TATA CONSULTANCY SERVICES

# The Walls Have Ears:

## Gauging Security Awareness in a Home Workspace

Gokul Jayakrishnan | Vijayanand Banahatti | Sachin Lodha

TCS Research, Tata Consultancy Services Limited

NDSS USEC, 27 February 2023

# Agenda

- Motivation
- Research Questions
- Serious Game
- Design Considerations
- Secure Workspace
- Design Model
- Learning Content
- Gameplay
- Study Evaluation
- Findings and Discussion
- Suggestions
- Limitations and Road Ahead
- Summary

# The **Motivation**

**"COVID-19"** : Initiated in the global 'work-from-home' (WFH) scenario

- Cybersecurity risks have **increased** during pandemic [1, 2]
- **Human error -** 95% of cyber-attacks and breaches result from human error [3].

## Are enterprise employees equipped to handle WFH securely?

## AIM:

To gauge the security awareness of enterprise workforce during WFH and to equip them with security knowledge in an interactive and fun manner.


1. Borkovich, Debra J., and Robert J. Skovira. "Working from home: Cybersecurity in the age of COVID-19."
2. Williams, Christina Meilee, Rahul Chaturvedi, and Krishnan Chakravarthy. "Cybersecurity risks in a pandemic." Journal of medical Internet research 22.9 (2020): e23692.
3. IBM Cyber Security Intelligence Index Report, World Economic Forum, https://cybernews.com/editorial/world-economic-forum-finds-that-95-of-cybersecurity-incidents-occur-due-to-human-error/

# Exploratory Study: Research Questions

1. Measure how the enterprise employees perform in identifying various security violations while working from home

2. To identify the security areas where they need more awareness building

➡ Study Method: *Serious Game*

# What is a Serious Game?

- *Serious games are games whose primary purpose is not mere entertainment, but education.* [a]

- "Serious games include 'using video games and games technologies outside entertainment"

  Benjamin Sawyer, the co-founder of 'The Serious Games Initiative, 2002'

- A category of computer-based games that are mainly designed for training users on a particular skill set [b].

- **Serious Games** have been successful in training in various domains (education, cybersecurity, medicine, cultural heritage, etc.).

a. Alvarez, Julian, and Damien Djaouti. "An introduction to Serious game Definitions and concepts." Serious Games & Simulation for Risks Management 11.1 (2011): 11-15.

b. 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. University of Athens, Greece. 2011.

# Why (Serious) Game?

- Games help in discovery learning and are non-monotonous and interactive unlike the one-way transmission of knowledge happening from reading training materials[c].
- Game-based cybersecurity awareness have been studied in the past with successful results.

- *E.g., Anti-Phishing Phil, Control-Alt-Hack, CyberCIEGE [d], Passworld, Phishy, PickMail etc.*
  - Awareness game on WFH dos and don'ts scarce in literature

Serious games for enterprise users:




c. Cone, Benjamin D., Cynthia E. Irvine, Michael F. Thompson, and Thuy D. Nguyen. "A video game for cyber security training and awareness." computers & security 26, no. 1 (2007): 63-72.

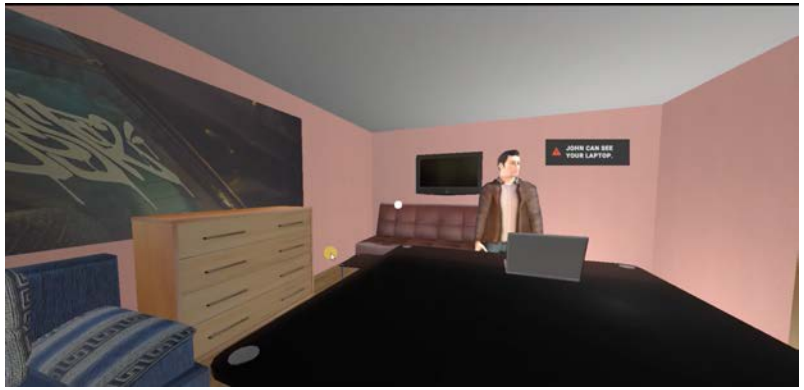
d. Hendrix, Maurice, Ali Al-Sherbaz, and Bloom Victoria. "Game based cyber security training: are serious games suitable for cyber security training?" International Journal of Serious Games 3.1 (2016): 53-61.

# Design Considerations

- “Cybersecurity Dos and Don’ts during Work from Home” – Shared internally within the enterprise
- **Experiential Learning Principle**
  - The text-based content converted to interactive action-based content for better engagement

# Game Environment and Mode

- **Setting**: **Apartment Complex** **|** Most preferred residential type [e]
- Game interface: Isometric view to minimize controls and learning curve
  - Primary test: First person mode
  - Virtual Reality mode avoided due to physical limitations of WFH





e. 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


# Secure Workspace: The Game

Pre-test → Game → Post-test

Immediate feedback

# Secure Workspace Game

**What?** Serious Game about various security practices that could happen during work from home

**Type:** **Single-player** | 3D interactive game | Isometric view

**Controls:** Keyboard + Mouse OR Mouse alone

**Learning Content:** **14 Scenarios** related to security practices during work-from-home

**Constraints:** Web browser-playable, Time limitation, Minimal Controls

# Secure Workspace: Design Model

- **LM-GM Model** [f]: To support intrinsic experiential learning

| Learning Mechanics * | Game Mechanics ** | In-game Implementation |
|---|---|---|
| Instructional Content | Game controls and instructions | 'Help' and 'Instructions' |
| Activity/ Task discovery | Interaction, Movement | 3D interactive virtual world with visible task to identify |
| Motivation | Relationship with the game | Simulation of real-world actions or objects in a WFH environment |
| Feedback | Immediate feedback | Enables reflection and imparts awareness |

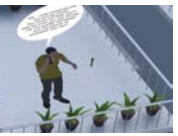
* Behaviors or actions that form the learning activity

** Methods or rules to interact with the game world

f. 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.

# Learning Content: 14 Scenarios

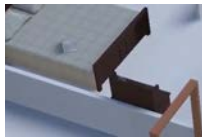




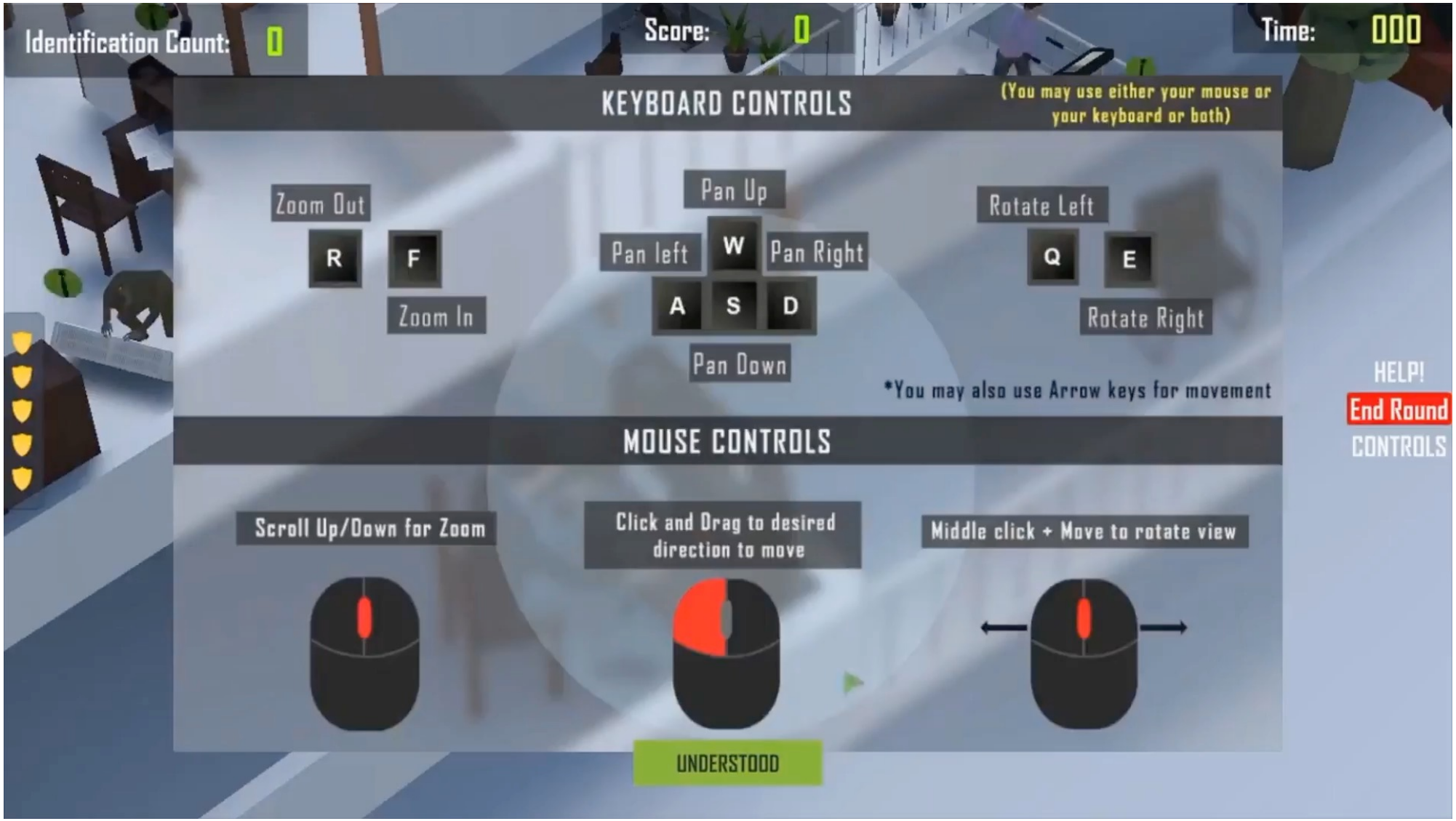


| Scenario | Description | Category |
|---|---|---|
| **S1** | Unlocked and attended laptop | **Unauthorized Disclosure** |
| **S2** | Sharing credentials | **Unauthorized Disclosure** |
| **S3** | Careless communication | **Unauthorized Disclosure** |
| **S4** | Checking official emails | Not a security violation |
| **S5** | Open and filled water bottle near laptop | ***Physical protection*** |
| **S6** | Confidential printouts unattended | **Unauthorized Disclosure** |
| **S7** | Mother working with an infant present nearby | Not a security violation |
| **S8** | Laptop kept at a vulnerable position | ***Physical protection*** |
| **S9** | Selfie with work device visible | **Unauthorized Disclosure** |
| **S10** | Checking game scores during work break | Not a security violation |
| **S11** | Personal laptop unattended, locked, on bed | Not a security violation |
| **S12** | Unattended laptop in a risky position, balcony | ***Physical protection*** |
| **S13** | Newspapers lying around | Not a security violation |
| **S14** | Infant pulling laptop cables | ***Physical protection*** |




# Secure Workspace: Gameplay




# Study Evaluation

# Study: Evaluation

**Participants: 36,390**

**Demographics:**

- CS/IT: **44.7%**
- Non CS/IT: **43.6%**

---

- 21-30: **60.8%**
- 31-40: **29.5%**
- 41-50: **5.0%**
- Above 50: **0.9%**

---

- Females: **37.6%**
- Males: **58.7%**

**Materials:**

- **Serious Game** with the set of **14 scenarios**

**Method:**

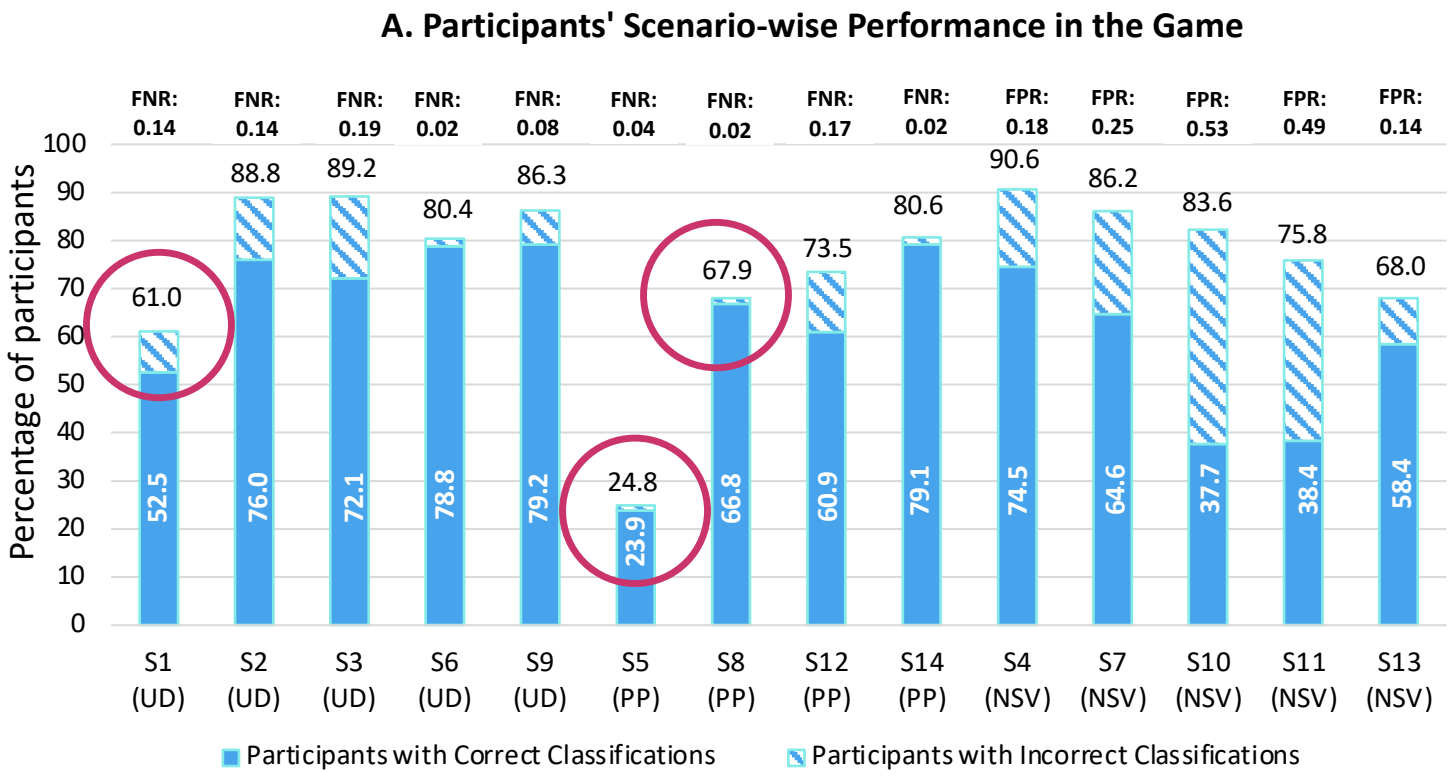
- **Pre-test** and **Post-test**
- Set of 5 questions each
- Yes/no questions on awareness of cybersecurity practices
- Measured in Likert Scale rating

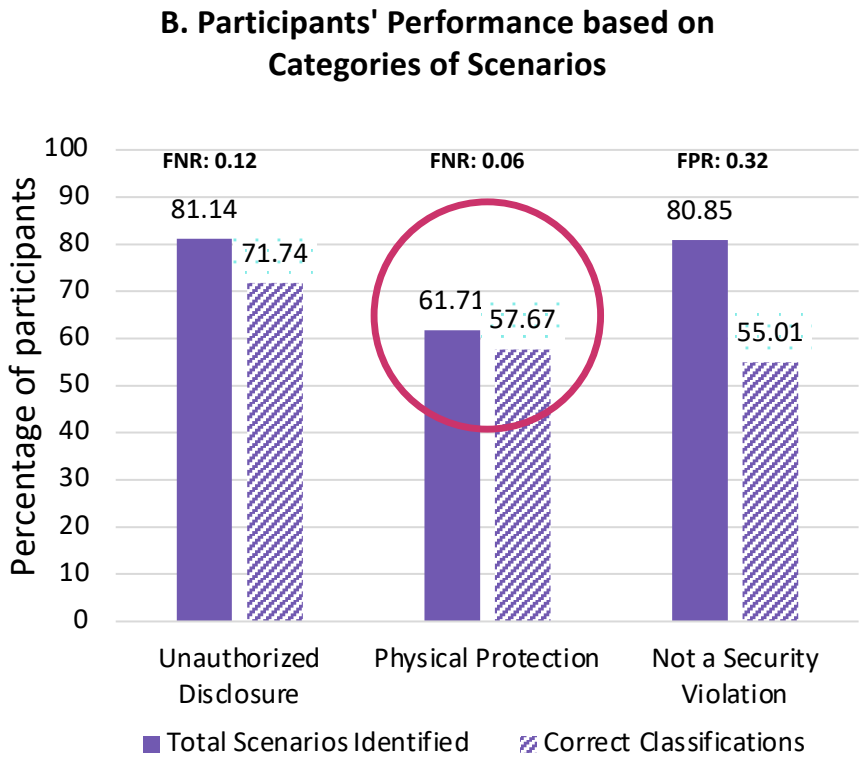
**Data Analysis Measures:**

- **FNR and FPR**
- **Correctness**

FPR = False Positive (FP) / (False Positive (FP) + True Negative (TN))
FNR = False Negative (FN) / (False Negative (FN) + True Positive (TP))
Correctness = (TP + TN) / (TP + TN + FP + FN)

# Study: Results



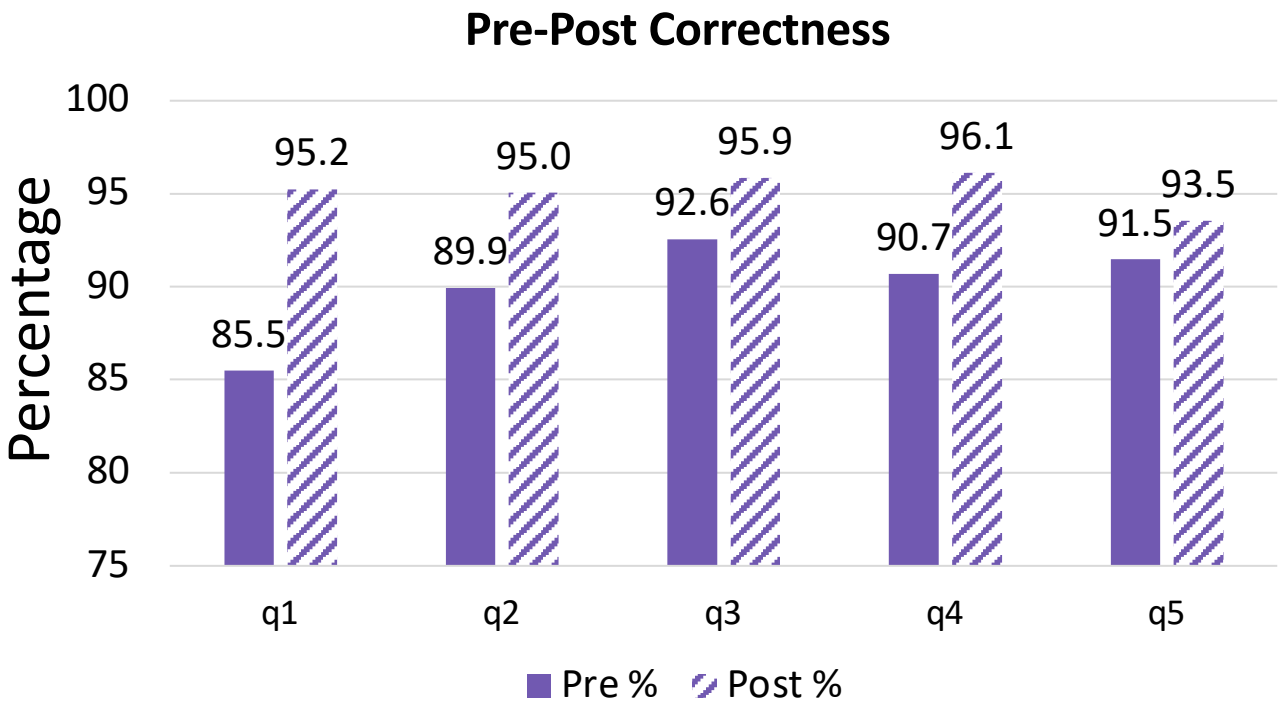



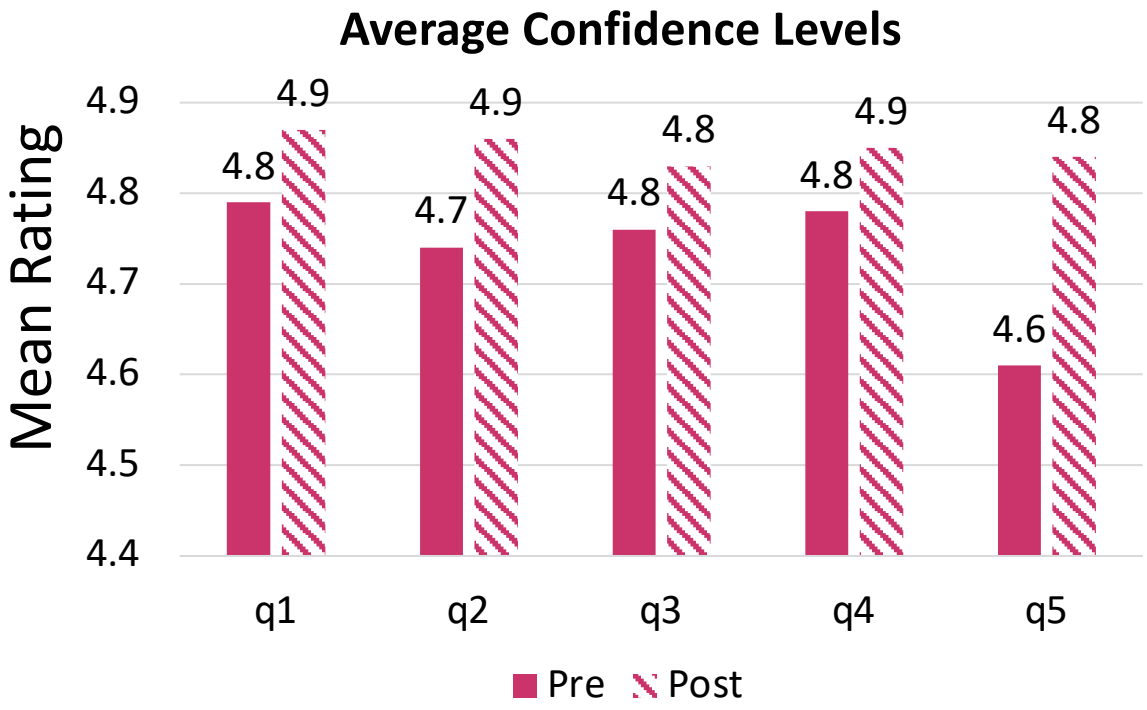

S1 Unlocked and attended laptop

S5 Open and filled water bottle near laptop

S8 Laptop kept at a vulnerable position

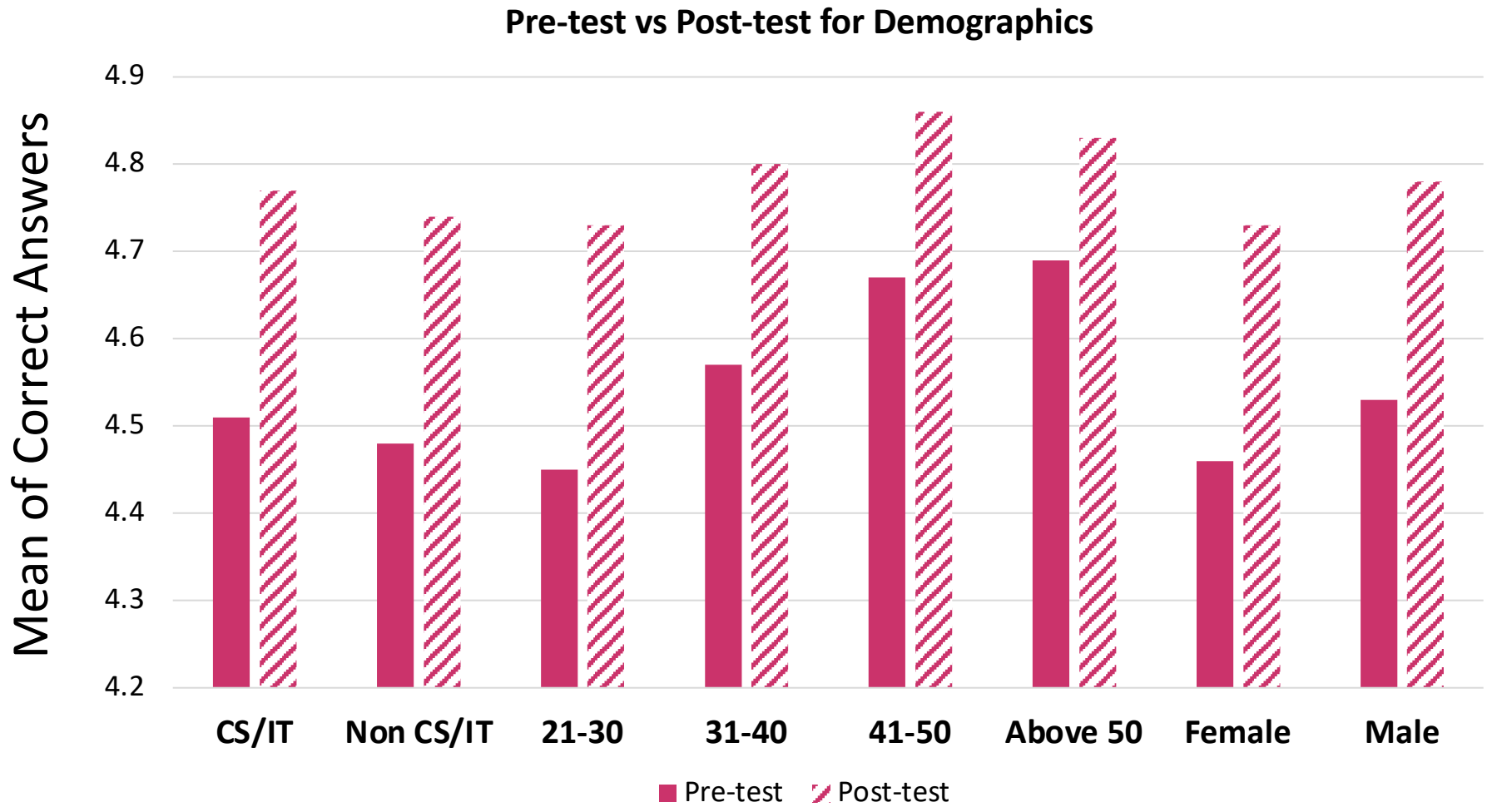
# Study: Pre-test vs Post-test



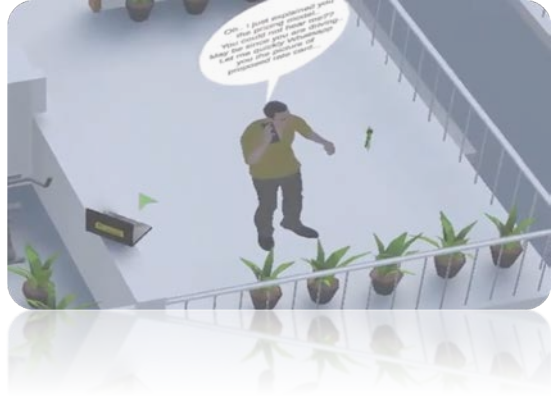




Overall, better performance for post-test as compared to pre-test

# Study: Pre-test vs Post-test



# Game Findings - 1



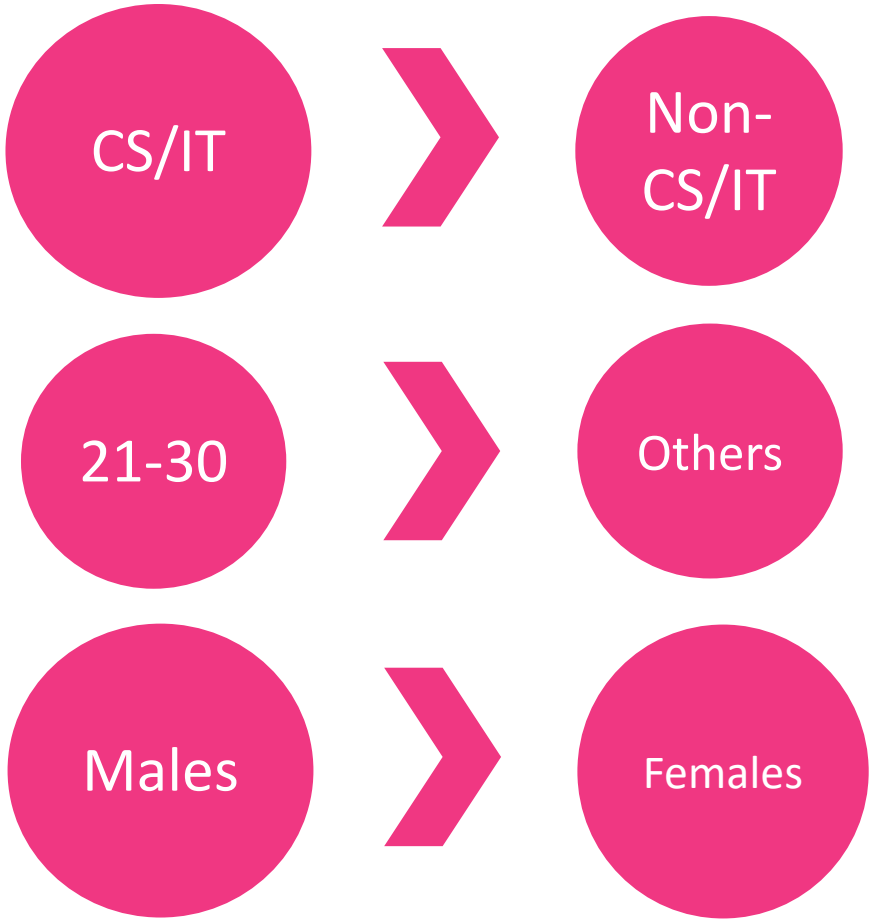
- **RQ1: Performance of Enterprise Employees**
  - Mean FPR: 0.35 | Mean FNR: 0.11 | Mean Correctness: 0.76
  - Higher pre-test scores denotes above average knowledge levels
  - For participants with lower correctness in pre-test, the mean correctness increased from 1.9 (pre-test) to 3.1 (post-test), showing a positive influence of the game

- **RQ2 : Where do participants need more focus?**
  - High FNR scenarios : **S3, S12**
  - Most missed scenarios : **S1, S5**
  - High FPR scenarios : **S10, S11**
  - Physical protection needs more care, as even the identifications were lesser

S3: Careless call (UD), S12: Laptop on balcony (PP)
S1: Unattended laptop (UD), S5: Water bottle (PP)
S10: Game scores (NSV), S11: Personal laptop (NSV)

# Game Findings - 2

- **Demographics-Related**

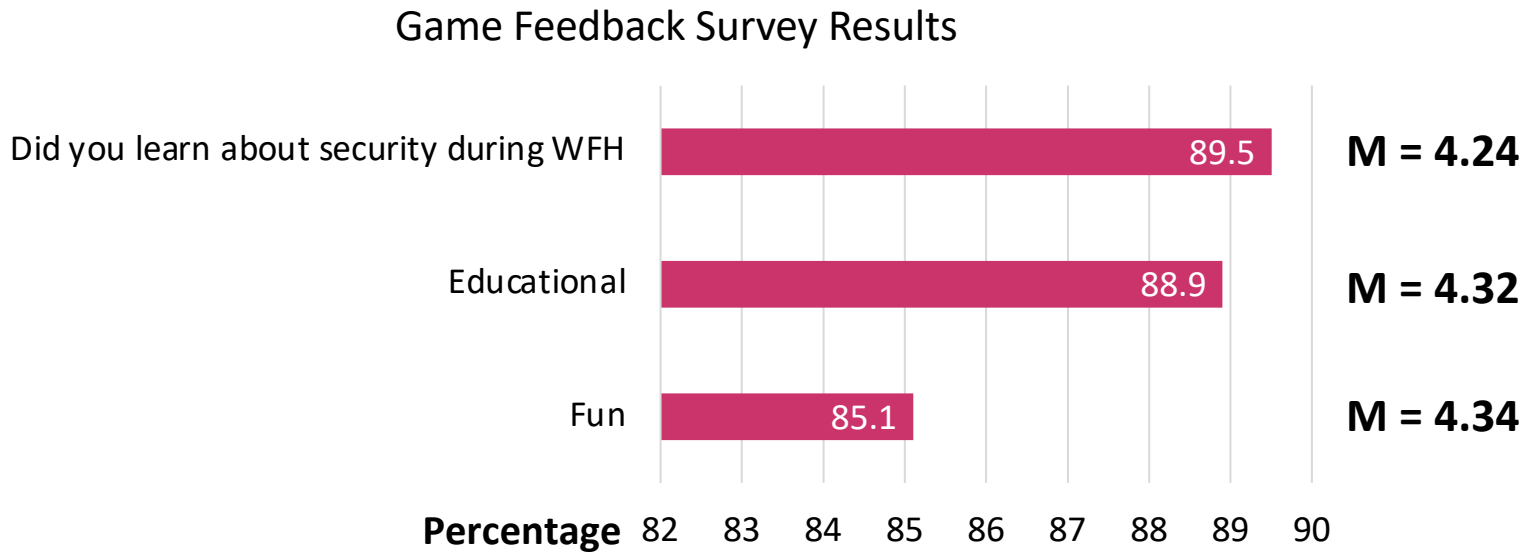



**Unauthorized Disclosure:**
Highest correctness

**Physical Protection:**
Least Correctness

# Game Findings - 3

## Game Feedback:




## Time Analysis:

**9:02**

Average Gameplay Time

**0:31**

Least: **S6**

**0:49**

Highest: **S12**

# Suggestions to Strengthen Control Measures:

- Auto-system **Lock**
- Thin clients and **centralized data**
- **Secure** conversations – organization-provided apps
- **MFA** and **OTPs** to prevent Unauthorized Disclosure

# Limitations

- Enterprise crowd
- Lack of control condition
- Unable to test knowledge retention
- Fewer number of pre-test and post-test questions

# Road ahead

**Learning Content**

*Increasing the learning content and categorization based on difficulty*

**Targeted Training**

*For different cybersecurity areas and different demographics*

**Repurpose & Upgrade**

*Modular approach in re-design to suit multiple domains beyond security, especially using Virtual Reality*

**Time Period**

*Extended studies to measure learning curve of players over a period*

# Summary


- Covid-19 induced WFH → Increase in security issues
- Exploratory study: **Research Questions**
  1. Measure security preparedness of enterprise audience
  2. Identify the areas with poor performance
- **Secure Workspace:** 3d interactive single-player game | gauge security awareness
- Participants: Over **36,000** | Pre-test/Post-test method
- Evaluation: Higher post-test scores and lower FNR values
  - High FNR : **S3, S12** | Most missed scenarios : **S1, S5** | High FPR : **S10, S11**
  - Physical security must also require focus
- **The walls do have ears. So beware!**

tcs Research

Inventing for impact

# QUESTIONS

Thank you

**The Walls Have Ears:**

Gauging Security Awareness in a Home Workspace

Contact: gokul.cj@tcs.com | vijayanand.banahatti@tcs.com | sachin.lodha@tcs.com