/workstations with others in a WFH environment.

We also added some seemingly harmless scenarios in the questionnaire (pre-test question 4) which falls under the 'non-security violations' category, because we didn't want to make it obvious that all the scenarios are security violations.

C. Scenarios in-game

The 14 scenarios shown in the game are provided below, with their options and answer description (which constitutes the feedback to the players). Certain words are redacted and enclosed within '< >'. The category in which each scenario belongs to is given in '()'.

1) An office laptop, unlocked and unattended on a table: (UD)

Did you notice any insecure practice here?

1. The laptop is unlocked and unattended
2. The laptop is kept safely on the table
3. Insecure laptop posture

Description: The laptop is left unlocked and unattended on the table. Always lock the laptop when you are moving away from it, even if it is for a short break.

2) An employee asking her spouse to check her official email and revert in case of urgency as she has a doctor's appointment (shown with the help of speech bubble): (UD)

Is she doing anything wrong?

1. Nothing wrong in sharing the credentials with spouse since he is also a <employee>
2. Encouraging others to use her <company> laptop
3. Credentials are being shared
4. Both 2. and 3.

Description: You should never share your credentials or encourage others (even family members) to use your company / customer issued laptop.

3) An employee communicating proprietary information over phone while standing on the balcony: (UD)

Is he doing anything wrong?

1. Sharing confidential information through social media platforms
2. Discussing confidential information from balcony since it may be heard by neighbors
3. Taking office call through his cellular network, instead of using <software>
4. Both 1. and 2.

Description: "Never share <company> or Customer information through social media and always be aware of your surroundings when discussing confidential matter.

4) An employee checking official emails: (NSV)

Select the most appropriate option

1. Sarath is checking <company> mails during work time, which is not allowed
2. Sarath is checking his <company> email which is his <redacted> activity, no issues noted
3. Tea / Coffee is kept away from laptop, which is a good practice
4. Both 2. and 3.

Description: Nothing wrong with this scenario. You should also ensure that the tea / coffee mug is kept away from the laptop to avoid accidental spillage.

5) An open, filled water bottle kept near laptop: (PP)

Is there anything wrong here?

1. A potential risk exists because of the open water bottle placed next to the laptop
2. The water bottle is kept in a very safe place.
3. Normal scenario, as associate has to work long hours. They have kept the water bottle near the laptop

Description: The water bottle is open and not kept in a safe place. It might accidentally fall over the laptop, causing a technical failure.

6) Confidential printouts lying in the open: (UD)
Did you notice an insecure practice here?
1. <company>confidential printouts being exposed to external persons
2. Nothing wrong here. The person repairing AC is trustworthy, since he visits us for last 5 years
3. Nothing wrong here - the <company> documents are safe since they are in the bedroom

Description: Business documents should be accessible only to authorized individuals. Always secure confidential materials in locked drawers.

7) A mother working with her infant close by: (NSV)
Is there an insecure practice here?
1. Anjana should work from a separate room with no family member around
2. Anjana should not attend to her child while she is working
3. It is all right to have your child play around as long as the laptop is secured

Description: Anjana is diligently working. Nothing wrong in this scenario.

8) A laptop kept at the edge of balcony, at the risk of falling: (PP)
What do you think is an insecure practice here?
1. The position of the laptop is risky. It may fall anytime.
2. The laptop is kept close to the owner. So, there is nothing wrong.
3. None of the above

Description: Always ensure that the laptop is placed in a secure and safe location / position to avoid accidental damages.

9) A child taking selfie-photos with his parent's official laptop unlocked, behind him: (UD)
What do you think is the insecure practice here?
1. The person is using his personal phone
2. The person is clicking a selfie with unlocked <company> laptop behind. It may expose confidential information inadvertently
3. Photography is prohibited in <company> office and this is home. So, there are no issues.

Description: Take care of your surroundings and ensure you are not exposing business information, even inadvertently.

10) An employee checking game scores on TV while working: (NSV)
Do you think something's wrong here?
1. Paul is watching TV while working, which is a highly insecure practice
2. Paul is sitting on a sofa in living room while working
3. Nothing wrong with Paul working, and also checking score of a match periodically

Description: Watching TV when you take a break from work is not an insecure practice.

11) Personal laptop, locked and kept on bed: (NSV)
Is there anything wrong with this laptop?
1. The laptop is kept unlocked and unattended on the bed
2. The laptop is playing some video or film
3. Nothing wrong here

Description: This looks like a personal laptop, without any <company> confidential information.

12) An employee running on a treadmill, with open laptop kept on the balcony: (PP)
Is this laptop secure?
1. Yes. It is kept locked
2. No, it is kept in the balcony; something can fall on it and damage it
3. None of the above

Description: This is an insecure practice as the laptop is kept in the balcony, where it is exposed to direct sunlight or rain. There is also a risk of something falling on it.

13) Newspapers lying around: (NSV)
What is an insecure practice here?
1. The newspapers are left unattended next to an external person
2. There is no insecure practice here

Description: As newspapers are not confidential material, there is no insecure practice happening here.

14) A child pulling the wires of an official laptop that is left unattended: (PP)
What can go wrong here?
1. The child may pull the laptop cable, causing the laptop to fall
2. Nothing can go wrong, as the child is small and is sitting on the floor

Description: There are chances of the kid pulling the laptop cable, thus causing it to fall.