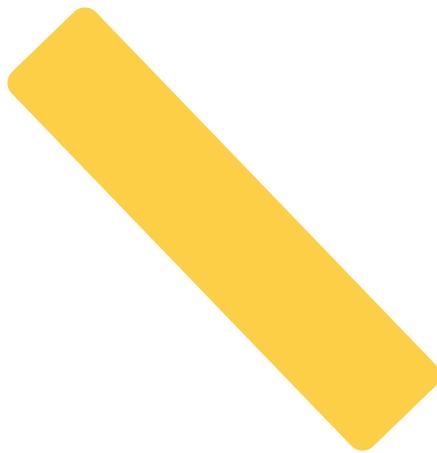
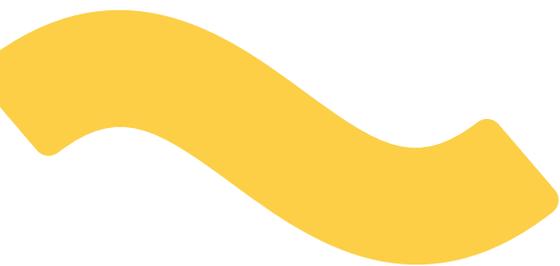
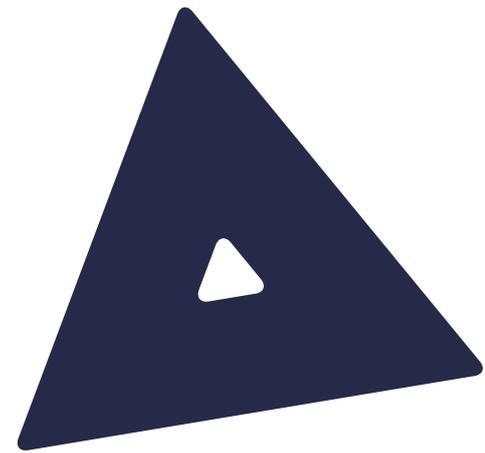
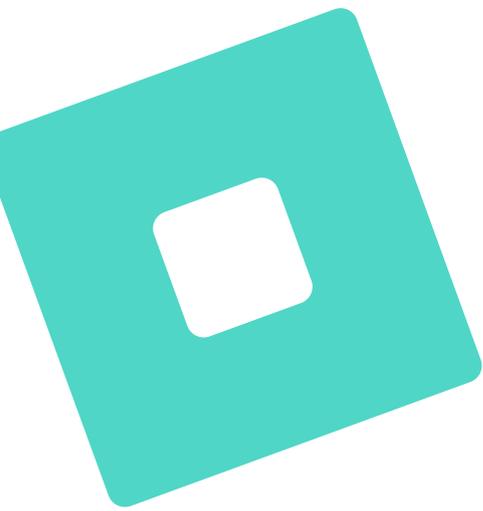


DIGITAL PLUG'N'PLAY LEARNING

IT security



Introduction

Improve the IT security skills with an engaging learning game



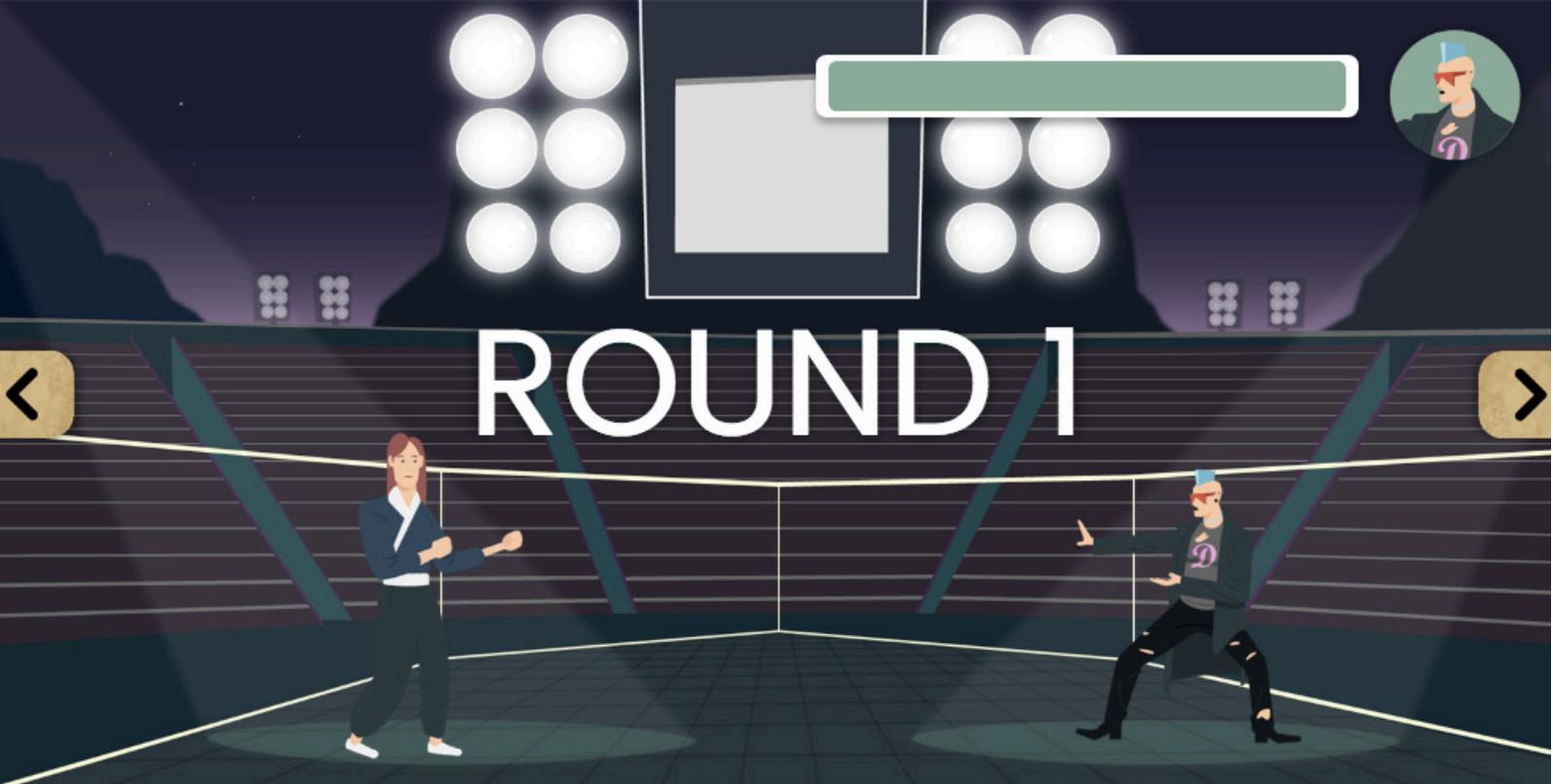
Cyber-attacks knock on the door more and more frequently at big and small companies across the world. The treat has gotten bigger as the increasing digitalization, and at the same time, your company's data is worth far more than ever before.

Your company is no stronger than its weakest link. That's why it's important to identify the company's weaknesses both in regard to the technical setup and also in regard to the employees' behavior and daily use. The biggest safety problems actually stem from the employees' behavior. It can be anything from a forgotten USB stick in the train to receiving an untrustworthy e-mail with a link to an unknown website.

It's easy enough to install a piece of software. However, the employees' behavior is the most difficult aspect of the security to get under control. That's why we have created a learning game about IT security for your employees.

Why

- **IT criminals go directly after employees that's why they have to watch their every step.**
- **To reduce the level of risk by informing the employees.**
- **As the interactive learning game teaches the employees the four most central principals that can prevent the majority of the cyber-attacks.**
- **As the learning game exposes the user to different scenarios that they can explore and fail – without paralyzing the company.**
- **To document the learning and ensure that the employees can identify security treats forward-looking.**



About the game

Shh! Top secret cyber training camp

The cyber police's task force takes your employees to their secret training area high up in an abandoned mountain range. Now the employee will learn cyber self-defense which consists of four principals: strong passwords, reality check, protection of data and devices, and to seek help if it's gone wrong. In the end, their new knowledge is tested in the fighting arena when they have to meet enemies like Device-Dina, Internet-Igor, E-mail-Eric, and Emergency-Eve who are hard-core cybercriminals, each with their field of expertise. Here the employees have to defend themselves when they are attacked through devices, websites, and e-mails. They are also tested in what they would do in an IT security emergency.

25 minutes of ambitious digital learning that is involving, informative, and fun for the employees while it's effective and preventive for your company.

Built by experts

When your employees play to get the black belt in IT security, it's based on learning content that is developed by psychologists, learning specialists and security experts from Open Systems. Together with learning designers, a learning universe has been created that can support the content, anchor the knowledge, and ensure the value of the training in the best possible way.

Practical information

- The game can be adapted to the customer's IT security policy.
- The game can be delivered in all languages.
- The game can be delivered as a SCORM file and can be implemented in all SCORM compatible learning platforms.



Trusted by



“At McDonald’s, we have a motto: ‘Be bold!’ This means having the courage to be brave, to stand out and to find new ways of doing things. I believe that’s what we have done here. This is definitely the most modern example of digital learning I have come across yet.”

Thorbjørn Milling, HR & Training Consultant,
McDonald’s

“It’s the first time I’ve been introduced to digital learning that I really believe in. Furthermore, the team is super inspiring and competent. It’s a real pleasure to work with them!”

Tina Brix Kjelgaard, HR Partner,
Reitan Convenience Denmark A/S

Try the game online. Book a demo at learningbank.dk/en

learningbank 

Copenhagen,
Denmark

learningbank.dk
+45 71 999 123