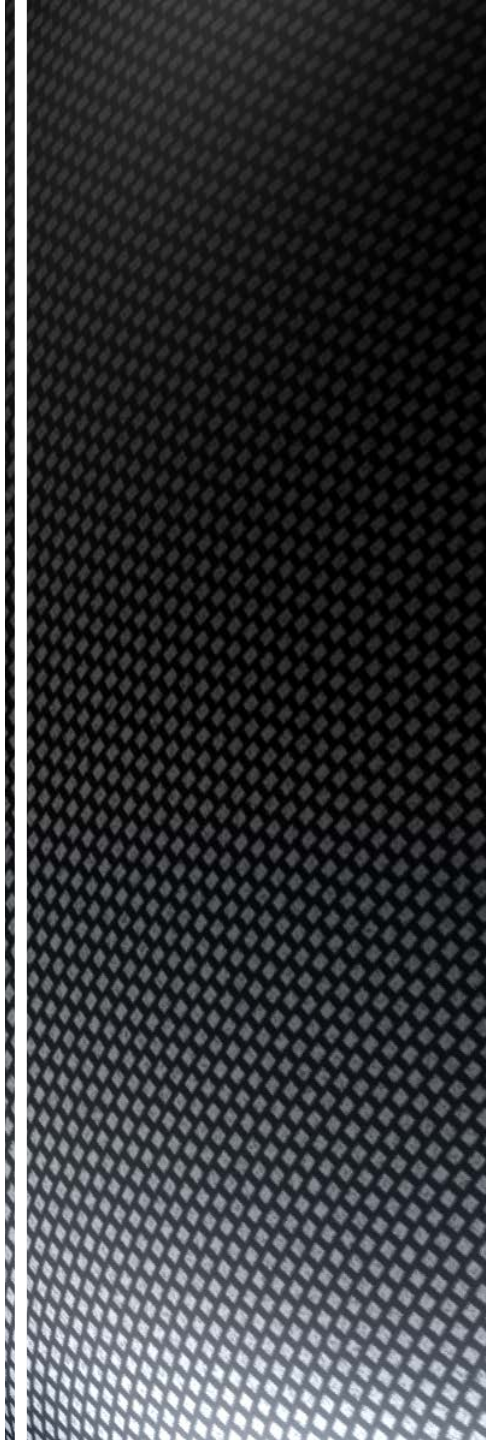
Cyber Awareness Challenge

Entry for FISSEA Security Awareness, Training, & Education Contest 2013

Submitted by DISA, SAIC, and Carney, Inc.



The Cyber Awareness Challenge is a serious game that simulates the decisions DoD and Federal government information systems' learners make every day as they perform their work. Players work to thwart and capture an unnamed hacker who is targeting government information systems in order to access sensitive government information.

In this serious game, developed for all authorized users of DoD and Federal systems, instructional topics for information assurance awareness are presented through rich media first-person simulations and mini-games that allow the player to practice and review information assurance concepts in an interactive manner. The principles and practices of game design are balanced with a comprehensive approach to full Section 508 compliance, and delivery through the web, CD-ROM, or any SCORM-conformant learning management system.

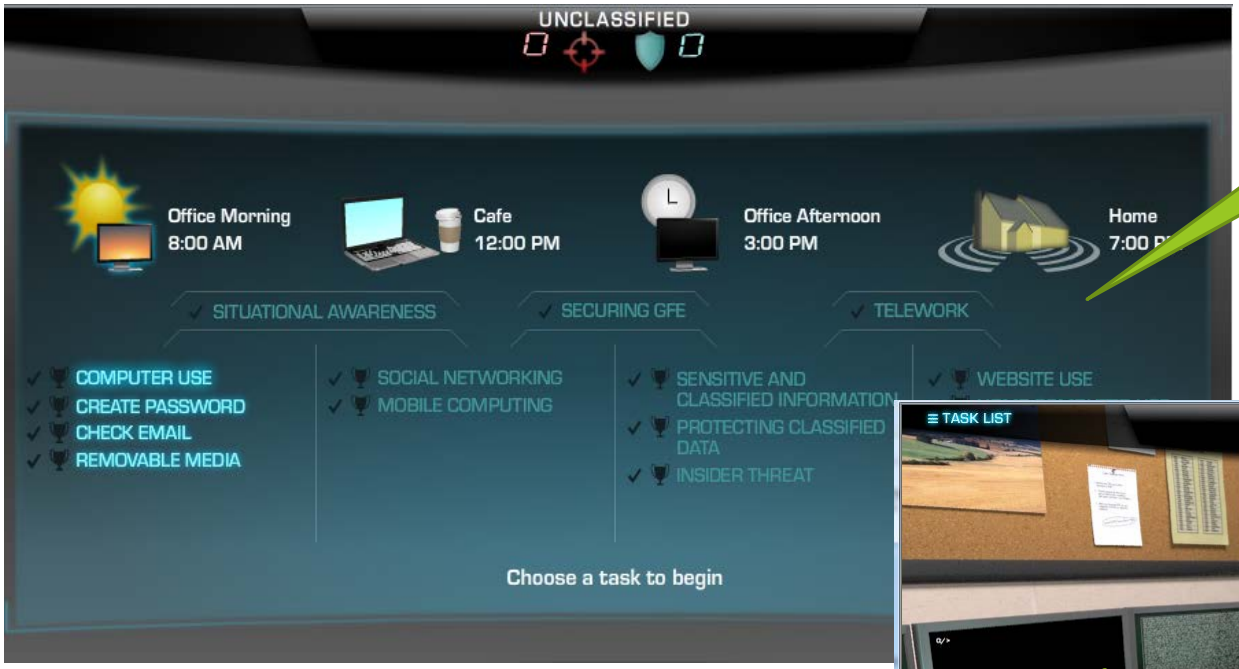
In the Introduction, players are welcomed to their new office and the game storyline is explained. Rich 3D graphics bring to life the environment.

Important Section 508 features include closed captioning, audio descriptions, and logical tabbing and reading order for on-screen components.

The Introduction also introduces persistent characters: the unnamed adversary and Jeff, the IT security specialist. Players receive positive or negative progress updates from Jeff throughout the game based on their performance.

The player's learning is measured through the completion of the series of tasks structured around a "typical workday" that make up the game. These tasks are divided into four groupings by time of day and environment and cover all information assurance content required and approved by DISA.

For each task, the learner completes some combination of activities made up of either a simulation or a mini-game. In simulations, the learners are presented with a scenario in which they must select the best course of action to protect information systems and sensitive information. In mini-games, learners apply information assurance concepts in a fun and interactive context.

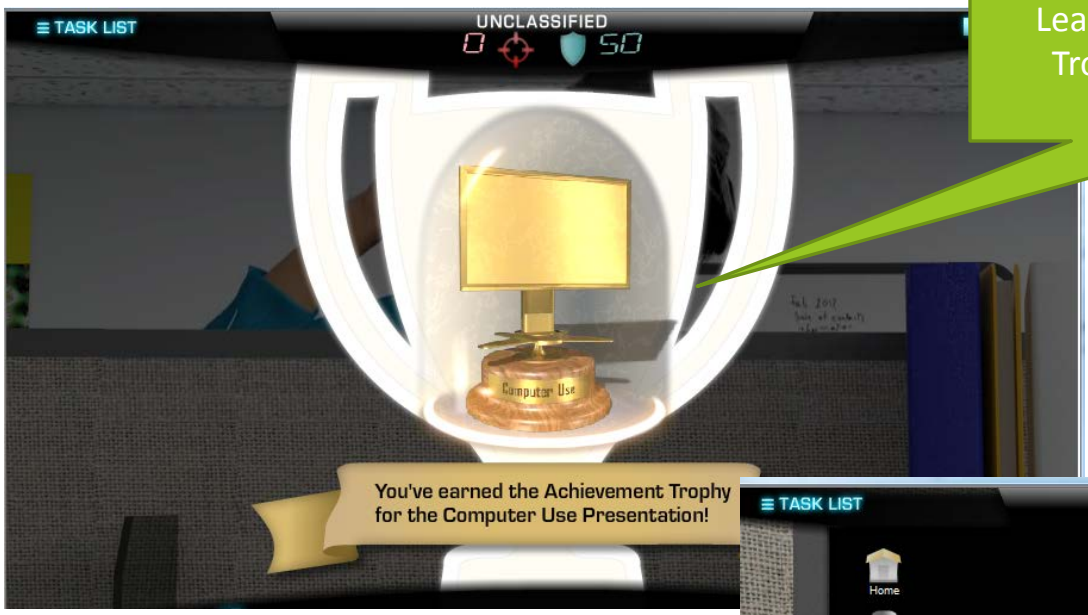


Learner's Task List

At each transition between task groupings, learners receive updates from Jeff. If learners have more points than the adversary, the updates are positive. If not, they are negative. Jeff offers encouragement throughout to keep learners motivated and engaged.

The primary incentive in the game is for learners to finish with more points than the adversary so that he is captured. Learners earn points by taking the correct action in simulations or by scoring points in a mini-game. If learners take actions that would jeopardize information security, the adversary earns points.

The game includes a secondary incentive in the form of “achievements,” or trophies which learners collect for performing tasks flawlessly.



Learners can earn Achievement Trophies for performing tasks flawlessly.

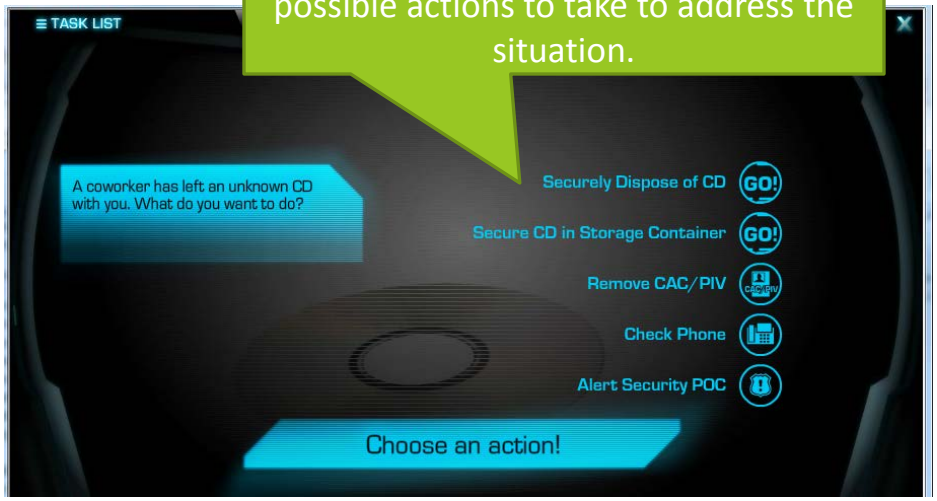
Learners have persistent access to their score vs. the adversary’s score to ensure motivation to perform well.

In many interactions, there may be a range of correct or incorrect options. In these interactions, learners earn more points for selecting the optimally correct response than a less optimal, but still correct response. Interactions are also weighted as to the impact player choices may have. Learners earn the most points for selecting the optimally correct response in situations in which the impact of the decision is high.

This scoring schema accounts for the nuanced and complex decision-making required in the Challenge and in the workplace. This approach rewards those who analyze a situation and make the best decision possible, while not punishing those who may have missed a small detail, leading them to select a technically correct, if not optimal, response.

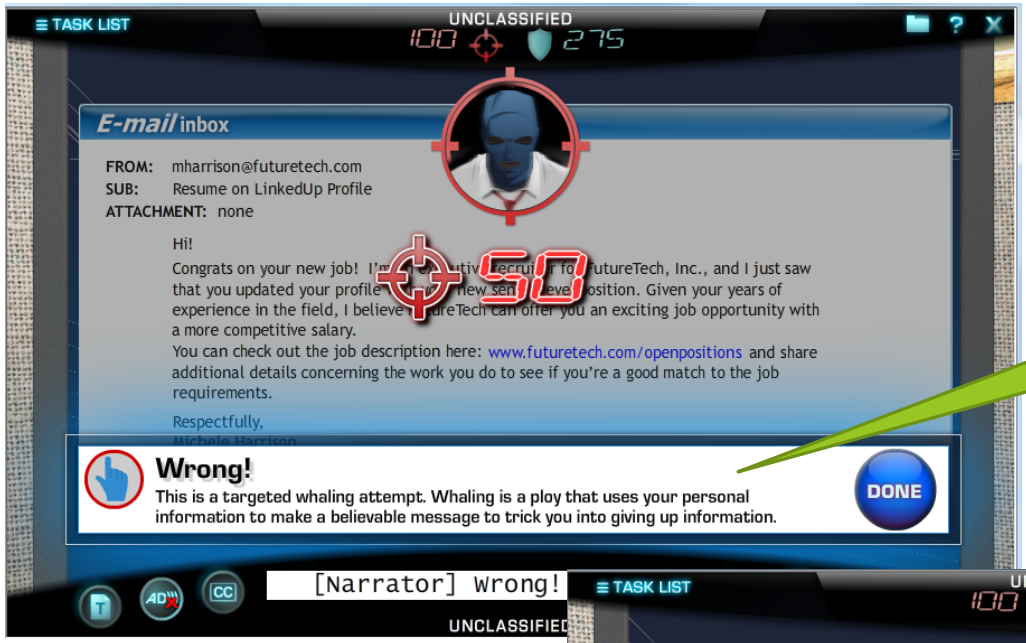
Sample Simulation: Learner is approached by a coworker in their office asking about unknown removable media (CD Rom)

The learner is then given a range of possible actions to take to address the situation.

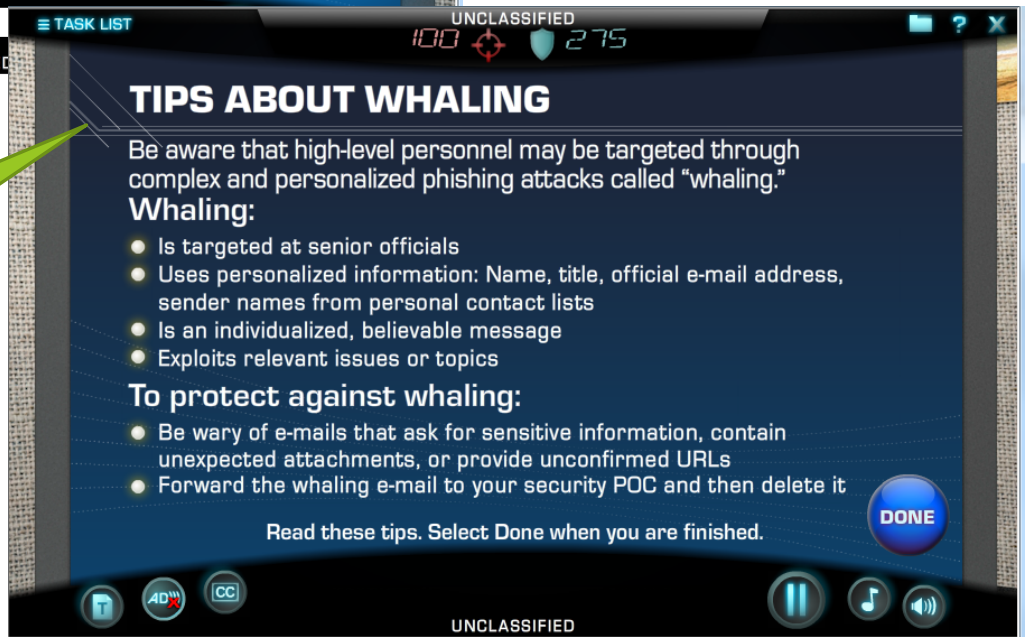


Learners receive feedback on their choices that explains why their action was correct or incorrect. This ensures they have a full grasp of the situation and understand the optimally correct response.

Each simulation and mini-game also includes periodic helpful tips about the given security topic.



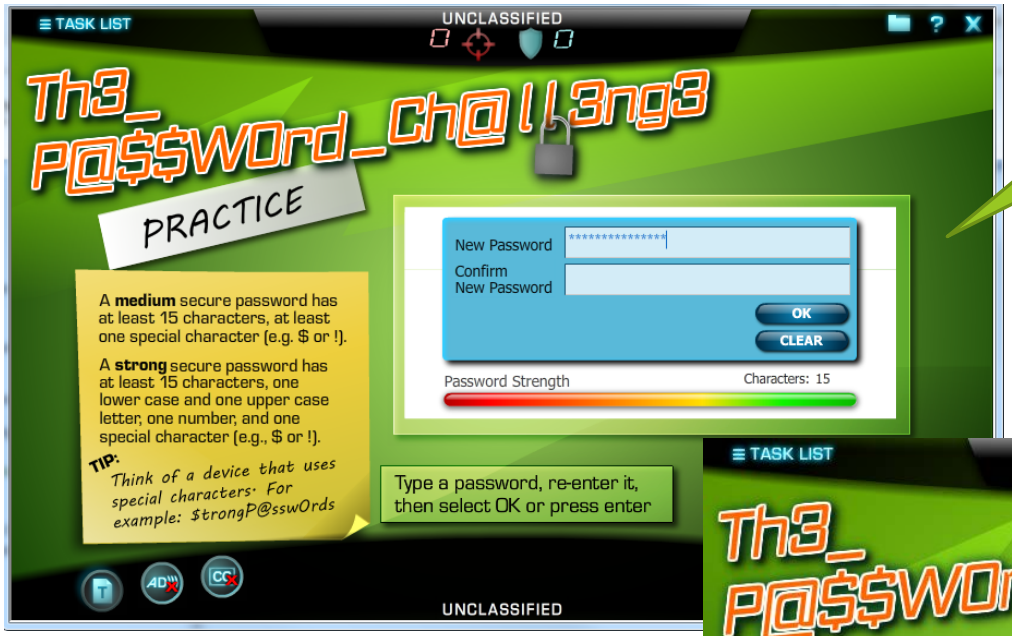
Sample learner feedback after making an incorrect choice. The adversary has earned points as a result of the incorrect action.



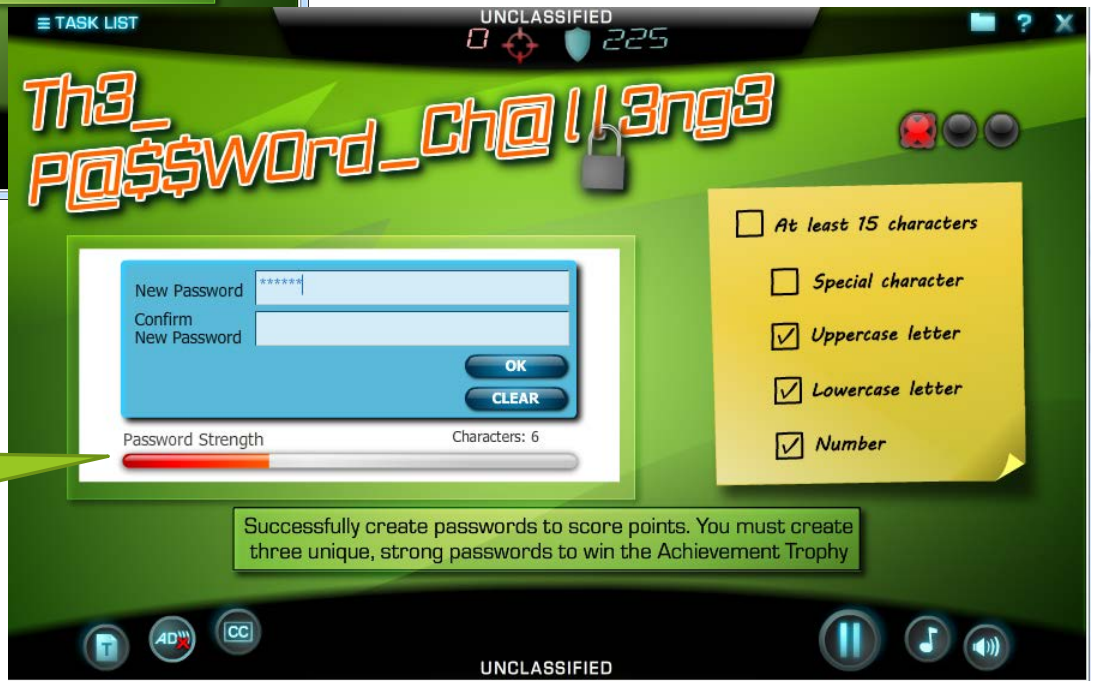
Helpful tips are provided throughout Cyber Awareness Challenge to ensure the learner ultimately receives appropriate guidance regardless of their performance in the task.

In this sample mini-game, The Password Challenge, learners must create a strong password according to provided guidelines. When learners first initiate the task, a Practice screen appears, providing the guidelines for creating a strong password and giving users an opportunity to practice playing the game before being scored.

In this mini-game, learners have five opportunities to create three unique strong passwords. If learners enter three strong passwords successfully with no mistakes, the Password Game Trophy is awarded.



Each mini-game includes an unscored "practice round" that learners can use to ensure they understand the rules and game play.



Learners are provided feedback as they play via the checklist on the right and the password strength indicator bar.

In this sample mini-game, “In-Boxing,” the learner controls one robot and the adversary controls the other. In the game, learners read nine e-mails, displayed in random order, and determine whether they are legitimate e-mails or scams.

After learners have responded to each e-mail, individualized feedback appears and either the learner or the adversary is awarded points based on the player’s response. At that time, either the learner or the adversary robot strikes a blow, based on whether the learner responded correctly to the e-mail. The first player to land five blows wins the “In-Boxing” match.

Learners have a range of actions to take: open the email, alert their security POC, delete the email, or click on the attachment within the email.

When the learner has completed all of the tasks in the Cyber Awareness Challenge, a conclusion to the storyline plays. If the learner has scored more total points than the adversary, a positive resolution occurs in which the adversary is captured. If the adversary has scored more points, the learner is notified that the adversary has escaped. In either possible concluding scenario, the learner is encouraged to go back to the task list and re-play the simulations and mini-games to improve their overall score.

Based on learner performance, in the Conclusion Scenario the adversary is either captured, or he escapes. The learner is encouraged to go back and re-play simulations and mini-games to improve his/her scores.