

Cyber Escape Room

Cyber Security Awareness Plattform



Definition



The **Cyber Escape Room** is derived from the Live Escape Room or **only Escape Room**, in which **small groups** of people are locked together in a physical room and have to leave their prison within **a given time** with the help of hidden clues and objects.

The group has to solve a **main task** with the help of many puzzles **building on each other** within the given time. They are **observed by a person** supervising the action, who intervenes if something wrong is done or the group does not make progress. The players can usually also become active themselves and request clues from the game leader.

Quelle: https://de.wikipedia.org/wiki/Escape_Game

With the Cyber Escape Room, in contrast to the Escape Room, you are in a virtual environment (in the **cyber space**) and the topic also serves as a **security awareness** measure in addition to the **entertainment** and **teambuilding** character.

Motivation

Forbes CommunityVoice Connecting expert communities to the Forbes audience. What is This?

2,278 views | Oct 4, 2017, 08:00am

Why You Should Gamify Your Cybersecurity Training

 **Stephen Baer** CommunityVoice
Forbes Agency Council CommunityVoice ⓘ

POST WRITTEN BY
Stephen Baer

Head of Creative Strategy and Innovation at [The Game Agency](#) and The Training Arcade, creating solutions that educate and activate audiences.



Shutterstock

Cyber security is more than just technology. In more than **30%** of security incidents, the attack begins with an error caused by humans (e.g. programming-error or a misconfiguration).

Various regulators have recognized this and placed an increased focus on compliance with awareness measures.

The Cyber Escape Room can quickly motivate people through the principle of **storytelling** and captivate them with fun in the topic area.

Through the existing descriptions, it is for the acting persons no problem to bring themselves independently closer to the solution and to obtain own success experiences. Due to the implemented vulnerabilities respectively security holes, it is possible to understand the most important attacks in a very short time

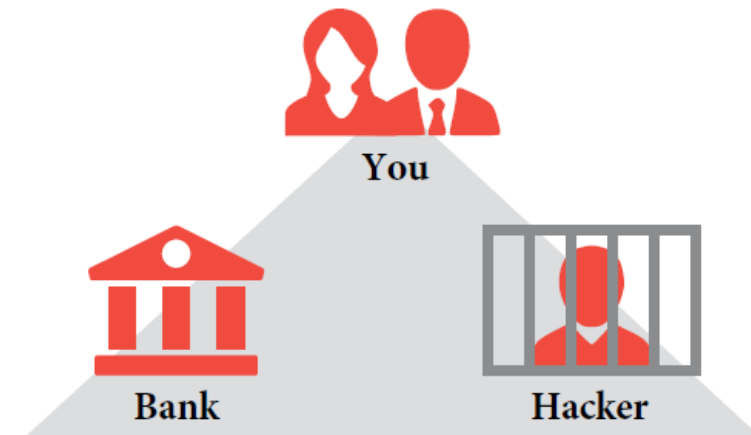
Introduction

Cyber Escape Room is a client-Server-based application developed for Cyber Security Awareness-Training

The application is in development since the beginning of 2018 in the german PwC Cyber Security & Privacy Team.

Have you always wanted to hack a bank?

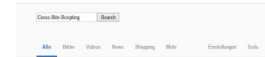
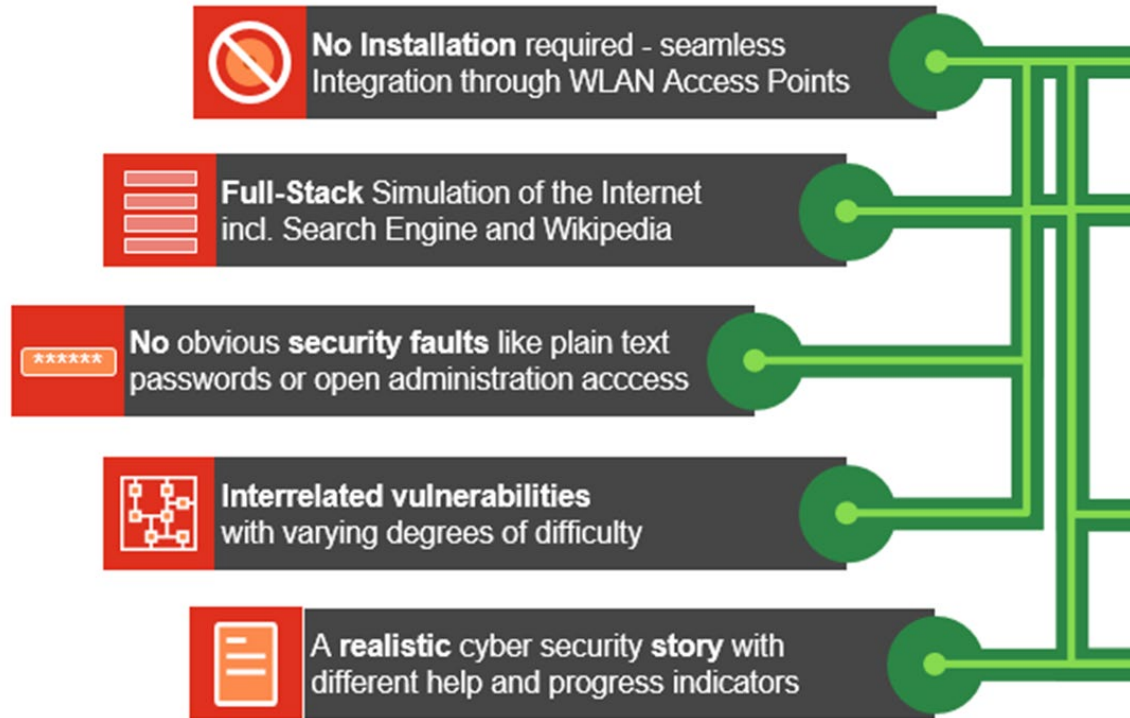
Using a classic triangle story, this cyber security simulation illustrates how insider knowledge, criminal energy and opportunity combined with **various attack techniques and existing security vulnerabilities** can be combined by a accomplices to do a cyber attack.



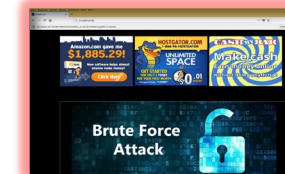
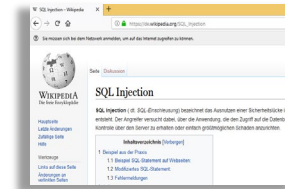
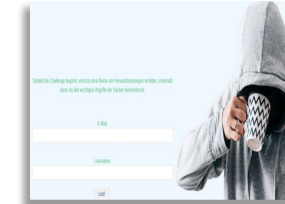
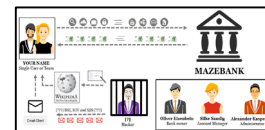
Specifically, a former disgruntled employee, in prison with limited access to the Internet, leads a cyber attack against his former employer, an inconspicuous bank with an exquisite clientele. The aim of the attack is to facilitate the bank account of the managing director.

As part of the story, you perform the cyber attack against the bank, familiarizing themselves with common attack methods such as SQL injection, Brute Force, and Cross Site Scripting (XSS).

Environment

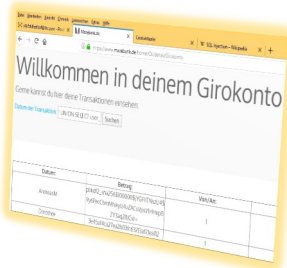
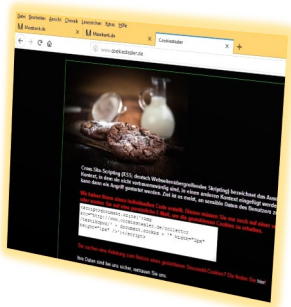



Wikipedia: Cross-Site-Scripting
 Cross-Site-Scripting (CSS) bezeichnet die Injektion einer Computersicherheitslücke in Webseiten. ...
 Ohne JavaScript werden Seiten nicht richtig dargestellt. ...




| Account | Account 1 | Account 2 | Account 3 | Account 4 | Account 5 | Account 6 | Account 7 |
|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|
| Account 1 | Account 2 | Account 3 | Account 4 | Account 5 | Account 6 | Account 7 | Account 8 |
| Account 1 | Account 2 | Account 3 | Account 4 | Account 5 | Account 6 | Account 7 | Account 8 |
| Account 1 | Account 2 | Account 3 | Account 4 | Account 5 | Account 6 | Account 7 | Account 8 |
| Account 1 | Account 2 | Account 3 | Account 4 | Account 5 | Account 6 | Account 7 | Account 8 |
| Account 1 | Account 2 | Account 3 | Account 4 | Account 5 | Account 6 | Account 7 | Account 8 |
| Account 1 | Account 2 | Account 3 | Account 4 | Account 5 | Account 6 | Account 7 | Account 8 |
| Account 1 | Account 2 | Account 3 | Account 4 | Account 5 | Account 6 | Account 7 | Account 8 |


Challenges




Path Traversal to use an application to gain unauthorized access to the file system 

Brute-Force attack that can, in theory, be used to decrypt any encrypted data 

Cross-Site scripting enables attackers to include client-side scripts into web pages 

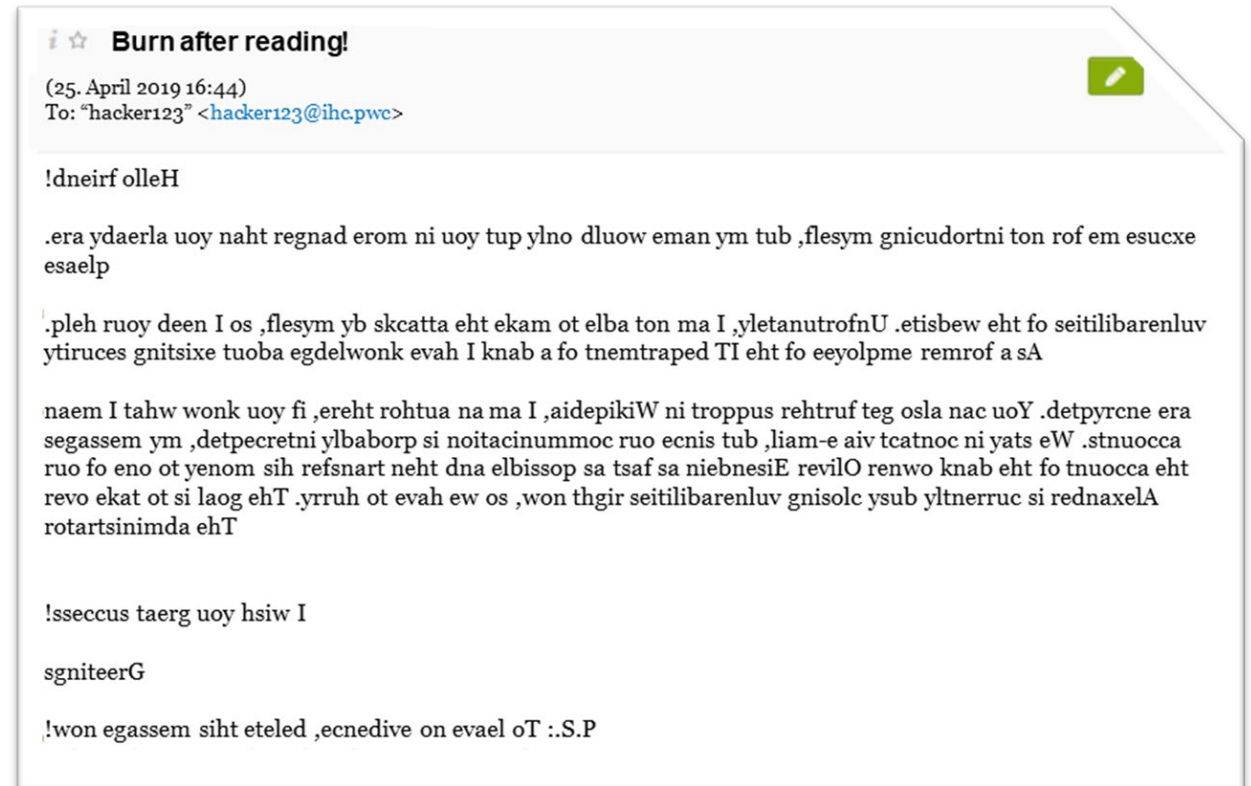
Sessions Stealing and URL Manipulation to get access to user accounts 

SQL Injections and Hash decryption allow to spoof identity and tamper with existing data 

Attack Preview: Story and Game Introduction

The story begins with an E-Mail stored in your mailbox like an attacker would use it in the 1990s.

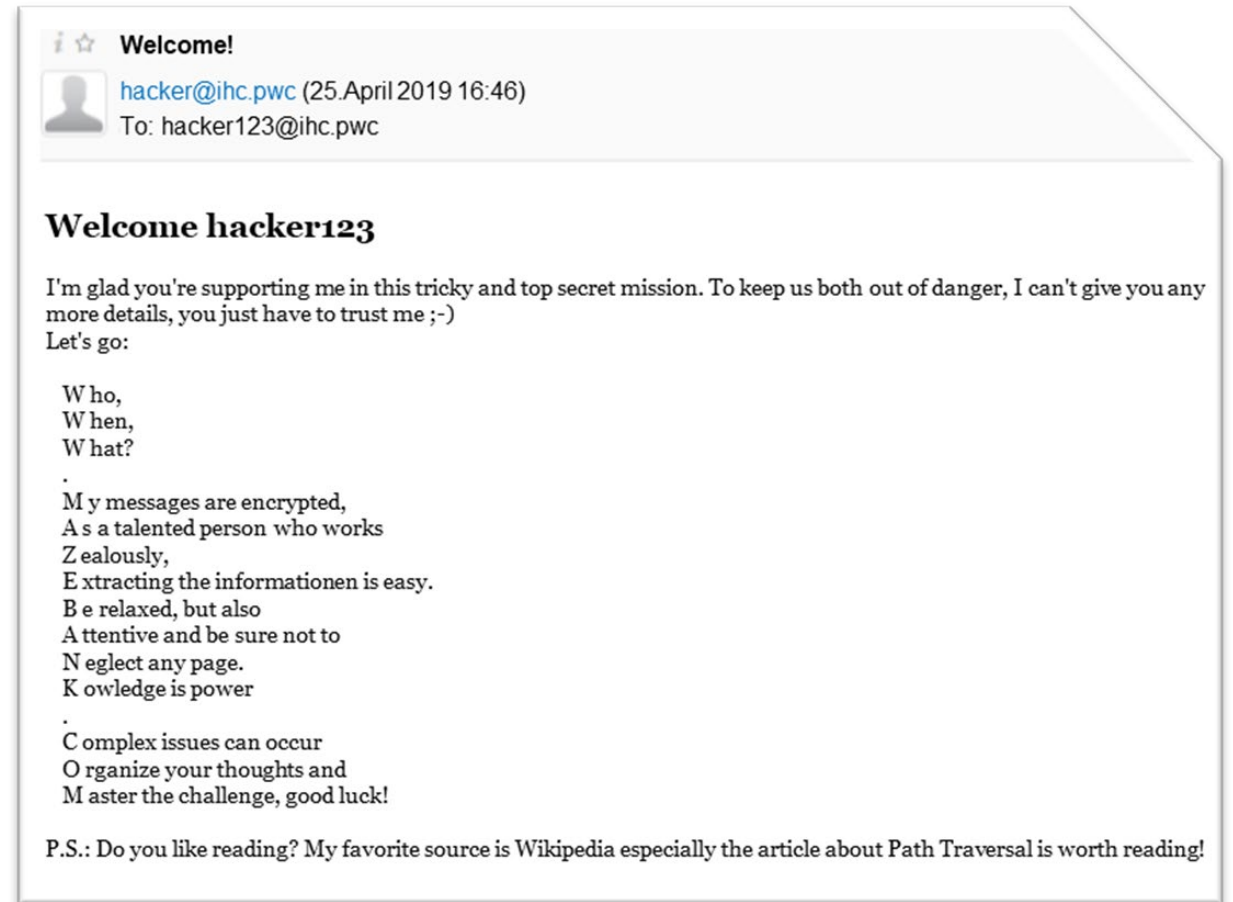
The E-Mail explains the story and is written backwards.
Can you read it?



Attack Preview: Path Traversal (1. Challenge)

The first challenge is presented as a riddle in an e-mail. The text guide you to the target bank website and introduce the use of Wikipedia.

Can you find the target bank website?



Your value

After a short introduction you can do the simulation in teams up to two persons on one of our provided laptops on your own. No detailed knowledge in IT-Security is necessary.

Further benefits are:

- Sustainable security awareness with PwC developed methodology
- New and exciting simulation with the help of gamification
- Prevent successful social engineering attacks
- Reduction of reputation damage
- Reduction of security incidents by optimally sensitized employees

We offer the simulation in our premises or in-house for a number of 10-20 employees. The participants need only ability to work on a laptop. For the introduction and progress display a projector or larger display is advantageous. Other hardware such as servers, wireless routers and client laptops are provided by PwC. The Simulation is offered in German and English language.

Your contact



Achim Schäfer

Cyber Security & Privacy

Phone: +49 69 9585-1022

E-Mail: achim.schaefer@pwc.com



Thomas Klir

Cyber Security & Privacy

Phone: +49 69 9585-3481

E-Mail: klir.thomas@pwc.com



Philipp Fath

Cyber Security & Privacy

Phone: +49 69 9585-3471

E-Mail: philipp.fath@pwc.com