
SPILBASERET TRÆNING TIL FORBEDRING AF
CYBERSIKKERHED OG INTERN MOTIVATION: EN
ITERATIV TILGANG TIL IDENTIFIKATION AF
PHISHING-EMAILS



Therkel Bue Larsen & Thomas Glensvig Larsen
10TH SEMESTER OF ENGINEERING PSYCHOLOGY



AALBORG UNIVERSITET
STUDENTERRAPPORT

The Faculty of Engineering and Design

Engineering Psychology

Frederik Bajers Vej 7B

9220 Aalborg Ø

Emner

Spilbaseret læring
Cybersikkerhed

Projekt periode

01/02/2024 - 31/05/2024

Medlemmer

Therkel Bue Larsen
Thomas Glensvig Larsen

Vejledere

Flemming Christensen

Sider: 81

Resumé:

I denne rapport er et spil blevet udviklet med det formål at træne brugere i at identificere phishing emails og vurdere dets evne til at fremme intern motivation. Spillets funktionalitet bestod i at præsentere brugerne for phishing-mails, som var gemt blandt almindelige mails i et Outlook-inspireret mailsystem. Spillet blev testet over tre iterationer, hvor nye spilmekanismer blev tilføjet ved hver iteration. Resultaterne viste indikationer på en læringseffekt, da der blev fundet statistisk signifikante forskelle i andelen af korrekt identificerede phishing emails mellem iterationerne. Dette tyder på, at forsøgspersonerne blev bedre til at identificere phishing emails over tid. Desuden indikerede resultaterne, at forsøgspersonerne oplevede et moderat niveau af indre motivation, hvilket antyder, at der er potentiale for yderligere forbedringer af systemet.



AALBORG UNIVERSITET
STUDENTERRAPPORT

The Faculty of Engineering and Design
Engineering Psychology
Frederik Bajers Vej 7B
9220 Aalborg Ø

Emner

Gamebased learning
Cybersecurity

Project periode

01/02/2024 - 31/05/2024

Members

Therkel Bue Larsen
Thomas Glensvig Larsen

Supervisors

Flemming Christensen

Pages: 81

Abstract:

In this report, a game was developed with the purpose of training users in identifying phishing email and evaluating the games ability to promote intrinsic motivation. The games functioned by presenting phishing mails, hidden among regular mails in an Outlook inspired email system. The game was tested over the course of three iterations, where each iteration introduced new game mechanics. The results indicated that the system had an effect on the participants learning outcome as statistical differences in the amount of correctly identified phishing emails was found between the iterations. This indicates that the participants improved in their ability to correctly identify the phishign emails as a result of their increased experience. Furthermore the results indicated that the participants had a moderate level of intrinsic motivation, which indicates that the game has room for further improvements.

The content of this paper is freely available for everyone, however publication (with source) may only happen with acceptance from the authors.

Indhold

1	Introduktion	1
1.1	Cybersikkerhed	1
2	Problemformulering	3
3	Teori	4
3.1	Indlæringsevne og informations genkaldelse	4
3.2	Cybersikkerhed - Undervisnings metoder	6
3.3	Gamification	7
3.3.1	Eksisterende gamification produkter	7
3.4	Spilopbyggelse	9
3.5	Målgruppe	11
4	Spillet	13
4.1	Selve spillet	14
4.2	Konstruktion af spillet	15
4.2.1	Første udgave	16
4.2.2	Anden udgave	17
4.2.3	Tredje udgave	17
4.3	Rekruttering til forsøg	17
5	Forsøg	19
6	Resultater fra dataanalyse	22
6.1	Præstationerne igennem spillet	24
6.2	Kroner og kranier	27
6.3	Tidsmæssig aspekt	29
6.4	Spørgeskema	30
6.4.1	Kontrolvariabler	33
6.4.1.1	Niveau af uddannelse	33
6.4.1.2	Erfaring med cybersikkerhed	34
6.5	Præstation sammenholdt med subjektiv evaluering	35
7	Diskussion	36
7.1	Præstation	38
7.2	Forsøgsopstilling	40
8	Konklusion	43
9	Litteratur	44

Appendikser	50
A Spørgeskema til evaluering af motivation	51
B Software appendiks	55
C Statistisk analyse	59
C.1	59
C.1.1 Præstation	59
C.1.2 Kranier og kroner	61
C.2 Spørgeskema	63
C.2.1 qqplots	63
C.3 Effekten af Køn og Alder	66
C.3.1 Alder	66
C.3.1.1 Interesse og spændning	67
C.3.1.2 Opfattet valg	67
C.3.1.3 Opfattet kompetance	67
C.3.1.4 Spændning og pres	67
C.3.2 Køn	67
C.3.2.1 Interesse og nydelse	67
C.3.2.2 Opfattet valg	68
C.3.2.3 Opfattet kompetence	68
C.3.2.4 Pressure/tension	68
C.3.3 Kontrolvariabler	68
C.3.3.1 Niveau af uddannelse	72
C.3.3.2 Erfaring med cybersikkerhed	76
D Samtykkeerklæring	81

*

1 | Introduktion

1.1 Cybersikkerhed

Verden er blevet mere globaliseret og digitaliseret, dette har medført at der er set en øget mængde af produkter og teknologier som bliver digitale og "smarte" [Cremer et al. (2022)]. Derfor er emnet cybersikkerhed et vigtigt emne for virksomheder at forstå, da forkert håndtering af de teknologiske hjælpemidler kan resultere i store problemer for både firmaer såvel som den individuelle person. Petrosyan (2023) har undersøgt hvilke gennemsnitlige omkostninger der er på databrud indenfor forskellige sektorer i perioden Marts 2022 til Marts 2023. Det er blevet estimeret at et databrud medbringer gennemsnitlige omkostninger på op mod 11 millioner USD i sundhedssektoren. Desuden fandt de at databrud i den offentlige sektor, som vurderes til at have den "laveste" gennemsnitlig omkostning, ligger på 2,6 millioner USD. [Petrosyan (2023)]. Det er dog ikke kun for virksomheder at cybersikkerhed er et problem, 47% af den danske befolkning der oplevede sikkerhedsproblemer i 2019 [Statistik (2020)]. Heraf har 43% af befolkningen været udsat for såkaldte "Phishing" angreb. Phishing er en metode som ligger under social engineering, hvilket er hvor man prøver at bedrage og manipulere mennesker til at få adgang til følsomme oplysninger, igennem menneskelige følelser og adfærd [Sonowal (2022)]. Her fisker angriberen efter oplysninger gennem forskellige medier såsom f.eks. emails. Derudover er der en øget tendens hvor phishing email er begyndt at blive til spearphishing. Spearphishing er en metodik blandt phishing hvoraf modtageren ikke modtager f.eks. en generaliseret email, men at emailen fremstår som værende fra en troværdig person som f.eks. deres overordnede. Phishing angreb er et af mange versioner af sikkerhedsbrud. Phishing angreb foregår ved at angriberen forsøger at sigte efter det svageste led i sikkerhedssystemet; mennesket [Ozkaya (2019)]. Disse angreb er ofte succesfulde grundet manglende information eller viden hos mennesket, og har ofte til formål at indsamle særlig information fra specifikke mennesker, såsom kodeord, konto detaljer, eller lignende. Phishing angreb bliver ofte udført ved at angriberen efterligner en autentisk person, såsom f.eks. en hjælpsom IT afdeling, administrator eller lignende, der ønsker informationer for at kunne hjælpe mennesket videre [Ozkaya (2019)].

Denne menneskelige faktor er også blevet identificeret af Nobles (2018), Services (2014), Ness et al. (2011), Evans et al. (2016) og Hancock and Tessian (2022) som værende den største årsag til data- og sikkerhedsbrud. Services (2014) fandt at over 95% af de efterforskede databrud i deres undersøgelse var forårsaget af menneskelige fejl, eller var muliggjort af menneskelige fejl. IBM har baseret disse fund på 91 millioner rapporterede angrebstilfælde. Heraf var de største årsager til menneske forårsaget databrud; svage kodeord, fejl konfigurerings af systemer, benyttelse af standard brugernavn og kodeord, lække information gennem inkorrekte email adresser og oftest ved at inficere filer eller få modtageren til at tilgå usikre hjemmesider. Evans et al. (2016) finder at 93% af 7255 databrud i UK er

grundet menneskelige fejl. Derudover beskriver Hancock and Tessian (2022) hvordan menneskelige fejl er den største faktor for databrud, og at disse fejl ofte sker i forbindelse med at mennesker oplever udbrændthed, træthed, stress, travlhed eller er distraheret. Heraf har 52% af de adspurgte været faldet for en spearphishing email der så ud som om den kom fra en chef eller øverststående kollega. Dog er det kun 26% der overordnet er faldet for ikke målrettede phishing emails.

Ozkaya (2019) redegør de mest almene typer for angreb. Disse inkluderer b.la. social engineering angreb. Et eksempel på et succesfuldt hackingforsøg gennem social engineering er databrudet hos Yahoo i 2013-2014, hvor milliarder af Yahoo brugers informationer blev kompromitteret [Matthews (2019)], [Williams (2017)]. Hackerne var succesfulde med deres hackingforsøg som foregik gennem phishing eller spearphishing metoden. Problematikken bag disse social engineering angreb er at det kun kræver en person der falder for et phishing angreb for at angriberen kan få adgang til f.eks. virksomhedssystemer.

Der er forskellige årsager til at angribere forsøger sig med phishing angreb. Her kan motivation for disse angrebene være; økonomisk, identitets svindel, industriel, malware eller anerkendelse. Økonomiske angreb er primært for at få penge. Identitet kan være for medicinske oplysninger, hvor at angriberen kan bruge informationen til at komme på skadestuen eller lignende. Industrielle angreb handler om at få mere viden om deres modstandere inden for et bestemt område, hvor de så f.eks. kan udvikle en teknologi først. Heraf er malware angreb hvor der bliver plantet et ondsindet program som kan stjæle data og/eller være ødelæggende. Til sidst er der anerkendelse, hvor at der er nogle hackere der ser det som en udfordring i at se hvor store firmaer de kan komme ind på, og herigennem opsøge anerkendelse hos venner og familie. [Sonowal (2022)].

Da mange af de fejl som ses indenfor brud på cybersikkerhed skyldes menneskefejl, er det derfor vigtigt at lærer den generelle befolkning hvordan de bedre kan navigere igennem de forskellige typer for phishing emails og hvordan de bedre genkender disse.

2 | Problemformulering

Dette har ledt til problemformuleringen:

"Hvordan konstrueres en spilbaseret trænings metode, med formål at skabe indre motivation indenfor undervisningen af cybersikkerhed?"

3 | Teori

3.1 Indlæringsevne og informations genkaldelse

Indlæringsevne bliver ofte kaldt for lethed ved at lære [Linja-aho (2006)]. Indlæringssevne bliver af Linja-aho (2006) beskrevet som hvor hurtigt et emne bliver lært, og hvor hurtigt korrekte interaktioner kan foretages af nye brugere. I cybersikkerheds sammenhænge vil dette være at brugeren hurtigt kan lære hvordan potentielle trusler identificeres, og håndteringen af potentielle databrud. Hertil er målet med god indlæringsevne at forbedre indlæringskurven for den underviste.

Gamification bliver ofte fundet til at have positive effekter i områderne det bliver benyttet indenfor [Koivisto and Hamari (2019)], [Seaborn and Fels (2015)]. Koivisto and Hamari (2019) fandt gennem en analyse af 66 kontrollerede kvantitative eksperimentelle studier at 28,7% af disse studier udelukkende rapporterede positive effekter af gamification. 47% af studierne rapporterede mest positive men også nogle negative effekter af gamification, hvoraf kun 3% af studierne udelukkende fandt negative effekter. Det var yderligere fundet at studier med undervisningsfokus havde rapporteret en højere mængde af udelukkende positive resultater, en helheden (35,7%) hvoraf studier med blandede men dog primært positive effekter blev fundet til at udgøre 32,1%. Heraf nævnes det også af Koivisto and Hamari (2019) at gamification falder naturligt ind i undervisningsområder da sværhedsgraden skridtvis kan øges og der er mulighed for at give feedback, men at det skal sættes i forhold til temaet, da f.eks. helbredsundervisning skal undervises mere sensitiv og med mere fokus på alvoren.

Ideen om at benytte spil til undervisning, medbringer store forskelle, afhængigt af det valgte medie [Kuo and Chuang (2016)]. Et eksempel på dette kan være forskellen mellem at have et fysisk spil i et undervisningslokale, heraf kan underviseren fleksibelt bøjse og opsætte spilrammerne afhængig af situationen. Dette er dog ikke på samme måde tilfældet ved digitaliseret spil, da man her vil skulle forudse alle potentielle spilmuligheder, samt adaptere spillet baseret på disse spilresultaterne. Videospil har dog den fordel at det ved at benytte fiktionalle kontekster, fortællinger, musik og grafik kan skabe en interesse for "ikke spilområder" såsom f.eks. undervisningsemnets historie [Watson et al. (2011)], [Dominguez et al. (2013)].

Motivationen er vigtig for at et individ kan lære, da dette medvirker til deltagelse og forståelse Legaki et al. (2020). Dette er yderligere med til at gøre det muligt for den studerende at få den nødvendige indlæring, som kan være med til at tage de korrekte beslutninger. Hertil er det fundet at forskellige typer af spil ideologier kan have forskellige effekter [Xi and Hamari (2019)]. Xi and Hamari (2019) fandt at præstation funktioner og sociale aspekter havde en positiv korrelation med bruger autonomi, kompetence og evnen til at sammenholde information. Resultaterne er yderligere bekræftet af Legaki et al. (2020) der fandt at præstations baserede spil forbedrer studerendes læringsresultat.

Motivation kan opdeles mellem indre og ydre motivation. Heraf er indre motivation, motivation der kommer af at individet finder opgaven eller udfordringen interessant eller fornøjelig. Ydre motivation er motivation der kommer af at det at udføre handlingen leder til et resultat. Heraf kan resultatet være at undgå en straf, at få en gave eller lignende [Deci et al. (2001)]. Denne form for ekstern motivation bliver ofte beskrevet til at være af lav kvalitet som kontraster med den indre motivation [Kuo and Chuang (2016)]. Dog finder Deci et al. (2001) at dette afhænger af benyttelsen af fysiske goder der kan opnås, f.eks. pizza eller en stjerne som belønning, havde en negativ effekt på den indre motivation. Dog har ekstern motivation i form af positiv feedback ikke en negativ effekt på den indre motivation. Et lavt niveau af indre motivation kan lede til reduceret indlæring, og det er her at gamification til undervisning, kan være med til at øge den indre motivation for ellers kedelige emner såsom regnskab og bogholderi [Kuo and Chuang (2016)], [Dominguez et al. (2013)].

Gamification er yderligere blevet fundet til at have en positiv indvirkning på indlæring ved at forbedre motivation og læringsresultat [Buckley and Doyle (2016)], [Legaki et al. (2020)], [Xi and Hamari (2019)], [Craighead (2004)], [Snider and Eliasson (2013)]. Buckley and Doyle (2016) fandt dog at effekten afhang af om den studerendes indre eller ydre motivation blev påvirket, da den indre motivation gav mere positive resultater. Gamification er også blevet fundet til at have en positiv effekt den undervistes evne til at huske undervisningsmaterialet [Lorenzo-Alvarez et al. (2020)], [Samuel et al. (2022)]. Lorenzo-Alvarez et al. (2020) benyttede sig af et konkurrencebaseret spil som undervisere kan benytte til radiolog undervisning. Her blev det fundet at deltagerne der havde fået spillet som undervisningsmateriale bedre huskede undervisningsmaterialet en måned efter undervisningen sammenlignet med en kontrolgruppe. Samuel et al. (2022) sammenlignede effekten af et digitalt videospil og et papir baseret spil, hertil fandt de at de studerende selvrapporterede at det digitale videospil øgede deres evne til at fremkalde undervisningsmaterialet.

Gamification kan yderligere være med til at øge kognitive elementer på flere måder [Cheng and Ebrahimi (2023)]. Eksempelvis kan spil elementer såsom trofæer og scoringstavler skabe en fornemmelse af konkurrence, og spænding som øger arousal og opmærksomhed. Dette er med til at gøre at gamification kan forbedre det kognitive engagement [Cheng and Ebrahimi (2023)]. Disse elementer kan yderligere fremme positive følelser såsom fornøjelse og nysgerrighed. Gamification er derfor en metode der tidligere har været stor succes med at bruge til at undervise flere forskellige emner.

3.2 Cybersikkerhed - Undervisnings metoder

Cybersikkerhed er et emne som er forsøgt undervist på flere måder og med flere forskellige metodiker [Kävrestad (2022)]. Her er der flere forskellige metoder, nogle i fysisk form, andre på en computer. Derudover foregår undervisningen både på individuelt plan og på holdsbasis. Kävrestad (2022) beskriver fem former for træning; Klasse eller hold, online træningsmateriale, E-Learning, simulationer og kontekstuel træning og gamificeret træning.

Den første form for træning er hold undervisning [Kävrestad (2022)]. Hold undervisning kan foregå både i fysisk rum, som f.eks. et klasse værelse, eller online, hvor der bruges et online medie til at afholde undervisningen. I Lastdrager et al. (2017) modtager en gruppe undervisning fra en underviser. Hertil var forsøgspersonerne der havde modtaget holdundervisning bedre til at detektere phishingmails lige efter forsøget. Lastdrager et al. (2017) beskriver dog hvordan at denne form for hold undervisning ikke er tilstrækkelige, eftersom at de skoleelever som blev undervist i cybersikkerhed, efter fire uger var på samme niveau som kontrolgruppen til at detektere phishingmails.

En anden form for undervisning, er hvor at små biter af undervisning bliver tilsendt til "eleven". Undervisningen kan herved blive uddelt på en dag eller uge. Deltageren kan så tilgå undervisningen når deltageren har tid til at tage det modul af undervisning [Al-Daeef et al. (2017)]. Dog argumentere Al-Daeef et al. (2017) for at denne form for undervisning hurtigt kan blive udfordret. Dette menes da det tilsendte materiale ikke nødvendigvis vil indfange deltagerens opmærksomhed, f.eks. fordi deltageren mener at de har ikke behøver yderligere information.

E-learning er en undervisningsplatform hvor brugeren har adgang til de forskellige moduler af undervisnings materialet, og selv har mulighed for at tilgå materialet uden instruktør eller underviser [Kävrestad (2022)]. Dog finder Stockhardt et al. (2016) at brugere foretrækker holdundervisning fremfor e-learning.

Simulations træning er beskrevet som et nyttigt redskab til cybersikkerheds træning af Aldawood and Skinner (2019) og Al-Daeef et al. (2017). Dog kan der være nogle problemer ved det etiske dilemma der kan forekomme ved at udsætte en for phishing email [Al-Daeef et al. (2017)].

Den sidste metode som også bliver beskrevet i Jayakrishnan (2020) er Gamificeret træning. Gamification kan være med til at øge den undervistes motivation som beskrevet af Jayakrishnan (2020). Al-Daeef et al. (2017) beskriver at gamificering kan have positiv effekt, dog mangler den underviste i nogle tilfælde den nødvendige viden for at kunne spille et spil. Dog mener Kävrestad (2022) at gamification eller spil kan benyttes i kombination med de ovennævnte undervisningsformer.

3.3 Gamification

Gamification bliver beskrevet som benyttelsen af spil elementer til andet end underholdningsspil, f.eks. undervisning [Kävrestad (2022)]. Desuden benyttes gamification til at motivere, give belønninger og feedback til brugeren, hvilket eks. kunne være i undervisningssammenhæng [Ioannis Deliyannis and Lampoura (2023)]. Dette kan f.eks. være i form af points som spilleren skal indsamle for at stige i niveau. Her bliver det også beskrevet som et begreb der ligger sig op af nudging [Erkmann and Lomholt (2018)]; [Silva et al. (2016)]. Nudging er et en metode hvorpå man kan ændre på et individs adfærd i en forudsigelig retning uden at begrænse individets muligheder [Thaler and Sunstein (2008)].

Gamification og undervisning kan også kombineres og hertil benyttes begrebet "game-design teaching and learning"(GDTL) [Gee and Price (2021)]. Begrebet benyttes til at beskrive aktionen af at benytte spilelementer til at forklare omverdenen [Gee and Price (2021)]. Her er det at man som bruger af et spil bliver præsenteret for forskellige problemstillinger man skal tage stilling til, og at man derved lærer, igennem det at forholde sig til problemstillingen [Gee and Price (2021)]. I Ioannis Deliyannis and Lampoura (2023) bliver det beskrevet at belønninger, under en læringsproces, kan have en positiv virkning. Her lærer vedkommende at der er en gevinst eller belønning ved at gøre noget bestemt eller bruge en rigtig metodik, og når de så bruger dette i den virkelige verden, erkender de værdien af de kompetencer de har opbygget gennem spillet. En del af de elementer som der bliver tilføjet, såsom point eller medaljer, kan være med til at øge den ydre motivation for brugeren, dog kan spildesigneren også bruge forskellige spilelementer til at påvirke den indre motivation, såsom fortællinger, plot eller frihed til at gå en anden vej igennem spillet [Ioannis Deliyannis and Lampoura (2023)].

Erkmann and Lomholt (2018) beskriver hvordan gamification kan benyttes til at lave simulerede opgaver. Her eksemplificerer de med simuleringer af fly, for piloter. Her kan de således simulere at de flyver et fly, hvor de kan lave forskellige manøvre eller forskellige opgaver uden at det vil koste fly selskabet penge eller gøre skade såfremt der sker en fejl, f.eks. ved at styrte et fly eller at der kommer nogle passagerer til skade. Herigennem kan piloterne afprøve alle funktionerne som der måtte være i et cockpit på et fly, og opbygge ekspertise i kontrollerede miljøer.

Det er beskrevet at "et godt spil"er designet således at spilleren kan opbygge sine evner, og hvor spilleren kan teste sine opbyggede evner på et senere bossniveau. Dette kan sammenlignes med at tage en test eller eksamen, i et fag efter undervisning i emnet [Gee and Price (2021)].

3.3.1 Eksisterende gamification produkter

Et eksempel på gamification som læringsmiddel, kan blandt andet findes i Jayakrishnan (2020), hvor brugerne skulle leve sig ind i at lave et kodeord. Her skulle forsøgspersonerne spille et spil der havde til formål at forøge deres evne til at lave et godt kodeord. I forsøget

blev der lavet en test før og efter spillet, hvor der blev fundet en forbedring blandt forsøgspersonerne, for beslutningstagningen ift. at lave et kodeord. I dette spil levede personerne sig ind i det at skulle lave et kodeord for at skulle beskytte et objekt, og hvor de efterfølgende skulle genkalde det kodeord de havde lavet. I forsøget fra Jayakrishnan (2020), blev disse kodeord så afprøvet gennem forskellige niveauer for at få motiveret spilleren.

Et andet eksempel er "kahoot!" som er blevet undersøgt gennem et litteraturreview af Wang and Tahir (2020). Her bliver der først og fremmest set på om kahoot kan blive brugt som et redskab til at undervise. Her bliver det fundet at det er et redskab som godt kan bruges. Dog var der større effekt for de højre klasser i skolen, samt videregående uddannelser som læger, ingeniører og matematik mm. Desuden bliver det også fundet, at det at spille og gøre undervisningen mere underholdende var med til at reducere nervøsitet for at deltage i undervisningen [Wang and Tahir (2020)]. Heraf deltog flere studerende i undervisningen, samtidig med at der blev stillet flere spørgsmål under undervisning, hvilket er en yderligere positiv effekt ved at bruge gamification.

Gamification er dog også set benyttet indenfor cybersikkerhed. Her er spillene konstrueret med det formål at vejlede brugeren til at tage de rigtige beslutninger i tilfælde af forsøgt internet svindel. Her er Hoxhunt et af de omtalte spil [Hox]; [Hox (2023)]. Dette spil er en tilføjelse til et emailsystem, hvor der bliver sendt simuleringer af phishing emails og lignende. Her skal de ansatte trykke på ikonet for Hoxhunt. I Hoxhunt applikationen er der lavet et system hvor brugeren kan få tildelt stjerner og belønninger når brugeren agerer korrekt på simulerede phishing angreb. Yderligere resulterer en forkert handling i at brugeren vil blive tildelt undervisning omhandlende hvordan lignende fejl undgås, således at brugeren kan agere rigtigt fremover. Denne form for undervisningsmetode, er en kontinuert læring, der fortsætter med at udfordre modtageren og forbedrer modtagerens evner. Hoxhunt har fundet at deres produkt forbedrer deltagerens præstation samt at deres deltagere bliver bedre til at identificere og rapportere phishingmail [Kuivala (2024)]. Dette måler de ved at undersøge deltagerens rapporteringsrate, hvor mange phishingmail deltagerene ikke identificerer og hvor mange de identificerer.

Et andet eksempel er The (2024) som er et tekstbaseret spil. Spillets omdrejningspunkt er at en ikkespilbar figur, skal løse en gåde, og spilleren skal assistere med dette. Her bliver spilleren placeret i forskellige situationer, hvor spilleren skal have styr på cybersikkerhed, for at komme igennem spillet. Dette er et spil der bliver gennemspillet en enkelt gang og skal fremstå som et alternativ til tavlelæring. Dog er benyttelsen af gamification til undervisning ikke enkelt, og der er derfor mange aspekter og overvejelser som er vigtige

3.4 Spilopbyggelse

Under konstruktionen og opbyggelsen af et spil er der forskellige elementer der skal inddrages og designes for at opnå et succesfuldt spil eller undervisning, hvor der er flere som har kommet med bud på hvad man skal være opmærksom på når man laver et spil [Gee and Price (2021)];[Basten (2017)];[Wilson and Hash (2003)]; [Erkmann and Lomholt (2018)].

Gee and Price (2021) beskriver at man skal være opmærksom på hvad slut målet med spillet, altså hvad vil man gerne have spilleren til at lære. Hertil er der også de små ryk man skal lave i spillet, man skal overveje. Hvilke mindre udfordringer bliver spilleren udsat for, og hvilke valg kan spilleren tage og således også hvornår der så skal være pauser så man kan reflektere. Desuden skal det kunne være muligt at gemme hvortil at enten gruppen eller individet er nået til [Gee and Price (2021)].

En anden artikel Basten (2017) beskriver tre overemner som er vigtige at overveje ved konstruktionen af et tematisk spil f.eks omhandlende cybersikkerhed. Først skal spildesigneren overveje hvilket system eller processer som spillet skal omhandle. For det andet hvilken slags adfærd der bliver promoveret gennem spillet. Sidste punkt er udviklingen og inkludering af spilelementer.

Her er det Basten (2017) fremhæver yderligere aspekter som skal passe overens med det ønskede budskab, disse aspekter er mekanismer, dynamikker og æstetik. Aspekterne er vigtige for at spillet succesfuldt kan promovere spillets ønskede budskab.

Mekanismer omhandler f.eks. om spilleren skal have points igennem spillet, om der skal være delmål eller andre elementer spilleren kan blive målt på i selve spillet.

Dog er det vigtigt at inddrage interessenter eller målgruppe under udvælgelse af dynamikkerne og æstetik. Dynamikker dækker over hvilke slags valg der kan blive taget i spilet og hvilke mindre delmål der kan være i spillet. Her skal dynamikkerne i spillet tilpasses hvor lang tid det skal tage at spille spillet. Sidst er æstetikken vigtig for at give spilleren en specifik følelse mens de spiller spillet. [Basten (2017)].

Wilson and Hash (2003) beskriver vigtigheden af at tilrettelægge fremgangsmåde i områder hvor det forsøges at advare mod trusler. Wilson and Hash (2003) beskrev her at der er forskel på hvilken slag årvågenhed man skal blive lært: Her bliver der beskrevet "*Awareness, Training og Education*".

De tre forskellige aspekter høre til hver sin grad af profession [Wilson and Hash (2003)]. Awareness, er til alle bruger, hvor det ikke helt tæller som træning, men det er med henblik på at give mere opmærksomhed til det underviste emne. Training er for brugere af it systemer, og skal være med til at klæde disse bruger på til at kunne befærde sig i disse it systemer på rette vis. Education er for dem som er professionelle eller er IT sikkerhed, dette er til at kunne skabe et team som kan være proaktivt imod cyber trusler. Dog er der en øget mængde af bevægelse på i cyber verdenen, heraf store mængder af børn og andre brugere der er dygtige til teknologi, men er uvidende omkring de farer de bevæger

sig rundt i [Rahman et al. (2020)]. Det er derfor ifølge Rahman et al. (2020) nødvendigt at undervise særligt de uvidende omkring de farer der befinder sig i cyberspace.

Wilson and Hash (2003) beskriver at det er vigtigt at overveje først hvorledes der er nationale eller lokale regler som skal være en central del af undervisnings målet. Efterfølgende skal der også blive fundet de roller som skal udspilles, men også hvem der kommer til at spille spillet. Dette bliver samlet til at undersøge hvilket undervisnings materiale der er relevant for målgruppen.

Erkmann and Lomholt (2018) påpeger at følgende aspekter er særligt vigtige at overveje under konstruktionen af et spil. Der skal overvejes om der skal være konkurrence i spillet, om hvorvidt at man kan konkurrere direkte i spillet, eller om der skal være en pointtavle, hvor man kan se hvem der har scoret flest point. Det skal overvejes om man skal lave det til et rollespil eller simulering, således at indlevningsevnen for spilleren bliver forbedret. Desuden skal det overvejes om det skal være aktionspræget, eller skal der være tid til at spilleren kan stoppe op, og reflekterer over sine valg. Til sidst beskriver Erkmann and Lomholt (2018) at man skal overveje det sociale i spillet, her er det hvorvidt man skal samarbejde med andre i en gruppe om at løse de problemstillinger som bliver præsenteret i spillet.

Erkmann and Lomholt (2018) beskriver seks punkter som de mener indgå i processen ved konstruktionen af en gamificeret aktivitet. Først skal det overvejes i hvilket rum spillet bliver spillet i og hvilken affordance som brugeren har. Det skal blandt andet overvejes hvorledes spillet skal være digitalt eller fysisk. Punkt to er fiktionen. Her skal der overvejes hvilken historie der skal udspille sig, hvilke roller der skal være med. Det skal også overvejes hvilke scenarier som spilleren skal sættes ind i, og om disse scenarier vil fremstå virkelighedsnære for spilleren. Det tredje punkt er hvilke regler skal der være med i spillet. Det er her hvor spildesigneren tænker over dynamikken i spillet. Her kan spildesigneren bl.a. overveje følgende; skal der tildeles point til brugeren, hvor stort et socialt aspekt skal der være, altså om brugeren skal spille mod eller med andre eller om der skal ske noget for brugeren, hvis vedkommende bryder en regel. Det fjerde punkt er frihed for spilleren. Det ligger sig lidt op af det forrige punkt, regler, men det er med fokus på hvor meget spilleren skal kunne gøre, og påvirke spillet. Det er også i det punkt hvor spildesigneren skal overveje om der er mulighed for at være nysgerrig, eller om der skal være meget stramme rammer for spileren. Der skal også her overvejes om de opgaver som spileren skal igennem er afhængige af f.eks sværhedsgrad eller niveau point, og kan spileren agere strategisk for at kunne påvirke resultatet. Punkt fem og seks er henholdsvis evaluering og test af det produkt der er konstrueret [Erkmann and Lomholt (2018)].

Det er vigtigt at overveje hvilke spilaspekter der skal indgå i spillet, konkurrencebaserede spil er fundet til at have positiv effekt på brugerens indre motivation af Erkmann and Lomholt (2018), Lorenzo-Alvarez et al. (2020) og Cheng and Ebrahimi (2023). Yderligere er en god metode at afprøve forsøgspersonernes evner ved at lave et "boss niveau"[Gee and Price (2021)].

3.5 Målgruppe

Alle er sårbare overfor hackerangreb. Dog er det særligt unge i aldersgruppen 16-34 år der bruger meget tid på internettet [Petrosyan (2024)]. Yderligere er det også fundet af Hancock and Tessian (2022) at det typisk er de yngre aldersgrupper der falder for f.eks. phishing hackerangreb. Her har 39% af de adspurgte 18-24 årige faldet for en phishing email. For de 25-34 årige er det 32% der er faldet for phishing emails, og for aldersgruppen 35-44 årige er det 28%. Lignende resultater er også fundet fra Census (2021). Her findes det at aldersgrupperne 25-34 og 35-44 år er mest tilbøjelige til at modtage phishing beskeder. Hvoraf aldersgruppen 35-44 år er mest tilbøjelige til at falde for disse. Census (2021) rapporterer dog ikke resultater for aldersgruppen 18-24 år da et for lille datasæt blev indsamlet for denne gruppe. Det er yderligere fundet af Bittner and Schipper (2014) at gamification produkter særligt har større effekt hos yngre brugere. Her er gamification bedre til at skabe indre motivation, mere nydelse. Yngre brugere opfatter også gamification som mere brugbart og føler der er bedre flow.

Udover hvem der oftest falder for phishing emails er det relevant at se hvor de største økonomiske tab forekommer. De største økonomiske tab der ses, forekommer af databrud hos virksomheder [Petrosyan (2023)]. Ifølge FBI (2023), blev der til FBI rapporteret 21,489 tilfælde af kompromitterede arbejds email. Dette ledte til et estimeret tab 2,9 milliarder USD. Arbejds emailen er ifølge FBI (2023) et medie der benyttes til at angribe både virksomhedsinformation såvel som personlige angreb. Det er både virksomheder såvel som større organisationer der særligt kan lide større tab, da disse ofte har større mængder af sensitiv information og mere værdi end enkelte individer. Dog betyder dette at større organisationer er så stærke som det svageste led. Et eksempel på dette er fundet i Broadhurst et al. (2018), der undersøgte hvor sårbare studerende var overfor svindel. Heraf fandt de at særligt målrettede beskeder, i dette tilfælde f.eks. i form af en email der omhandler en ændret eksamensdato, succesfuldt snød $\approx 50\%$ af forsøgspersonerne. Denne form for sårbarhed overfor målrettede angreb kan være skelsættende for store organisationer.

Yderligere er det valgt at indskrænke hvornår at individer der har været studerende for nyligt kan deltage i dette projekts forsøg. Hertil er resultaterne fra Ellis et al. (1998) revideret. I forsøget udført af Ellis et al. (1998) blev 1626 studerende og tidligere studerendes evne til at fastholde og anvende undervist information undersøgt. Det blev her fundet at det først var efter tre år at der blev set et kraftigt fald i forsøgspersonernes evne til at fremkalde informationen. Dette medfører at studerende og de der er blevet færdige bør fastholde information de har erfareret sig på op til tre år efter.

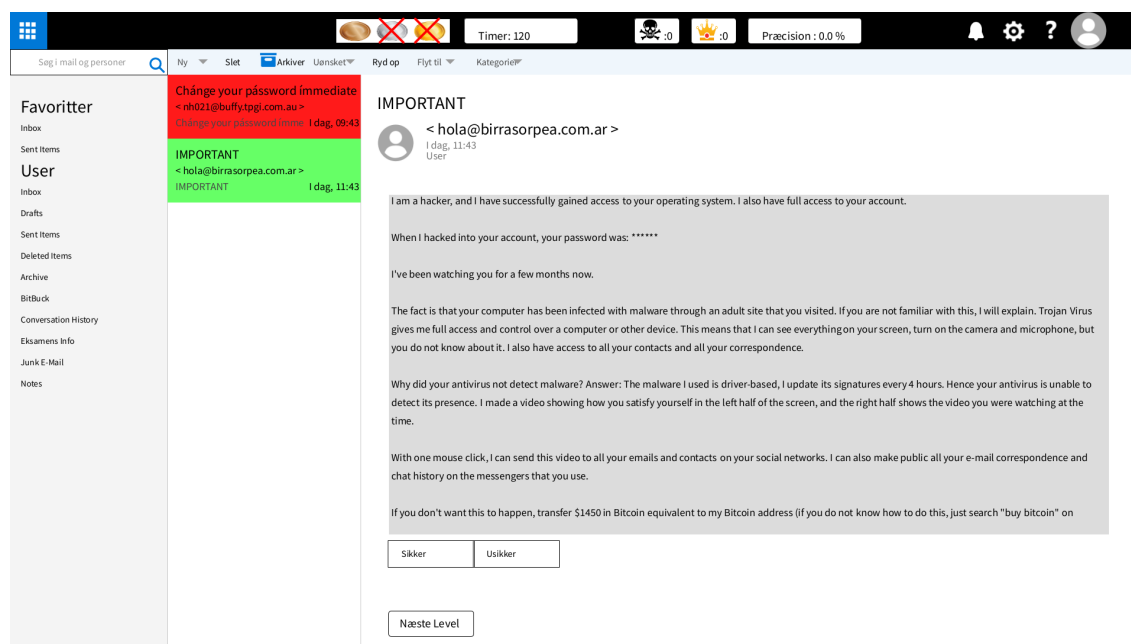
Dette leder til at det gamification sandsynligvis vil kunne have størst indvirkning på aldersgruppen 18-34 år, der er studerende eller har færdiggjort studie indenfor de sidste tre år, da disse oftest modtager f.eks. phishing beskeder, og oftest falder for disse hacker forsøg [Petrosyan (2024)], [Hancock and Tessian (2022)], [Census (2021)]. Yderligere er det indikeret at gamification vil kunne have den største positive effekt på yngre aldersgrupper, da disse er mere modtagelige overfor gamification konceptet [Bittner and Schipper (2014)].

Målgruppen der vil blive arbejdet videre med vil være studerende i aldersgruppen 18-34 år, da disse ofte benytter emails til kommunikation, samt er sårbare overfor de samme angreb da de er en del af større organisationer.

4 | Spillet

Spillets struktur efterligner den af producenten HoxHunt. HoxHunt er et trænings form hvor man kan optjene points når man opdager en Phishing email, og dette spil er et som allerede er på markedet og har mange brugere [Kuivala (2024)]. Heraf er der blevet taget inspiration til også at skulle lave et emailsystem som brugeren skulle arbejde rundt i. Desuden har de også konstrueret at deres træning er kontinuerligt, hvilket vi også har taget inspiration af. At spillet er kontinuerligt er et undervisningsaspekt der har stor værdi, særligt grundet Ebbinghaus' forglemmelses kurve [Chun and Heo (2018)]. Ebbinghaus' forglemmelses kurve angiver at der er en negativ korrelation mellem hukommelse og tid, at jo længere tid efter man er blevet undervist, jo sværere er det at fremkalde informationen. Dog er det fundet at ved adspredte men gengående læringsprocesser, vil denne forglemmelse ske over længere tid. Dette betyder at med en kontinuerlig læringsproces, vil brugerne være i stand til bedre at kunne fremkalde informationen, og forglemmelsen vil ske langsommere. Hvilket kan medføre mere robust læring end der ses ved typisk engangsundervisning.

Spillet var besluttet at blive opsat som et emailsystem hvor forsøgspersonerne skulle evaluere om de email de blev præsenteret for var et phishing email forsøg eller ej. Hertil blev spilrammen konstrueret som en version af browser-Outlook, hvilket kan ses på 4.1, med phishing emails og almene emails der ville ligge i forsøgspersonens indbakke. Forsøgspersonerne ville her blive stillet et valg hvor de skulle beslutte om emailen var ondsindet og forsøgte at snyde information ud af dem, eller om emailen var en almen email. For at forsøgspersonerne havde et ligende udgangspunkt for at evaluere disse emails blev et fiktivt scenarie opstillet hvor det blev simuleret at forsøgspersonen var studerende på Universitet.dk. Forsøgspersonerne fik universitets email domæne at vide for at sikre at forsøgspersonerne havde det samme udgangspunkt for at identificere email domæner samt evaluere hvilke emails der kunne fremstå som typisk relevant information fra et universitet. Dog blev det besluttet at forsøgspersonernes uddannelsesbaggrund, om de var studerende, deres køn, alder og cybersikkerhedserfaring indsamlet for at identificere om disse variabler påvirkede forsøgspersonernes resultater.



Figur 4.1: Et billede af hvordan selve spillet så ud i version 3

Når forsøgspersonerne havde færdiggjort spillet ville de få fremvist hvilke emails de havde bedømt korrekt og hvilke emails de havde fejlbedømt, samt en forklaring på hvorfor en fejlbedømt email var fejlbedømt. Denne form for feedback er med til at assistere forsøgspersonens læring, samt klargøre hvor eventuelle fejl og mangler er foregået. For at sikre at forsøgspersonerne var i stand til at gennemføre spillet og havde den nødvendige forståelse af hvordan spillet skal gennemspilles, blev en tvungen introduktion implementeret i spillet. Denne tvungne introduktion blev implementeret således at før forsøgspersonen kunne igangsætte spillet, skulle de navigere gennem flere skærme der forklarede spilmekanikeme, samt hvordan introduktionen kunne genfindes efter påbegyndt spil. Yderligere blev introduktionen opdateret mellem iterationerne med hvad der var vigtigt at holde øje med i forbindelse med phishing emails.

4.1 Selve spillet

Første udgave af spillet indeholdte niveau 1, 2 og 3 phishing emails. Anden udgave indeholdte niveau 2, 3 og 4 phishing emails. Tredje udgave indeholdte en blanding af phishing emails fra niveau 2, 3 og 4, som set fra første og anden udgave, samt have et tidsmæssigt aspekt for at udfordre hvor hurtigt forsøgspersonerne kunne færdiggøre spillet for at simulere en form for eksamen eller "boss niveau". Som beskrevet skulle disse runder være med til at øge motivationen samt udfordre forsøgspersonen på en underholdende måde [Erkman and Lomholt (2018)]. I alle udgaverne er der lige mange phishingemails som der var almene emails, som forsøgspersonerne skulle sortere i. Dette var til for at få forsøgspersonerne

sonerne til at være mere omhyggelig med deres svar, når de skulle tilkendegive emailen. Disse phishing emails var konstrueret på baggrund af Gardner and Thomas (2014) og Fette et al. (2007). Gardner and Thomas (2014) påpeger hvad formålet ofte er med phishing emails, dvs. hvilke informationer disse målretter sig, og nogle af metodikkerne og det bagvedliggende information der ofte bliver benyttet til at konstruere disse emails. Fette et al. (2007) pointerer vigtigheden og det farlige ved at have links koblet til phishing emails, da det ofte er herfra at ofret kan indskrive sin information der kan udnyttes af angriberen. De almene email var konstrueret således at de passede ind i det opstillede scenarie. Her var scenariet at forsøgspersonen var en studerende på universitetet *Unversitet.dk*, og at de skulle gennemgå deres email, som en daglig rutine. Emailene som forsøgspersonerne skulle gennemgå er inspireret af de emails som tidligere har været sendt til gruppedlemmernes studiemail.

Niveau 1 emails bestod af emails med mange tydelige indikationer på at emailen var en phishing email. Det vil sige at hele emailen var tydeligt indikerende for at afsenderen var ude på noget suspekt. Her kunne det f.eks. være at over 80% af bogstaverne i emailen havde et accent aigu tegn i sig.

Niveau 2 emails bestod af emails med to eller flere åbne fejl, dog uden at hele emailen tydeligt var en phishing email. Heraf er f.eks. fejl i email domænet, stavfejl og åbenlyse falske links eksempler på fejl der kunne forekomme. Her ville en ondsindet email f.eks. kunne indeholde tydeligt ondsindede links til hjemmesider, tydelige fejl i afsenderens email domæne eller lignende fejl.

Niveau 3 emails bestod af emails med en åben fejl, som f.eks. en lille fejl i email domænet eller links. Dette var nogle af de emails, hvor der var enkelte fejl i, det kunne være at email domænet havde nogle fejl i sig. I niveau 3 blev spearphishing emails også introduceret. Spearphishing emailene var målrettet mere sandsynlige situationer som forsøgspersonen ville kunne stå i, f.eks. at en person kontakter dem over et fundet id kort, eller på lignende metode forsøge at benytte et sandsynligt kendskab til forsøgspersonen for at snyde dem.

Niveau 4 emails bestod af gemte links, som krævede at forsøgspersonen granskede links adresserne grundigt. Yderligere bestod niveau 4 af mange emails omhandlende spearphishing også i kombination med gemte links for at yderligere besværliggøre identifikationen af rigtige og forkerte emails.

4.2 Konstruktion af spillet

Spillet var konstrueret til at være et kontinuerligt spil, men grundet tidsbegrænsningen af projektførelsen blev det besluttet at komprimere det kontinuerlige aspekt til et forløb over tre uger. Over disse tre uger ville forsøgspersonerne modtage et nyt spil hver uge, spille spillet indenfor ugens omløb, for at modtage spillet igen mandag ugen efter. Spillets informationer og link til download af iterationerne af spil blev sendt over email, for at sørge for at forsøgspersonerne ville tjekke og spille spillet i sammenhænge hvor de alment ville

tjekke deres email.

Dette var valgt for at tillade forsøgspersonerne at færdiggøre spillet på deres egne præmisser og i konteksten af hvornår de ellers ville tjekke deres email, for på denne måde at holde forsøget mere økologisk. For at opnå dette blev forsøgsspillet konstrueret gennem Processing 4, da det igennem dette program ville være hurtigt at konstruere en brugergrænseflade med de nødvendige krav for at opstille forsøgsrammerne, samt at det er muligt at eksportere spillet og sende det til forsøgspersonerne så disse kan spille spillet fjernt.

Yderligere har det været valgt at benytte spørgeskemaer der skulle evaluere forsøgspersonernes motivations niveau, samt at forsøgspersonerne blev bedt om at tilbagesende en datafil som programmet udskrev med resultater fra deres spilgennemgang.

Datafilen dokumenterede forsøgspersonens forsøgsidentifikation, deres bedømmelser af om de præsenterede emails var phishing emails eller almene emails. Fra anden iteration dokumenterede datafilen også hvor mange links forsøgspersonerne interagerede med, og om disse tilhørte almene emails eller phishingemails. Fra tredje udgave inkluderede denne datafil også information om hvor hurtigt de gennemførte spillet, dette var for at se hvor lang tid en bruger brugte på at gennemføre spillet, samt for at undersøge hvordan forsøgspersonerne prioriterede hastighed og præcision i dette simulerede miljø. Disse data var indsamlet for at kunne sammenligne forsøgspersonernes præstation på tværs af udgaverne og for at kunne analysere om programmet lykkedes med at skabe en vedvarende læringsoplevelse samt forsøgspersonernes motivationsniveau.

Spørgeskemaet der er brugt er baseret på self-determination teorien (SDT) og benyttes til at undersøge motivation hos forsøgspersonerne [Kooiman et al. (2016)], [Ryan and Deci (2020)]. SDT antager at mennesket er naturlig tiltrukket psykologisk vækst og integration, og heraf læring, beherskelse og at skabe forbindelser med andre [Ryan and Deci (2020)]. Dog er disse proaktive tendenser ikke set som værende automatiske, men at disse tendenser kræver robuste støttende konditioner for at de proaktive tendenser trives. Spørgeskemaet er opdelt i flere parametre. Heraf er de parametre som vil blive benyttet denne undersøgelse, interesse og nydelse, opfattet kompetence, opfattet valg og til sidst spænding og pres. Her er det parameteren interesse og nydelse, som er den bedste indikator for indre motivation. Dog ses det at der er en korrelation mellem interesse og nydelse, og opfattet kompetence og opfattet valg. Heraf er parameteret spænding og pres en negativ indikator for om der er indre motivation [for self-determination theory (2022)].

4.2.1 Første udgave

I første udgave af spillet blev forsøgspersonerne bedt om at gennemgå og bedømme niveau 1,2 og 3 af phishingemails samt almene emails. Hertil blev kun deres præstationsevne målt, samt rapporteret til forsøgspersonerne. Altså var det mest konkurrence drevne aspekt af denne iteration forsøgspersonernes evne til at følge med i deres egen præstation hvilket er med til at øge den indre motivation. I starten af spillet blev forsøgspersonerne bedt om at gennemlæse og give samtykke, se figur D.1. Herefter blev de bedt om at udfylde

et spørgeskema der indspurgte til demografisk information såsom forsøgspersonernes køn, alder, højeste færdiggjorte studieniveau, erfaringer med cybersikkerhed og hvor ofte de tjekkede deres emails. Herefter ville de gennemgå spillet ud fra de spillemekanismer der er beskrevet i afsnit 4. Til slut ville de blive bedt om at udfylde spørgeskemaet omhandlende motivation og kommentere hvis de havde yderligere kommentarer til spilforløbet. Selve samtykkeerklæringen kan blive set i appendisk D.

4.2.2 Anden udgave

Til forskel fra første udgave havde anden udgave niveauerne 2,3 og 4 af phishingemails samt almene emails. Hertil blev linkene i emailene gemt væk, men hjemmeside adresserne fremstod hvis forsøgspersonen holdt musen henover disse. Yderligere blev det indbygget at forsøgspersonerne kunne trykke på linksne for at indsamle kroner. Dette var gjort for at inkludere et nyt spilaspekt samt opfordre forsøgspersonerne til at interagere med linksne. Dog blev der også inkluderet kranier som blev aktiveret hvis forsøgspersonen trykkede på et link der var tilkoblet en phishing email, for på denne måde også at kunne holde øje med forsøgspersonernes interaktioner med emailene da et tryk på et af disse links ville tydeliggøre at emailen var en phishing email, og vi vil derfor kunne undersøge hvilke af disse links forsøgspersonerne faldt for.

4.2.3 Tredje udgave

Tredje udgave var en form for eksamination, hvor forsøgspersonerne blev fremvist niveau 2,3 og 4 af phishingmails, med de tidligere spilaspekter. Dog var der tilføjet et tidsmæssigt aspekt, her kunne forsøgspersonerne følge med i hvor lang tid det tog dem at klare sig igennem spillet. Hertil blev det valgt at tilføje trofæer man kunne opnå hvis man gennemføre spillet indenfor tidsgrænserne som hvert trofæ havde, for både at simulere et mere tidspresset og stresset miljø, hvor der oftere opstår fejl [Hancock and Tessian (2022)]. Yderligere udfordrede dette også forsøgspersonerne til at skulle vælge mellem et speed-accuracy tradeoff, hvor præcision er vigtigst i denne simulering, jævnføre at hvis man laver en fejl kan det koste mange penge, men prioriteringen af hastighed har fået værdi.

4.3 Rekruttering til forsøg

Til dette projekt blev forsøgspersonerne erhvervet på nogle forskellige måder. Den første metode var ved at lave et opslag på facebook både som et offentligt opslag, men også på AAU forsøgsperson facebook gruppe og linkedin, hvor at folk kunne skrive til os, eller kunne indskrive deres email i et erhvervnings spørgeskema, som simpelt bestod i den samme korte beskrivelse, som i opslaget, og at de skulle svare på spørgsmålet med den email, som de gerne ville modtage forsøget på.

Herud over blev forsøgspersonerne også indsamlet ved en konvniens samle, hvor der der mundtligt blev spurgt om forsøgspersonerne ville deltage i forsøget, dette blev også spredt


ved mund til mund metode, hvor der blev spurgt rundt i de forskellige sociale omgangskredse, om der var nogle som ville deltage i forsøget.

5 | Forsøg

For at udføre forsøget blev et undervisningsspil konstrueret, spillet kan ses i bilag 2. Det var her besluttet at forsøgsrammerne skulle fremstå velkendte og lignende noget forsøgspersonerne havde erfaring med. Det blev derfor besluttet at undervisningsspillet skulle efterligne internet versionen af Outlook, da denne ofte bliver benyttet i både studie og arbejdsammenhænge og derfor ville passe ind i simuleringen af et studiemiljø.

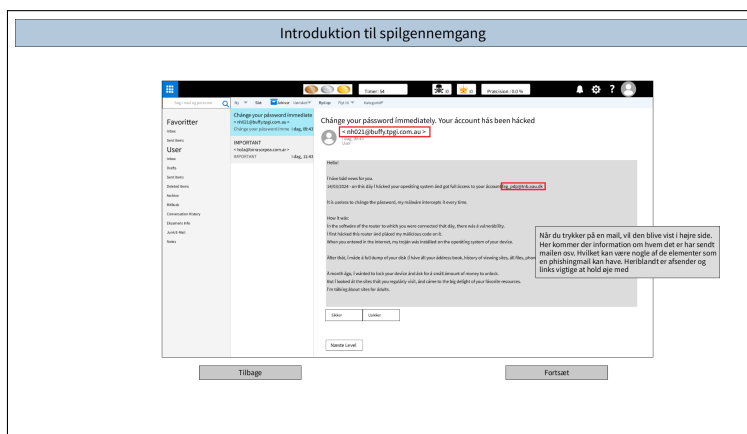
Spillet og forsøget blev designet med tanke på at det skulle kunne udføres til trods for at der ikke ville være en forsøgsleder til stede til at assistere forsøgspersonerne. Forsøgspersonerne blev derfor tilsendt en forsøgsvejledning i sammenhæng med når forsøgspersonerne fik tilsendt et link til spillet. Det første forsøgspersonerne blev præsenteret for ved opstart af spillets første gang, var samtykkeerklæringen som de var nødt til at erklære sig enig i for at kunne gå videre med spillet. Flowchart for første iteration af spillet kan ses i appendiks B, figur B.1. For yderligere at begrænse mulighederne for at forsøgspersonen kunne spille spillet forkert blev det besluttet at automatisk åbne et spørgeskema på en internetfane når de accepterede samtykkeerklæringen. Dette var gjort for at minimere risikoen for at forsøgspersonerne kunne undgå at udfylde de nødvendige dataindsamlinger. Dette er gjort for at kompensere for manglen på en fysisk tilstedeværende forsøgsvejleder. I slutningen af dette spørgeskema blev forsøgspersonen bedt om at genåbne spillet.

Forsøgspersonen ville herefter blive mødt af skærmen der kan ses på figur 5.1. Her blev forsøgspersonen bedt om at indskrive deres forsøgs identifikation, som var tilsendt med i forsøgsvejledningen. Dette blev gjort for at sikre at det ville være muligt at identificere forsøgspersonernes data efterfølgende, samt give en variabel der ville kunne bruges til at angive forsøgspersonens kononavn.

The image shows a simple web interface for registration. It consists of a white rectangular area with a thin black border. In the center, there is a text input field with the placeholder text 'Indgiv forsøgs ID'. To the right of the input field is a grey button with the text 'Fortsæt' in white.

Figur 5.1: Skærm til indskrivning af forsøgspersonens identifikation.

Efter forsøgspersonen havde logget ind i spillet ville de blive mødt af en række introduktions-skærme der havde til formål at vejlede forsøgspersonerne i hvordan de skulle interagere med spillet, sætte fokus på nye spilmekanismer og metoder til at identificere phishing emails. Et eksempel på dette kan ses på figur 5.2. Denne introduktion blev styret af en særskilt variabel, som var separeret fra den spiltilstandsvariabel der blev benyttet. Dette var valgt for at kunne tillade forsøgspersonerne at kunne gå tilbage og gense introduktions vejledningen uden at miste deres fremgang i spillet.



Figur 5.2: Vejledning som set i tredje iteration af forsøget.

Efter forsøgspersonerne havde gennemgået introduktions vejledningen ville spillet påbegynde. Her var det konstruerede spil en kopi af Outlook, med samme størrelsesforhold og farvevalg. Yderligere var alle knapper i spillet udstyret med den samme feedback som kan ses ved Outlook systemet. Dette var valgt, for at gøre spilrammen mere virkelighedsnært og være med til at promovere helhedsfølelsen af at forsøgspersonen interagerede med et almindeligt emailsystem. Samt forberede forsøgspersonerne på en potentielt virkelig tilsvarende situation [Gee (2013)].

Spillet blev designet med samme udgangspunkt som Basten (2017), hvor formålet var at forsøgspersonerne skulle gennemse emails for herefter korrekt at identificere hvilke emails der tilhørte henholdsvis phishingmails eller sikre emails. Formålet med spillet var at promovere en kritisk og forsigtig adfærd hos forsøgspersonerne, samt oplyse forsøgspersonerne om farerne således at der opstår færre fejl og at forsøgspersonerne undgår i fremtiden at falde for en phishing email. Til sidst har det hertil været valgt at prøve at skabe et kompetitivt miljø i spillet, hvor forsøgspersonerne løbende kan følge med i deres præstation under spillet, hvilket er med til at øge autonomi, kompetence, evnen til at fastholde informationen og læringsresultat [Xi and Hamari (2019)]; [Legaki et al. (2020)]. Yderligere er det valgt at spilleren skal kunne sætte tempoet ned i spillet og tage sig tiden til at overveje og bedømme emailene efter bedste mulighed for at promovere forsøgspersonernes præstation.

Efter spilleren har vurderet og tilegnet alle de fremviste emails en kategori, vil spilleren have

mulighed for at forøge spillets niveau ved at trykke på knappen "næste niveau". Såfremt denne knap bliver trykket på vil systemet tjekke at spilleren har givet alle emailene en kategori for at undgå potentielle mangler i datasættet.

Til anden og tredje iteration af spillet var der blevet tilføjet kroner og kranier. Dette var et spilelement som var tilføjet for at prøve at skabe en indre motivation for at spilleren kunne teste sig selv på at skaffe så mange kroner som muligt, uden at trykke forkert, på kranier. Dette er inspireret af Erkmann and Lomholt (2018) og Deci et al. (2001). Forsøgspersonerne kunne tilgå disse spilelementer ved at trykke på forskellige links, som var blevet præsenteret i emailene, hvis man trykkede på et "dårligt" link ville man få vidst et kranie på midten af sin skærm, og hvis man trykkede på et "godt" link ville man se en krone. Hertil var linksne blevet lavet blå, svarende til den blå som links har i en Outlooks email system. Flowchart for systemets funktionalitet i anden iteration kan findes i appendiks B, figur B.2.

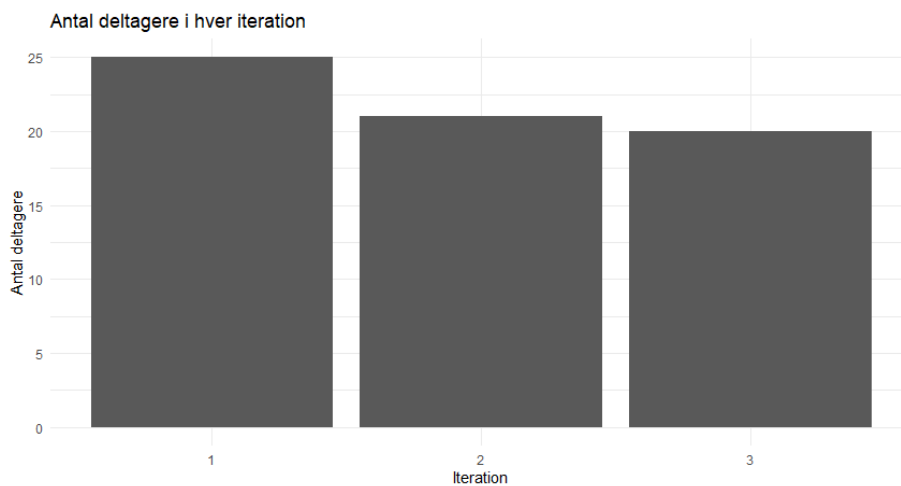
Scoren af hvor mange kranier og kroner, blev både vist i email systemet løbende, men også til slut ved den sidste side, hvor at forsøgspersonerne kunne se hvordan de havde klaret sig igennem spillet, hvilket blandt andet understøtter Ioannis Deliyannis and Lampoura (2023) om at belønninger til deltager i spillet, kan have en positiv effekt på indlæringen.

I tredje version af spillet, blev der tilføjet en anden form for motiverende spilelement, hvilket var en kombination af tid og tre medaljer. Her kunne forsøgspersonerne få en guld, sølv eller bronze medalje ud fra deres præstation. Dette blev gjort for at afprøve forsøgspersonernes evner de har bygget op under et sidste boss niveau [Erkmann and Lomholt (2018)]. Hvilket i dette tilfælde skulle være en kamp mod tiden, og det at få den bedste medalje som muligt. Flowchart for systemets funktionalitet i tredje iteration kan findes i appendiks B, figur B.3.

Efter spilleren har gennemført tredje niveau vil de blive fremvist en resultats skærm, hvor de vil blive præsenteret for deres præstation målt i andel procent de havde vurderet rigtigt, mængden af kranier og kroner og hvor lang tid det tog spilleren at gennemføre spillet. Yderligere får spilleren også feedback på hvilke potentielle fejl de kan have lavet igennem deres spilgennemgang, samt en forklaring af hvorfor det var en fejl. Dette var implementeret for at tilbyde spilleren en måde at evaluere deres præstation eller lære af potentielle fejl såfremt de ønskede det for at tilbyde feedback, men på spillerens præmis [Deci et al. (2001)]; [Koivisto and Hamari (2019)].

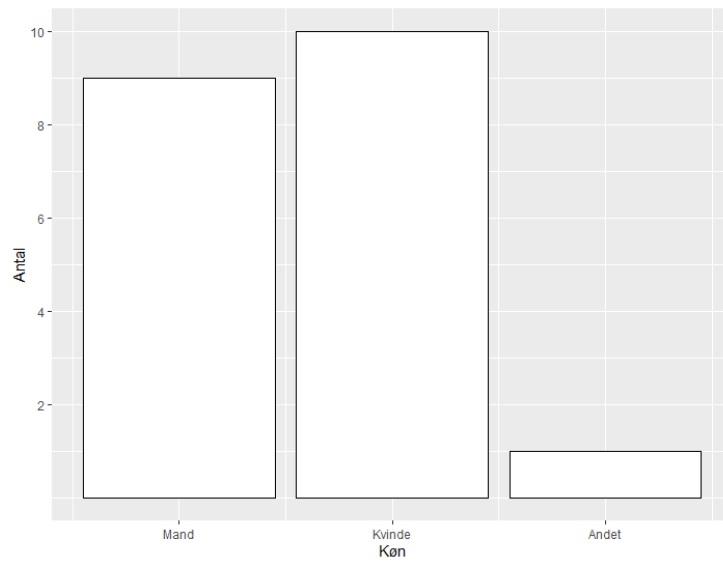
6 | Resultater fra dataanalyse

Til forsøget blev 37 forsøgspersoner erhvervet. Dog blev det efter gentagne test identificeret at spillet ikke virkede efter hensigten såfremt det blev tilsendt forsøgspersoner med Macbooks. Yderligere var der forsøgspersoner der havde tilmeldt sig at deltage i forsøget der ikke besvarede eller udførte forsøget, hvilket medførte at der blev indsamlet data fra mindre end de 37 forsøgspersoner. I første iteration blev data fra 25 forsøgspersoner indsamlet. Databehandlingen kan ses i bilag 1. I anden og tredje iterationer var der flere forsøgspersoner der ikke angav respons og der var derfor 21 og 20 forsøgspersoners data der var repræsenteret i anden og tredje runde, se figur 6.1 for graf over forsøgspersondeltagelse.



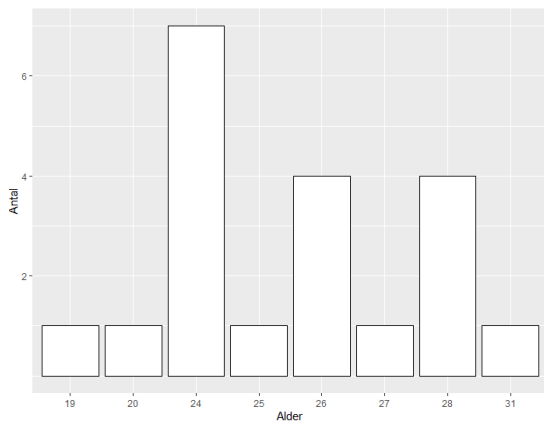
Figur 6.1: Data indsamlet fra deltagere igennem iterationerne.

Desuden var der 9 der svarede at de identificerede sig som mand, 10 som kvinde og én der identificerede sig som andet, hvilket kan ses på figur 6.2.

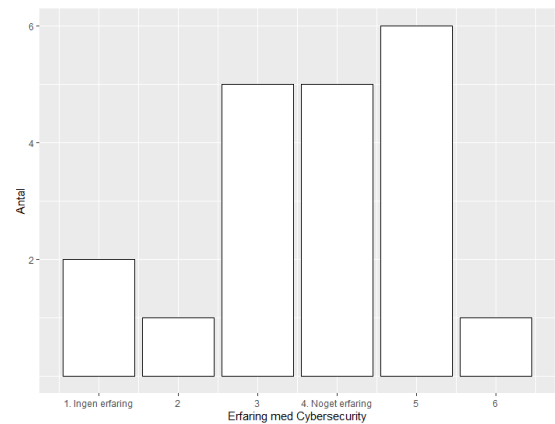


Figur 6.2: Data indsamlet fra deltagere igennem iterationerne.

Yderligere kan der ses på figur C.12 og 6.4, fordelingen af alder, uddannelses niveau, hvor ofte man tjekker sin email, og hvor meget erfaring forsøgspersonerne havde med cybersikkerhed.

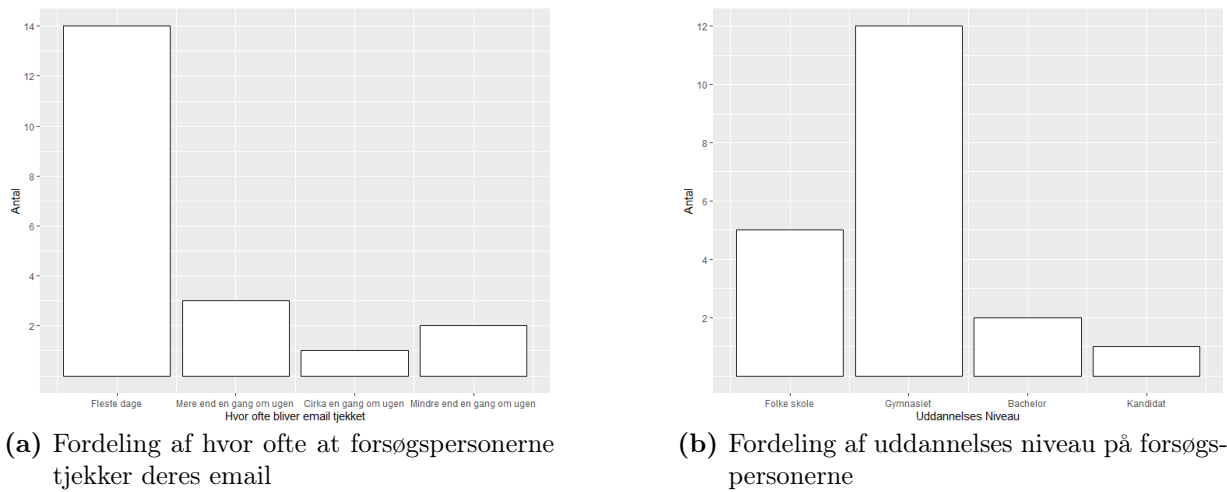


(a) Fordeling af alder på forsøgspersonerne



(b) Fordeling af erfaring på forsøgspersonerne

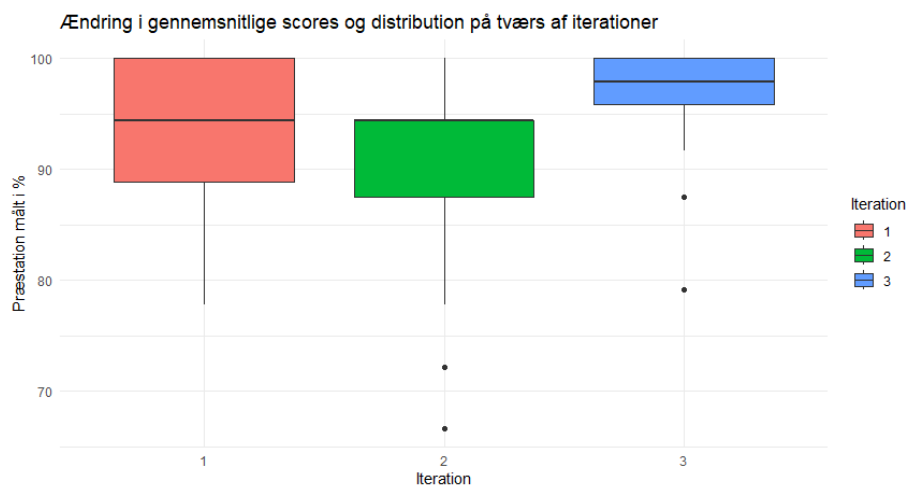
Figur 6.3: ret



Figur 6.4: ret

6.1 Præstationerne igennem spillet

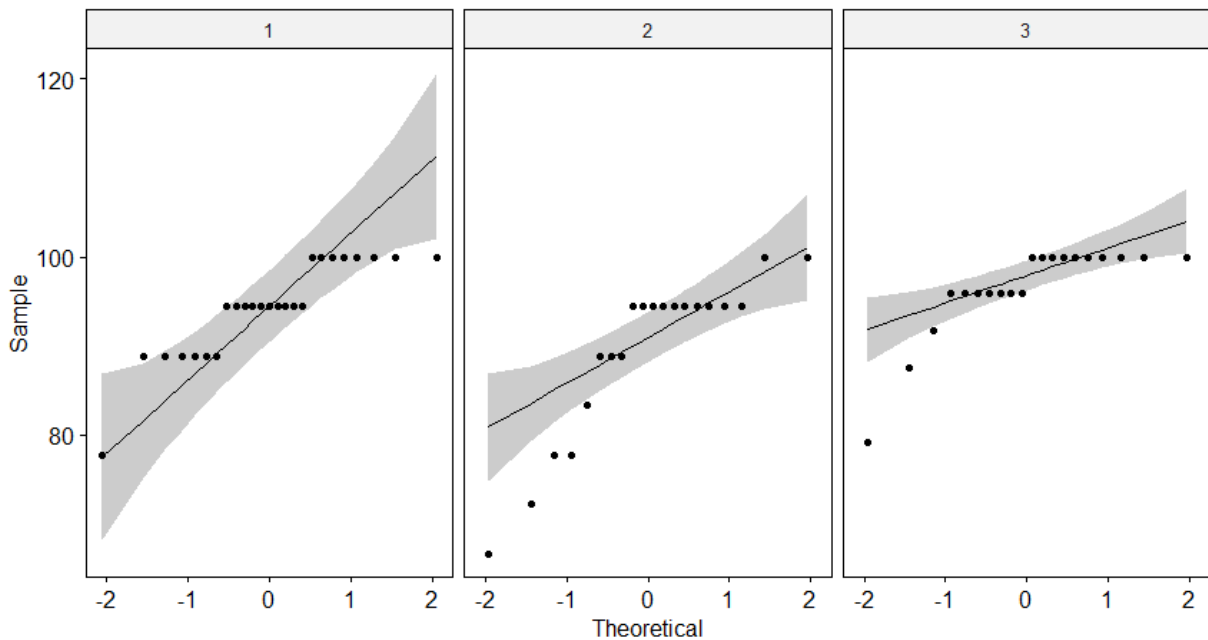
Yderligere blev der i forsøget målt hvor godt forsøgspersonerne klarede sig igennem iterationerne ift. at korrekt identificere phishing emailene fra de almene emails. Her blev forsøgspersonernes besvarelser omregnet til hvor stor en andel af emailene forsøgspersonerne besvarede korrekt. Herved er forsøgspersonernes data blevet beregnet som deres præstation afmålt i procent, hvilket er en indikation af den procentmæssige fordeling af emailene som forsøgspersonerne korrekt identificerede. Forsøgspersonernes resultater kan ses af figur 6.5.



Figur 6.5: Gennemsnitscore igennem iterationerne

Det kan af figur 6.5 ses at forsøgspersonerne havde en gennemsnitspræstation på 94,2% korrekt identificerede emails. Denne præstation var lavere i anden iteration hvor forsøgspersonerne

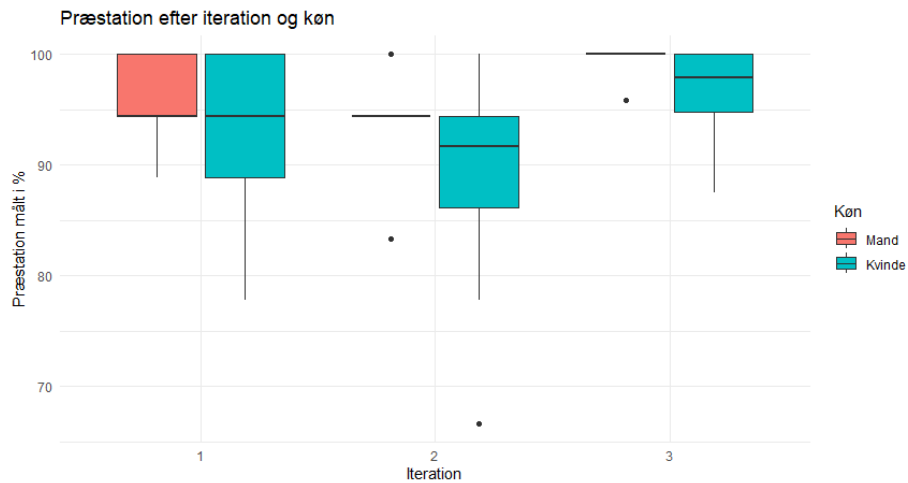
sonerne gennemsnitligt identificerede 89,5% af emailene korrekt. I tredje iteration formåede forsøgspersonerne at korrekt identificere 96,5% af emailene og havde dermed forbedret deres præstation fra anden iteration. Dataen overholdte ikke krav for at være parametriske, da en shapiro-wilk test gav statistiske signifikante resultater for alle iterationsdataene ($p < 0.01$) og er yderligere bekræftet af en Q-Q plot, dette kan ses figur 6.6.



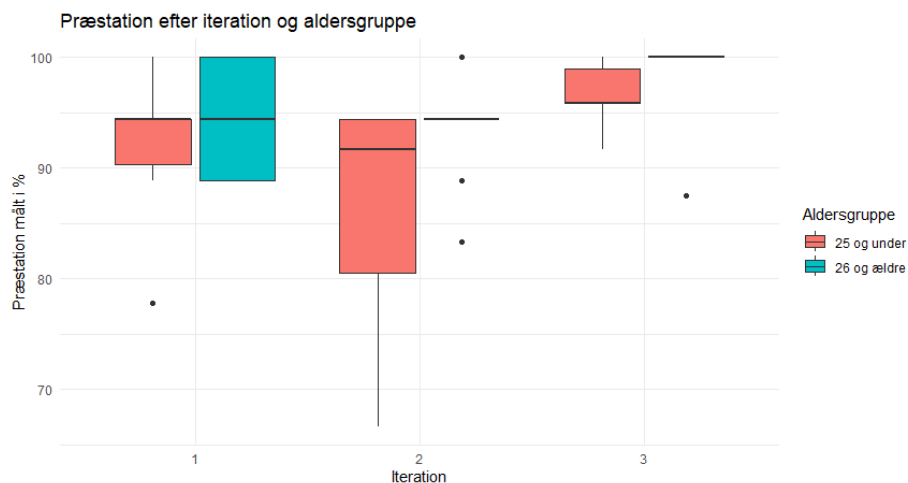
Figur 6.6: Q-Q plot for forsøgspersonernes præstation igennem spillet

Da data ikke er parametrisk vil der, istedet for en repeated measures ANOVA, blive benyttet en Friedman test, der fungerer som et nonparametrisk alternativ til repeated measures ANOVA. Her blev de forsøgspersoner som ikke deltog i alle forsøgs iterationerne, fjernet da det er et krav for testen. Friedman testen viste at der var signifikant forskel mellem iterationerne ($p < 0.01$). For at identificere hvor denne forskel mellem iterationerne var, blev en multiple comparison benyttet. Her blev der fundet statistisk signifikant forskel mellem anden og tredje iteration ($p < 0.01$). Der blev dog ikke fundet signifikant forskel mellem første og anden iteration samt første og tredje iteration.

Det er yderligere blevet undersøgt om der var signifikans som resultat af kontrolvariablerne, heraf forsøgspersonernes køn og alder indenfor iterationerne. Ingen af grupperings dataen overholdt kravene om normalfordeling efter undersøgelse ved brug af en shapiro-wilk ($p < 0.05$), hvoraf en Kruskal Wallis test blev benyttet til videre at undersøge om der var signifikante forskelle.



Figur 6.7: Boxplot over forsøgspersonernes præstation indenfor de køn som funktion af iterations nummeret.



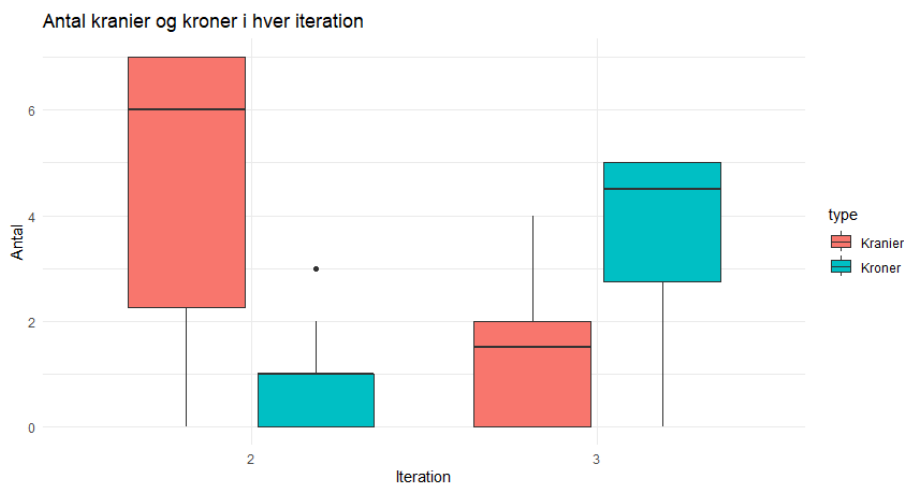
Figur 6.8: Boxplot over forsøgspersonernes præstation indenfor de forskellige iterationer som funktion af forsøgspersonernes alder.

Der blev dog ikke fundet nogle signifikante forskelle mellem mænd ($n = 9$) og kvinders ($n = 9$) præstation indenfor nogle af iterationerne ($p > 0.05$). Forsøgspersonernes alder blev inddelt mellem forsøgspersonerne i alderen 25 ($n = 9$) eller under og forsøgspersonerne over alderen 25 ($n = 10$). Der blev dog ikke fundet nogle statistiske signifikante forskelle mellem disse to aldersgruppers præstation indenfor iterationerne ($p > 0.05$).

Der var dog ikke en ligelig fordeling af forsøgspersoner indenfor de resterende kontrolvariabler: hyppighed af emailbrug, uddannelsesniveau og erfaring med cybersikkerhed. Dette medførte at det ikke var muligt at udføre inferentiell statistik, men kun at redegøre for disse kontrolvariabler deskriptivt. Dette kan ses i appendiks C.1.1

6.2 Kroner og kranier

Yderligere blev forsøgspersonernes antal indsamlede kranier og kroner dokumenteret for at opfordre forsøgspersonerne til at med negative links. Heraf er både kranier og kroner blevet sammenholdt for at identificere om forsøgspersonerne blev bedre til at identificere korrekte links, samt om de undgik negative links. I anden iteration af forsøget var det muligt for forsøgspersonerne at indsamle seks kroner, hvorimod det i tredje iteration var muligt for forsøgspersonerne at indsamle seks kranier. Til databehandlingen er forsøgspersonernes mængde af fundne kroner blevet omregnet til hvor stor en procentdel af det maksimale antal kroner de har fundet. Data af dette kan ses på figur 6.9.

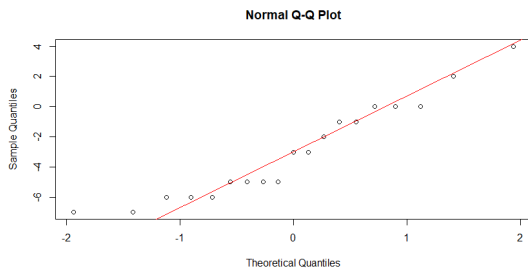


Figur 6.9: Boxplot over forsøgspersonernes indsamlede kranier og kroner som funktion af iterations nummeret.

Det blev fundet at forsøgspersonerne i anden iteration fandt gennemsnitligt 5,86 kranier og 1,27 kroner. Fra anden til tredje iteration var der dog en stor forbedring i deres fund af kranier og kroner. I tredje iteration fandt forsøgspersonerne gennemsnitligt 2,17 kranier og 4,30 kroner. Denne udvikling er undersøgt for statistisk signifikans. Det blev her fundet at kun kranie dataet overholdt kravene om normalfordeling ($p = 0.14$), dette er også bekræftet af Q-Q plottet der kan ses på figur 6.10a. Dataen for indsamlede kroner viste sig dog ikke at være normalfordelt ($p < 0.05$), denne fordeling kan ses på 6.10b.

Da dataen for kranierne var normalfordelt blev denne udvikling mellem iterationerne undersøgt med en paired t-test. Det blev her fundet at der var en statistisk signifikant forskel mellem iterationerne ($t(18) = 4.008, p < 0.001$). Dataen for kronerne viste sig ikke at være normalfordelt hvoraf en wilcoxon signed rank test blev benyttet istedet for. Her blev statistisk signifikant forskel fundet mellem iterationerne ($p < 0.001$).

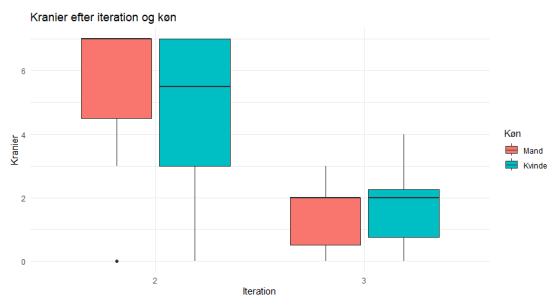
Det blev yderligere undersøgt om forsøgspersonernes køn ville have en indflydelse på indsamlingen af kranier og kroner. Datafordelingen kan ses på figur 6.11.



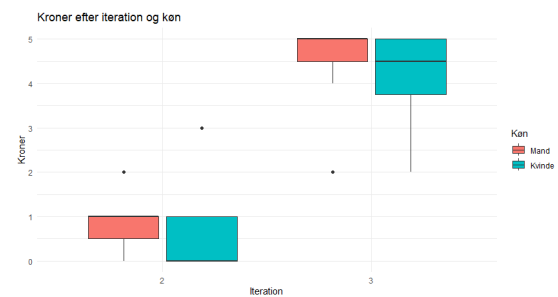
(a) QQplot for residual fordelingen over antal kranier fundet af forsøgspersonerne



(b) QQplot for residual fordelingen over antal kroner fundet af forsøgspersonerne

Figur 6.10: QQplots for kranie og krone dataerne.

(a) Boxplot for antal indsamlede kranier fordelt på forsøgspersonens køn som funktion af iterationen.



(b) Boxplot for antal indsamlede kranier fordelt på forsøgspersonens køn som funktion af iterationen.

Figur 6.11: Boxplots for kranie og krone data fordelt på forsøgspersonernes angivelse af køn.

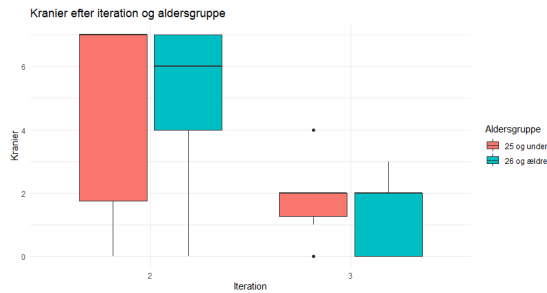
Dataen viste sig ikke at være normalfordelt for hverken anden eller tredje iterations indsamling af kranier og kroner ($p > 0.05$). Dataen blev derfor undersøgt ved brug af en kruskal wallis test, men ingen statistisk signifikant forskel blev fundet mellem kønnenes fund af kranier og kroner ($p > 0.05$).

Det blev også undersøgt om forsøgspersonernes alder havde en effekt på deres fund af kranier og kroner. Data fordelingen for disse kan ses på figur 6.12.

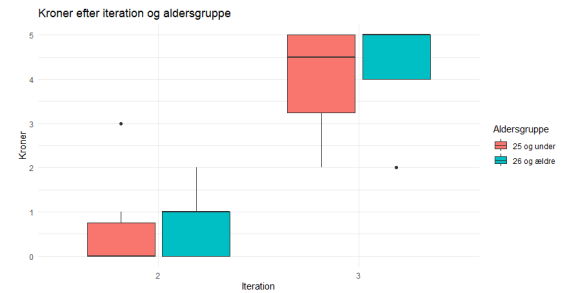
Dataene blev testet for normalfordeling, dog viste en shapiro-wilk test at data ikke var normalfordelt ($p < 0.05$). Det blev derfor undersøgt om alderen havde en effekt på forsøgspersonernes fund af kranier og kroner gennem kruskal wallis test. Dog blev ingen statistisk signifikant forskel fundet mellem forsøgspersonernes alder og hvor mange kranier eller kroner der blev fundet i iterationen ($p > 0.05$).

Data for kranier og kroner var ligesom ved præstations analysen tiltænkt at opholde mængden af funde kranier og kroner med hvor ofte forsøgspersonerne tjekkede deres email. Selve fortolkning og boxplots kan ses i afsnit C.1.2.

Sidst har det været tiltænkt at undersøge sammenhængen mellem forsøgspersonernes sub-



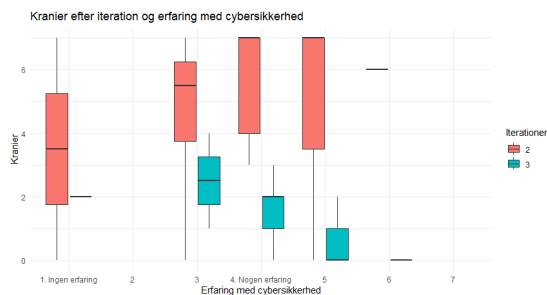
(a) Boxplot for antal indsamlede kranier fordelt på forsøgspersonens alder som funktion af iterationen.



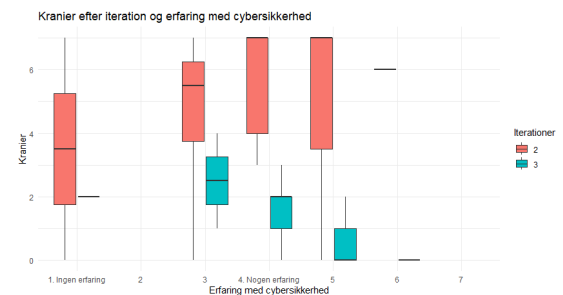
(b) Boxplot for antal indsamlede kranier fordelt på forsøgspersonens alder som funktion af iterationen.

Figur 6.12: Boxplots for kranie og krone data fordelt på forsøgspersonernes angivelse af alder, opdelt i to grupper: dem over 25 og dem på 25 eller yngre.

jektive erfaring med cybersikkerhed før påbegyndelsen af forsøget, og forsøgspersonernes indsamlede antal af kranier og kroner. Dataen heraf kan ses på figur C.6.



(a) Boxplot for antal indsamlede kranier fordelt på spil iterationen som funktion af forsøgspersonernes subjektive erfaring med cybersikkerhed.



(b) Boxplot for antal indsamlede kroner fordelt på spil iterationen som funktion af forsøgspersonernes subjektive erfaring med cybersikkerhed.

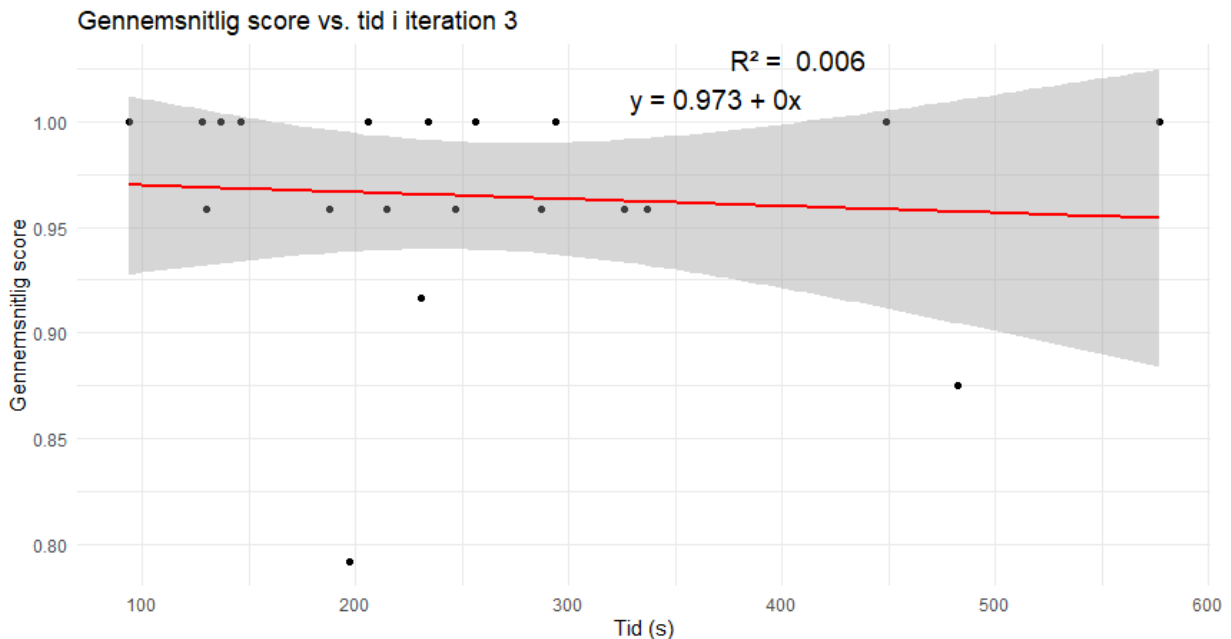
Figur 6.13: Boxplots for kranie og krone data fordelt på forsøgspersonernes angivelse af hvor meget erfaring de havde med cybersikkerhed før forsøgets påbegyndelse.

Af dataen fremkommer en tendens til at forsøgspersoner med mere erfaring med cybersikkerhed indsamlede flere kranier i første iteration af spillet, men færre i anden omgang. Dette er dog ikke sikkert og kan ikke bekræftes da det som nævnt ikke har været muligt at lave meningsfuld statistik.

6.3 Tidsmæssig aspekt

Det har yderligere været indsamlet hvor hurtigt forsøgspersonerne færdiggjorde tredje iteration af spillet. I spillet var der indsat en 10 sekunders tidsstraf for at svare forkert og indsamle kranier. Denne tidsstraf blev modregnet tiden det tog forsøgspersonerne at gen-

nemføre spillet før databehandling. Det tog gennemsnitligt forsøgspersonerne 258 sekunder at færdiggøre spillet. Tiden var indsamlet for bl.a. at identificere om hvordan forsøgspersonerne prioriterede præcision og hastighed, og om dette kunne ses. Resultaterne af dette kan ses på figur 6.14.



Figur 6.14: Speed-accuracy linear regression. $R^2 = 0.006$

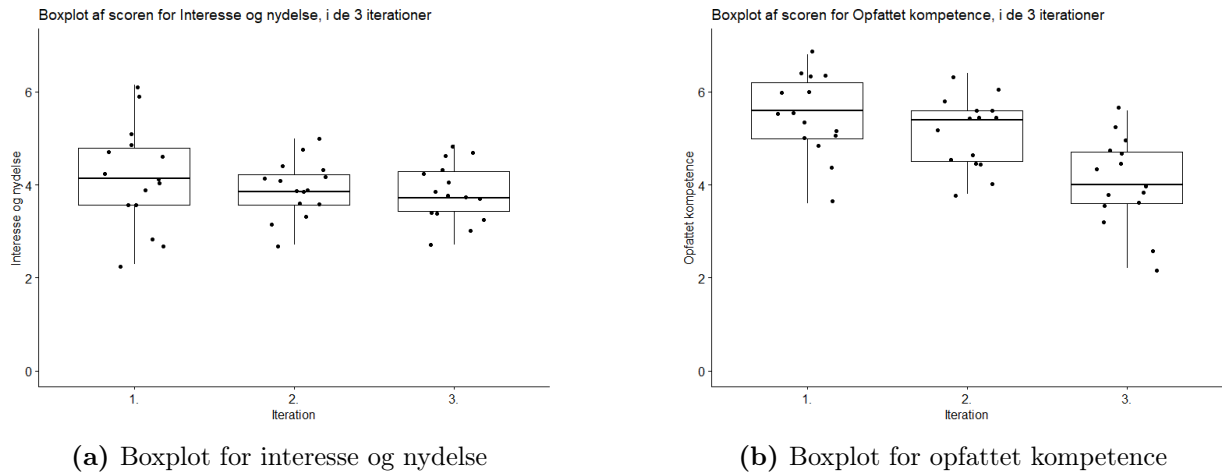
Det kan af figuren ses at der ikke var et forhold mellem forsøgspersonernes hastighed og deres præcision ($R^2 = 0.06$). Der er derfor ikke lavet yderligere undersøgelser på dette.

6.4 Spørgeskema

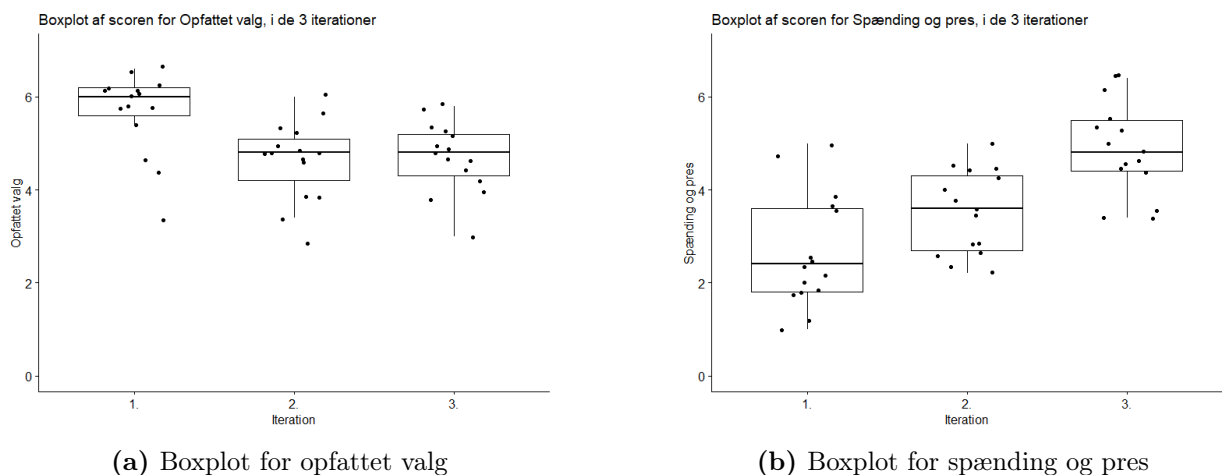
Dataen indsamlet fra det indre motivations spørgeskema blev behandlet efter anbefalingerne fra for self-determination theory (2022). Her blev værdierne fra spørgsmål 2, 9, 11, 14, 19 og 21 vendt, ved at trække de pågældende værdier fra 8, da disse spørgsmål var negativt formuleret i forhold til nogle af de andre spørgsmål. Dette var nødvendigt for at sikre konsistensen i analysen, det blev gjort for alle tre omgange af dataindsamlingen. Spørgeskemaet kan ses i appendiks A.

Når alle spørgsmålene var lagt sammen, kunne man beregne et gennemsnit. Disse gennemsnit kunne man derefter anvende til at lave statistiske undersøgelser, hvor de også fik betegnet underemner ("*Interesse og nydelse, Opfattet kompetence, Opfattet valg og Pres og spænding*"). Boxplots for de forskellige runder kan ses i figurene 6.15 og 6.16. Her kan det ses at der gennemsnitligt blev givet en score for Interesse og nydelse, for første iteration =

4.17, anden iteration = 3.91 og tredje Iteration = 3.84. Hernæst kunne det ses at gennemsnits scoren for opfattet kompetence var hhv. 5.51, 5.11 og 4.05. efterfølgende kan det ses for opfattet valg med hhv. et gennemsnit på 5.68, 4.63 og 4.71 for de tre iterationer, og til sidst kan de ses at for spænding og pres, var gennemsnit scoren på hhv. 2.67, 3.52 og 4.89.



Figur 6.15: Boxplot af data fra interesse og nydelse, og opfattet kompetence



Figur 6.16: Boxplots af data opfattet valg og spænding og pres

Ud fra boxplottene, kan det ses at både Interesse og nydelse og Opfattet kompetence falder og iterationerne, dog kan det også ses at Opfattet valg først stiger fra første til anden iteration, men falder efterfølgende, hvor at pres og spænding har den modsatte udvikling. Her falder pres og spænding fra første til anden iteration, men så stiger igen i tredje iteration.

Her blev der kun testet på de forsøgspersoner som indgik i alle iterationerne. Efter at data var blevet justeret, blev der lavet qqplots og shapiro-Wilks tests på alle underemnerne for

hver runde for at undersøge om der var tale om en sample size der var normalfordelt. Resultaterne viste, at data var normalfordelt for underemnerne Interesse og nydelse, Opfattet kompetence og Pres og spænding, dog var Opfattet valg ikke normalfordelt, p-værdierne fra shapiro-wilks test kan ses på tabel 6.4. For qqplotene for data i de tre iterationer, se C.2.1.

Underemne	Runde 1	Runde 2	Runde 3
Interesse og nydelse	p = 0.97	p = 0.99	p = 0.92
[H] Opfattet kompetence	p = 0.72	p = 0.60	p = 0.95
Opfattet valg	p < 0.01	p = 0.44	p = 0.80
Pres og spænding	p = 0.18	p = 0.33	p = 0.38

På baggrund af disse fund blev der anvendt en Repeated anova for Interesse og nydelse, Opfattet kompetence og Pres og spænding, og der blev anvendt Friedman's ANOVA test for at undersøge, om der var en effekt af spil elementerne på de forskellige underemner.

Her blev det fundet at Interesse og nydelse havde en p-værdi ($p = 0.29$), Opfattet kompetence ($p < 0.01$), Opfattet valg ($p < 0.01$) og Pres og spænding ($P < 0.01$). Hertil blev der lavet post hoc test på de underemner der var signifikante.

Efter at der var lavet en Pairwise t-test, for opfattet kompetence, var der fundet at der var en signifikant forskel mellem første og tredje iteration ($p < 0.01$) og mellem anden og tredje iteration ($P < 0.01$).

For Opfattet valg blev der brugt en Willcoxon signed rank test som post hoc. Denne viste at der var en signifikant forskel mellem første og anden iteration ($p < 0.01$) og mellem første og tredje iteration ($p < 0.01$).

For underemnet Pres og spænding blev der brugt en pairwise t-test som post hoc analyse. Resultatet af den viste at der var en signifikant forskel mellem alle iteratione. For første og anden iteration ($p = 0.04$), første og tredje iteration ($p < 0.01$) og for anden og tredje iteration ($p < 0.01$).

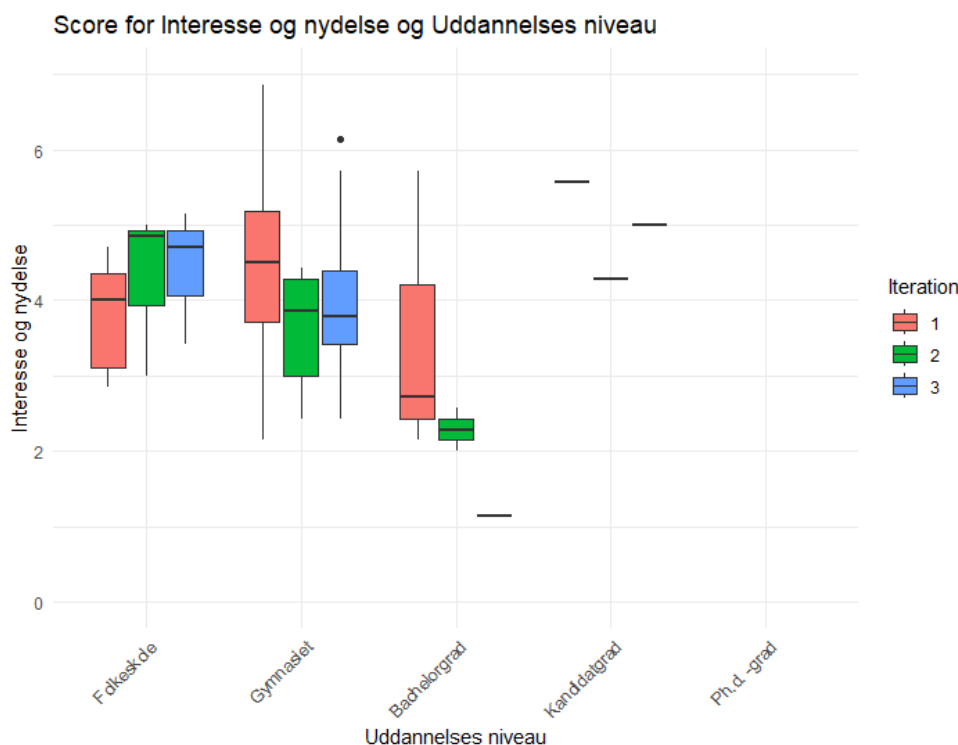
Der blev set på om køn, alder, niveau af uddannelse, erfaring med cybersikkerhed og hvor ofte man tjekker sin email, havde en effekt på hvordan forsøgspersonerne svarede på de forskellige underemner. Her blev der lavet en shapiro-wilk test for normal fordeling og efterfølgende blev der lavet en statistisk analyse for både køn og alder. For Uddannelses niveau, erfaring med cybersecurity og hvor ofte man tjekker sin email, blev der lavet boxplot for fremstilling af data. Dog var der ikke tilstrækkelige besvarelser til at man kunne lave god grupperinger at lave inferentiel statistik på, så dette data blev præsenteret gennem boxplot.

6.4.1 Kontrolvariabler

For emnerne: ("hvor ofte man tjekker sin email", "Uddannelsesniveau" og "hvor meget erfaring forsøgspersonerne havde med cybersikkerhed" blev der lavet boxplot for at se hvordan data fordelte sig, ud fra hvordan forsøgspersonerne havde svaret, og forsøgspersonernes uddannelses niveau, erfaring med cybersikkerhed og hvor ofte de tjekker deres email. I appendiks C.3.3 og C.3, kan boxplot for forsøgspersonernes køn og alder, da der her ikke var nogle statistisk signifikante resultater eller synlige tendenser.

6.4.1.1 Niveau af uddannelse

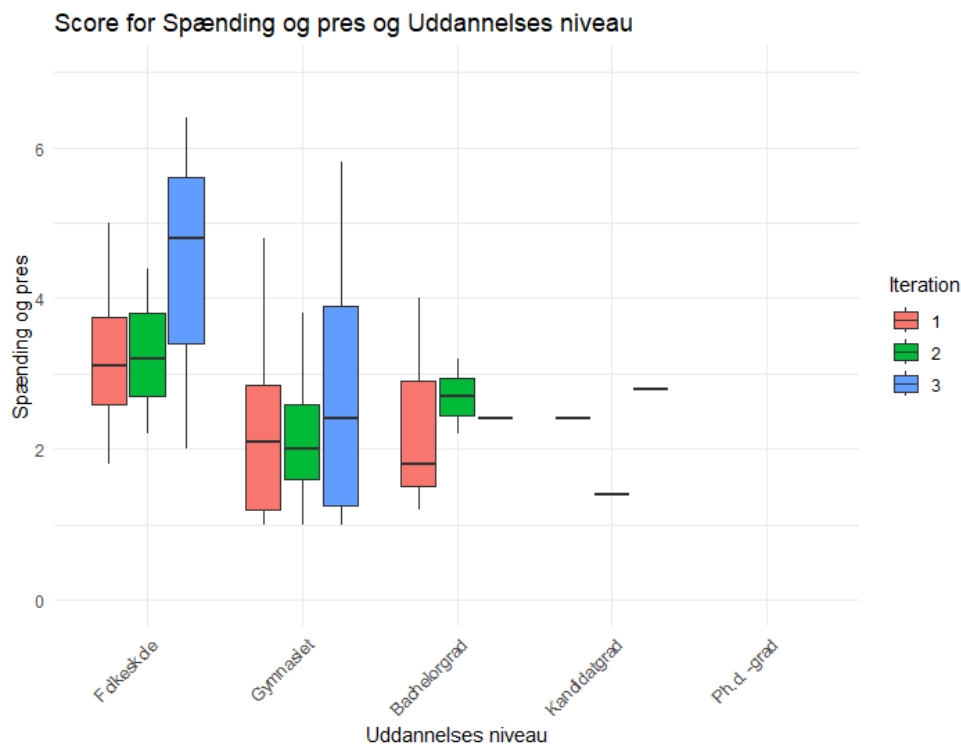
Der blev opstillet boxplot mellem hvor høj en uddannelse forsøgspersonerne havde, og hvordan de svarede på de fire under emner. Her ses interesse og nydelse stillet op med uddannelses niveau.



Figur 6.17: Boxplot af interesse og nydelse og hvad uddannelses niveau forsøgspersonerne senest havde færdiggjort

For dette underemne, var det for den gruppe som havde færdiggjort folkskolen sidst, at interesse og nydelse var stigende over iterationerne, men for dem som senest havde færdiggjort gymnasiet og bachelor, var der en tendens til at den var faldende. Dog har det ikke været muligt at bekræfte dette da der ikke har været nok data til at lave inferentiell databehandling.

Yderligere er det undersøgt om forsøgspersonernes uddannelse har haft en effekt på deres opfattede spænding og pres niveau.

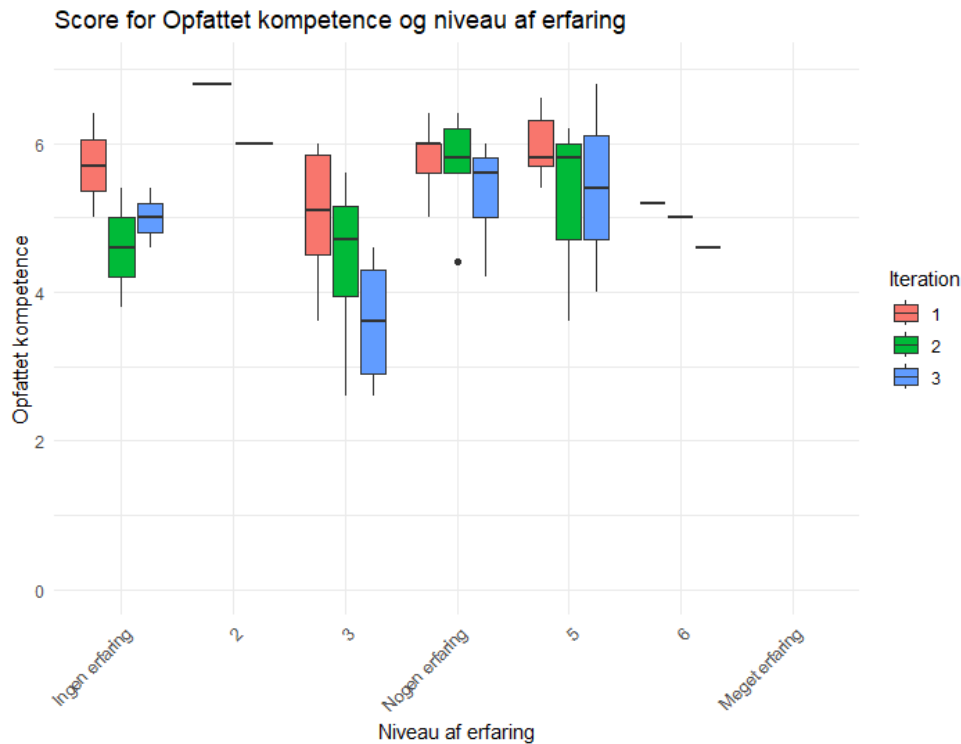


Figur 6.18: Boxplot af pres og spænding og hvad uddannelses niveau forsøgspersonerne senest havde færdiggjort

På figur C.24 kan det ses at dem med lavest uddannelses niveau har svaret at de føler sig mere presset end dem som har gennemført højere niveauer af uddannelse.

6.4.1.2 Erfaring med cybersikkerhed

Yderligere blev der lavet boxplot for de fire underemner og hvor meget erfaring forsøgspersonerne havde med cybersikkerhed. Hvor der her ses boxplot mellem opfattet kompetence og hvor meget erfaring med cybersikkerhed er sat op.



Figur 6.19: Boxplot af opfattet kompetence og hvor meget erfaring forsøgspersonerne har med cybersecurity

På figur C.26 ses det at for alle erfarings niveauer at opfattet kompetence falder over iterationerne, og at hvis man havde højere erfaring, var der tendens til at forsøgspersonerne svarede højere på opfattet kompetence.

6.5 Præstation sammenholdt med subjektiv evaluering

For at undersøge om der var en forskel mellem forsøgspersonernes subjektive bedømmelse og deres præstation blev disse sammenholdt indenfor hver iteration og undersøgt ved brug af en faktoriel ANOVA. Dog blev det fundet at intet af dataen levede op til kravet om normalfordeling ($p < 0.05$) hvoraf en ART ANOVA blev brugt som den nonparametriske pendant. Hertil blev kun en statistisk signifikant forskel fundet mellem præstation og og forsøgspersonernes opfattet kompetence. Denne statistiske signifikante forskel kunne ses i forsøgspersonernes besvarelser til den anden iteration ($F(11) = 8.626, p = 0.026$).

7 | Diskussion

Cybersikkerhed er et vigtigt emne for virksomheder såvel som individuelle personer, hvoraf at bruden på denne sikkerhed kan have store omkostninger. I denne forbindelse er phishing emails et stort problem, som kan ramme alle personer. Dog er det set at målgruppen unge mellem 18 og 34 år er dem som oftest falder for phishing emails. En måde som før er set benyttet til at undervise omkring faren ved phishing emails og andre cybersikkerhedsbrud er ved gamification. Ved brug af gamification i læringsperspektiv, kan der blive konstrueret et spil som kan motivere og på bedre måde fange og lærer den valgte målgruppe om phishing emails og hvad det er vigtigt at være opmærksom på. I denne rapport er der konstrueret et spil som efterligner Outlook emails design, hvor spilleren skal lærer at identificere phishing emails. Dette gøres ved at spilleren får fremstillet forskellige former for emails og derefter skal kategorisere dem som værende phishing eller almene emails. De phishing emails som blev præsenteret for spilleren blev konstrueret således at der var forskellige niveauer af sværhedsgrad. Det har dog været en udfordring at validere hvorvidt den iteration af email systemet blev opfattet som indeholdende sværere phishing email sammenlignet med dem fra tidligere iterationer. Den indsamlede data viser dog at forsøgspersonerne havde en lavere andel korrekt identificerede phishing email fra første til anden iteration af spillet hvor sværhedsgraden blev forøget. Dog kunne det have været en overvejelse at konstruere sværere phishing email, hvor phishing emailene ville approksimere spearphishing endnu mere. Dog ville en sværere spearphishing email kræve mere information fra forsøgspersonerne end hvad der var indsamlet i dette forsøg. Årsagen til at mere information ville have nødvendigt er, at de forsøg på at lave spearphishing email der blev benyttet i dette forsøg var baseret på den opstillede simulation og hvad der ville være sandsynlige scenarier forsøgspersonen ville kunne befinde sig i. Dog er disse scenarier ikke målrettet forsøgspersonens adfærd, sociale mønstre eller afsendt fra en person som forsøgspersonen har valideret som en sikker afsender. Af denne årsag ville det være nødvendigt at omstrukturere forsøget, og målrette spearphishing emailene til hver eneste forsøgsperson, hvilket ville medføre at det ville være sværere at verificere effekten af spillet. Dette ville være tilfældet da hver eneste forsøgsperson ville skulle have givet et unikt sæt af emails baseret på information omkring deres adfærd, sociale mønstre eller typiske kommunikationsemner og kommunikationspartnere.

Et andet forslag til email designet kunne være at lave forskellige niveauer, der hver især fokuserede på specifikke aspekter af phishing-teknikker, hvilket muligvis ville kunne gøre det lettere at formidle læringsmålne. Dette ville kunne være tilfældet da et niveau f.eks. kunne have temaet, identificering af farlige links, og gøre det lettere at målrette læringsmetodikker og feedback, da alle phishing emailene ville have samme tema. Dog ville dette muligvis kunne gøre simuleringen mere virkelighedsfjern da der sjældent ses en indbakke hvoraf alle emailene har et link de ønsker at man benytter.

Et andet udviklingspunkt, foruden emailene, kunne være at man kunne bruge kroner til at købe andet i spillet, såsom et anderledes udsende eller noget lignende dette [Erkmann and Lomholt (2018)]. Hvis der havde været et såkaldt formål med de objekter som man kunne samle i spillet, ville det evt. kunne have givet mere motivation til forsøgspersonerne, dog ville denne form for ydre motivation kun være kortvarig ifølge fund af Deci et al. (2001). En metode hvorpå man kunne hjælpe med indlæringen indenfor gamification, kunne være at påvirke den indre motivation [Deci et al. (2001)]. Her kunne et socialt scoreboard, til at kunne se sin egen præstation opholdt mod andres præstation, være en mulig ide. Dette var dog også forsøgt med det tidsmæssig aspekt i den 3. iteration, hvor at man kunne få en guld medalje alt efter hvor godt man klarede sig. Det tidsmæssige aspekt var dog mere stressende end motiverende, eftersom at det kun var pres og spænding, som steg i sidste iteration, hvor at interesse og nydelse var faldende. Her ville det måske havde været mere optimalt, hvis der var en bedre mulighed for at forsøgspersonerne kunne havde opnået en guldpræstation, i stedet for at det var svært at skaffe guldmedaljen. Yderligere ville en social scoretavle der sammenlignede brugerens tid med de resterende brugeres tid åbne op for at brugeren ville kunne gennemføre spillet med fokus på præcision eller det tidsmæssige aspekt, således at de kan sammenholde deres præcision og hvor lang tid de brugte med andre spillere. Dette ville give spilleren flere valgmuligheder ift. at tilpasse deres spillestil som ville skabe mere indre motivation for spilleren [Ioannis Deliyannis and Lampoura (2023)]. Det kunne derudover også ses at presset for forsøgspersonerne steg over iterationerne, se figur 6.15 og 6.15. Dette kan muligvis være sket grundet tilføjelsen af flere spilelementer som f.eks. at der var tilføjet en timer, som forsøgspersonerne kunne se tælle op. Dog kunne det ses at dem som havde uddannelses niveau på bachelor eller over, var overordnet mindre presset, se figur C.24.

Desuden ses der også at opfattet kompetence falder som funktion af iterationsnummeret. Her er det muligt at forsøgspersonerne først tænker at det er et nemt spil, og at de klarer sig okay, men gradvist falder både på deres opfattet kompetence og deres gennemsnitlige score. Her ses det at forsøgspersonernes opfattet kompetence falder igen i tredje iteration, men at deres gennemsnitlige score stiger, hvilket muligvis ville kunne forklares med Dunning Kruger teorien [Kruger and Dunning (1999)]. Dunning kruger teorien er at folk ser sine egne kompetencer i et særligt positivt lys i mange sociale og intellektuelle områder. Teorien er baseret på at individer kan fremkomme til denne konklusion, grundet et manglende forståelses grundlag, og at når disse individer tilegner sig mere viden vil de identificere hvor lidt de faktisk ved [Kruger and Dunning (1999)]. Personen genfinder selvtilliden i emnet, når man forstår og har lært mere. Dette kunne eventuelt være tilfældet med vores forsøgspersoner, hvor man efter en længere periode kan se, at forsøgspersonerne ville give en højere score til opfattet kompetence. Dette var dog ikke muligt, givet den periode der var til projektet.

7.1 Præstation

I dataanalysen blev statistiske signifikante forskelle fundet for forsøgspersonernes præstation mellem anden og tredje iteration. Denne forskel kan være fremkommet som et resultat af at forsøgspersonerne havde lært af deres erfaringer fra de tidligere iterationer, da der ikke var tilføjet sværere spørgsmål. Derfor kunne forsøgspersonerne fremvise deres indlæring og signifikant forbedre deres præstation mellem anden og tredje iteration. En sådan udvikling ville være understøttet af Ebbinghaus' forglemmelses kurve [Chun and Heo (2018)]. Ebbinghaus' forglemmelses kurve pointerer at ved vedvarende læring vil forglemmelses kurven aftage i hældning og forsøgspersonen vil kunne vedvare den nødvendige information over længere tid [Chun and Heo (2018)]. Dog har Ebbinghaus' forglemmelses kurve ikke været et undersøgelsespunkt for dette studie, og det er derfor uvist om forsøgspersonernes forbedring kan være fremkommet af denne årsag. Yderligere er det muligt at forsøgspersonerne ikke nødvendigvis har lært af deres fejl, men bare har været i stand til at huske hvilke emails der var phishing emails til den tredje iteration. Dette kunne være tilfældet da tredje iteration genbrugte emails der havde været fremvist i første og anden iteration.

Dog blev det fundet at forsøgspersonernes præstation i tredje iteration ikke har været statistisk signifikant anderledes fra deres præstation i første iteration hvor de ikke havde tidligere viden om emailsystemet eller de fremviste emails. For at sikkert kunne bekræfte om forsøgspersonerne fastholdt informationen bedre og havde lettere ved at fremkalde informationen ville det være nødvendigt at fortsætte forsøget over en betydeligt længere tidsperiode og med flere forsøgspersoner end hvad det var muligt at rekruttere i dette forsøg. Denne form for forsøg er dog produceret af Hoxhunt der fandt at deres brugere var blevet seks gange så gode til at identificere og rapportere phishing angreb i løbet af den første måned, og at dette udviklede sig til op mod ti gange så gode sammenlignet med da de startede [Kuivala (2024)].

Yderligere kunne dataen til dels indikere at forsøgspersoner der startede med mere erfaring indenfor cybersikkerhed, klarede sig bedre i iterationerne, desuden kunne det også ses at hvis forsøgspersonerne havde mere erfaring kunne der være en tendens til at de svarede højere på opfattede kompetence (see figur C.26, der var dog ikke et bredt nok dataset til at kunne bekræfte at dette var tilfældet. Det ville derfor være af interesse at genduføre forsøget på mere erfarne forsøgspersoner for at identificere om disse får samme udbytte af undervisningsspillet.

For at sikre at forsøgspersonerne havde lært særligt at evaluere videregående internet links de modtog i deres email blev mængden af gange forsøgspersonerne interagerede med disse links talt. Hertil blev forsøgspersonerne opfordret til at indsamle så mange kroner som muligt. Kronerne var her et symbol for at de identificerede og trykkede på et velment internetlink. Modsat ville forsøgspersonerne blive tildelt et kranie såfremt de valgte at trykke på et ondsindet link. Det var kun muligt at modtage en krone får hvert positive link der var tilstede i spillet. Modsat var det muligt at indsamle en ubegrænset mængde af kranier hvis forsøgspersonen gentagne gange blev ved med at interagere med de ondsindede inter-

net link. Resultaterne fra forsøget tegnede på at forsøgspersonerne hurtigt lærte at i større grad identificere ondsindede links fra de positive links. Der blev her fundet en statistisk signifikant udvikling på tværs af både kranier og kroner mellem anden og tredje iteration, med et fald i mængden af indsamlede kranier og en forøgning i mængden af indsamlede kroner. Dataen indsamlet i forsøget tegner dog på at forsøgspersoner med højere mængde cybersikkerhedserfaring var mere tilbøjelige til at interagere med ondsindede links i første iteration. Dog er der ikke nok data til at konfirmere dette, men med mere tid ville det være interessant at videre undersøge om dette var tilfældet. Såfremt at denne erfaring blev fundet efterfølgende kunne det være en indikation på at spillet skulle videreudvikles. Dette kunne være tilfældet da forsøgspersoner med erfaring muligvis identificerer at en hjemmeside i sig selv ikke nødvendigvis er skadelig, men at hjemmesiden kan kræve information af forsøgspersonen som gør den skadelig. I dette tilfælde vil det ikke være skadeligt at trykke på linket, men være skadeligt at udfylde information på hjemmesiden der bliver åbnet af dette. Dog var spillet i disse iterationer ikke sat op til at simulere eksterne hjemmesider der ønskede information af forsøgspersonen. Yderligere ville opsætningen af eksterne hjemmesider som forsøgte at lokke information ud af forsøgspersonen muligvis være en dårlig sammenkobling med et simuleret miljø. Dette kunne være tilfældet da forsøgspersonerne muligvis ikke ville være tilbøjelige til at indskrive deres information på disse hjemmesider, da forsøgspersonerne ville vide at disse hjemmesider ikke ville have nogen funktion udenfor det simulerede miljø.

Sidst har det været forsøgt at undersøge om forsøgspersonerne havde lavet en hastighed-nøjagtigheds afvejning, men det kunne ikke findes i dette forsøg. Yderligere var der en statistisk signifikant forskel på forsøgspersonernes subjektive opfattelse af parameteret Spænding og pres på tværs af iterationerne. Dette indikerer at eksistensen af det tidsmæssige aspekt havde en effekt på forsøgspersonernes præstation under forsøget, men det også kan have haft en indflydelse på forsøgspersonerens opfattelse af presset og spændingen i spillet. Dog er det muligt at det tidsmæssige aspekt har været med til at gøre forsøget mere interessant og nydeligt for forsøgspersonerne, da det ellers kunne forventes at noget af spillets nyhedsværdi ville forsvinde til sidste iteration, da ingen nye spillemekanikker blev introduceret. Det er derfor muligt at det tidsmæssige aspekt har haft en positiv indflydelse på f.eks. forsøgspersonernes interesse og nydelse af spillet, men at dette kun har modvirket den faldende nyhedsværdi. Ydermere ses det også på figur C.21 at interessen falder for forsøgspersonerne jo højere uddannelses niveau de har, desuden faldt det også over iterationerne, hvilket kan ses på figur 6.15, for interesse og nydelse, hvor det umiddelbart kan være nyhedsværdien i spillet som falder. For at modvirke denne effekt kunne der været udviklet en funktionalitet der havde fokus på at forsøgspersonen ville kunne gøre mere aktivt, og ikke bare være en passiv brik [Gee (2013)]. Dette kunne muligvis være modvirket ved at implementere et socialt scoretavle hvor forsøgspersonerne kan sammenligne sine egne resultater med andres resultater. Nyhedsværdien for et produkt falder hele tiden, medmindre der bliver tilføjet spilelementer, nye fortællinger eller lignende til spillet.

Overordnet har det desværre ikke været muligt at undersøge flere af kontrolvariablenes effekt i den detaljegråd det har været ønsket. Dog har den indsamlede data ikke indikeret

at kontrolvariablerne har haft en påvirkning på forsøgspersonernes besvarelser. Dette er med undtagelse af forsøgspersonernes erfaring med cybersikkerhed, hvor resultaterne kunne indikere en effekt på forsøgspersonernes præstation. Det har desværre ikke været muligt at bekræfte eller afkræfte om kontrolvariablerne har en effekt.

7.2 Forsøgsopstilling

I denne rapport var målgruppen studerende mellem 18 og 34 år, der studerer eller har færdiggjort deres studie indenfor de sidste tre år. Dog har det ikke været muligt at indsamle tilstrækkelig data til statistisk at undersøge om forsøgspersonernes uddannelses niveau, brugsfrekvens af deres email eller deres erfaringer med cybersikkerhed. yderligere har der ikke været nogle indikationer af at forsøgspersonernes køn eller alder har haft en betydning for deres præstation og opfattelse af forsøget. Det er desværre som nævnt uvist hvilken effekt de yderligere kontrolvariabler kan have haft, men af den indsamlede data er der indikationer mod at forsøgspersonernes erfaring med cybersikkerhed er den kontrolvariabel der kunne have størst betydning for forsøgspersonernes præstation igennem forsøget. Dog ville det være ønsket at gentage forsøget med flere forsøgspersoner for at identificere hvilken effekt kontrolvariablerne kan have haft. Det kunne i den forbindelse være interessant at indsamle forsøgspersoner i alle aldersgrupper og som ikke har været studerende indenfor de sidste tre år, for at identificere om simuleringen af en studiemail ville have samme effekt på forsøgspersoner der ikke er vant til de modtagne email.

Dog ville det også være muligt at udvide målgruppen betydeligt hvis forsøget i stedet for at være en spilsimulering, ville være inkorporeret direkte i forsøgspersonernes email, som gjort i f.eks. Hoxhunts program og forsøget udført af Broadhurst et al. (2018). I begge disse tilfælde ville forsøgspersonen modtage en email på deres personlige email. I Hoxhunts tilfælde vil forsøgspersonen skulle markere om emailen var sikker eller usikker på samme måde som i forsøget der blev opstillet i denne rapport. I forsøget af Broadhurst et al. (2018) blev forsøgspersonen bedt om at logge ind på en hjemmeside der var designet til at snyde dem for at indsamle deres login oplysninger. I begge tilfælde foregik forsøgene over forsøgspersonernes egen email konto, og emailene ville derfor være naturligt gemt væk bag emails der var realistiske for forsøgspersonen.

Dog fremkommer denne form for forsøg svært at introducere spearphishing email til, da forsøgspersonerne har individuelle interesser, typer af email der forekommer i deres email indboks og kan være meget forskellige steder i livet. Denne problematik er forsøgt løst ved at opstille et mere simuleret miljø hvor alle forsøgspersonerne skal forestille sig at være studerende, hvilket letteregøre processen i at konstruere email til spillet, og sørge for at forsøgspersonerne har samme forudsætninger for at gennemføre forsøget.

Dog kunne det ses i forsøget at flere af forsøgspersonerne ikke fik gennemført hele forsøget hvilket kan være et resultat af at forsøget kunne tage tage sted hvorend det passede forsøgspersonen og at vi ikke havde mulighed for at føre direkte opsyn med at forsøgspersonerne

gennemførte forsøget. Yderligere har forsøget foregået over tre iterationer, fordelt over tre uger. Dette har betydet at nogle forsøgspersoner har fået for travlt til at deltage i forsøget, eller har undgået at gennemføre forsøget til trods for gentagne forsøg på at minde forsøgspersonerne om at gennemføre forsøget. En anden problematik der kan være opstået er at forsøgspersonerne såfremt de ønskede, ville være i stand til at åbne den genereret datafil og ville kunne ændre den data der blev indsamlet. Dog er det antaget at forsøgspersonerne ikke aktivt har ønsket at gå imod forsøgspræmisserne og at det derfor har været muligt at antage data som troværdig. Dette er også bekræftet i at forsøgspersonerne sjældent fik 100% præcision igennem forsøget.

Med denne dataindsamlingsmetode og forsøgsopstilling er det nødvendigt at have en stor mængde forsøgspersoner da det ikke har været muligt at kontrollere eksterne variabler under forsøget, såsom at forsøgspersonerne kan have fået hjælp til at gennemføre forsøget. Det er dog som nævnt tidligere antaget at forsøgspersonerne har overholdt præmisserne for forsøget. Såfremt at forsøget foregik fysisk i et kontrolleret miljø ville flere af disse potentielle eksterne faktorer være lettere at kontrollere. Dog ville forsøgspersonerne ikke længere kunne gennemføre spillet i de miljøer hvor de almindeligvis ville tjekke deres emails. Yderligere ville et fysisk forsøg også kunne virke negativt på rekrutteringsprocessen, da det ville kræve mere af forsøgspersonen end at åbne et spil i deres egne rammer og tilbagesende en email med deres resultat.

Dog har det i forsøget ikke været muligt at erhverve flere forsøgspersoner til trods for at at rekrutteringsopslagene er blevet set op mod 2000 gange over LinkedIn, Facebook, forsøgspersons erhvervingsgrupper, og gennem direkte opfordringer til deltagelse i forsøget. En måde hvorpå det muligvis ville være muligt at erhverve flere forsøgspersoner ville være at tilbyde en kompensation for deres tid. Denne kompensation kunne evt. være i form af en økonomisk belønning der blev udgivet efter forsøgets afslutning. Dog har økonomisk kompensation ikke været tilbudt i dette forsøg, og det har ikke været muligt.

For den indre motivation kunne det ses ud fra spørgeskemaet, at interesse og nydelse blev vurderet til et niveau på ca. 4. Hvilket i sig selv er en middel vurdering, (se figur 6.15 og 6.16 for middel vurderingerne). Dog blev det fundet at den indre motivation var aftagende som et resultat af at forsøgspersonerne spillede spillet flere gange, til trods for de ændringer der var lavet. Ses der emnerne; opfattede kompetence og det opfattede valg, som er to af de tre emner der benyttes til at estimere indre motivation, har forsøgspersonerne vurderet disse emner over median værdien fire hvilket indikerer at forsøgspersonerne har oplevet en grad af indre motivation. Emnet interesse og nydelse der også benyttes til at estimere den indre motivation har dog en lidt lavere middel score, der bevæger sig lige under median værdien fire. Dog kan det ses at disse tre emner alle udvikler sig i en negativ retning i forbindelse med at forsøgspersonerne har spil iterationerne. Dette bliver og så bekræftet af parameteret spænding og pres. Der her en udvikling i positiv retning for emnet spænding og pres, som fungerer som en negativ indikator for indre motivation. Ved en sammenligning af alle parametrene er der en indikation af at det har været muligt at skabe noget indre motivation, men at denne effekt er hurtigt aftagende,

og at der derfor bør itereres på programmet. Dog er et udmærket resultat sammenlignet med resultaterne fra Lepper et al. (2005), som undersøgte på det indre motivationsniveau hos folkeskoleelever i USA. Her blev der fundet højere motivations niveauer hos de yngre elever, men der blev set et fald i de indre motivations niveauer i forbindelse med at de studerende havde læst længere, hvor at de studerende der gik i det tilsvarende til en dansk syvende klasse havde et middelt indre motivations niveau. Dog dækker undersøgelsen ikke over universitetsstuderende eller forsøgspersoner der har færdiggjort gymnasiet, så det er uvidst om dette fald i indre motivation fortsat ville være nedadgående. Såfremt at faldet fortsat ville være nedadgående, er det en indikation af at programmet konstrueret i dette forsøg har været succesfuldt i at skabe lidt mere indre motivation sammenlignet med klasseundervisning.

Videre udvikling I denne rapport blev et undervisningsspil konstrueret. Dog har dette spil fungeret som et proof of concept, da der har været lav skalerbarhed ved selve spillet. Dette er tilfældet da emailene som brugerne har været bedt om at bedømme, har været manuelt konstrueret. Dette har dog ikke været en problematik i projektets forløb grundet simuleringstilgangen. Dog betyder dette at der manuelt skal laves iterationer gentagne gange for at forsøge at skabe en interesse for forsøgspersonerne at gentage spillet. Det ville i stedet være optimalt hvis den manuelle konstruktion af emailene kunne udskiftes med en machine learning tilgang. Dog ville denne fremgang kræve et stort træningsdatasæt, som allerhelst ville skulle indholde phishing email samt forsøgspersoners subjektive bedømmelse af hvor svære disse var at detektere. Ud fra denne form for data ville et program kunne trænes i at konstruere niveau differencerede phishing email, som dermed ville kunne være med til at gøre forsøget mere skalerbart.

Såfremt at spillet bliver mere skalerbart vil det også være muligt at udvikle spillet i en lignende retning som det set af GeoGuessr [Girgin (2017)]. GeoGuessr er et populært spil der blandt andet kan benyttes til geografi undervisning. I GeoGuessr bliver spilleren givet et tilfældigt genereret billede fra Google Maps, og skal her deduktere hvor i verdenen at billedet er taget. Hertil får spilleren point afhængig af hvor tæt på den korrekte lokation de gætter. Yderligere er der også en mulighed for at spille mod andre spillere hvor en timer vil blive startet såfremt den ene spiller foretager et gæt på hvor lokationen er. I spillet konstrueret i dette forsøg er der både en præcision samt en timer inkluderet, hvoraf at der ville kunne tages inspiration i GeoGuessr metodik og med samme struktur opsætte en mulighed for at spillerne ville kunne udfordre hinanden i hvem der hurtigst og med størst præcision ville kunne identificere de genererede phishing emails. Dette ville sandsynligvis også være med til at øge den indre motivation hos spillerne da det vil udnytte ideen om social konkurrence [Erkman and Lomholt (2018)]. Såfremt at en udvikling i retning af GeoGuessr's model vil øge den indre motivation hos forsøgspersonerne kan det muligvis være med til at modvirke noget af den faldende nyhedsværdi i programmet.

8 | Konklusion

I dette projekt blev der udviklet og testet et spil med det formål at træne brugere i at identificere phishing-mails. Gennem tre iterationer blev spillets design og indhold videre udviklet. Der blev fundet signifikante forskelle i præstationer mellem anden og tredje iteration, hvilket kan tyde på en læringseffekt. Resultaterne viste også, at forsøgspersoner med højere uddannelsesniveaue og erfaring med cybersikkerhed klarede sig bedre, men der var ikke tilstrækkelig data til at konkludere dette med sikkerhed. Heraf kan spilbaseret læring kan forbedre forsøgspersonernes evne til at identificere phishing-mails, men der er behov for yderligere forskning og udvikling for at optimere spillets effektivitet. Yderligere blev det fundet at gamification skaber et mellem niveau af indre motivation. Dog blev det fundet at dette motivations niveau var faldende. Det er mistænkt at dette hænger sammen med en faldende interesse og nydelse, opfattet kompetence og opfattet valg i forbindelse med at forsøgspersonerne genspillede spillet. Dette kan skyldes spillets faldende nyhedsværdi og den tilføjede kompleksitet der gradvist blev tilføjet hver gang forsøgspersonerne spillede spillet.

Projektet viser at der er en mulig tendens til at studerende kan forbedre deres cybersikkerhed og reducere risikoen for databrud forårsaget af menneskelige fejl, såsom phishing-angreb, ved at deltage i spilbaseret træning. Projektet tyder på, at gentagne træningssessioner i et realistisk og udfordrende spilmiljø kan øge evnen til at identificere phishing-mails. For at opnå varige resultater bør træningsmetoderne løbende forbedres og tilpasses for at fastholde interesse og engagement. Dog bør der laves yderligere undersøgelser.

Som svar til problemformuleringen:

Hvordan konstrueres en spilbaseret trænings metode, med formål at skabe indre motivation indenfor undervisningen af cybersikkerhed?

Det har været muligt at konstruere en spilbaseret træningsmetode. Dog har det ikke været muligt at entydigt bekræfte at denne træningsmetode skaber indre motivation. Yderligere er der indikationer af at den indre motivation er faldende, og at der derfor skal itereres på det konstruerede spil for at opfylde kravene om at skabe indre motivation, fastholde de indre motivations niveauer og øge læringsudbyttet.

9 | Litteratur

- Frank Cremer, Barry Sheehan, Michael Fortmann, Arash N. Kia, Martin Mullins, Finbarr Murphy, and Stefan Materne. Cyber risk and cybersecurity: a systematic review of data availability. *Geneva papers on risk and insurance. Issues and practice*, 47(3):698–736, 2022. ISSN 1018-5895.
- Ani Petrosyan. Average cost of a data breach worldwide from may 2020 to march 2023, by industry, 2023. URL <https://www.statista.com/statistics/387861/cost-data-breach-by-industry/>.
- Danmarks Statistik. Halvdelen har oplevet it-sikkerhedsproblemer, 2020. URL <https://www.dst.dk/da/Statistik/nyheder-analyser-publ/nyt/NytHtml?cid=41944>.
- Gunikhan Sonowal. *Phishing and Communication Channels A Guide to Identifying and Mitigating Phishing Attacks*. Apress, Berkeley, CA, 1st ed. 2022. edition, 2022. ISBN 1-4842-7744-9.
- Erdal Ozkaya. *Cybersecurity : the beginner's guide : a comprehensive guide to getting started in cybersecurity*. Packt, Birmingham, 2019. ISBN 1-5231-2530-6.
- Calvin Nobles. Botching human factors in cybersecurity in business organizations. *HOLISTICA—Journal of Business and Public Administration*, 9(3):71–88, 2018.
- IBM Global Technology Services. Ibm security services 2014 cyber security intelligence index, 2014. URL <https://i.crn.com/sites/default/files/ckfinderimages/userfiles/images/crn/custom/IBMSecurityServices2014.PDF>.
- Jonathan Ness, Shon Harris, Chris Eagle, Terron Williams, Gideon Lenkey, and Allen Harper. *Gray Hat Hacking The Ethical Hackers Handbook, 3rd Edition*. McGraw-Hill Osborne Media, <country>US</country>, 2011. ISBN 0071742557. doi: 10.1036/9780071742566. URL <https://www.mhebooklibrary.com/doi/book/10.1036/9780071742566>.
- Mark Evans, Leandros A. Maglaras, Ying He, and Helge Janicke. Human behaviour as an aspect of cybersecurity assurance. *Security and Communication Networks*, 9(17):4667–4679, 2016. doi: <https://doi.org/10.1002/sec.1657>. URL <https://onlinelibrary.wiley.com/doi/abs/10.1002/sec.1657>.
- Jeff Hancock and Tessian. Understand the mistakes that compromise your company's cybersecurity, 2022. URL <https://f.hubspotusercontent20.net/hubfs/1670277/%5BCollateral%5D%20Tessian-Research-Reports/%5BTessian%20Research%5D%20Psychology%20of%20Human%20Error%202022.pdf?>

__hstc=&__hssc=&hsCtaTracking=8cc3440e-eb09-43bc-962f-51403868c8e0%7C37fefaef-476b-4bea-b78b-6a469a28172a.

Kayla Matthews. Iotw: Multiple yahoo data breaches across four years result in a 117.5 million settlement, 2019. URL <https://shorturl.at/XWu8v>.

Martyn Williams. Inside the russian hack of yahoo: How they did it, 2017. URL <https://www.csoonline.com/article/560623/inside-the-russian-hack-of-yahoo-how-they-did-it.html>.

Minttu Linja-aho. Creating a framework for improving the learnability of a complex system. *Human Technology: An Interdisciplinary Journal on Humans in ICT Environments*, 2: 202–224, 10 2006. doi: 10.17011/ht/urn.2006519.

Jonna Koivisto and Juho Hamari. The rise of motivational information systems: A review of gamification research. *International Journal of Information Management*, 45:191–210, 2019. ISSN 0268-4012. doi: <https://doi.org/10.1016/j.ijinfomgt.2018.10.013>. URL <https://www.sciencedirect.com/science/article/pii/S0268401217305169>.

Katie Seaborn and Deborah I. Fels. Gamification in theory and action: A survey. *International Journal of Human-Computer Studies*, 74:14–31, 2015. ISSN 1071-5819. doi: <https://doi.org/10.1016/j.ijhcs.2014.09.006>. URL <https://www.sciencedirect.com/science/article/pii/S1071581914001256>.

Ming-Shiou Kuo and Tsung-Yen Chuang. How gamification motivates visits and engagement for online academic dissemination – an empirical study. *Computers in Human Behavior*, 55:16–27, 2016. ISSN 0747-5632. doi: <https://doi.org/10.1016/j.chb.2015.08.025>. URL <https://www.sciencedirect.com/science/article/pii/S0747563215301011>.

William R. Watson, Christopher J. Mong, and Constance A. Harris. A case study of the in-class use of a video game for teaching high school history. *Computers and education*, 56(2):466–474, 2011. ISSN 0360-1315.

Adrian Dominguez, Joseba Saenz-de Navarrete, Luis de Marcos, Luis Fernandez-Sanz, Carmen Pages, and Jose-Javier Martinez-Herraiz. Gamifying learning experiences: Practical implications and outcomes. *Computers and education*, 63:380–392, 2013. ISSN 0360-1315.

Nikoletta-Zampeta Legaki, Nannan Xi, Juho Hamari, Kostas Karpouzis, and Vassilios Assimakopoulos. The effect of challenge-based gamification on learning: An experiment in the context of statistics education. *International Journal of Human-Computer Studies*, 144:102496, 2020. ISSN 1071-5819. doi: <https://doi.org/10.1016/j.ijhcs.2020.102496>. URL <https://www.sciencedirect.com/science/article/pii/S1071581920300987>.

Nannan Xi and Juho Hamari. Does gamification satisfy needs? a study on the relationship between gamification features and intrinsic need satisfaction. *International Journal of Information Management*, 46:210–221, 2019. ISSN 0268-4012. doi: <https://doi.org/10.1016/j.ijinfomgt.2018.12.002>. URL <https://www.sciencedirect.com/science/article/pii/S0268401218307436>.

- Edward L. Deci, Richard Koestner, and Richard M. Ryan. Extrinsic rewards and intrinsic motivation in education: Reconsidered once again. *Review of Educational Research*, 71(1):1–27, 2001. ISSN 0034-6543.
- Patrick Buckley and Elaine Doyle. Gamification and student motivation. *Interactive learning environments*, 24(6):1162–1175, 2016. ISSN 1049-4820.
- Christopher W. Craighead. Right on target for time-series forecasting. *Decision sciences journal of innovative education*, 2(2):207–212, 2004. ISSN 1540-4595.
- Brent Snider and Janice B. Eliasson. Beat the instructor: An introductory forecasting game: Beat the instructor. *Decision sciences journal of innovative education*, 11:147–157, 2013. ISSN 1540-4595.
- Rocio Lorenzo-Alvarez, Teodoro Rudolphi-Solero, Miguel J. Ruiz-Gomez, and Francisco Sendra-Portero. Game-based learning in virtual worlds: A multiuser online game for medical undergraduate radiology education within second life. *Anatomical sciences education*, 13(5):602–617, 2020. ISSN 1935-9772.
- Vivian Magdi Samuel, Maria Blesilda Blesilda Llaguno, Mini Rani Mary Beth, Medel Oabel Cabalsa, and Heba Mahmoud Mahmoud. Digital gamification: An innovative pedagogy for anatomy and physiology course among medical-surgical nursing students. *Assiut Scientific Nursing Journal*, 10(28):1–14, 2022.
- Cecilia Cheng and Omid V. Ebrahimi. Gamification: a novel approach to mental health promotion. *Current psychiatry reports*, 25(11):577–586, 2023. ISSN 1523-3812.
- Joakim Kävrestad. Context-based micro-training: Enhancing cybersecurity training for end-users, 2022.
- Elmer Lastdrager, Inés Gallardo, Marianne Junger, and Pieter Hartel. How effective is anti-phishing training for children?, 07 2017.
- Melad Mohamed Al-Daeef, Nurlida Basir, and Madihah Mohd Saudi. Security awareness training: A review. In *Lecture Notes in Engineering and Computer Science*, volume 2229, pages 446–451, Hong Kong, 2017. International Association of Engineers. ISBN 9789881404749.
- Simon Stockhardt, Benjamin Reinheimer, Melanie Volkamer, Peter Mayer, Alexandra Kunz, Philipp Rack, and Daniel Lehmann. Teaching phishing-security: Which way is best? In *ICT Systems Security and Privacy Protection*, volume 471, pages 135–149, Cham, 2016. Springer International Publishing. ISBN 3319336290.
- Hussain Aldawood and Geoffrey Skinner. Reviewing cyber security social engineering training and awareness programs—pitfalls and ongoing issues. *Future internet*, 11(3):73–, 2019. ISSN 1999-5903.
- Gokul Chettoor Jayakrishnan. Passworld: A serious game to promote password aware-

- ness and diversity in an enterprise, Aug 2020. URL <https://www.usenix.org/system/files/soups2020-jayakrishnan.pdf>.
- Sofia Maria Poulimenou Ioannis Deliyannis, Polyxeni Kaimara and Stamatella Lampoura. *Gamification - Analysis, Design, Development and Ludification*. IntechOpen, 2023. ISBN 1-80356-262-5.
- Malene. Erkmann and Pernille. Lomholt. *Gamification : læring gennem spil og konkurrence*. Samfundslitteratur, Frederiksberg, 1. udgave. edition, 2018. ISBN 9788759331927.
- T.H. Silva, C.S.F.S. Celes, J.B.B. Neto, V.F.S. Mota, F.D. da Cunha, A.P.G. Ferreira, A.I.J.T. Ribeiro, P.O.S. Vaz de Melo, J.M. Almeida, and A.A.F. Loureiro. Chapter 3 - users in the urban sensing process: Challenges and research opportunities. In Ciprian Dobre and Fatos Xhafa, editors, *Pervasive Computing, Intelligent Data-Centric Systems*, pages 45–95. Academic Press, Boston, 2016. ISBN 978-0-12-803663-1. doi: <https://doi.org/10.1016/B978-0-12-803663-1.00003-6>. URL <https://www.sciencedirect.com/science/article/pii/B9780128036631000036>.
- Richard H Thaler and Cass R Sunstein. *Nudge: Improving Decisions about Health, Wealth, and Happiness*. Concentrated knowledge for the busy executive. Yale University Press, New Haven, USA, 1 edition, 2008. ISBN 0300122233.
- James Paul Gee and Amy Price. Game-design teaching and learning. *Strategies (Reston, Va.)*, 34(3):35–38, 2021. ISSN 0892-4562.
- Alf Inge Wang and Rabail Tahir. The effect of using kahoot! for learning – a literature review. *Computers and education*, 149:103818–, 2020. ISSN 0360-1315.
URL <https://www.hoxhunt.com/>.
- Hoxhunt launches breakthrough human risk management platform, 2023.
- Petri Kuivala. A human cyber-risk report with hope, for a change, 02 2024. URL <https://www.hoxhunt.com/blog/practical-phishing-cybersecurity-behavior-trends>.
- Cybersecurity games - texas am universitet, 03 2024. URL <https://it.tamu.edu/security/cybersecurity-games/index.php>.
- Dirk Basten. Gamification. *IEEE Software*, 34(5):76–81, 2017. doi: 10.1109/MS.2017.3571581.
- Mark Wilson and Joan. Hash. *Building an information technology security awareness and training program*. NIST special publication ; 800-50. Computer security. U.S. Dept. of Commerce, Technology Administration, National Institute of Standards and Technology, Gaithersburg, MD, 2003.
- Nuhan Rahman, I. Sairi, N. Zizi, and Fariza Khalid. The importance of cybersecurity education in school. *International Journal of Information and Education Technology*, 10:378–382, 01 2020. doi: 10.18178/ijiet.2020.10.5.1393.

- Ani Petrosyan. Average daily time spent using the internet by 3rd quarter 2023, by age and gender, 2024. URL <https://www.statista.com/statistics/1378510/daily-time-spent-online-worldwide-by-age-and-gender/>.
- Census. Phishing attacks – who is most at risk?, 2021. URL <https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/phishingattackswhoismostatrisk/2022-09-26>.
- Jenny Bittner and Jeffrey Schipper. Motivational effects and age differences of gamification in product advertising. *Journal of Consumer Marketing*, 31:391–400, 08 2014. doi: 10.1108/JCM-04-2014-0945.
- FBI. Internet crime report, 2023. URL https://www.ic3.gov/media/pdf/annualreport/2023_ic3report.pdf.
- Roderic Broadhurst, Katie Skinner, Nick Sifniotis, Bryan Matamoros-Macias, and Yuguang Ipsen. Phishing and cybercrime risks in a university student community. *SSRN Electronic Journal*, 11 2018. doi: 10.2139/ssrn.3176319.
- John A. Ellis, George B. Semb, and Brian Cole. Very long-term memory for information taught in school. *Contemporary Educational Psychology*, 23(4):419–433, 1998. ISSN 0361-476X. doi: <https://doi.org/10.1006/ceps.1997.0976>. URL <https://www.sciencedirect.com/science/article/pii/S0361476X97909760>.
- Bo Ae Chun and Hae Ja Heo. The effect of flipped learning on academic performance as an innovative method for overcoming ebbinghaus' forgetting curve. In *Proceedings of the 6th International Conference on Information and Education Technology*, ICIET '18, page 56–60, New York, NY, USA, 2018. Association for Computing Machinery. ISBN 9781450353595. doi: 10.1145/3178158.3178206. URL <https://doi.org/10.1145/3178158.3178206>.
- Bill Gardner and Valerie Thomas. *Building an Information Security Awareness Program: Defending Against Social Engineering and Technical Threats 1st Edition*. 08 2014. ISBN ISBN-10: 0124199674 ISBN-13: 978-0124199675.
- Ian Fette, Norman Sadeh, and Anthony Tomasic. Learning to detect phishing emails. pages 649–656, 05 2007. doi: 10.1145/1242572.1242660.
- Brian Kooiman, Wenling Li, Michael Wesolek, and Heeja Kim. Validation of the relatedness scale of the intrinsic motivation inventory. *International Journal of Multidisciplinary Research and Modern Education*, 1:302–311, 01 2016.
- Richard M. Ryan and Edward L. Deci. Intrinsic and extrinsic motivation from a self-determination theory perspective: Definitions, theory, practices, and future directions. *Contemporary Educational Psychology*, 61:101860, 2020. ISSN 0361-476X. doi: <https://doi.org/10.1016/j.cedpsych.2020.101860>. URL <https://www.sciencedirect.com/science/article/pii/S0361476X20300254>.

Center for self-determination theory. Intrinsic motivation inventory (imi). 2022.

James Paul. Gee. *Good video games and good learning : collected essays on video games, learning and literacy*. New literacies and digital epistemologies vol. 67. Peter Lang, New York, second edition edition, 2013. ISBN 1-4539-1162-6.

Justin Kruger and David Dunning. Unskilled and unaware of it: How difficulties in recognizing one's own incompetence lead to inflated self-assessments. *Journal of personality and social psychology*, 77(6):1121–1134, 1999. ISSN 0022-3514.

Mark R Lepper, Jennifer Henderlong Corpus, and Sheena S Iyengar. Intrinsic and extrinsic motivational orientations in the classroom: Age differences and academic correlates. *Journal of educational psychology*, 97(2):184–196, 2005. ISSN 0022-0663.

Mustafa Girgin. Use of games in education: Geoguessr in geography course. 1(1):1–, 2017. ISSN 2602-2885.

Appendikser

A | Spørgeskema til evaluering af motivation

Spørgsmålene som der er i spørgeskemaet. Disse skal vurderes af forsøgspersonerne fra 1 til 7. Hvor 1 svare til "Not true at all", 4 svare til "somewhat true" og 7 svare til "very true".

- 1. While I was working on the task I was thinking about how much I enjoyed it.
- 2. I did not feel at all nervous about doing the task.
- 3. I felt that it was my choice to do the task.
- 4. I think I am pretty good at this task.
- 5. I found the task very interesting.
- 6. I felt tense while doing the task.
- 7. I think I did pretty well at this activity, compared to other students.
- 8. Doing the task was fun.
- 9. I felt relaxed while doing the task.
- 10. I enjoyed doing the task very much.
- 11. I didn't really have a choice about doing the task.
- 12. I am satisfied with my performance at this task.
- 13. I was anxious while doing the task.
- 14. I thought the task was very boring.
- 15. I felt like I was doing what I wanted to do while I was working on the task.
- 16. I felt pretty skilled at this task.
- 17. I thought the task was very interesting.
- 18. I felt pressured while doing the task.
- 19. I felt like I had to do the task.
- 20. I would describe the task as very enjoyable.
- 21. I did the task because I had no choice.
- 22. After working at this task for awhile, I felt pretty competent.

Herunder kan det ses hvordan spørgeskemaet var præsenteret for forsøgspersonerne.

What is your designated ID? (It can be viewed in the received mail)

FORRIGE NÆSTE

28%

Figur A.1: Side 1 af spørgeskemaet

The following questions will be shown in a scale, and we will be asking you to evaluate the following questions based on your experience with the educational game. It is important that you answer to the best of your ability. There are no wrong answers.

FORRIGE NÆSTE

42%

Figur A.2: Side 2 af spørgeskemaet

While I was working on the task I was thinking about how much I enjoyed it.

1. Not at all true	2.	3.	4. Somewhat true	5.	6.	7. Very true
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

I did not feel at all nervous about doing the task.

1. Not at all true	2.	3.	4. Somewhat true	5.	6.	7. Very true
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

I felt that it was my choice to do the task.

1. Not at all true	2.	3.	4. Somewhat true	5.	6.	7. Very true
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

I think I am pretty good at this task.

1. Not at all true	2.	3.	4. Somewhat true	5.	6.	7. Very true
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

I found the task very interesting.

1. Not at all true	2.	3.	4. Somewhat true	5.	6.	7. Very true
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

I felt tense while doing the task

1. Not at all true	2.	3.	4. Somewhat true	5.	6.	7. Very true
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

I think I did pretty well at this activity, compared to other students

1. Not at all true	2.	3.	4. Somewhat true	5.	6.	7. Very true
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

FORRIGE NÆSTE

57%

Figur A.3: Side 3 af spørgeskemaet

A. Spørgeskema til evaluering af motivation

Doing the task was fun

1. Not at all true 2. 3. 4. Somewhat true 5. 6. 7. Very true

I felt relaxed while doing the task

1. Not at all true 2. 3. 4. Somewhat true 5. 6. 7. Very true

I enjoyed doing the task very much

1. Not at all true 2. 3. 4. Somewhat true 5. 6. 7. Very true

I did not really have a choice about doing the task

1. Not at all true 2. 3. 4. Somewhat true 5. 6. 7. Very true

I am satisfied with my performance at this task.

1. Not at all true 2. 3. 4. Somewhat true 5. 6. 7. Very true

I was anxious while doing the task.

1. Not at all true 2. 3. 4. Somewhat true 5. 6. 7. Very true

I thought the task was very boring.

1. Not at all true 2. 3. 4. Somewhat true 5. 6. 7. Very true

FORRIGE NÆSTE

71%

Figur A.4: Side 4 af spørgeskemaet

I felt like I was doing what I wanted to do while I was working on the task.

1. Not at all true 2. 3. 4. Somewhat true 5. 6. 7. Very true

I felt pretty skilled at this task.

1. Not at all true 2. 3. 4. Somewhat true 5. 6. 7. Very true

I thought the task was very interesting.

1. Not at all true 2. 3. 4. Somewhat true 5. 6. 7. Very true

I felt pressured while doing the task.

1. Not at all true 2. 3. 4. Somewhat true 5. 6. 7. Very true

I felt like I had to do the task

1. Not at all true 2. 3. 4. Somewhat true 5. 6. 7. Very true

I would describe the task as very enjoyable.

1. Not at all true 2. 3. 4. Somewhat true 5. 6. 7. Very true

I did the task because I had no choice

1. Not at all true 2. 3. 4. Somewhat true 5. 6. 7. Very true

After working at this task for awhile, I felt pretty competent.

1. Not at all true 2. 3. 4. Somewhat true 5. 6. 7. Very true

FORRIGE NÆSTE

85%

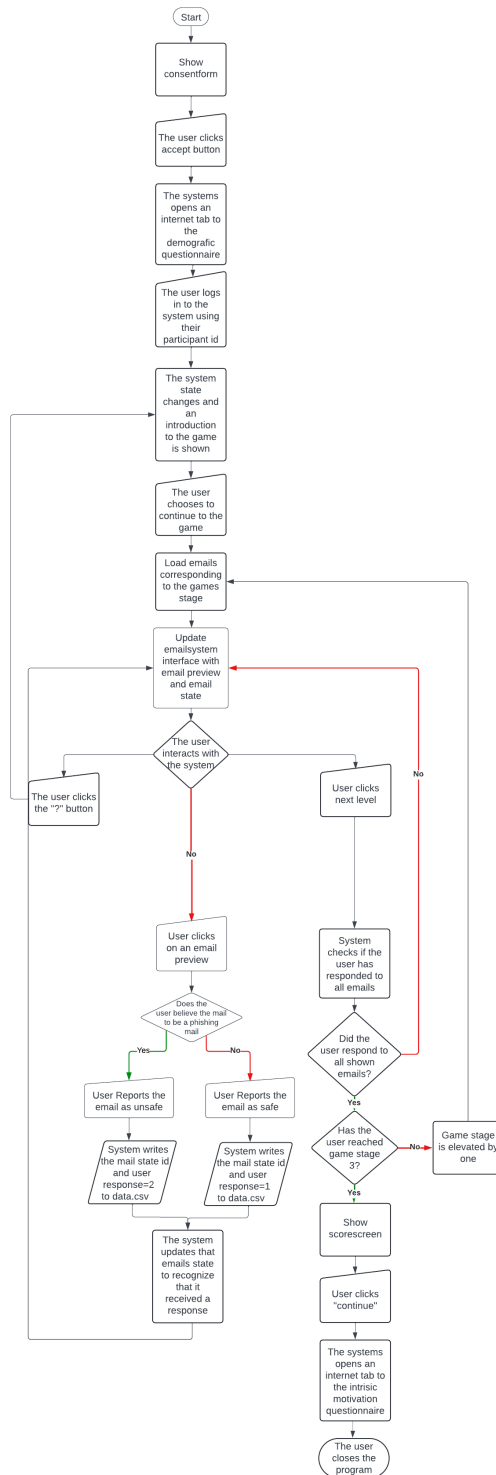
Figur A.5: Side 5 af spørgeskemaet

The screenshot shows a survey form interface. At the top left, there is a small circular logo. Below it, the text reads: "Vi vil bede dig om at besvare den Email du har modtaget fra os med den data fil der ligger inde i din mappe med programmet. Navnet på filen er **data.csv**". This is followed by: "Filen er placeret inde i den udfoldede mappe hvor du fandt programmet. Har du nogen yderligere kommentarer til dette forløb?". Below the text is a text input field. At the bottom left, there are two buttons: "FORRIGE" and "AFSLUT". On the right side, there is a dark blue progress bar that is nearly full, with "100%" written at its end.

Figur A.6: Side 6 af spørgeskemaet

B | Software appendiks

Her er der præsenteret flow chart over de tre iterationer af spillet.



Figur B.1: Flowchart af 1. iteration

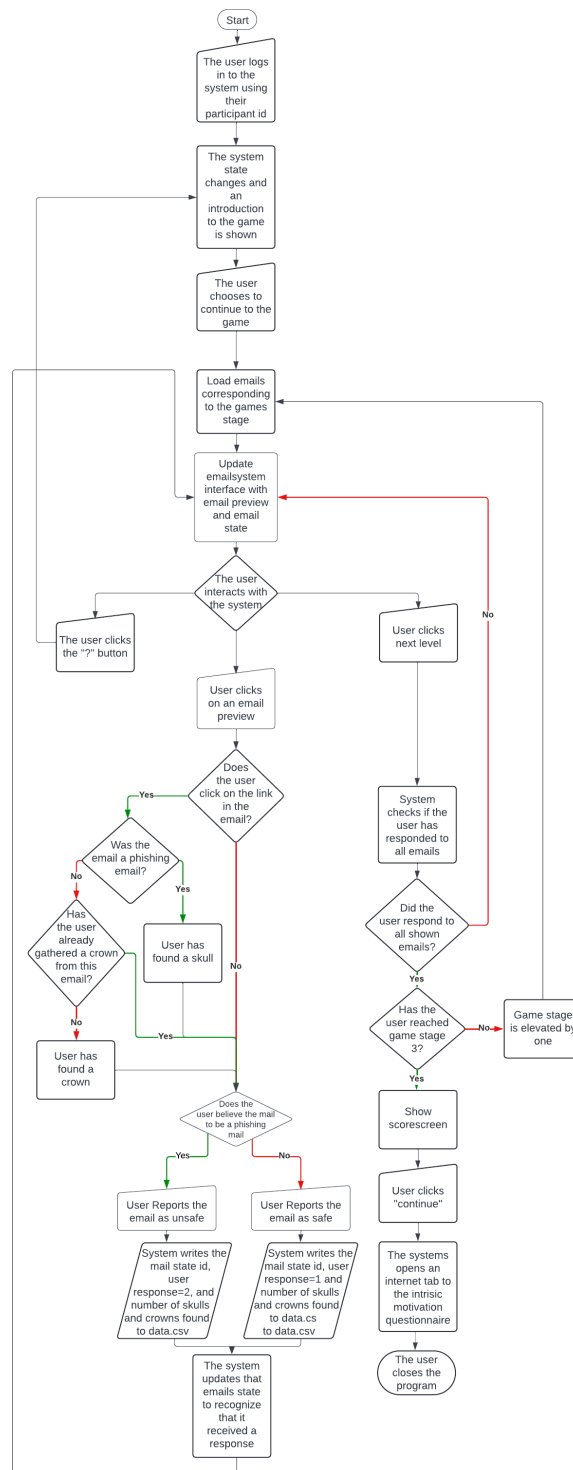


Figure B.2: Flowchart of 2. iteration

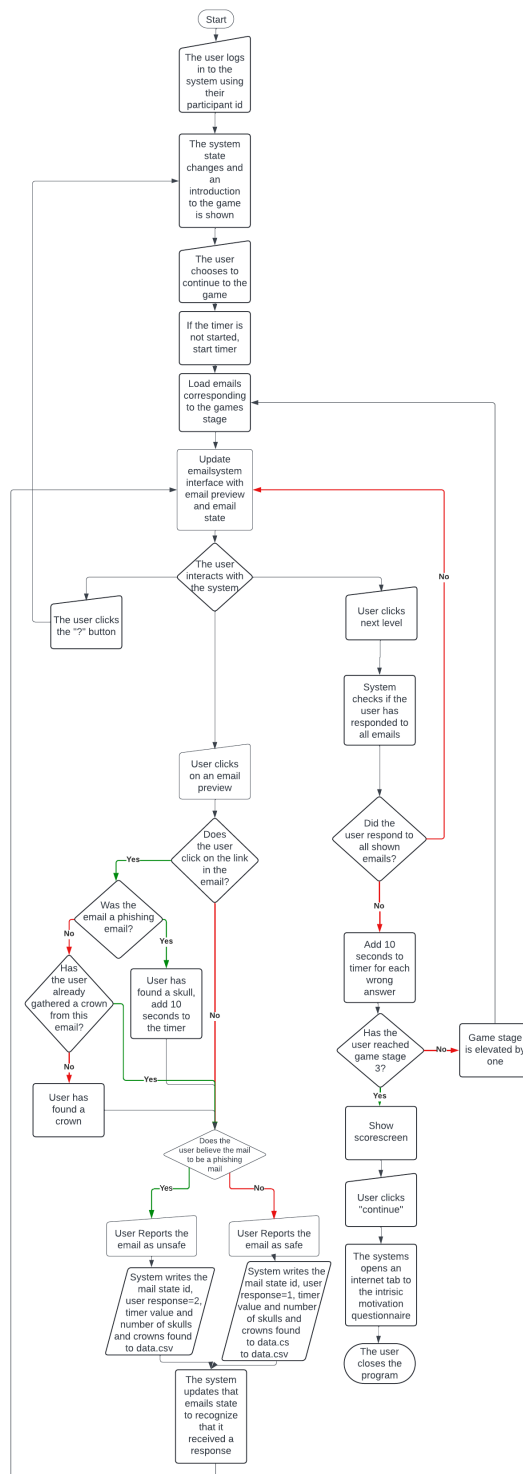


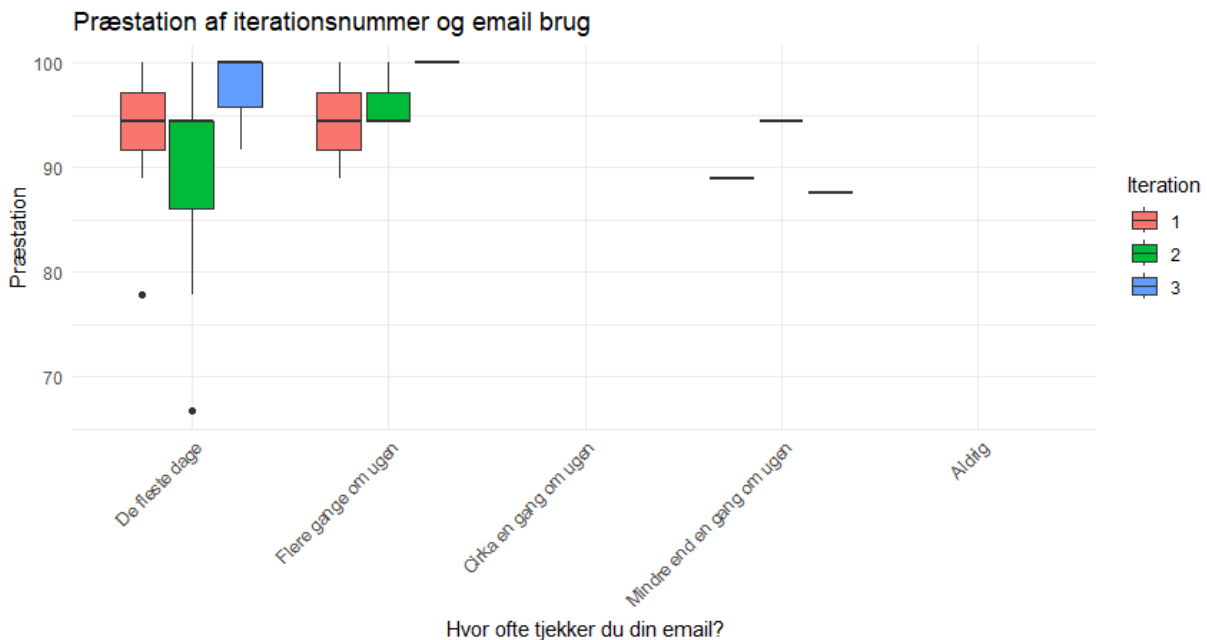
Figure B.3: Flowchart of 3. iteration

C | Statistisk analyse

C.1

C.1.1 Præstation

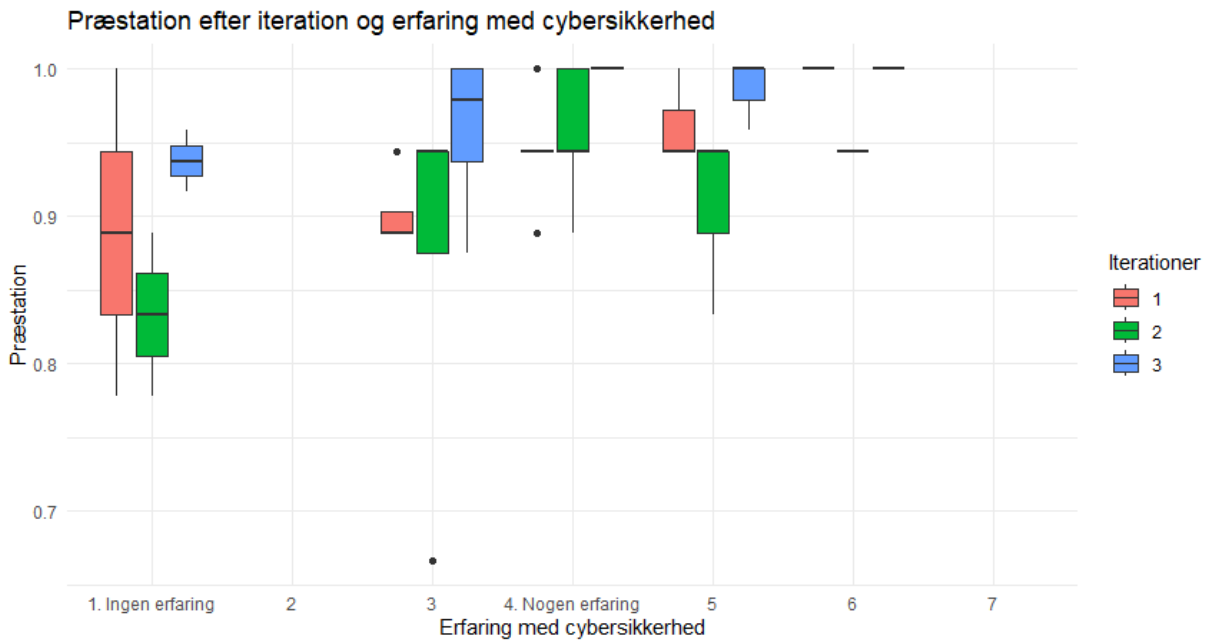
På figur C.1 kan forsøgspersonernes præstation som udtryk af hvor ofte de tjekker deres email ses.



Figur C.1: Boxplot over forsøgspersonernes præstation indenfor de forskellige iterationer som funktion af hvor ofte de benytter deres email.

Det kan på figuren ses at der ikke umiddelbart er stor forskel på forsøgspersonernes præstation afhængig af om de benytter deres email de fleste dage, eller kun flere gange om ugen. Dog er fordelingen af data ikke repræsentativ og det vælges derfor ikke at benytte inferentiell statistik.

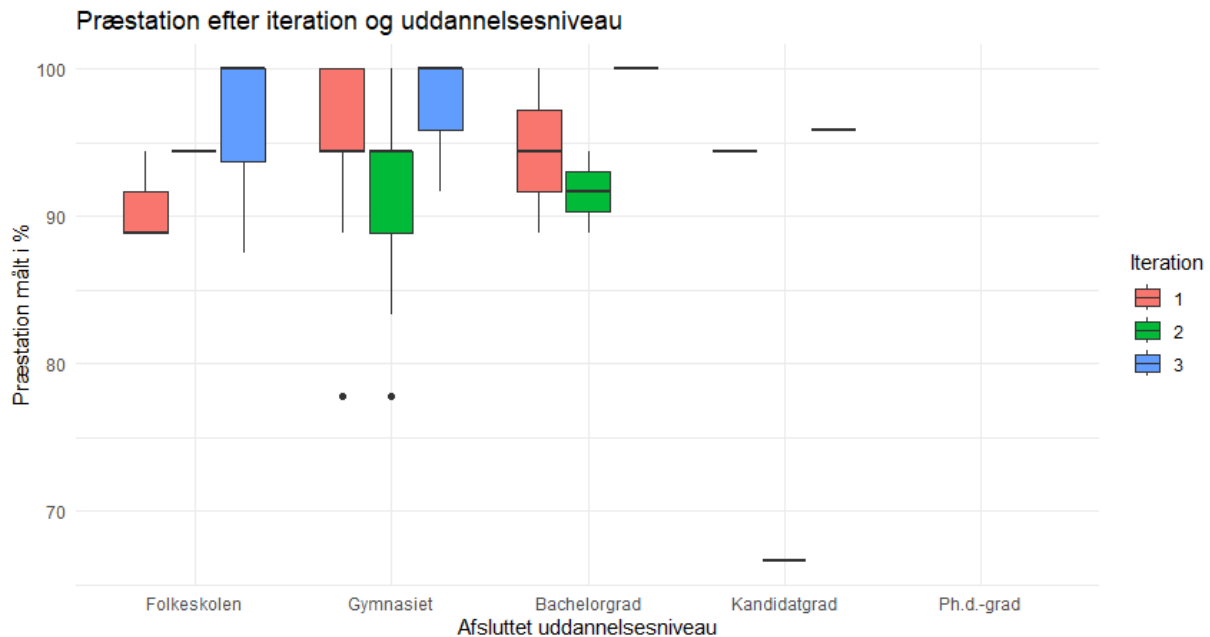
Potentielle sammenhæng mellem forsøgspersonernes præstation og deres erfaring med cybersikkerhed var også tiltænkt undersøgt, dog igen grundet en begrænset mængde forsøgspersoner der var ulige fordelt på grupperne var det ikke muligt at lave inferentiell statistik på dataen. Resultaterne kan dog ses på figur C.2.



Figur C.2: Boxplot over forsøgspersonernes præstation indenfor de forskellige iterationer som funktion af deres erfaring med cybersikkerhed før påbegyndelsen af forsøget.

Det kan her ses en mulig opadgående tendens der kunne indikere at mere erfaring betød at forsøgspersonerne ville præstere bedre under forsøget. Det har dog ikke været muligt at lave meningsfuld statistik der ville kunne bekræfte dette.

Yderligere har det været besluttet at undersøge om forsøgspersonernes uddannelses baggrund ville have en effekt på deres præstation i spillet. Dog har det igen ikke været muligt at lave inferentiell statistik på dette data grundet få forsøgspersoner og en ujævn fordeling af disse. Dataen kan ses på figur C.3.



Figur C.3: Caption

På figuren er der ikke indikation af at der skulle være en effekt af forsøgspersonernes uddannelsesniveau før forsøgsstart og hvordan de præsterede under forsøget. Dette er dog uvist grundet få forsøgspersoner og mangel på mulighed for at lave meningsfuld statistik på emnet.

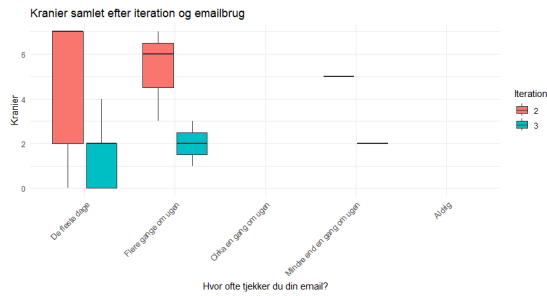
C.1.2 Kranier og kroner

Følgende var det ligesom ved præstations analysen tiltænkt at opholde mængden af funde kranier og kroner med hvor ofte forsøgspersonerne tjekkede deres email. Dog er det af samme årsager: få forsøgspersoner og ulige fordeling, ikke muligt at lave meningsfuld inferentiell statistik. Datafordelingen kan ses på figur C.4.

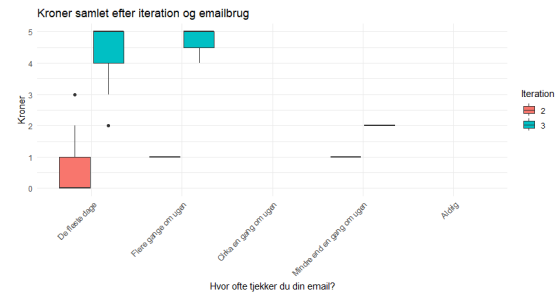
Det ser umiddelbart ud til at udviklingen i fundne kranier og kroner følger den samme udvikling som kan ses på figur 6.9. Det er dog ikke vidst om dette er tilfældet da det ikke har været muligt at lave meningsfuld statistik for at bekræfte eller afkræfte om email brug har en effekt.

Det samme har været tilfældet for sammenligning mellem forsøgspersonernes uddannelsesniveau og mængden af funde kranier og kroner. Datafordelingen kan ses på figur C.5.

Dataen indikere umiddelbart ikke at forsøgspersonens uddannelsesniveau har haft en effekt på deres fund af kranier og kroner. Dette er dog ikke sikkert da det ikke er muligt at lave meningsfuld inferentiell statistik grundet en ujævn fordeling af forsøgspersoner og få forsøgspersoner i grupperingerne.

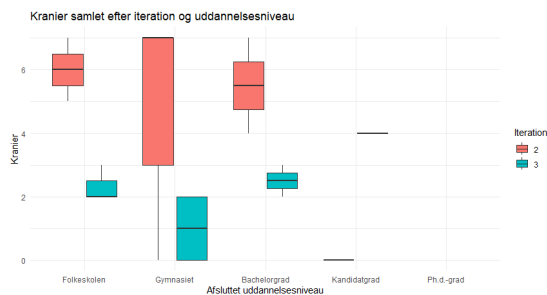


(a) Boxplot for antal indsamlede kranier fordelt på spil iterationen som funktion af forsøgspersonernes email brug.

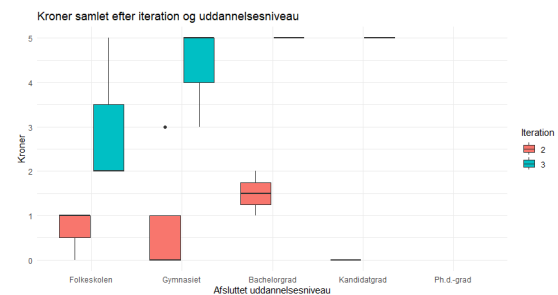


(b) Boxplot for antal indsamlede kroner fordelt på spil iterationen som funktion af forsøgspersonernes email brug.

Figur C.4: Boxplots for kranie og krone data fordelt på forsøgspersonernes angivelse af hvor ofte de benytter deres email.



(a) Boxplot for antal indsamlede kranier fordelt på spil iterationen som funktion af forsøgspersonernes færdiggjort uddannelsesnivea.

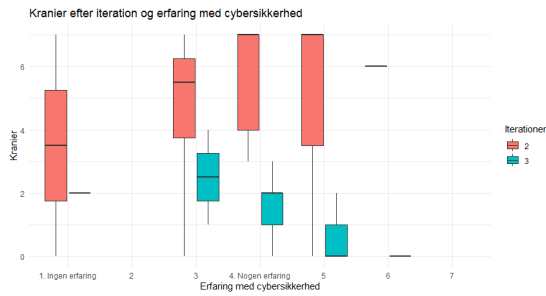


(b) Boxplot for antal indsamlede kroner fordelt på spil iterationen som funktion af forsøgspersonernes færdiggjort uddannelsesnivea.

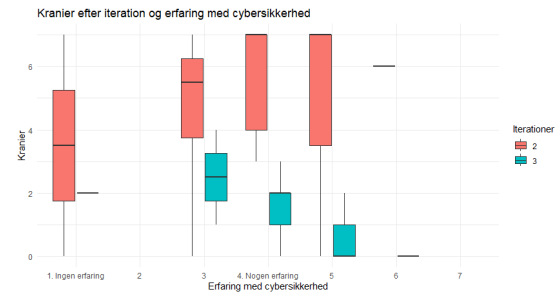
Figur C.5: Boxplots for kranie og krone data fordelt på forsøgspersonernes angivelse af hvilket uddannelsesnivea forsøgspersonerne har færdiggjort.

Sidst har det været tiltænkt at undersøge sammenhængen mellem forsøgspersonernes subjektive erfaring med cybersikkerhed før påbegyndelsen af forsøget, og forsøgspersonernes indsamlede antal af kranier og kroner. Dataen heraf kan ses på figur C.6.

Af dataen fremkommer en tendens til at forsøgspersoner med mere erfaring med cybersikkerhed indsamlede flere kranier i første iteration af spillet, men færre i anden omgang. Dette er dog ikke sikkert og kan ikke bekræftes da det som nævnt ikke har været muligt at lave meningsfuld statistik.



(a) Boxplot for antal indsamlede kranier fordelt på spil iterationen som funktion af forsøgspersonernes subjektive erfaring med cybersikkerhed.

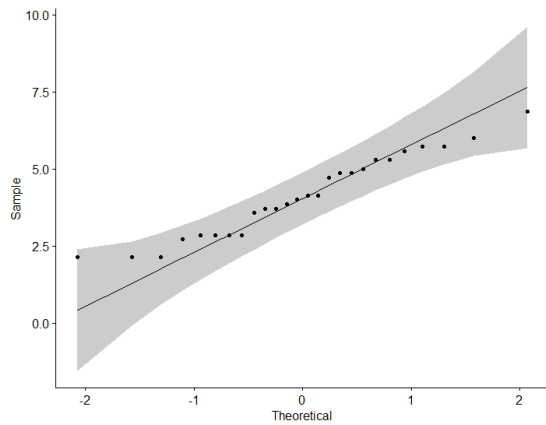


(b) Boxplot for antal indsamlede kroner fordelt på spil iterationen som funktion af forsøgspersonernes subjektive erfaring med cybersikkerhed.

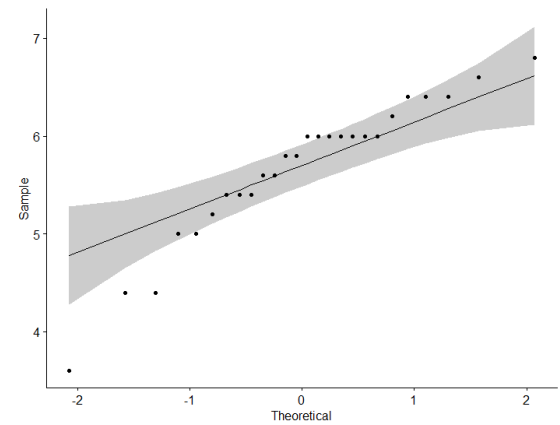
Figur C.6: Boxplots for kranie og krone data fordelt på forsøgspersonernes angivelse af hvor meget erfaring de havde med cybersikkerhed før forsøgets påbegyndelse.

C.2 Spørgeskema

C.2.1 qqplots

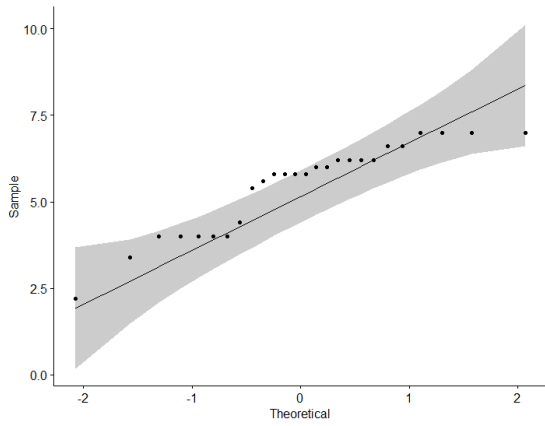


(a) Fordeling af alder på forsøgspersonerne

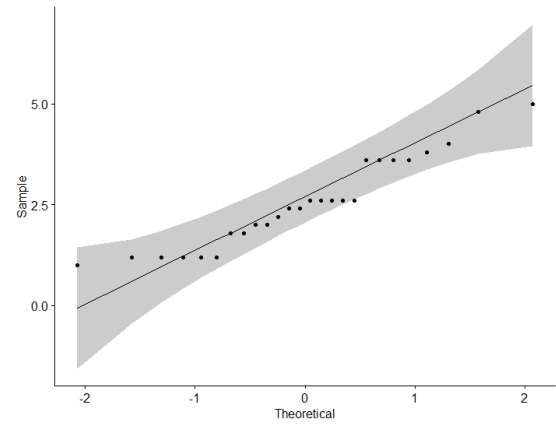


(b) Fordeling af erfaring på forsøgspersonerne

Figur C.7: ret

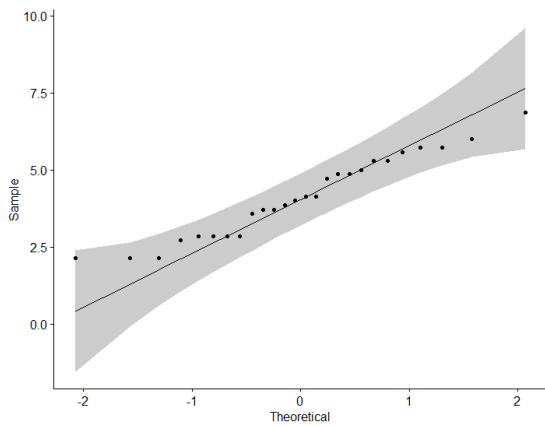


(a) Fordeling af alder på forsøgspersonerne

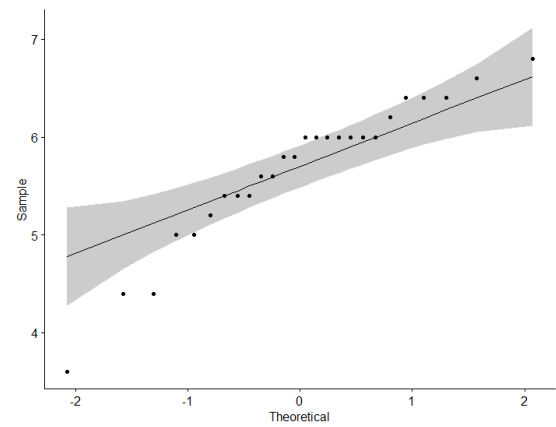


(b) Fordeling af erfaring på forsøgspersonerne

Figur C.8: ret

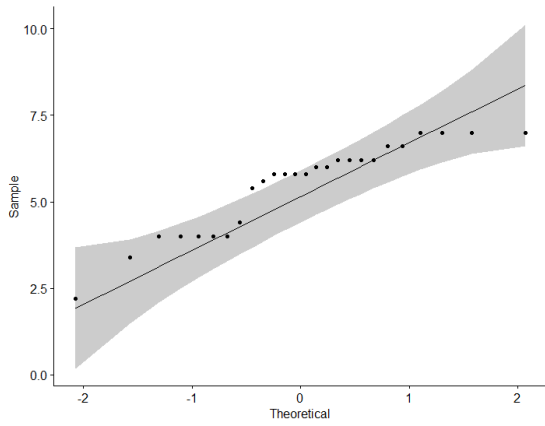


(a) Fordeling af alder på forsøgspersonerne

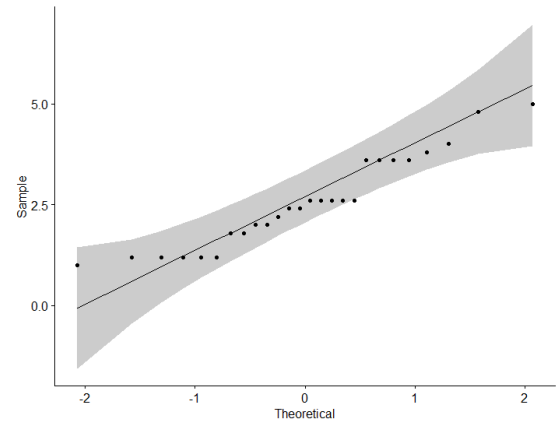


(b) Fordeling af erfaring på forsøgspersonerne

Figur C.9: ret

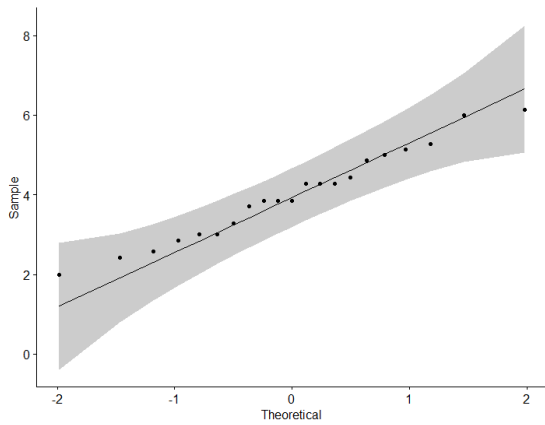


(a) Fordeling af alder på forsøgspersonerne

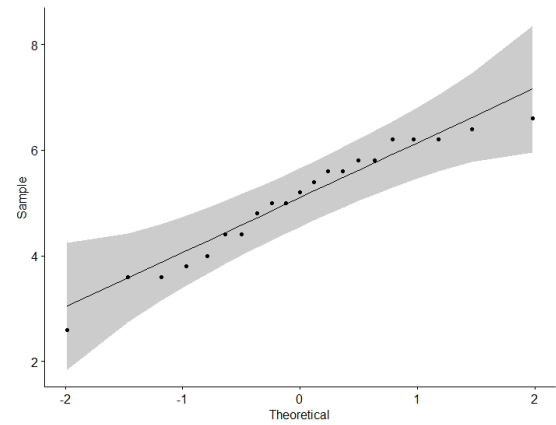


(b) Fordeling af erfaring på forsøgspersonerne

Figur C.10: ret

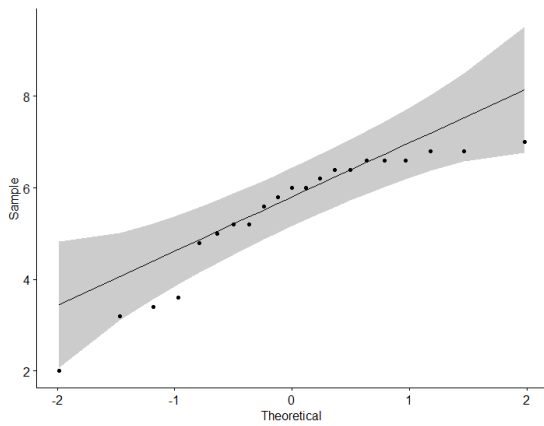


(a) Fordeling af alder på forsøgspersonerne

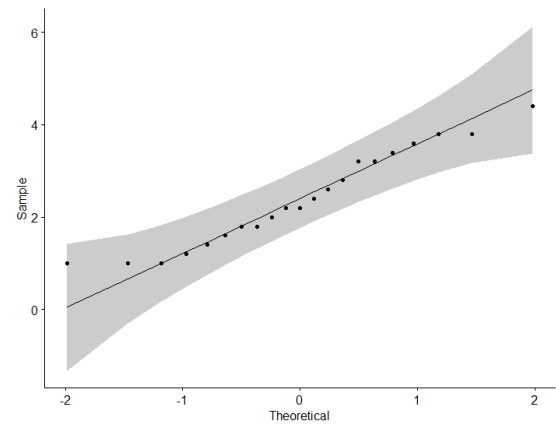


(b) Fordeling af erfaring på forsøgspersonerne

Figur C.11: ret

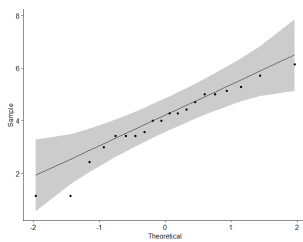


(a) Fordeling af alder på forsøgspersonerne

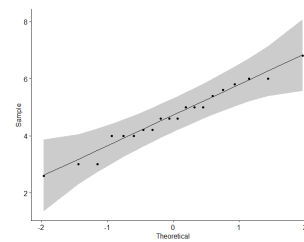


(b) Fordeling af erfaring på forsøgspersonerne

Figur C.12: ret

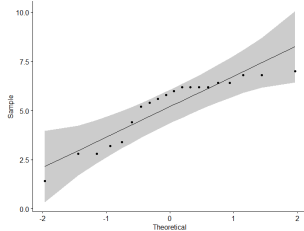


Figur C.13: intereset/enjoyment

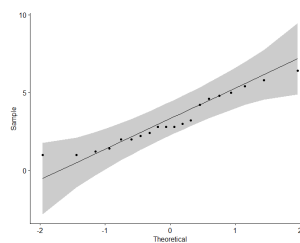


Figur C.14: Percived Competence

[h]



Figur C.15: Percived Choice



Figur C.16: Presure/tension

C.3 Effekten af Køn og Alder

C.3.1 Alder

Først blev data testet for om der det var en normalfordeling, hvilket blev testet igennem en shapiro-wilks test og qqplot.

C.3.1.1 Interesse og spændning

Først blev der set på underemnet interesse og spændning, hvor at resultatet for shapiro-wilks testen var, at alle tre iterationer var normalfordelt ($p > 0.05$). Her var normalfordelingerne for iteration et, to og tre, ($p = 0.47$, $p = 0.85$ og $p = 0.31$). Eftersom at data var normalfordelt, blev der brugt en repeated measures ANOVA test, for at se om der var en sammenhæng. Hvilket der ikke var for nogle af iterationerne, med ($p > 0.05$). Her ses det at for første, anden og tredje iteration, var ($p = 0.57$, $p = 0.17$ og $p = 0.1$).

C.3.1.2 Opfattet valg

For opfattet valg var alle iterationerne ikke normalfordelt, ($p < 0.05$). Eftersom at shapiro-wilk testen, viste at data ikke var normalt fordelt, blev der brugt kruskal wallis test for at se om der var en effekt. Her var der ikke nogle effekt af alderen på hvordan de svare på opfattet valg, her var værdierne for iteration et, to og tre ($p = 0.4$, $p = 0.08$ og $p = 0.08$).

C.3.1.3 Opfattet kompetance

En shapiro-wilks test blev lavet på opfattet kompetence, for at se om der var at gøre med en normalfordeling. Her var p-værdierne for iteration et, to og tre ($p = 0.25$, $p = 0.32$ og $p = 0.82$). Hertil blev der brugt repeated measure ANOVA eftersom at data var normalfordelt. P-værdierne for iteration et, to og tre var ($p = 0.51$, $p = 0.2$ og $p = 0.38$). Her ses det at der ikke var nogle effekt af forsøgspersoners alder på hvordan forsøgspersonerne svarede på opfattet kompetence spørgsmålene.

C.3.1.4 Spændning og pres

For spændning og pres blev der lavet en shapiro-wilk test. Her var p-værdierne for iteration et, to og tre på ($p = 0.07$, $p = 0.28$ og $p = 0.18$). Hertil blev der brugt repeated measure ANOVA eftersom at data var normalfordelt. Her ses det at der ikke var nogen effekt af forsøgspersoners alder på hvordan forsøgspersonerne svarede på spændning og pres spørgsmålene, eftersom at p-værdierne for iteration et, to og tre var på ($p = 0.36$, $p = 0.34$ og $p = 0.69$).

C.3.2 Køn

Samme procedure blev også lavet for Køn, hvor der blev testet for normalfordeling og en statistisk analyse.

C.3.2.1 Interesse og nydelse

Der blev lavet en Shapiro-wilks test, for at se om data var normalfordelt. Testen viste at for iteration et, to og tre var på ($p = 0.47$, $p = 0.36$ og $p = 0.95$).

Hertil blev der brugt repeated measures ANOVA eftersom at data var normalfordelt. Testen viste for iteration et, to og tre at p-værdien var på ($p = 0.63$, $p = 0.17$ og $p = 0.1$).

Her ses det at der ikke var nogle effekt af forsøgspersonerne køn på hvordan forsøgspersonerne svarede på interesse og nydelse spørgsmålene.

C.3.2.2 Opfattet valg

Der blev lavet en normalfordelings test, med testen shapiro wilks. Her viste det at alle iterationerne var signifikante med en p-værdi ($p < 0.05$).

Eftersom at shapiro-wilk testen, vidste at data ikke var normalt fordelt, blev der brugt kruskal wallis testen for at se om der var en effekt. Denne test viste at for iteration et, to og tre med en p-værdi på ($p = 0.35$, $p = 0.08$ og $p = 0.08$). Her var der ikke nogle effekt af køn på hvordan de svare på opfattet valg.

C.3.2.3 Opfattet kompetence

Der blev lavet en Shapiro-wilks tet, for at se om data var normalfordelt. Testen viste at for iteration et, to og tre var på ($p = 0.19$, $p = 0.23$ og $p = 0.85$).

Hertil blev der brugt repeated measures ANOVA eftersom at data var normalfordelt. Testen viste for iteration et, to og tre at p-værdien var på ($p = 0.56$, $p = 0.2$ og $p = 0.38$).

Her ses det at der ikke var nogle effekt af forsøgspersonerne køn på hvordan forsøgspersonerne svarede på opfattet kompetence spørgsmålene.

C.3.2.4 Pressure/tension

For spænding og pres, blev der også lavet en shapiro-wilks test. Her viste den at for iteration et, to og tre, var p-værdierne ($p = 0.07$, $p = 0.75$ og $p = 0.15$).

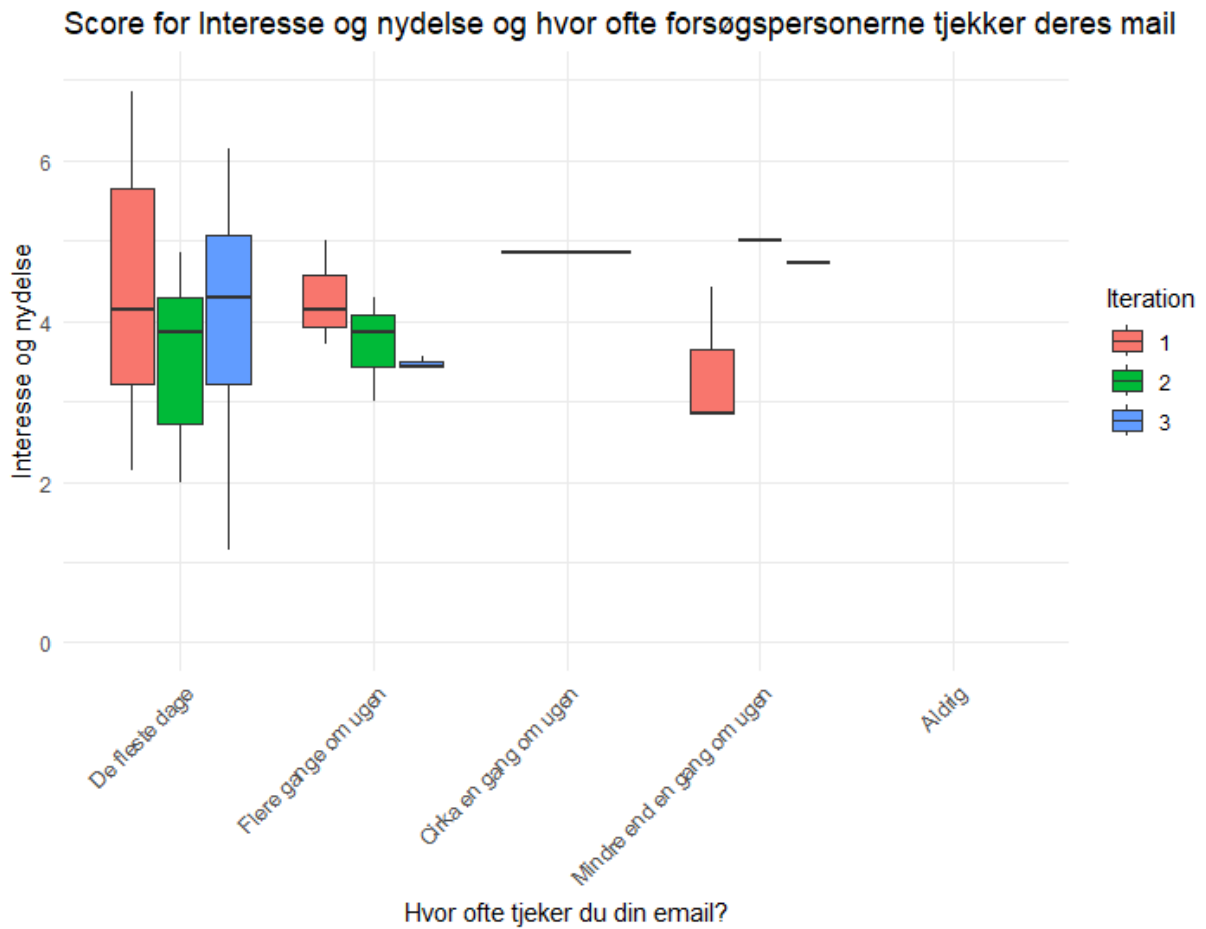
Hertil blev der brugt repeated measures ANOVA eftersom at data var normalfordelt. Testen viste for iteration et, to og tre at p-værdien var på ($p = 0.46$, $p = 0.34$ og $p = 0.69$).

Her ses det at der ikke var nogle effekt af forsøgspersonernes køn på hvordan forsøgspersonerne svarede på spænding og pres spørgsmålene.

Heraf var det kun opfattet valg der ikke var normalt fordelt, men der var ikke nogle effekt, af denne faktore, køn, på hvordan forsøgspersonerne havde svaret.

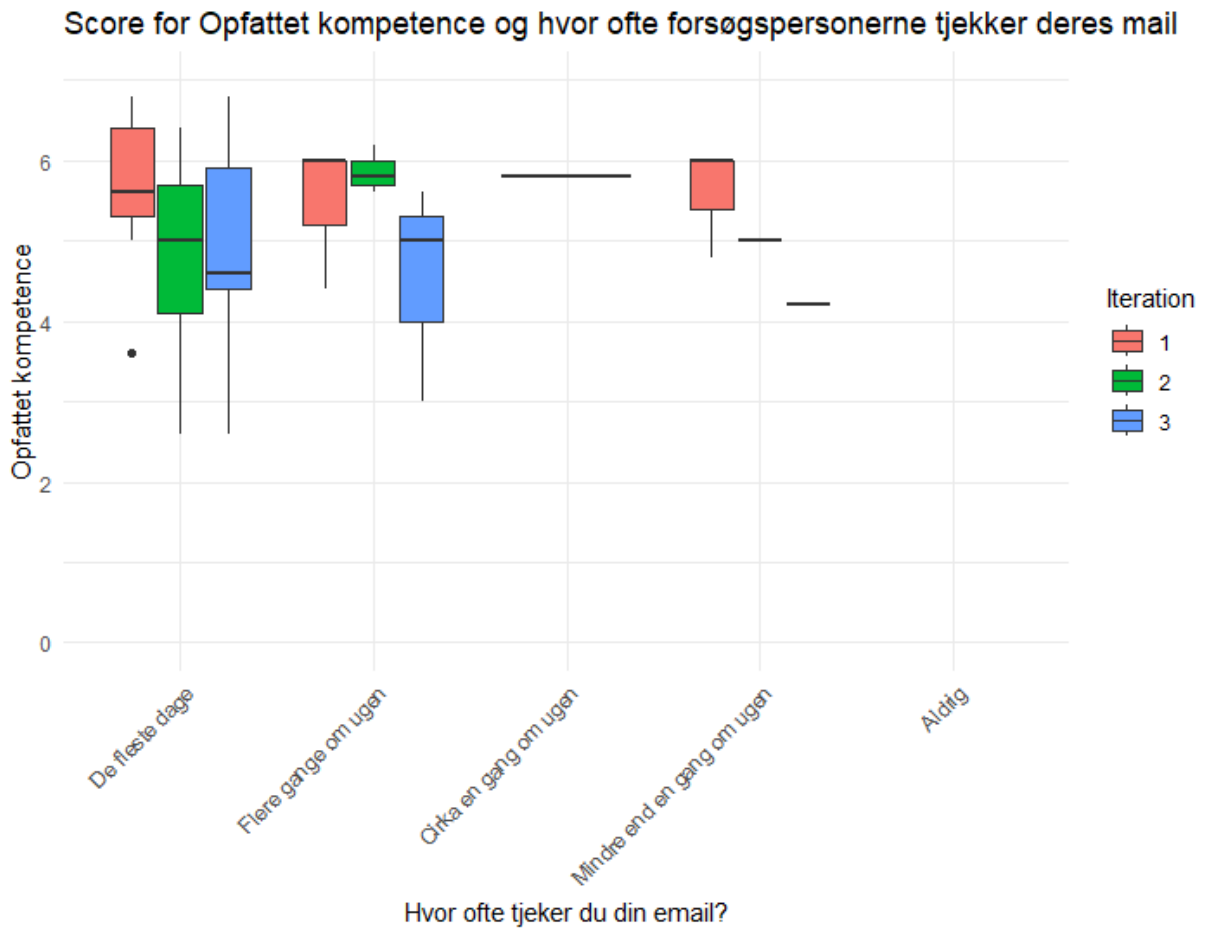
C.3.3 Kontrolvariabler

Først blev der lavet boxplot for de fire underemner, og hvor ofte forsøgspersonerne tjekkede deres mail.



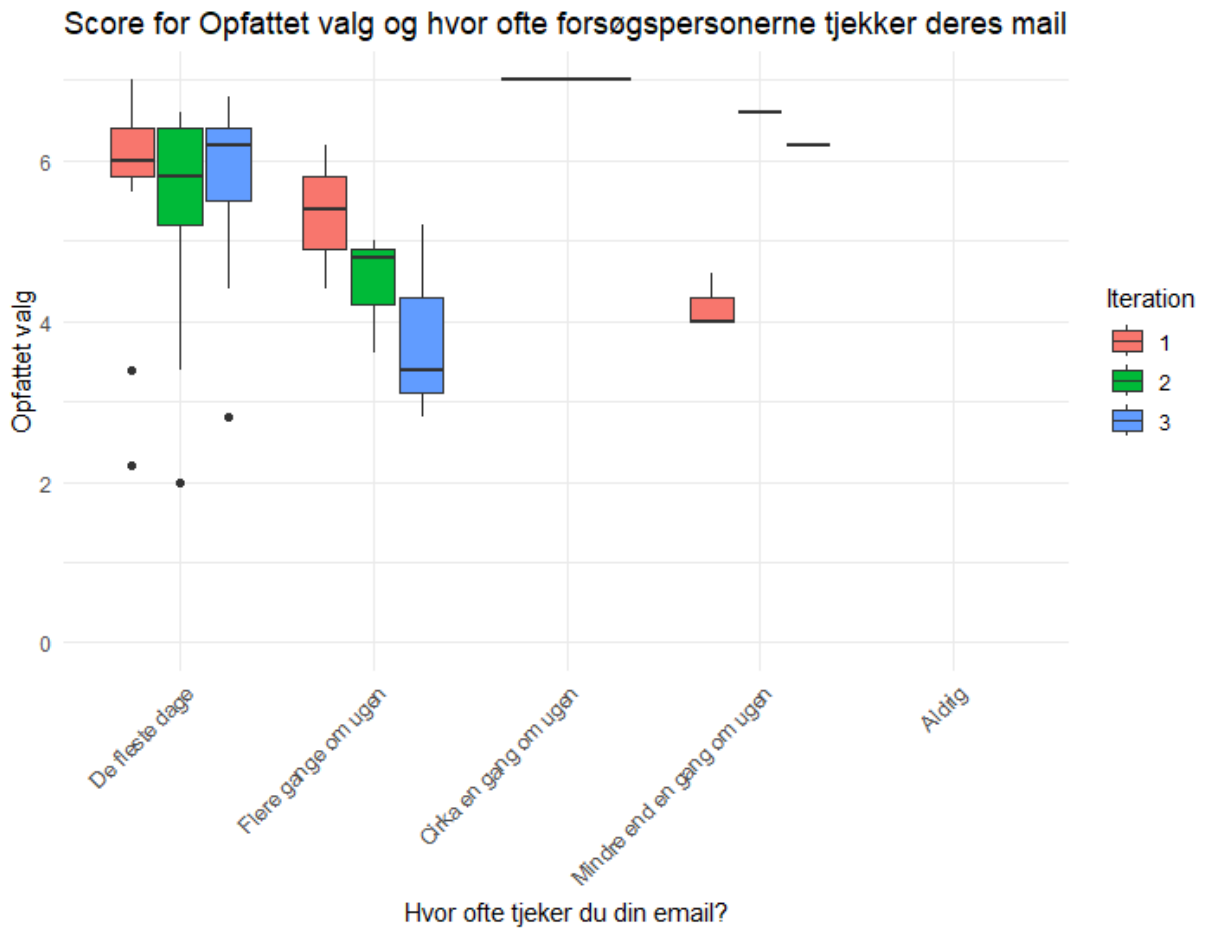
Figur C.17: Boxplot af Interest og hvor ofte forsøgspersonerne tjekker deres mail

For figur C.17, kan det ses at forsøgspersonerne har vurderet dette aspekt til at være middelt, med median bedømmelser omkring en værdi på fire.



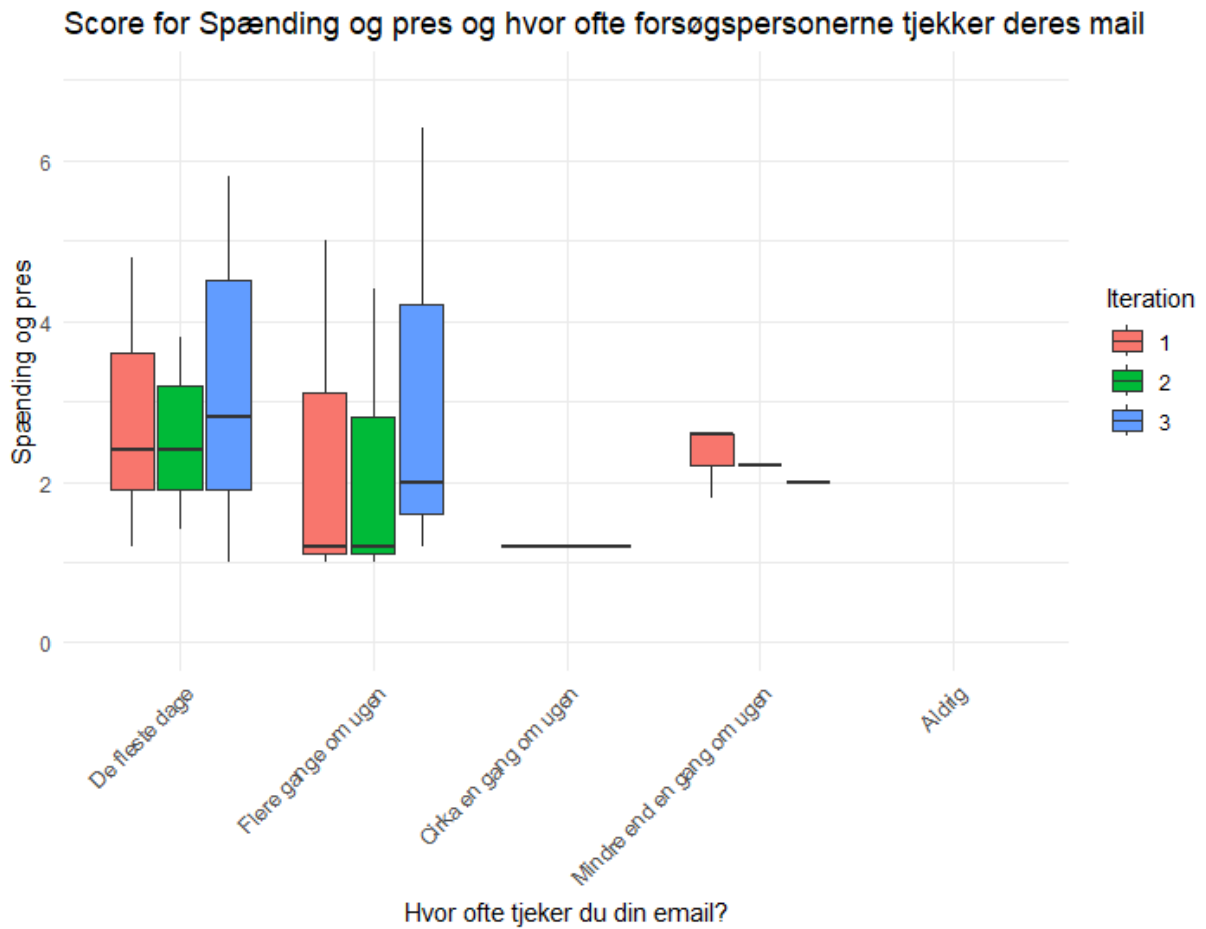
Figur C.18: Boxplot af Percived competence og hvor ofte forsøgspersonerne tjekker deres mail

For denne sammenligning er der en mulig tendens til at forsøgspersonernes perceived competence faldt for alle forsøgspersoner uagtet hvor ofte de tjekkede deres email. Dog har det ikke været muligt at bekræfte dette da der ikke har været nok data til at lave inferentiell databehandling.



Figur C.19: Boxplot af Percived choice og hvor ofte forsøgspersonerne tjekker deres mail

For figur C.19 ses en mulig tendens til at forsøgspersonerne har vurderet dette parameter lavere såfremt de sjældnere tjekker deres email. Dog har der igen ikke været nok data til at bekræfte om denne tendens er statistisk signifikant.

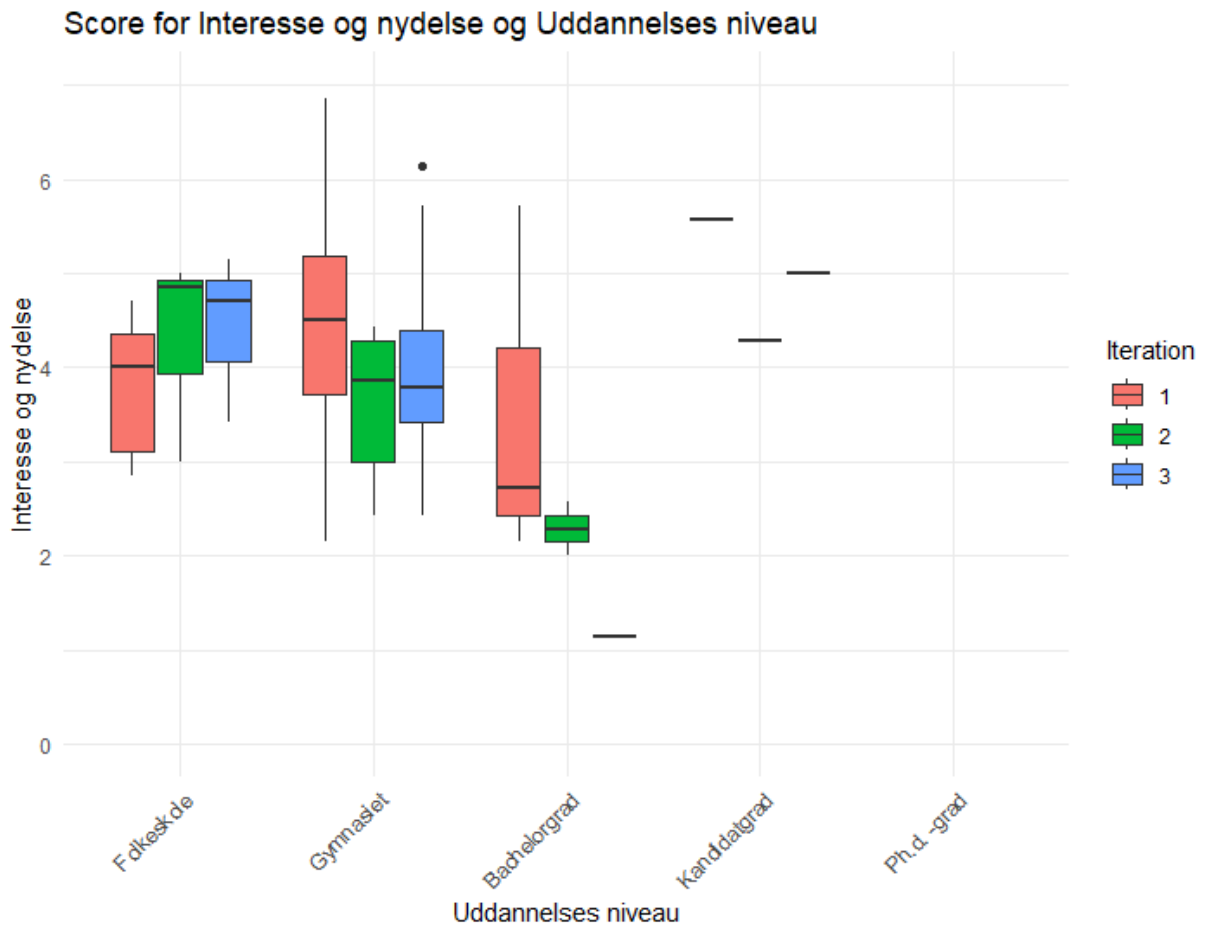


Figur C.20: Boxplot af Pressure og hvor ofte forsøgspersonerne tjekker deres mail

Til sidst ses det at dem som tjekker mails oftere, svarer at de er mere pressede end dem som tjekker mails mere end en gang om ugen.

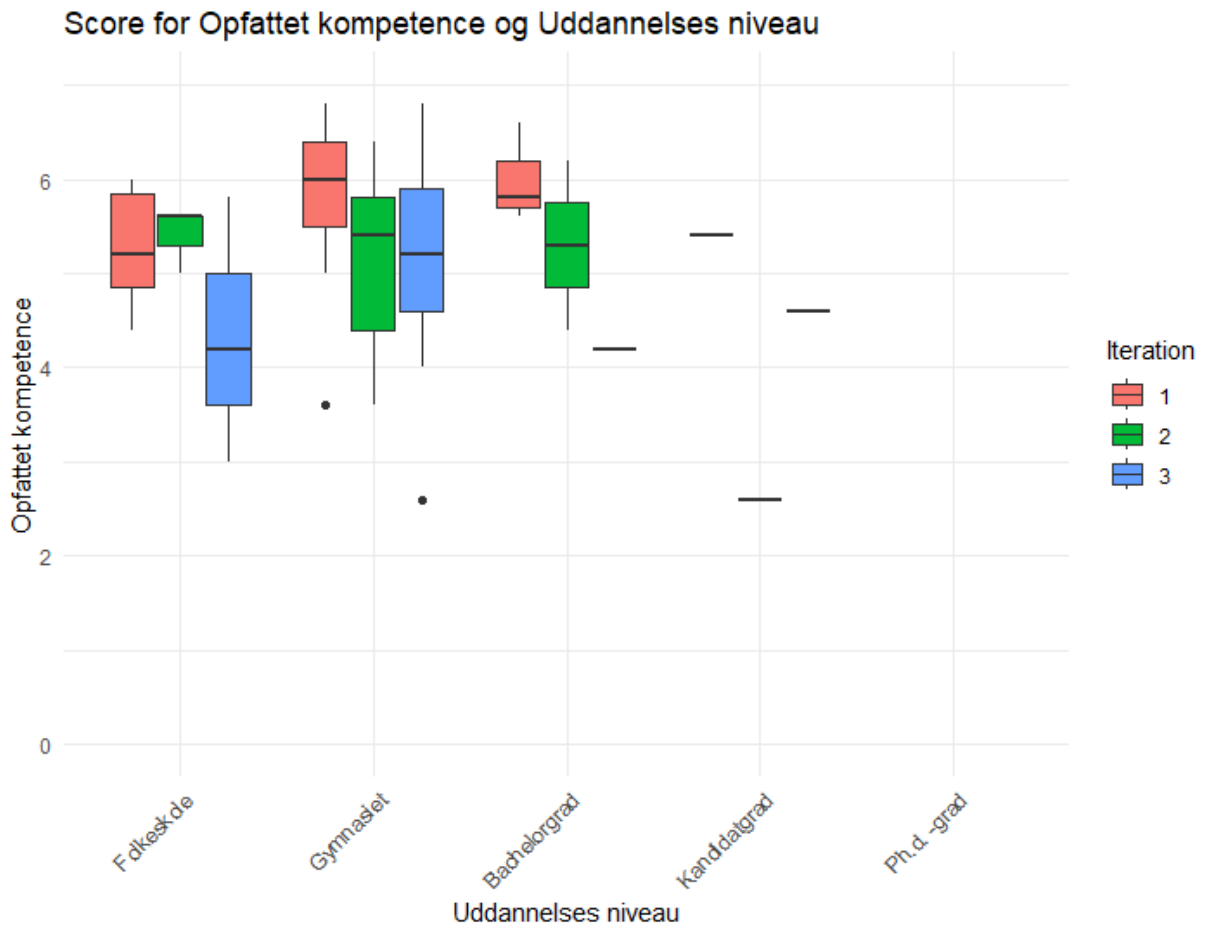
C.3.3.1 Niveau af uddannelse

Der blev også opstillet boxplot mellem hvor høj en uddannelse forsøgspersonerne havde, og hvordan de svarede på de fire under emner.



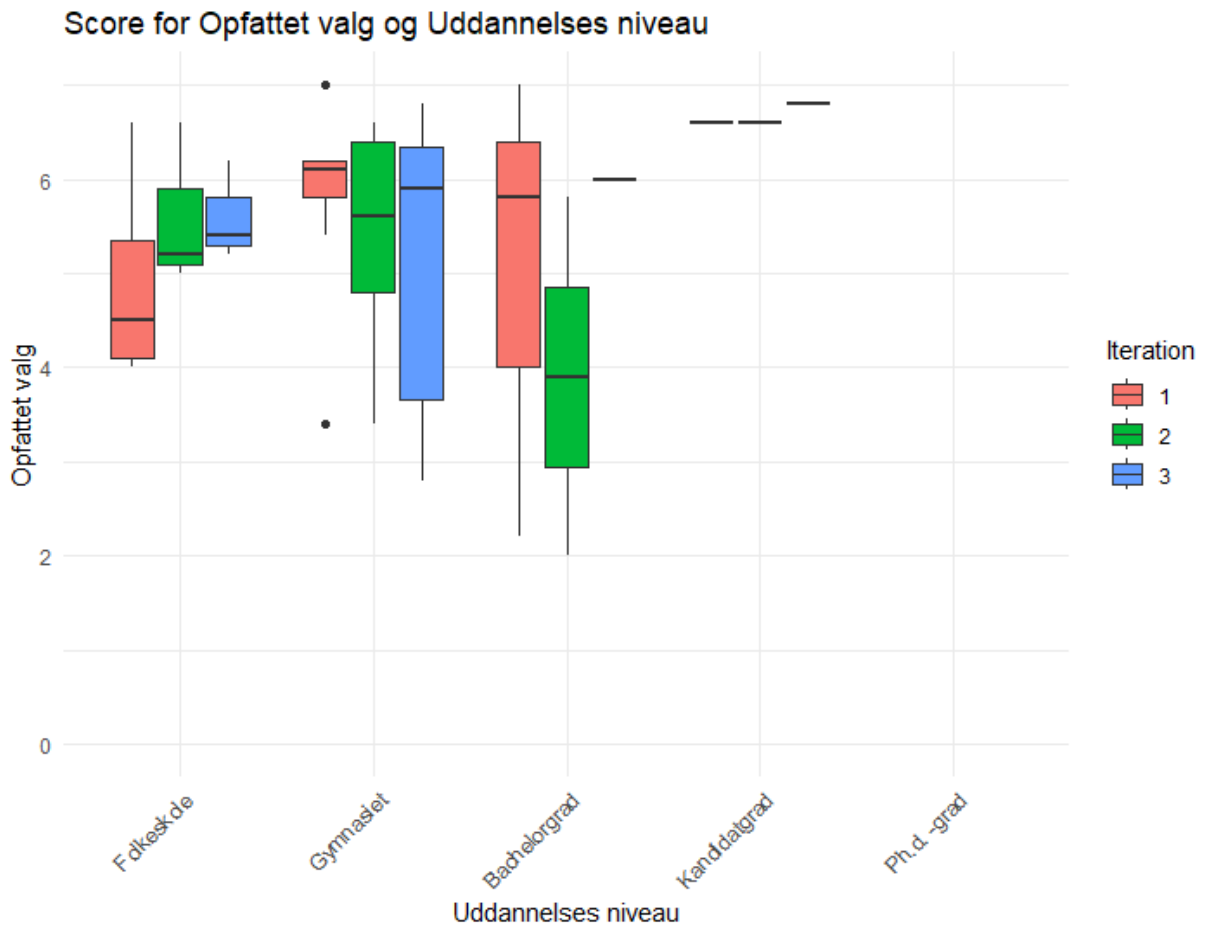
Figur C.21: Boxplot af Interest og hvad uddannelses niveau forsøgspersonerne senest havde færdiggjort

For dette aspekt, var det for den gruppe som havde færdiggjort folkskolen sidst, at interesse og nydelse var stigende over iterationerne, men for dem som senest havde færdiggjort gymnasiet og bachelor, var der en tendens til at den var faldende. Dog har det ikke været muligt at bekræfte dette da der ikke har været nok data til at lave inferentiell databehandling.



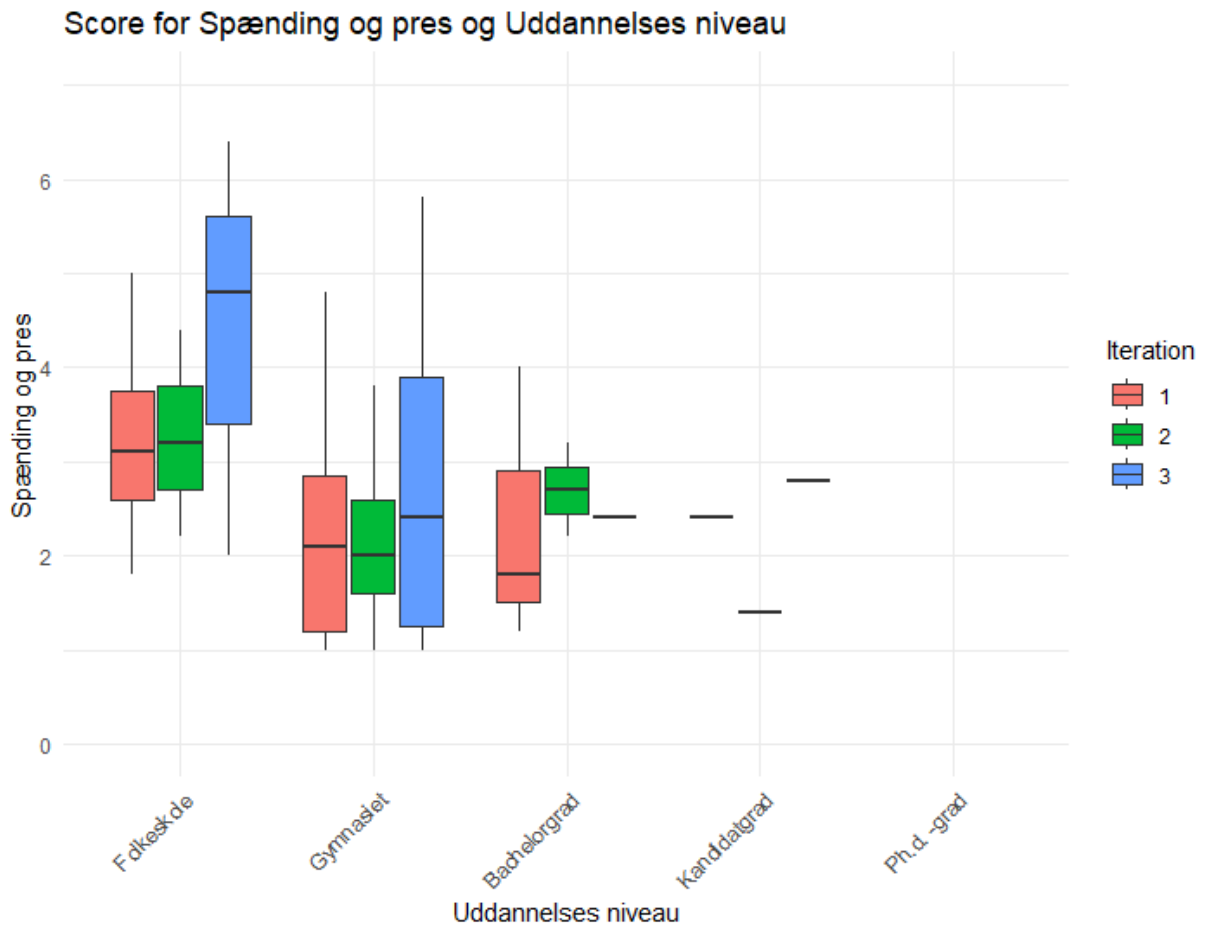
Figur C.22: Boxplot af Percived competence og hvad uddannelses niveau forsøgspersonerne senest havde færdiggjort

For Percived competence og uddannelses niveau, kan det ses at for både, folkeskole, gymnasiet og bachelorene, at deres percived competence falder med interaktionerne.



Figur C.23: Boxplot af Percived choice og hvad uddannelses niveau forsøgspersonerne senest havde færdiggjort

For figur C.23 ses det at i alle grupperne er der scoret 4 eller over på medianerne.

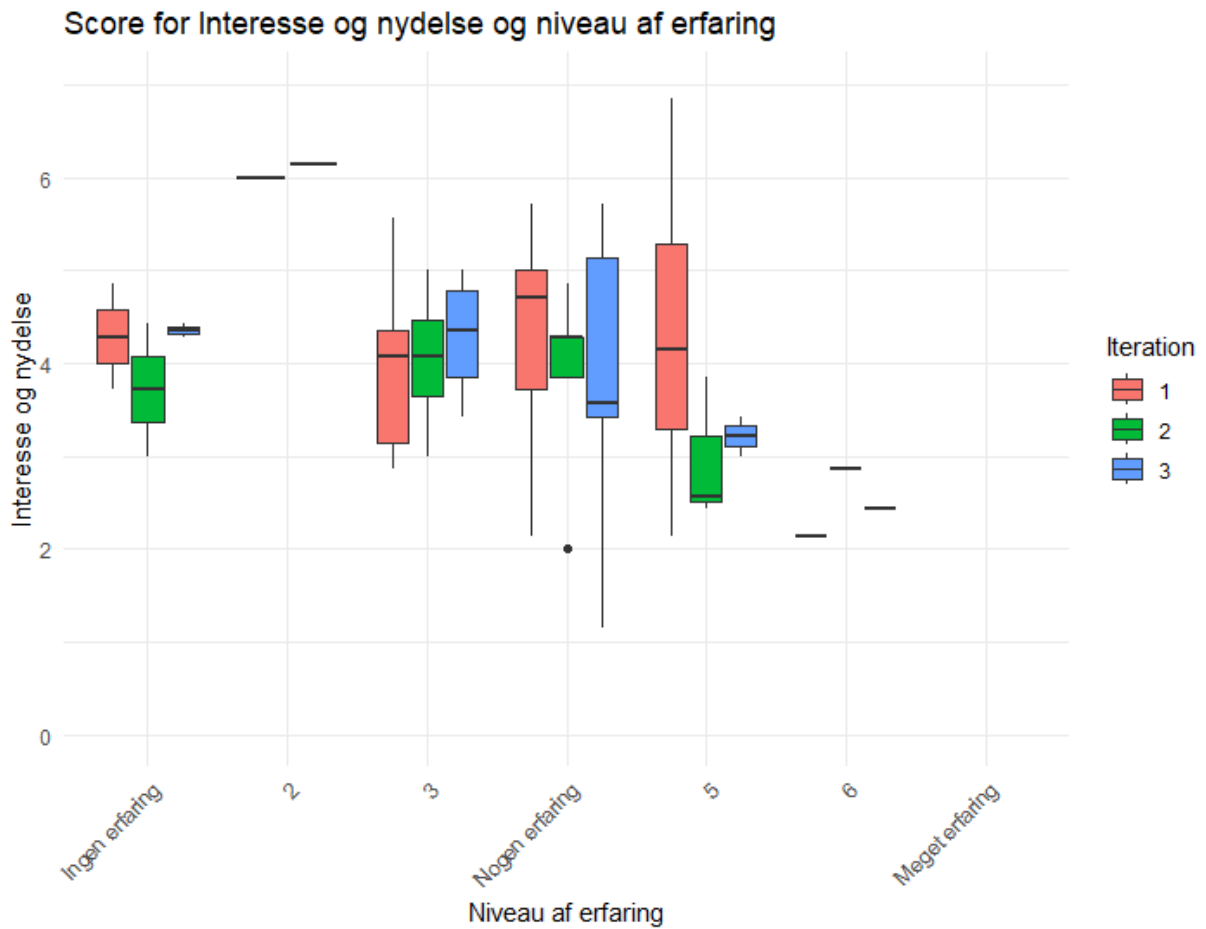


Figur C.24: Boxplot af Pressure og hvad uddannelses niveau forsøgspersonerne senest havde færdiggjort

På figur C.24 kan det ses at dem med lavest uddannelses niveau har svaret at de føler sig mere presset end dem som har gennemført højere niveauer af uddannelse.

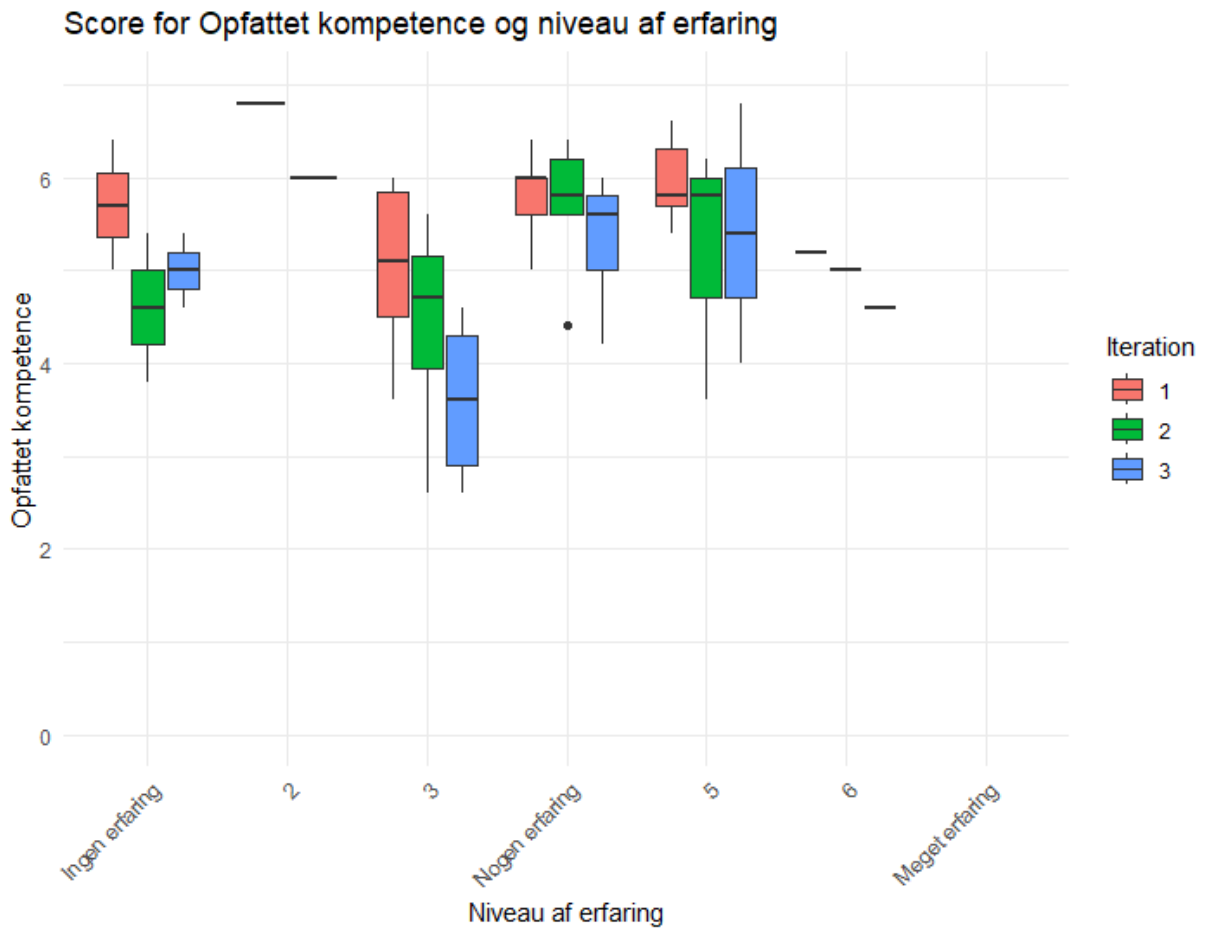
C.3.3.2 Erfaring med cybersikkerhed

Yderligere blev der lavet boxplot for de fire underemner og hvor meget erfaring forsøgspersonerne havde med cybersikkerhed.



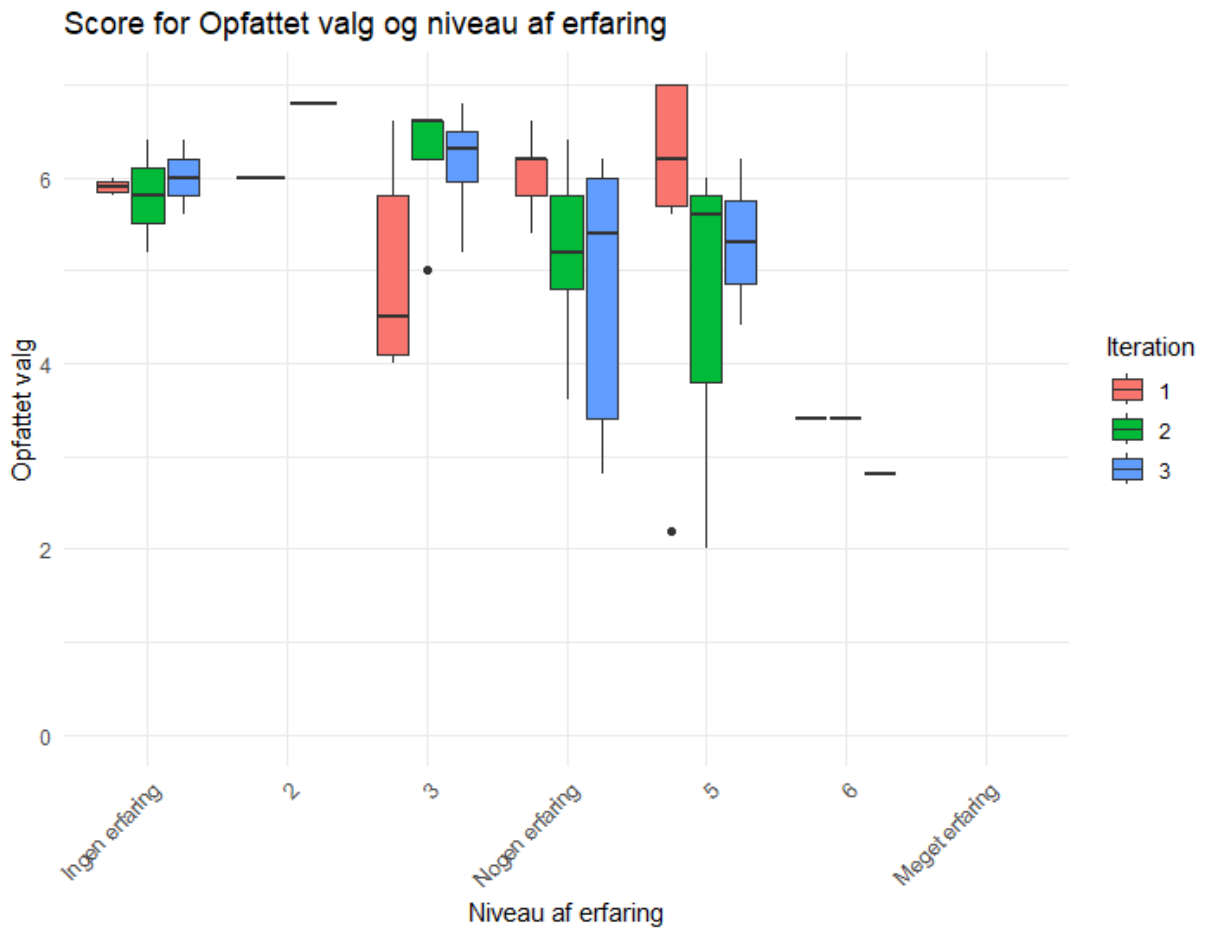
Figur C.25: Boxplot af interesse og hvor meget erfaring forsøgspersonerne har med cybersecurity

Ud fra figur C.25, ses der ingen tydelige tendenser mellem erfaring med cybersikkerhed og deres interesse og nydelse af spillet. Dog er der ikke nok datapunkter til at lave inferentiell statistik og dermed bekræfte eller afkræfte en sammenhæng.



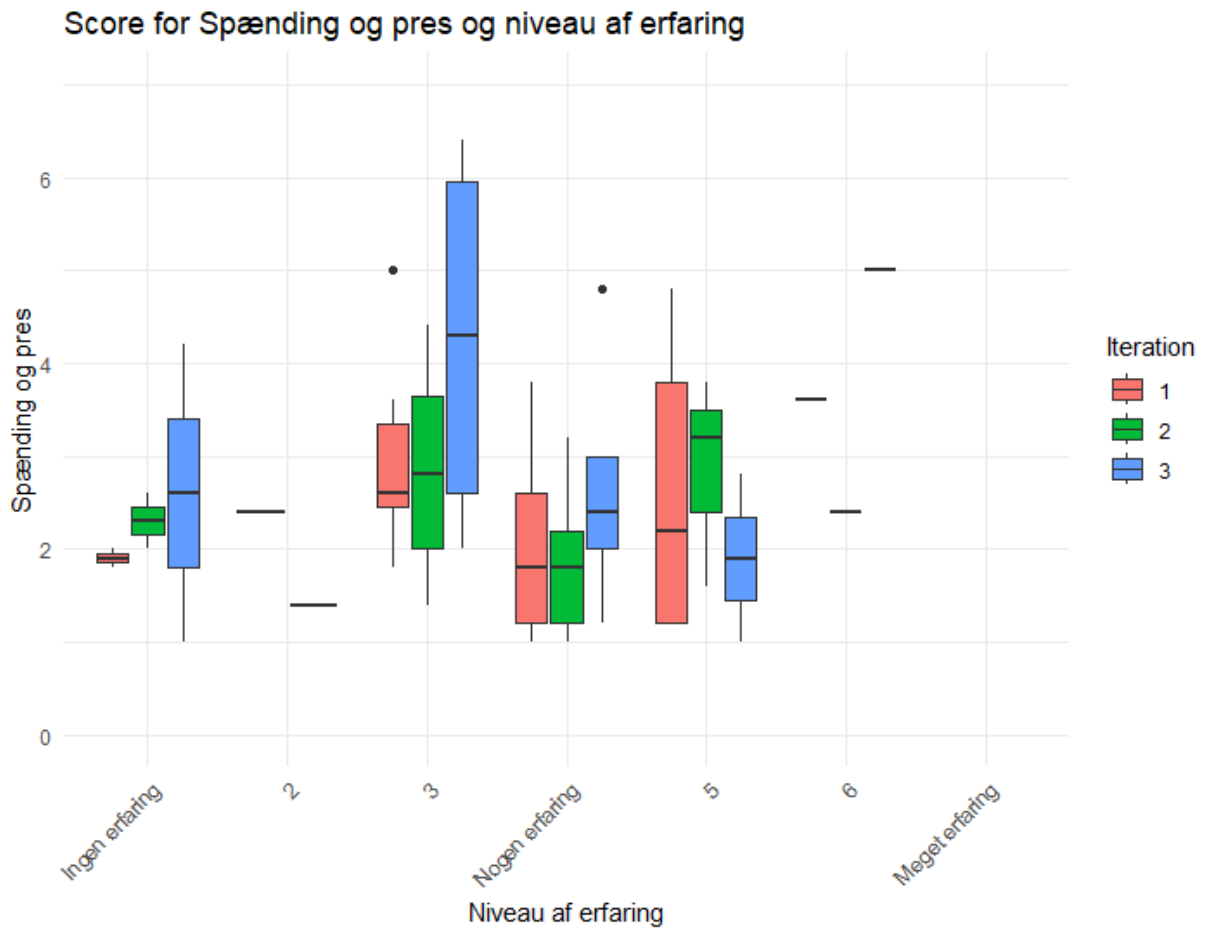
Figur C.26: Boxplot af Perceived competence og hvor meget erfaring forsøgspersonerne har med cybersecurity

På figur C.26 ses det at for alle erfarings niveauer at Percived competence falder over iterationerne, og at hvis man havde højere erfaring, var der tendens til at forsøgspersonerne svarede højere på opfattet kompetence.



Figur C.27: Boxplot af Percived choice og hvor meget erfaring forsøgspersonerne har med cybersecurity

På figur C.27 ses det at alle grupperne af erfarings niveauer, har en bedømt median på over en Percived choice på 4, med undtagelse af den gruppe med en erfaring på 6.



Figur C.28: qqplot af alders effekt på presure opfattelsen

Figur C.28 ses der en tendens til at bedømmelsen af presure, stiger på tværs af forsøgspersonerens selvrappede niveau af erfaring.

D | Samtykkeerklæring

Vi er to studerende fra Produkt- og designpsykologi, der undersøger interaktionen mellem Gamification og Læring.

Ved at deltage i dette eksperiment giver du samtykke til, at vi bruger dine data fra spillet, så vi senere kan analysere det og bruge det i vores rapport. Derudover beder vi dig også om at udfylde spørgeskemaer i begyndelsen og ved afslutning af spillet.

Alle dine data vil blive anonymiseret, hvilket betyder at dine data ikke vil blive direkte knyttet til dit forsøgs ID, eller dig som person.

Alt data vil blive opbevaret i overensstemmelse med GDPR, og vil blive slettet senest 1 uge efter, at vi har bestået vores eksamen.

Du har til enhver tid lov til at forlade eksperimentet uden yderligere spørgsmål.

Vi takker dig for at deltage i denne undersøgelse.

Hvis du accepterer ovenstående, bekræft venligst dette ved:

- 1) Udfyld spørgeskemaet lige nedenfor
- 2) Indskriv dit forsøgs ID nedenfor, og tryk på "Fortsæt"

I dette spils scenarie er du en studerende på Universitet.dk. Hertil modtager du og afsender ofte mails tilknyttet universitetet og studie/arbejdslivsrelaterede. Hertil omhandler spillet at du skal sortere i dine Universitets mails, her skal du finde ud af hvilke mails de er sikre og hvilke der er usikre.

Når du har en ide om hvorvidt en mail er sikker eller usikker, angiver du dit svar ved at klikke på mailen, og så klikke på "sikker" eller "usikker" knappen.

Fortsæt til spørgeskema

Figur D.1: Et billede af hvordan samtykkeerklæringen blev præsenteret i spillet for forsøgspersonerne.