Journal of Information & Optimization Sciences
ISSN 0252-2667 (Print), ISSN 2169-0103 (Online)
Vol. 47 (2026), No. 5-A, pp. 1727–1734
DOI : 10.47974/JIOS-2263

Implementing game-based learning techniques to enhance data security awareness among employees in tech industries

Sagarkumar S. Badhiye [†]
Department of Computer Science and Engineering
Symbiosis Institute of Technology
Nagpur Campus
Symbiosis International (Deemed University)
Nagpur 440008
Mahrashtra
India

Pratibha V. Kashid *
Department of Information Technology
Sir Visvesvaraya Institute of Technology
Nashik 422102
Maharashtra
India

Sunil Thakur [§]
School of Engineering & Technology
Noida International University
Greater Noida 203201
Uttar Pradesh
India

Shwetambari Pandurang Katake [‡]
Department of Computer Engineering
Vishwakarma Institute of Technology
Pune 411037
Maharashtra
India

[†] *E-mail:* sagarbadhiye@gmail.com
* *E-mail:* wajepratibha23@gmail.com (Corresponding Author)
[§] *E-mail:* sunil.thakur@niu.edu.in
[‡] *E-mail:* shwetambari.katake@vit.edu

Yatin Gandhi [@]
Competent Softwares
Pune 411069
Maharashtra
India

Abstract

It is very important to keep data safe, especially in the tech field where private data is often at risk. Traditional ways of training don't get people involved, which make them less successful. A fun and participatory way to learn about hacking is through game-based learning (GBL). GBL helps people remember what they've learnt and encourages them to use security best practices by using chores, role-playing, and real-life situations. This paper shows a GBL framework made just for the tech industry. It uses safety ideas and game mechanics to create a safe workplace. The suggested method aims to raise knowledge among employees and lower the hacking risks facing the organization.

Subject Classification: *68M25, 68M99.*

Keywords: *Game-based learning, Data security, Cybersecurity, Employee engagement, Tech industry.*

1. Introduction

Data security is still very important for businesses, especially in the tech field where private data is often at risk in a world where technology is changing so quickly [1]. Cyber dangers are getting bigger and more complicated all the time, so companies are always looking for good ways to make their workers more aware of data security. Traditional ways of teaching workers don't always get them interested, which means they don't stay with the company or follow security

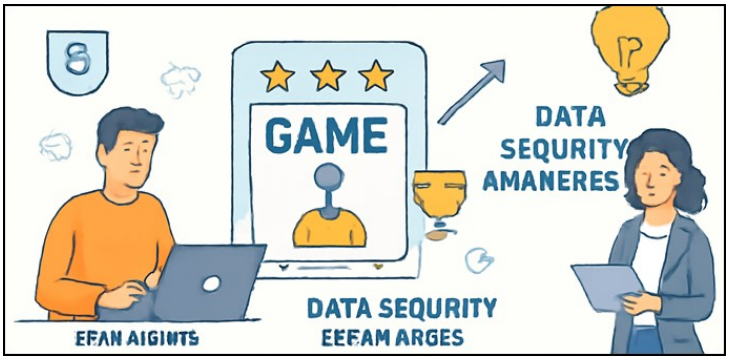

Figure 1
Game-Based Learning for Enhancing Data Security Awareness in Tech Employees

[@] *E-mail:* gyatin33@gmail.com

procedures [2, 3]. Game-Based Learning (GBL), on the other hand, has become a hopeful answer because it teaches difficult topics, like hacking, in a fun and dynamic way. Through game features like tasks, situations, and role-playing, GBL lets people learn in a realistic setting where they can practice security rules and behaviours that they would use in real life [4, 5]. Figure 1 shows interactive learning approach to improve data security awareness in employees.

This method not only helps people remember what they've learnt, but it also gets them involved with the material, which raises understanding about data security overall [6]. This article suggests a GBL framework that is specifically designed for the needs of people who work in the tech industry. It incorporates safety ideas into the game rules to create a safer workplace environment [7, 8, 9].

2. Method Work

2.1. *Selection of participants*

Employees from a wide range of tech businesses will be taking part, making sure that all jobs are represented. People with different levels of hacking knowledge will be given more weight during the choosing process [10, 11].

Total participants (N) = Number of employees selected from various tech companies.

$$N = N1 + N2 + N3 + \ldots + Nk$$

where N1, N2, ..., Nk represent the number of participants from different job roles.

Weightage of cybersecurity knowledge (W) = Weight assigned based on employee's experience with cybersecurity.

$$W = \frac{E}{T} \tag{1}$$

where E is the employee's experience in years and T is the total years of experience in the selected participant pool.

Employee categories: Divide participants into categories based on their cybersecurity expertise: C1, C2, C3, where:

C1: Beginner, C2: Intermediate, C3: Advanced

Number of participants per category:

$$N_{C1} = \frac{N}{3}, N_{C2} = \frac{N}{3}, N_{C3} = \frac{N}{3} \tag{2}$$

Selection probability for each category:

$$P(C1) = \frac{N_{C1}}{N}, P(C2) = \frac{N_{C2}}{N}, P(C3) = \frac{N_{C3}}{N} \tag{3}$$

Balanced representation check: Ensure no category exceeds more than 10% of the total number:

$$|N_{C1} - N_{C2}| < 0.1N \tag{4}$$

Skill assessment score (S) for each participant, based on a standardized test:

$$Si = \Sigma Xj \tag{5}$$

where Xj represents the score in different cybersecurity areas, and m is the number of assessment categories.

Participant qualification: Select participants with a score greater than a threshold (S_threshold):

$$Si \geq S_{threshold}$$

Final participant selection:

$$N_{selected} = \Sigma\, 1(Si \geq S_{threshold}) \quad (6)$$

where 1 is the indicator function.

Participant distribution by job roles (J):

$$\boldsymbol{J} = \{\boldsymbol{J1}, \boldsymbol{J2}, \ldots, \boldsymbol{Jm}\} \quad (7)$$

where J1, J2, ..., Jm represent various job roles, such as Developers, Analysts, etc.

Job role balance check:

$$\left| N_{Ji} - N_{Jj} \right| < 0.1N$$

where Ji, Jj are two different job roles.

2.2. *Game design framework*

There will be tasks, role-playing, exercises, and scenes in the game, all of which are meant to be like real-life hacking situations [12]. These parts are meant to get workers involved in making decisions and help them get better at solving problems [13, 14].

Game levels (L) = Different stages in the game to represent varying difficulty.

$$L = L1, L2, \ldots, Lk$$

Scenario creation (S) for each game level, with m predefined real-world security challenges:

$$S = \{S1, S2, \ldots, Sm\}$$

where each scenario involves a different cybersecurity problem (e.g., phishing, malware).

Challenge difficulty (D) for each scenario:

$$D(Si) = \frac{C(Si)}{T(Si)} \quad (8)$$

where C(Si) is the complexity factor and T(Si) is the time required to solve the challenge.

Role-play interactions: Define roles as R for participants:

$$R = \{R1, R2, \ldots, Rn\}$$

where each Ri represents a role like "Security Analyst," "Attacker," etc.

Simulation length (T_sim) for each role-play event:

$$T_{sim} = T_{start} - T_{end} \quad (9)$$

Reward system (W_reward) based on performance:

$$W_{reward(P)} = Points\ earned = \Sigma\, R(Si) \quad (10)$$

where R(Si) is the reward points for successfully completing a challenge.

Feedback mechanism (F): Immediate feedback is given after each task completion:

$$F = \frac{T_{feedback}}{T_{task}}$$

where T_feedback is time spent providing feedback, and T_task is the time to complete a task.

Simulation complexity scaling: As players progress, increase scenario complexity:

$$D(Si+1) > D(Si) \forall\, i \in \{1, 2, \ldots, m-1\} \quad (11)$$

Player's progression rate (P_progress) is calculated based on completed levels:

$$P_{progress} = \frac{Levels\ completed}{Total\ levels} \quad (12)$$

Group performance (G_performance) across roles:

$$G_{performance} = \Sigma\, P_{progress(Ri)} \quad (13)$$

Scenario-based learning efficiency (E_learning):

$$E_{learning} = \Sigma \frac{W_{reward(Pi)}}{T_{total}} \quad (14)$$

where T_total is the total time spent on simulations.

3. Proposed Game-Based Learning Framework

3.1. *Core elements of the GBL model*

The GBL model will have clear rules, data in real time, and benefits to help people stay on track. These parts keep people interested, help them remember what they've learnt, and encourage them to follow security procedures.

$$R = \{R1, R2, \ldots, Rn\}$$

where R1, R2, ..., Rn are individual game rules.

Player's current level (Lp): The current game level of a player.

$$Lp = \{L1, L2, L3, \ldots, Lk\}$$

where L1 is the basic level and Lk is the highest level.

Time spent on task (T_task): Time taken by the player to complete each task.

$$T_{task} = Tend - Tstart$$

where Tend and Tstart are the end and start times, respectively.

Feedback function (F_feedback): Function for providing feedback to players after each task.

$$F_{feedback(P)} = \frac{T_{feedback}}{T_{task}} \quad (15)$$

where T_feedback is the time taken for providing feedback.

Rewards system (W_reward): Points or rewards earned based on task completion.

$$W_{reward(P)} = \Sigma\, R(Si) \quad (16)$$

where R(Si) represents reward points for completing a task Si.

Player's progress rate (P_progress) is calculated based on completed tasks:

$$P_{progress} = \frac{Completed\ Tasks}{Total\ Tasks} \quad (17)$$

Progression rules (P_progression): Rules that define progression between game levels.

$$P_{progression(Lp)} = \frac{Tasks\ Completed}{Tasks\ Required\ to\ Advance} \quad (18)$$

Difficulty scaling (D_scale): Difficulty adjustment for each level based on player progress.

$$D_{scale(Lp)} = f\left(P_{progress(Lp)}\right) \quad (19)$$

where f is a scaling function based on player progression.

Motivation function (M_motivation): Motivation based on player engagement.

$$M_{motivation(Lp)} = \Sigma\, W_{reward(Pi)} \quad (20)$$

where W_reward(Pi) represents reward points for completing tasks.

Time per task ratio (T_task ratio) is the average time spent per task across levels:

$$T_{task}ratio = \Sigma \frac{T_{task(Lp)}}{k} \quad (21)$$

Player's feedback reception (F_reception): Measure of how well the player receives feedback.

$$F_{reception} = \frac{T_{feedback}}{T_{task}} \quad (22)$$

4. Result and analysis

Table 1 shows the rates of employee involvement and finish for each game level. 92% of people who started the Basic level finished it, and it took them an average of 20 minutes to do so.

Table 1

Employee Engagement and Completion Rates

Game Level	Number of Participants	Completion Rate (%)	Average Engagement Time (Minutes)
Basic	50	92	20
Intermediate	50	85	25
Advanced	50	78	30

The success rate went down a little to 85% at the Intermediate level, but the amount of time spent on the task went up to 25 minutes.

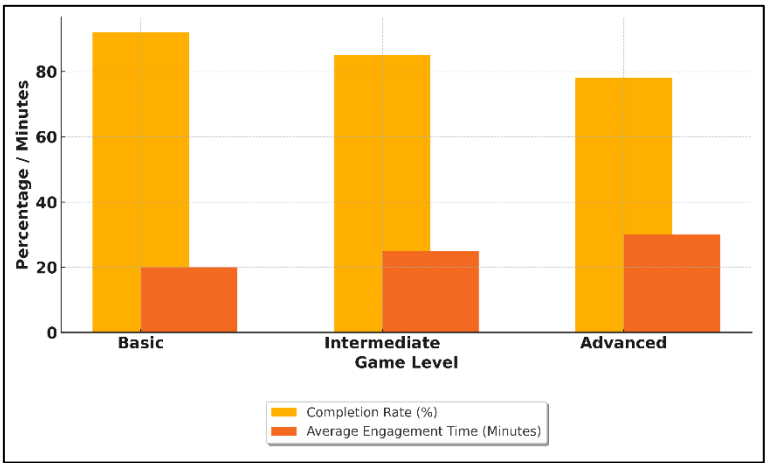

Figure 2

Game Level Performance: Completion Rate vs. Engagement Time

Only 78% of people who started the Advanced level finished it, and it took them an average of 30 minutes to do so (illustrate in Figure 2). These results show that people are getting more interested in harder levels, but the number of people who finish them is slightly going down.

5. Conclusion

Using Game-Based Learning (GBL) methods is a fun and active way to make tech workers more aware of data security. By using real-life hacking tasks, situations, and engaging parts, GBL encourages active learning and helps students remember what they've learnt. Feedback, awards, and role-playing all work together to keep workers inspired to follow best practices and stay alert to new threats. This framework gives organizations a complete way to create a culture that cares about security, which will eventually lower their risks and make their total data protection stronger.

References

[1] T. Balon and I. Baggili, "Cyber competitions: A survey of competitions, tools, and systems to support cybersecurity education," *Educ. Inf. Technol.*, vol. 28, pp. 11759–11791 (2023).

[2] I. Corradini, "Building a cybersecurity culture," in Building a Cybersecurity Culture in Organizations: How to Bridge the Gap Between People and Digital Technology. Berlin, Germany: Springer International Publishing, pp. 63–86 (2020).

[3] F. Di Nocera, G. Tempestini, and F. Presaghi, "Reliability and validity of the cybersecurity awareness inventory (CAIN)," *Behav. Inf. Technol.*, pp. 1–12 (2024).

[4] D. Gaurav, Y. Kaushik, S. Supraja, M. Yadav, M. P. Gupta, and M. Chaturvedi, "Empirical study of adaptive serious games in enhancing learning outcome," *Int. J. Serious Games*, vol. 9, pp. 27–42 (2022).

[5] S. Hart, A. Margheri, F. Paci, and V. Sassone, "Riskio: A serious game for cyber security awareness and education," *Comput. Secur.,* vol. 95, Art. no. 101827 (2020).

[6] W. He, I. Ash, M. Anwar, L. Li, X. Yuan, L. Xu, and X. Tian, "Improving employees' intellectual capacity for cybersecurity through evidence-based malware training," *J. Intellect. Cap.,* vol. 21, pp. 203–213 (2020).

[7] B. K. Payne, W. He, C. Wang, D. E. Wittkower, and H. Wu, "Cybersecurity, technology, and society: Developing an interdisciplinary, open, general education cybersecurity course," *J. Inf. Syst. Educ.*, vol. 32, pp. 1334 (2021).

[8] J. Pruemmer, T. van Steen, and B. van den Berg, "A systematic review of current cybersecurity training methods," *Comput. Secur.*, vol. 136, Art. no. 103585 (2023).

[9] S. V. Shinde, T. Shitole, S. Mundhe, S. Kalamkar, and V. Rajput, "Exploration of recommendation system for service discovery," *Int. J. Adv. Comput. Theory Eng.*, vol. 14, no. 1, pp. 11–15 (Apr. 2025).

[10] V. Švábenský, P. Čeleda, J. Vykopal, and S. Brišáková, "Cybersecurity knowledge and skills taught in capture the flag challenges," *Comput. Secur.*, vol. 102, Art. no. 102154 (2021).

[11] G. Tempestini, E. Rovira, A. Pyke, and F. Di Nocera, "The cybersecurity awareness inventory (CAIN): Early phases of development of a tool for assessing cybersecurity knowledge based on the ISO/IEC 27032," *J. Cybersecur. Priv.,* vol. 3, pp. 61–75 (2023).

[12] P. Sahane, M. Gulhane, N. Rakesh, S. M. M. Naidu, M. Grover, and V. Mahajan, "Evaluating lightweight encryption schemes for resource-constrained devices in wireless sensor networks," *J. Discrete Math. Sci. Cryptogr.,* vol. 28, no. 5-A, pp. 1803–1812 (2025), doi: 10.47974/JDMSC-2180.

[13] C. D. Kokane, S. D. Babar, P. N. Mahalle, and S. P. Patil, "Word sense disambiguation: Mathematical modelling of adaptive word embedding technique for word vector," *J. Interdiscip. Math.,* vol. 26, no. 3, pp. 475–482 (2023).

[14] S. Yadav, R. Sharma, A. Dabas, C. Arora, G. Mitra, A. Aggarwal, A. Rehalia, S. Sanyal, and M. Arora, "Improved security in credit cards via duplicitous contract detection," *J. Inf. Optim. Sci.,* vol. 46, no. 1, pp. 75–79 (2025), doi: 10.47974/JIOS-185.

Received April, 2025