Security Awareness Training Through Experiencing the Adversarial Mindset

Jens Christian Dalgaard | **Niek Janssen** | Oksana Kulyk | Carsten Schürmann

IT UNIVERSITY OF COPENHAGEN

USEC'23 | 27TH February 2023 | San Diego

Existing IT Security Awareness

- Traditional
  - Checklists
  - E-learnings
  - Posters
  - Videos

Virus & Malware Prevention
Are You *Protected?*
Install Anti-Virus/ Malware Software
Keep Your Anti-Virus Software Up to Date
Run a Malware & Virus Scan Regularly

How to Prevent

CEO FRAUD

SECURITY AWARENESS TRAINING is one of the most effective tools for fighting CEO Fraud.

- **FOLLOW WRITTEN PROCEDURES** for the approval of all financial transactions.
- Employees should **QUESTION AND VERIFY** all confidential requests, especially those deemed urgent by the CEO or other senior executives within the company.
- Use **MULTIFACTOR AUTHENTICATION** on all email accounts.
- Implement a **TWO-STEP VERIFICATION** process for all payments which includes a non-email check such as a telephone or verbal authentication.
- **DO NOT POST SENSITIVE INFORMATION** on company websites or on social media.

Keep data secured by locking your computer and devices **when not in use**.

Don't make life easy for cyber criminals.

Motivation

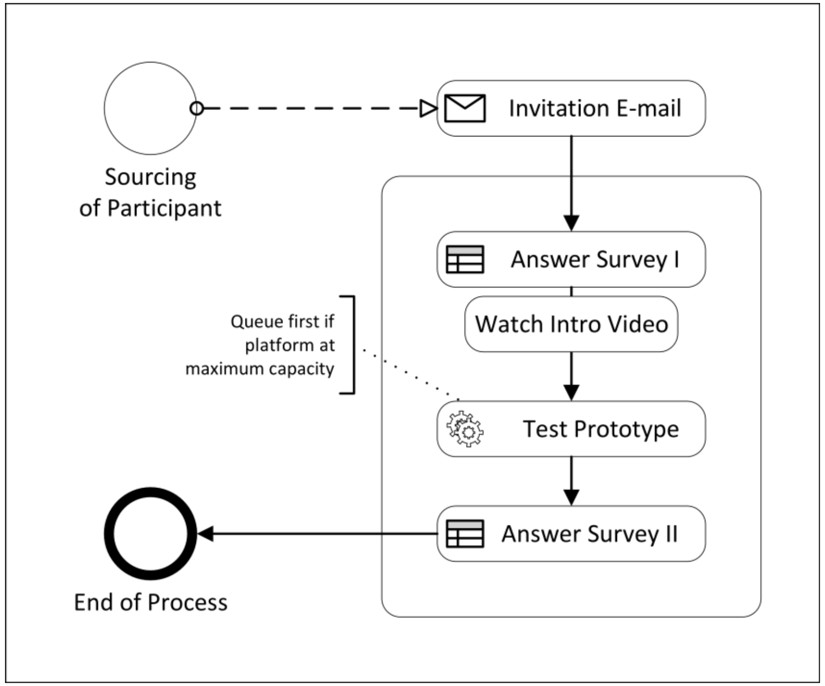
- IT Security Awareness training more common
  - Increase knowledge vs behavioral change
- Capture the Flag exercises in Introduction to IT Security courses
- Goal: **Increase understanding**

Research Question

Does experiencing IT security from an attacker's perspective motivate users towards better security behavior?

Study Design

- Protection Motivation Theory[1] (PMT)
  - Threat Appraisal & Coping Appraisal
- Prototype
- Pre-Post Study[2]
  - 34 participants
  - Private Organizations
  - Office Employees



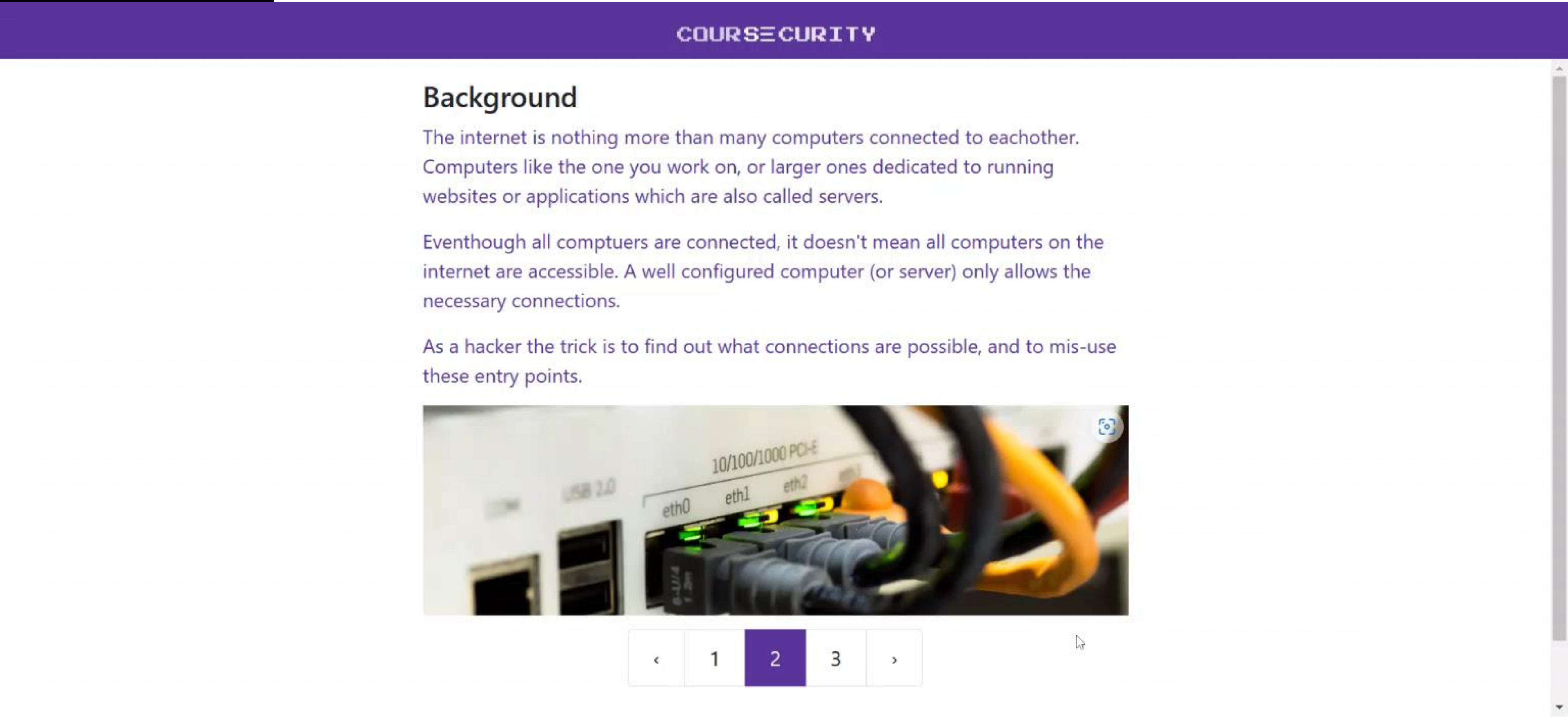
[1] Rogers, 1975
[2] Kirkpatrick & Kirkpatrick, 2006

Learning Design

- **Experiencing being the hacker**
  - Interactive / Game-Like
  - Real(-allistic)
- Understanding over knowledge
- Instructional Design Principles[1]

[1] Zhang-Kennendy & Chiasson (2021)

Prototype



Background

The internet is nothing more than many computers connected to eachother. Computers like the one you work on, or larger ones dedicated to running websites or applications which are also called servers.

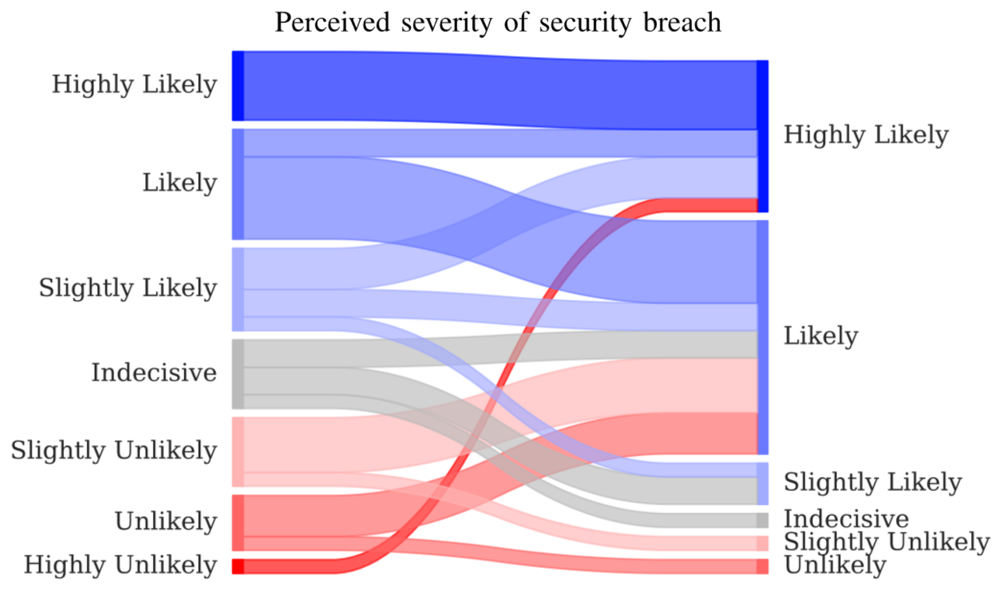
Eventhough all comptuers are connected, it doesn't mean all computers on the internet are accessible. A well configured computer (or server) only allows the necessary connections.

As a hacker the trick is to find out what connections are possible, and to mis-use these entry points.

Results

- Increased Motivation

- Free-text Answers
  - Effect on Compliance Intention
  - Effect on Awareness



“It made me realize how IT-security always depends on the weakest link in the chain.”

“The patterns in passwords made an impression and will give cause to a change in my own behavior.”

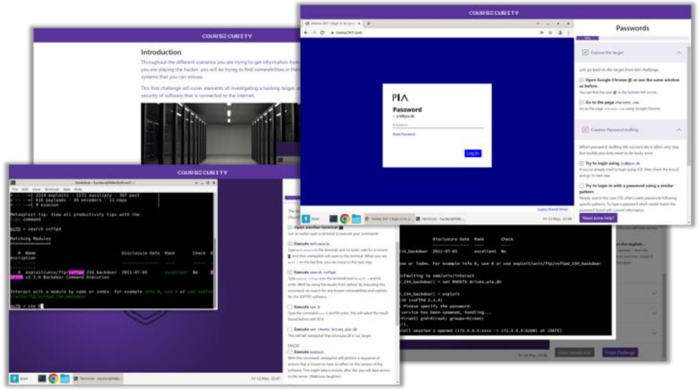
“I knew it [getting hacked] would be easy, but not that easy.”

Summary

- Simulation Based Tool
- Motivation vs. Teaching

- Indicating change in motivation
  - For “Office workers”

- Expansion of content covered



Perceived Severity of Security Breach	**+1,31**
Response Efficacy	**+0,34**
Security Policy Compliance Intention	**+0,31**

(N=34) | (7-point scale)