FORTRA™

GUIDE (TERRANOVA SECURITY)

Gamification for Cyber Security Awareness Training Success

Reducing the Human Risk in Cyber Threats

TABLE OF CONTENTS

SUMMARY

Corporate cyber security awareness training needs to change. Employees are busy, managing multiple deliverables and have minimal desire to participate in corporate training sessions.

Gamification gives employees relatable, engaging, motivating, and interesting training. When used as part of corporate cyber security awareness program that uses proven training methodologies grounded in science – gamification takes learning to the next level.

Companies cannot afford to hope that their cyber security awareness training is working. Measurable results, employee monitoring, and reactive training modules give security awareness leaders the real facts on training success.

Humans want to trust each other. It is natural to believe that no one would set out to purposefully steal, deceive, or trick – that inherently, everyone is good.

However, this unfortunately is very far from reality. The biggest threat to cyber security is human.

Malicious emails, texts, voicemails, and other phishing attacks costs a company on average, $1.1 million.

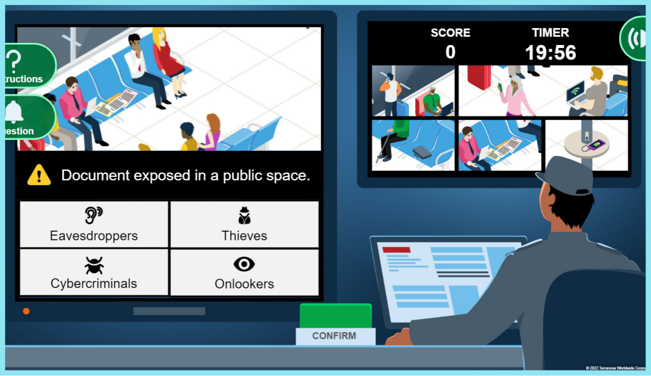
People are the biggest risk factor companies have when it comes to cyber security threats. But these same people are a powerful corporate asset in defense of cyber security threats.

People-centric training enables companies to develop a proven cyber security culture that is alert to cyber criminals using savvy social engineering techniques to steal, trick, and deceive.

The human desire to trust is always there, but with a greater understanding of how cyber criminals work, people become empowered to protect themselves and their organization.

One of the challenges is that compliance and security awareness training can often come off as being serious and dry. The content might be perfect, but people just aren't engaging with the training. Deep down, most people still believe that "it couldn't happen".

Enter gamification.

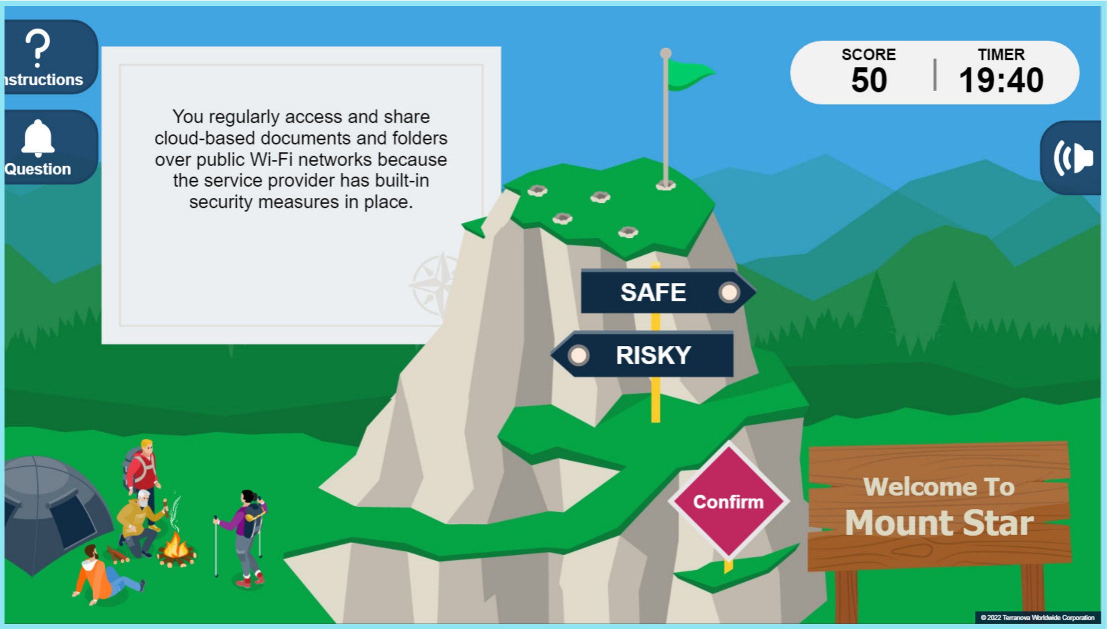


Document exposed in a public space.

Cyber Challenge - Traveling Securely

Malicious emails, texts, voicemails, and other phishing attacks costs a company on average

$1.1 million



You regularly access and share cloud-based documents and folders over public Wi-Fi networks because the service provider has built-in security measures in place.

Cyber Challenge - Cloud Services

Motivating and Engaging with Gamification

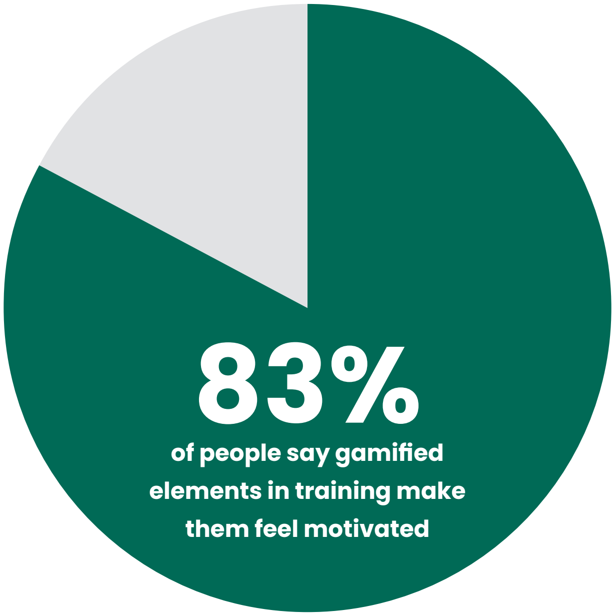
Gartner defines gamification as:

Gamification is the use of game mechanics to drive engagement in non-game business scenarios and to change behaviors in a target audience to achieve business outcomes. Many types of games include game mechanics such as points, challenges, leaderboards, rules and incentives that make game-play enjoyable. Gamification applies these to motivate the audience to higher and more meaningful levels of engagement. Humans are "hard-wired" to enjoy games and have a natural tendency to interact more deeply in activities that are framed in a game construct.This approach to cyber security training and awareness is powerful. People are engaged, interested, and actively motivated to keep learning.

Gamification puts people in real-life scenarios that create a direct connection between their actions and how they impact the security of their colleagues and organization.

When gamification is used as part of a cyber security awareness training program, people see first-hand the relevancy and applicability of what they're learning in their daily lives.

- 83% of people say gamified elements in training make them feel motivated
- Boredom levels with training drops to 10%
- 33% of people want more game-like effects in their training courses

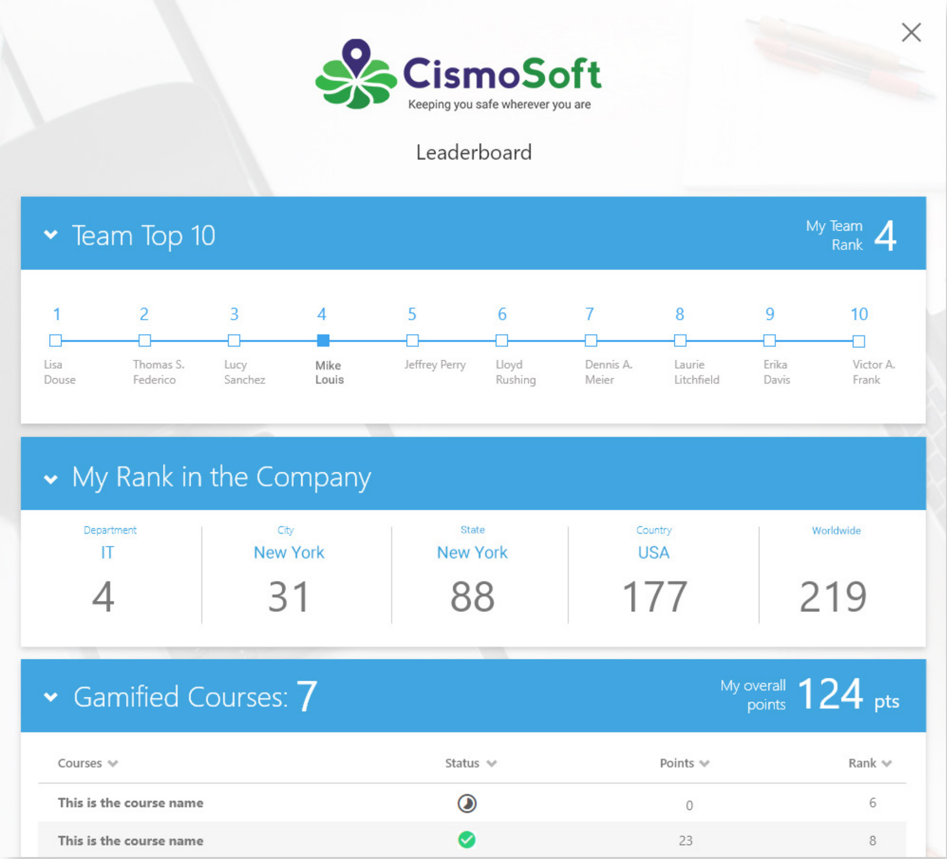


Gamification Supports Actionable Learning

People learn by doing. They want to do something, try something, test something. They want to win and see their results. Gamification of cyber security training allows them to do just that.

People are motivated by seeing their success, earning badges, solving problems, and seeing their names on the top of the cyber security leaderboard. Actionable and engaging learning gets employees talking about the training challenges, comparing results, and discussing what they're learning.

Example of a gamified leaderboard on the Terranova Security Awareness Platform



CismoSoft
Keeping you safe wherever you are

Leaderboard

Team Top 10 — My Team Rank 4

1	2	3	4	5	6	7	8	9	10
Lisa Douse	Thomas S. Federico	Lucy Sanchez	Mike Louis	Jeffrey Perry	Lloyd Rushing	Dennis A. Meier	Laurie Litchfield	Erika Davis	Victor A. Frank

My Rank in the Company

Department IT	City New York	State New York	Country USA	Worldwide
4	31	88	177	219

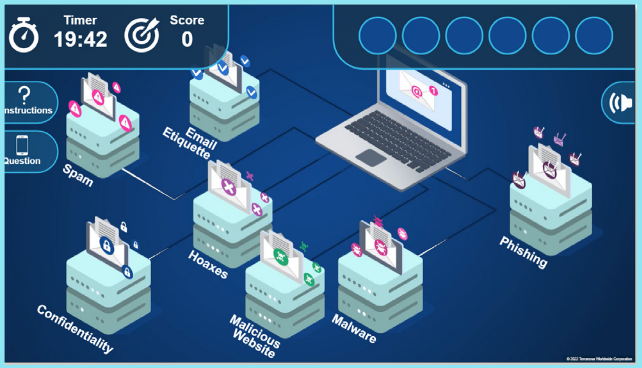
Gamified Courses: 7 — My overall points 124 pts

Courses	Status	Points	Rank
This is the course name	◔	0	6
This is the course name	✓	23	8

Gamification points are earned by the user based on responses during the training and added to the SCORM tracking information. As each points-based activity is completed, points are accumulated and displayed on the leaderboard.

The trickle-down impact of gamification in cyber security training is the development and fostering of a cyber security aware culture. People know the real risks of phishing, malware, BEC, and other cyber threats. Employees understand how their proactive actions against cyber threats can protect their colleagues, organization, and themselves.

However, it is not enough to simply add interactive graphics or to award badges for completing the training.



Cyber Challenge - Email

Real-World Impacts of Social Engineering

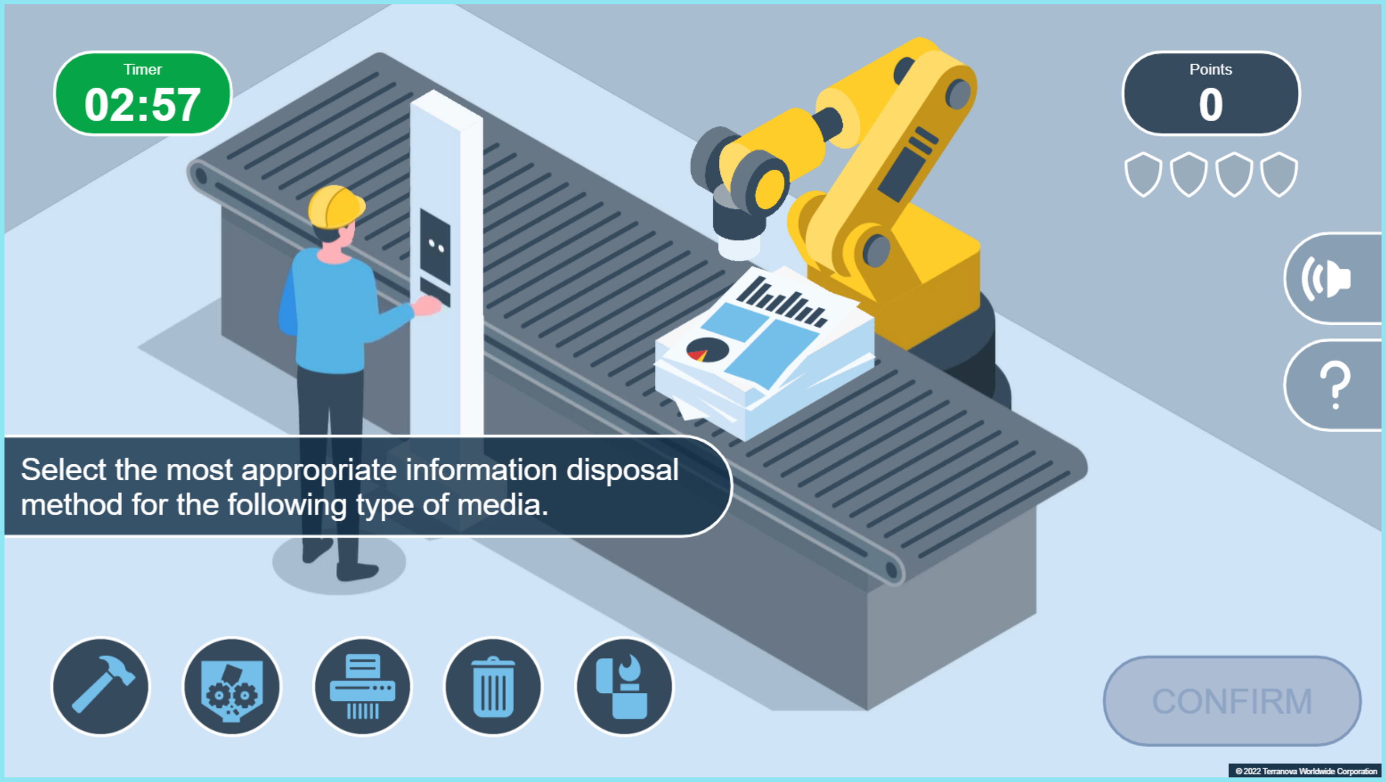
People need an emotional connection to the training and what they're doing. They need to internalize the realities of not reading an email carefully, not scrutinizing the sender's email address closely, or not questioning an email requesting them to urgently transfer funds.

To do this effectively, gamification must be part of a broader cyber security awareness platform. It's critical that a security awareness platform provides a range of training types including modular courses, phishing simulation tools, microlearnings, gamification, and corporate communication tools.

This coupled with the ability to monitor employee training success rates, engagement levels, and areas for improvement and additional cyber security awareness training – enables actionable learning.

People are motivated by feedback. And this is exactly what gamification does – it gives leaders and employees instant feedback on engagement rates, success levels, and areas for improvement.

> **People are motivated by feedback. And this is exactly what gamification does – it gives leaders and employees instant feedback on engagement rates, success levels, and areas for improvement.**



Select the most appropriate information disposal method for the following type of media.

Cyber Challenge - Information Lifecycle

Why Gamification?

Gamification engages employees with cyber security awareness training. The risks of disengaged employees are too high for any organization to absorb.

Training approaches that include slides, lunch and learns, or corporate emails do not work. Past experience tells employees that these are boring and not relevant to them.

Gamification changes the learning paradigm by showing people that yes, they are at risk for cyber attacks and that they need to know how to protect themselves and the organization.

Gamification delivers:

1. Engagement

When gamification is used effectively, it gives people a purpose. They understand why they're doing the training and can feel proud about their success rate

2. Behavioral Change

The key to building a cyber secure culture is with behavioral change. When employees understand how their actions impact the organization, they are more likely to learn and change.

3. Instant Feedback

People are motivated by success. When they can work through a cyber security challenge and score top points, they feel empowered and encouraged to do more learning. Gamification enables employees to feel confident about their cyber security knowledge and to engage in advanced learning and cyber hero roles.

4. Knowledge Retention

People learn by doing and by repetition. Savvy gamification techniques reinforce key messages in different formats, resulting in intrinsic learning. Research shows that the retention rate for actively engaging training is 75%, compared to 20% in traditional passive learning approaches.

5. Safe Learning Environment

Within a gamification training environment, the consequences of downloading an attachment or responding to a phishing email are not severe. People get first-hand lessons on how their decision affects them and others – with zero negative impacts. The key is in giving employees the opportunity to redo the training challenge, thereby letting them directly apply the lessons they learned in a safe environment.

It is not easy to get employees to care about cyber security. Companies need to think beyond traditional training methodologies and use modern approaches that are relatable, interesting, and effective.

Five Key Questions To Ask About Gamification and Cyber Security Awareness Training

When reviewing cyber security awareness training options, leaders and decision-makers must ask these five questions before making a decision:

1. Are there rules?

Rules keep people in check and guide decision-making. Ensure there is the freedom to set rules about what the training needs to achieve. Once these rules or goals are defined, the gamified training has both purpose and value. Keep the rules simple, making it easy for employees to focus on learning.

2. How does it support behavioral change?

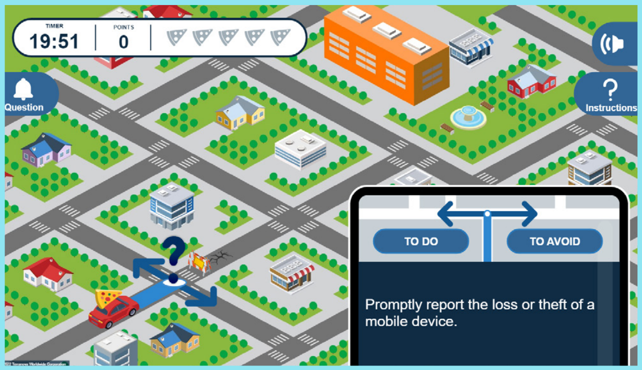
Training that rewards people with points, badges, leaderboard ranking, or real prizes helps drive behavioral change. Science proves that winning creates a dopamine or feel-good effect in the brain, encouraging people to want to achieve more. Progress happens and people begin to practice the behavior they were rewarded for during training.

3. Is it flexible and customizable?

No two organizations are the same. Cookie-cutter training does not work. Ensure that gamification features can be modified as employee needs change. Additionally, points scoring is unique to each corporate culture – some employees might respond better to private scoring rather than a shared social leaderboard. Corporate leaders and decision-makers must retain control over how the training fits into the culture and overall goals.

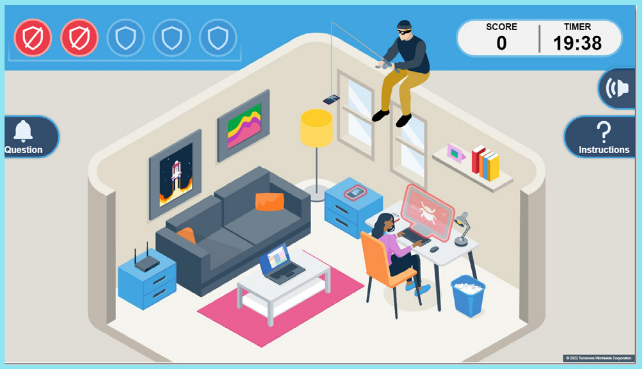
4. Is the training active or passive?

Human error and inattention are to blame for the bulk of cyber security attacks. Companies cannot afford to let



Promptly report the loss or theft of a mobile device.

Cyber Challenge – Mobile Devices



Cyber Challenge - Protecting Your Home Office

Why Gamification?

Gamification engages employees with cyber security awareness training. The risks of disengaged employees are too high for any organization to absorb.

Training approaches that include slides, lunch and learns, or corporate emails do not work. Past experience tells employees that these are boring and not relevant to them.

Gamification changes the learning paradigm by showing people that yes, they are at risk for cyber attacks and that they need to know how to protect themselves and the organization.

Gamification delivers:

1. Engagement

When gamification is used effectively, it gives people a purpose. They understand why they're doing the training and can feel proud about their success rate

2. Behavioral Change

The key to building a cyber secure culture is with behavioral change. When employees understand how their actions impact the organization, they are more likely to learn and change.

3. Instant Feedback

People are motivated by success. When they can work through a cyber security challenge and score top points, they feel empowered and encouraged to do more learning. Gamification enables employees to feel confident about their cyber security knowledge and to engage in advanced learning and cyber hero roles.

4. Knowledge Retention

People learn by doing and by repetition. Savvy gamification techniques reinforce key messages in different formats, resulting in intrinsic learning. Research shows that the retention rate for actively engaging training is 75%, compared to 20% in traditional passive learning approaches.

5. Safe Learning Environment

Within a gamification training environment, the consequences of downloading an attachment or responding to a phishing email are not severe. People get first-hand lessons on how their decision affects them and others – with zero negative impacts. The key is in giving employees the opportunity to redo the training challenge, thereby letting them directly apply the lessons they learned in a safe environment.

References

https://www.techrepublic.com/article/cyberattacks-now-cost-businesses-an-average-of-1-1m/

https://www.gartner.com/it-glossary/gamification-2

https://elearningart.com/blog/gamification-tips-karl-kapp/

https://www.talentlms.com/blog/gamification-survey-results/

https://www.educationcorner.com/the-learning-pyramid.html

Learn how people-centric security awareness continues to train millions of cyber heroes, change behavior and instill security culture globally

REQUEST DEMO

FORTRA™

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.

© Fortra, LLC and its group of companies. All trademarks and registered trademarks are the property of their respective owners.