



Norwegian University of  
Science and Technology

# Evaluation of Technology and Electronic Devices for Cheating on Exams

**Matias Halsteinli Unsvåg**

Master of Science in Computer Science

Submission date: June 2018

Supervisor: Guttorm Sindre, IDI

Norwegian University of Science and Technology  
Department of Computer Science



## Abstract

Currently, most exams on Norwegian universities are paper-based written exams. With the evolvment of technology and its possibilities, university students can transition from old fashion ways of cheating, such as cheat sheets, to using technological devices that are available for purchase online. There are several vendors specializing in selling these types of technological devices, leading to a variety of devices being available. It is uncertain to what extent students and exam invigilators are aware of these types of devices, and there is still little research related to the topic of such devices and their applicability. This motivates for research on the functionality and viability of cheating using different types of technological devices for cheating on academic exams.

The aim of this thesis was to investigate various electronic devices that can be used to cheat on exams. A comprehensive mapping of available vendors and devices was conducted, that can contribute to increasing the knowledge and awareness of exam organizers regarding possible methods for cheating. A selection of the devices were purchased and used in experiments simulating cheating on an exam by using these types of devices. The goal of the experiment was to assess the viability of this type of cheating, the likelihood of being caught, and to evaluate potential countermeasures against this type of cheating.

Through the online mapping it was discovered that there are multiple vendors providing electronic devices meant for cheating on exams. These devices had varying quality and functionality, but the devices tested in the experiments worked well for their purpose, and were small and difficult to detect. The experiments indicate that some devices are particularly useful for exams with multiple choice structure or that require short specific answers, but not necessarily exams that require long textual answers.

The thesis contains several suggestions for potential countermeasures. Although some could successfully be implemented, some of the most efficient countermeasures unfortunately require too much resources, and some leads to students being disturbed or leads to an invasion of privacy.

## Sammendrag

Per i dag, er de fleste eksamener som blir gjennomført på NTNU og andre norske universiteter skriftlige eksamener, som hovedsaklig er papirbasert. Juks på eksamen er stadig et alternativ, og med fremgangen innenfor teknologi kan vi nå et punkt der studenter går over fra vanlig "gammeldags" juks, med for eksempel jukselapper eller ved å gjemme ulovlige pensummaterialet, og over til bruk av teknologiske hjelpemidler og elektroniske enheter. Denne typen enheter er tilgjengelig til salgs på internett, og kan føre til en ny tilnærming til juks på eksamen. Det finnes en rekke ulike leverandører som tilbyr denne typen enheter til salgs på nett. Det er stor variasjon i både utstyr og prisklasser, og flere butikker reklamerer spesifikt mot studenter som skal jukse på eksamen. Det er usikkert hvilken grad studenter, og særlig eksamensvakter er klar over denne typen teknologi og utstyr. I tillegg er det svært lite forskning på bruk av denne typen juks, hva slags funksjonalitet slike elektroniske enheter har, og mulighetene det gir.

I denne oppgaven ble det gjort en kartlegging av teknologiske enheter som er tilgjengelig og leverandørene som selger de, og et utvalg enheter ble kjøpt inn. Dette utvalget enheter ble deretter testet i et eksperiment. Det gikk ut på å simulere et scenario der et utvalg studenter skal løse en eksamen, og jukse ved å bruke disse enhetene. Målet med eksperimentet var å vurdere muligheten for å gjennomføre denne typen juks. Det innebar vurdering av muligheten for å lykkes, sannsynligheten for at man blir tatt, i tillegg til å vurdere mulige mottiltak som kan gjøre det mindre mulig med denne typen juks.

Resultatene fra forskningen viser at det finnes en rekke ulike leverandører som selger slike enheter for juks over nett. Disse enhetene hadde varierende kvalitet, men de som ble brukt i eksperimentet hadde i hovedsak god kvalitet. I tillegg var de små, vanskelige å oppdage, og ville trolig fungert godt ved juks på en reell eksamen, spesielt ved eksamen med multiple choice format.

Oppgaven presenterer også en rekke ulike mottiltak som kan implementeres for å motvirke juks. Selv om noen ville funket godt, er det desverre mange av de mest effektive mottiltakene som er vanskelig, eller umulig å gjennomføre fordi det blir for ressurskrevende, i tillegg til å bli forstyrrende for studenter, eller bryte med retten til privatliv.

## **Preface**

This thesis was written for the Department of Computer Science at the Faculty of Information Technology and Electrical Engineering at the Norwegian University of Science and Technology. The idea for this master thesis was partly suggested by Guttorm Sindre, and partly based on the findings from my specialization project conducted during the fall semester of 2017.

First of all I would like to thank my supervisor Guttorm Sindre for his useful feedback regarding ideas and inspiration, as well as contributions towards the experiment and the report. Second, I would also like to thank Excited, and Ida Knutsen for their financial aid and logistics regarding purchasing and acquiring the devices used in the experiments. Finally, I would like to thank everyone who contributed in the experiments and allowed me to conduct the research properly.

Trondheim, June 6, 2018

Matias Fehn Unsvåg

# Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
1.1	Introduction and Background . . . . .	1
1.2	Objectives . . . . .	2
1.3	Approach . . . . .	2
1.4	Contribution . . . . .	3
1.5	Limitations and Challenges . . . . .	4
1.5.1	Focus on Standard Written Exams . . . . .	4
1.5.2	Focus on Cheating During Exam . . . . .	5
1.5.3	Focus on Cheating Without Assistance from University Employees . . . .	5
1.6	Thesis Structure . . . . .	5
<b>2</b>	<b>Theoretical and Practical Background</b>	<b>7</b>
2.1	Exam Practices at NTNU . . . . .	7
2.2	Cheating . . . . .	8
2.2.1	Definition . . . . .	8
2.3	Types of Cheating . . . . .	9
2.3.1	Impersonation . . . . .	9
2.3.2	Plagiarism . . . . .	10
2.3.3	Assistance . . . . .	10
2.3.4	Using Unpermitted Aids . . . . .	11
2.3.5	Unfair Time Advantage . . . . .	11
2.3.6	Lying to Get Unfair Advantages . . . . .	11
2.3.7	Attack Trees . . . . .	12
2.3.8	Risk Assessment . . . . .	13
<b>3</b>	<b>Research methods</b>	<b>16</b>
3.1	Online Content Analysis/Mapping . . . . .	16
3.1.1	Theory and Possible Approaches . . . . .	16
3.1.2	Selected Approach . . . . .	18
3.2	Experiment with Devices . . . . .	22
3.2.1	Experiment as Research Strategy . . . . .	22

3.2.2	Acquiring Devices . . . . .	25
3.2.3	Preliminary Experiment Research . . . . .	26
3.2.4	Test Environment . . . . .	29
3.2.5	What Was Done . . . . .	30
3.3	Ethical Concerns . . . . .	33
<b>4</b>	<b>Related Work</b>	<b>36</b>
4.1	Commonality of Cheating on Exams . . . . .	36
4.2	Cheating Using Technology and Electronic Devices . . . . .	37
4.2.1	Incidents . . . . .	37
4.2.2	Related Studies . . . . .	38
4.2.3	Cheating using technology . . . . .	38
<b>5</b>	<b>Marketplaces and Devices</b>	<b>39</b>
5.1	Usage . . . . .	39
5.1.1	Communication Possibilities . . . . .	39
5.1.2	Ease of use . . . . .	40
5.2	General eCommerce Vendors . . . . .	40
5.2.1	eBay . . . . .	40
5.2.2	dealExtreme . . . . .	41
5.3	Vendors specializing on devices for cheating . . . . .	41
5.3.1	Monorean . . . . .	41
5.3.2	Unseeeyn . . . . .	41
5.3.3	Gsm-earpiece . . . . .	41
5.4	Purchased devices . . . . .	42
5.4.1	List of purchased items . . . . .	42
5.4.2	Camera Pen . . . . .	42
5.4.3	Camera Pen with Wifi transmission . . . . .	43
5.4.4	Suit button Camera . . . . .	44
5.4.5	Bluetooth Earpiece with Neck-loop . . . . .	45
5.4.6	Bluetooth Earpiece with Glasses . . . . .	46
5.4.7	Wifi Camera . . . . .	47
<b>6</b>	<b>Results</b>	<b>49</b>
6.1	Device Usage Results . . . . .	49
6.2	Exam Results . . . . .	50
6.3	Detecting Cheating . . . . .	50
6.3.1	Providing Answers to Assistant . . . . .	51
6.3.2	Receiving Answers from Assistant . . . . .	51
6.4	Threats on Validity . . . . .	51

6.4.1	Internal Validity . . . . .	52
6.4.2	External Validity . . . . .	52
<b>7</b>	<b>Discussion</b>	<b>54</b>
7.1	Discussion . . . . .	54
7.1.1	RQ1: What devices are available? . . . . .	54
7.1.2	RQ2: Is it a viable option to cheat using these types of devices? . . . . .	55
7.1.3	RQ3: What countermeasures can be taken to make cheating less viable to students? . . . . .	59
7.2	Summary and Conclusions . . . . .	62
7.3	Recommendations for Further Work . . . . .	63
7.3.1	Test on Real Exams . . . . .	63
7.3.2	Purchase Devices From Specialized Vendors . . . . .	63
7.3.3	Replicate Real Scenarios . . . . .	64
7.3.4	Retest After a few Years . . . . .	64
	<b>bibliography</b>	<b>64</b>
<b>A</b>	<b>NTNU – Exam Rules</b>	<b>69</b>
A.1	Arrival . . . . .	69
A.2	Calculators and other aids . . . . .	69
A.3	During the examination . . . . .	69
A.4	Terminated examination . . . . .	70
A.5	At the end of the examination . . . . .	70
<b>B</b>	<b>NTNU – Cheating On Exams</b>	<b>71</b>
B.1	Examples of cheating . . . . .	71
B.2	Cheating on other assignments . . . . .	71
B.3	Checks for plagiarism . . . . .	72
<b>C</b>	<b>NTNU – Instructions to invigilators</b>	<b>73</b>
C.1	At the start . . . . .	73
C.2	During the exam . . . . .	74
C.3	Suspicion of cheating . . . . .	75
C.4	At the end of the exam . . . . .	75
<b>D</b>	<b>Questions and Solutions for the Exam Used in the Experiment</b>	<b>77</b>
D.1	Exam Spring 2015 TIØ4258 - Technology Management . . . . .	77
D.1.1	Questions . . . . .	77
D.1.2	Solutions . . . . .	84



# List of Figures

1.1	Chosen strategy for the proposed research . . . . .	3
2.1	Attack tree of cheating by receiving local assistance without using technology or electronic devices . . . . .	12
2.2	Top level of attack tree showing cheating by receiving remote assistance . . . .	13
2.3	Attack tree showing ways of providing answers to assistant, required before receiving remote assistance . . . . .	13
2.4	Attack tree showing ways of cheating by remote assistance receiving answers from assistant . . . . .	13
3.1	Search Results Example 1 . . . . .	20
3.2	Search Results Example 2 . . . . .	21
3.3	Search Results Example 3 . . . . .	22
3.4	Overview of the test environment . . . . .	33
3.5	Search results on YouTube . . . . .	34
5.1	Mini Spy Pen . . . . .	43
5.2	Camera Pen . . . . .	44
5.3	Suit button Camera . . . . .	45
5.4	Neckloop audio earpiece . . . . .	46
5.5	Glasses with audio earpiece . . . . .	47
5.6	Wifi Camera . . . . .	48

# List of Tables

2.1	Risk Table . . . . .	15
2.2	Risk Matrix . . . . .	15
3.1	Most commonly used words in searches for relevant vendors and devices . . .	19
6.1	Exam Cheating Results . . . . .	50

# List of Acronyms and Abbreviations

**GSM** Global System for Mobile Communications, originally Groupe Spécial Mobile

**SEB** Safe Exam Browser

**UiO** University of Oslo

**UiB** University of Bergen

**NTNU** Norwegian University of Science and Technology

**B2C** Business-to-Consumer

**P2P** Person-to-Person

**B2B** Business-to-Business

**FTA** Fault tree analysis

**MTTF** Mean time to failure

**Ofqual** Office of Qualifications and Examinations Regulation

# Chapter 1

## Introduction

This chapter introduces and defines the project scope, in addition to presenting the background and underlying motivation for the project. Then, the research method and research questions for the project are presented.

### 1.1 Introduction and Background

As mentioned by D.A. Bjørke, more than 120 000 exams are conducted at the Norwegian University of Science and Technology (NTNU) each year[1]. Most of these are paper-based [2], but NTNU as well as the University of Oslo (UiO) and University of Bergen (UiB) continue to work on increasing the amount of digital exams each year [3].

As Ina Blau points out in her article, there is no correct generalizing answer to whether students have higher tolerance for digital or non digital cheating [4].

"Some researchers have shown that students tolerate digital academic dishonesty (committed by using digital devices) more than they tolerate "traditional dishonesty" committed without the use of digital devices (e.g. Grieve & Elliott, 2013; Ma et al., 2008). However, others couldn't find any difference between digital and traditional academic dishonesty (e.g. Stephens et al., 2007)."

Moore's Law states that the number of transistors able to fit in a square inch will double every two years [5]. In practice, this means that computers and other types of technology have the possibility to be either twice as good, or half the size every two years. This improvement, along with the growth of eCommerce, and several other factors has lead to an evolvement of more, better and smaller technology available for a lower price. This technology has become available to students through online marketplaces like eBay, Alibaba, DealExtreme, Amazon etc. Small electronic devices such as hidden cameras and earpieces are available for pur-

chase on the Internet, and there has been a growth in the marketing of such devices towards students and the purpose of cheating on exams. The online market is large and growing [6], and using technology and electronic devices becomes a more viable solution for cheating, there is a lack of research that evaluates the functionality of these types of devices. In particular, studies should be conducted to investigate the categories of available devices in terms of technology and price, how can they be acquired to cheat on exams, and to which degree the devices function as promised. Based on this, this thesis will contribute to the field of study by mapping available devices that can be used for academic cheating and investigating their functionality and applicability for cheating on exams. In addition, this thesis will consider possible precautions and countermeasures that can be taken to prevent cheating on exams.

## 1.2 Objectives

**Goal:** *Investigate electronic devices that can possibly be used by students to cheat on exams.*

The objective and goal of this research project is to investigate different electronic devices that can be used by students to cheat on academic exams. In order to accomplish this goal, a mapping of available electronic devices will first be conducted. Then, the functionality and possible achievements of the devices will be evaluated through experiments. Lastly, possible countermeasures will be considered to avoid this type of cheating. The objective is split into the following research questions:

**RQ1:** *What devices are available?*

**RQ2:** *Is it a viable option to cheat using these types of devices?*

**RQ3:** *What countermeasures can be taken to make this type of cheating less viable for students?*

## 1.3 Approach

In the book *Researching Information Systems and Computing*, B.J. Oates provides a figure suggesting different “paths” of work methods [7]. Figure 1.1 shows the work method chosen for this project, marked in red.

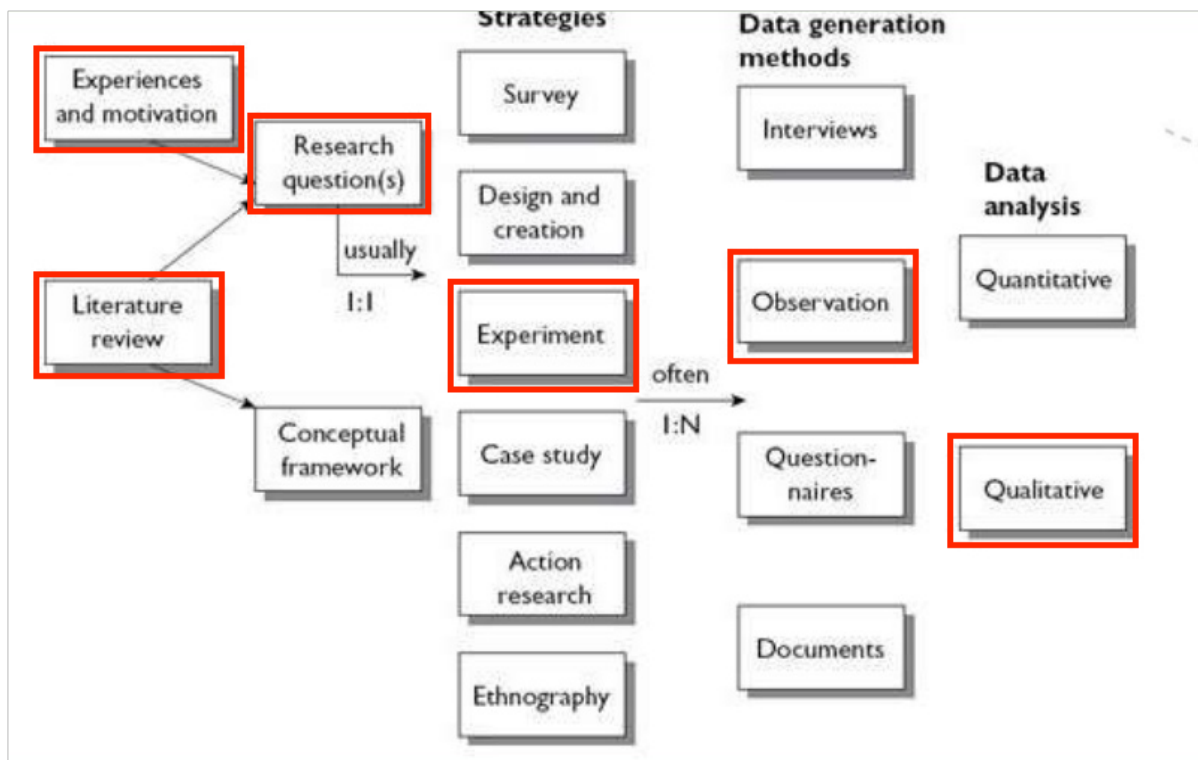


Figure 1.1: Chosen strategy for the proposed research

As the red markings presents, this project begun by looking at previous experiences and finding topics that could be interesting to research. In addition, the research in the specialization project was on the topic of cheating. This lead to discovering more subjects that could be interesting, including cheating with digital devices. The selection of topic and research theme was later materialized in research questions. After evaluating potential suitable courses of action, experiment, case study, action research combination was evaluated to be the most fitting approach. The idea was to understand how, or if the devices work, and how well they work and what they can provide. To be able to determine this, it was necessary with hands on experience which meant that acquiring the devices, and conducting experiments similar to a real world scenario and testing the devices was a logical course of action. The results from the experiments came from observation, along with unstructured interviews with the participants to get their opinions and insight. With the decision to go in depth on certain devices, the results were a qualitative analysis.

## 1.4 Contribution

The first contribution from this project, is a mapping of available devices and vendors that sell devices for cheating on exams. The overview of devices can be used to provide awareness and education for university employees, invigilators, examiners, making it easier for them to detect and properly handle this type of cheating. Secondly, a product of this research is the

analyzed results from the experiments. These results should give an indication on whether it is likely or not that students are cheating on exams using electronic devices and technology. It can also give an indication to whether this is likely to be a more prominent solution for cheating now and in the future contrary to the past. In addition, the results can also provide a suggestion to whether checking students further before the starts of exams is warranted. At exams at NTNU and other universities, students are told to put away their belongings and clear their desks of all prohibited items before the exam begins. Unfortunately, being a resource and time consuming process there are few inspections making sure this is actually done [8]. In fact, multiple students that participated in the survey in the specialization project conducted during the fall semester of 2017 specified that they had cheated, or felt it would be incredibly easy to cheat using mobile phones or other digital devices [9].

If the results conclude that students could easily cheat by purchasing technology online, more checks and security mechanisms should be implemented. Even though it is impossible to do a airport, preflight-like security check, using metal detectors etc, it could be implemented some physical checks to avoid cheating, or perhaps handing in your mobile phone could be mandatory. If the experiments with the devices show that no cheating is possible or that other methods of cheating is likely to be a more viable solution, the resources could be distributed accordingly to avoid cheating.

Lastly, the final contribution is an overview of possible countermeasures against this type of cheating, along with an explanation of why they would work well or not.

## **1.5 Limitations and Challenges**

In this section limitations of the research are presented. The main limitations were that the focus was only on cheating during exams, cheating without assistance from university employees, and on standard written exams. Other challenges and difficulties related to the experiment, e.g., difficulties related to creating the test environment, are explained in Chapter 3.

### **1.5.1 Focus on Standard Written Exams**

One of the first limitations of the research is that the focus is almost solely on standard written exams. Cheating on oral exams, where students do not write down their answers, but are evaluated based on what they say, or home exams where students are not required to complete the exam at a location provided by the university, but is allowed to complete the task at home, both lead to quite different scenarios from standard written exams. The risk profiles could be different, and the potential ways of cheating could vary. That the main focus is on

written exams, and not home exams makes sense, because spy technology and other technological gadgets would be less useful in home exams, or term papers, where it is highly likely that the assistance these devices could provide would be available in other ways. Regarding oral exams, some types of spy technology and electronic devices could potentially be useful, however, the context makes it more difficult to effectively cheat, compared to written exams. Therefore, this research the mainly focuses on written exams.

### 1.5.2 Focus on Cheating During Exam

The second limitation is that the focus is only on cheating during the exam, and not before or afterwards. It could also be possible to cheat beforehand, for instance by hacking, bribing university employees to be able to receive the exam questions beforehand. This would be considered cheating, and could greatly improve a students grade, without cheating during the exam itself. Furthermore, it could also be possible to cheat after the exam. By either bribing an examiner or hacking into the universities computer systems a student could be able to change their grade for the better. Neither of these types of cheating are included in the research, and the focus is only on cheating during the exam itself.

### 1.5.3 Focus on Cheating Without Assistance from University Employees

Lastly, the focus of this thesis is only on types of cheating that do not involve any cooperation with university employees, but only students in cooperation with other students, or students cooperating with outsiders. It could most definitely be possible to cheat by cooperating with a corrupt employee, either a professor, or and invigilator. However, in those scenarios, spy technology and electronic devices, which are the focus point of this research, are less relevant because the student who is cheating could receive an advantage in other ways that would be a lot easier.

## 1.6 Thesis Structure

This outline contains an overview of how the remaining part of the thesis is organized.

**Chapter 2, Theoretical and Practical Background** identifies and provides the theoretical background needed in this thesis, including common exam practices at NTNU, types of cheating and a risk assessment.

**Chapter 3, Research Method** introduces the approach to the research and the experiment, what and how it was performed.



**Chapter 4, Related Work** presents articles and studies relevant and similar to the research in this project.

**Chapter 5, Marketplaces and Devices** provides an overview of available and selected devices, and where they can be purchased.

**Chapter 6, Results** includes results and the main findings in this research and the discussion related to the results.

**Chapter 7, Discussion** discusses the experimental results along with a conclusion and suggestions for further work.

# Chapter 2

## Theoretical and Practical Background

This chapter presents the theoretical and practical background relevant for the rest of the thesis. It contains exam practices at NTNU, a definition of cheating, as well as theory related to experiment as research strategy.

### 2.1 Exam Practices at NTNU

Each semester more than 60,000 exams are conducted at NTNU, with the most common type of exam being paper-based written exams [10]. Although paper based exams are currently most common, NTNU and several other Norwegian universities are transitioning towards more digital exams [3]. Historically, the exams at NTNU are most often conducted in large halls at “Trondheim Spektrum” [10], but classroom or lecture hall sized rooms on Campus have also been used. In recent time, NTNU has also signed a deal to conduct at Postterminalen, instead of Spektrum, which increases the capacity and facilitates for a larger amount of digital exams[11]. These smaller rooms are more commonly used for continuation exams or exams for students that require special examination arrangements. When students have allergies, chronic diseases or other issues they can be allowed to have extended time, special aids, e.g., computer, or adjustable chairs or tables [12]. Since there are fewer students with special requirements it is more practical to conduct the exams in smaller rooms, instead of the large halls.

There are several rules and restrictions regarding permitted aids, often varying for exams [13]. Commonly this means that no written aids are permitted, and only specified types of simple calculators. These rules are enforced by invigilators, who inspect whether students have brought any illegal aids when exam tasks are handed out. There are usually no further physical measures taken to make sure students do not bring unpermitted aids. There is, however, given a verbal message specifying that cellphones must be shut off, placed in back-

packs and stowed away, and that the use of smart watches and other electronic devices is prohibited. The exam invigilators are often more than 60 years old, and might not have substantial knowledge about technology and new types of electronics. This could make them more prone to not detecting students with electronic devices for cheating. The exam office at NTNU have expressed that they do not have or are not allowed to hand out any statistics or information regarding age or technical knowledge, or abilities of the invigilators, meaning that this stereotype is currently based on personal opinions and experiences. During the exam itself the students are not allowed to talk, or move away from their desk. They are however, allowed to ask the invigilators to be accompanied to the bathroom.

## 2.2 Cheating

### 2.2.1 Definition

NTNU provides a document with guidelines for handling cheating and attempts at cheating on exams at NTNU. In this document they have used a broad, generalized definition of cheating. These guidelines states that cheating can be defined as:

Behaviour which is in conflict with the rules for exams, and which, in an unfair manner, leads to that the exam candidate is able to be evaluated as better than they otherwise would have. (Translated from Norwegian, as an English version was not provided by NTNU)

NTNU does not provide any more specified definitions, but rather explanations, along with consequences, paired with several examples of cheating [14]. Some of the examples are only focused on plagiarism, and not highly relevant to this project. Some of the most relevant examples for this project, not only related to plagiarism are:

- Providing an answer taken from the Internet that is wholly or partly presented as your own answer.
- Providing an answer that was wholly or partly prepared by another person.
- Submitting practical or artistic work that was created by someone other than the student him- or herself.
- Copying quotes from textbooks or other academic sources, other people's theses, information taken from the Internet or the like which is supplied without stating the source of the information and without clear marking that it is not original work.
- Illegal aids that you take with you to the exam.

The focus on this study is cheating using illegal aids, or being assisted by other students, and/or using their material as your own. Further on in this thesis the definition provided by University of California, Berkeley's definition will be used. It states that cheating is defined as:

*"fraud, deceit, or dishonesty in an academic assignment, or using or attempting to use materials, or assisting others in using materials that are prohibited or inappropriate in the context of the academic assignment in question"*[15]

In this case, the materials that are prohibited in the context of the academic assignment includes the technological devices used in this experiment.

## 2.3 Types of Cheating

There exists multiple types of cheating. In this section, the most common types of cheating are explained along with possible mitigation strategies, and a risk assessment.

Several articles describe different ways of cheating on exams. In their article M. Hosny et. al. describe approaches such as copying from other students, extracting answers from instructors, and paying someone for doing their own assignment [16]. Sara Shariffuddin, wrote an article about cheating in college, where the types of cheating that were found include bringing illicit materials, receiving help from other students, and distracting invigilators [17]. Some of these methods for cheating are very specific, while others are high level. Aparna Vengdla and Guttorm Sindre conducted a comparative analysis of cheating on paper based vs. computer based exam [18]. Similar to their structure, a high level categorization of cheating is presented below. In addition, types of cheating specific only to computer based exams were not a focus of this research. The main cheating alternatives that were evaluated are the ones who work on both types of exams, or at least on paper based exams.

### 2.3.1 Impersonation

Impersonation is a category of cheating where a student provides answers for another student by delivering their own exam with their name or candidate number. It could be a person with fairly similar looks that takes the exam for them. Since the student taking the exams are required to show ID, it would require the looks of the students to be similar. Another alternative is to provide a fake ID, with the impersonators photograph, which would make the invigilators believe the person taking the exam is another student. This type of cheating has very high reward, as the original student does not have to study at all, because the imposter will do all the work. There is however potentially a very high risk for everyone in-

volved. Especially as any teacher or other person with a personal relationship to the student would easily recognize that it is someone else taking the exam. Although a university employee might recognize a student whom they have a personal relationship with, might not be relevant for all scenarios. Subjects with more than 100 students taking the exam, often means that the teacher does not know every student on a personal basis. Furthermore there is usually only the invigilators who looks at the ID, and could recognize students with fake ID's etc [8]. Teachers and professors are usually only present during the Q/A sequence of the exam, where there are no checks for ID.

### **2.3.2 Plagiarism**

Another well known category of cheating is plagiarism, which essentially means presenting other work as your own. This includes lack of citation or failure to mention sources, and can be accomplished by copying text from permitted aids they have brought, or by smuggling in illegal cheat sheets where word by word is copied to the exam answers. Plagiarism is a slightly less risky alternative than impersonation, as the student can plead ignorance and have plausible deniability. The chance of getting caught is however very big, especially if the exam is computer based, as many universities, including NTNU have proper plagiarism controls [19] [14].

### **2.3.3 Assistance**

Assistance involves cheating based on help from others. This means that a student taking an exam writes down the answers by themselves, but receives help to provide the answers. This can be done locally or remotely. Locally, a student can receive help from a fellow student sitting nearby. Examples of locally assistance include communication through whispering, talking, code signals, or peeking on other students work. Teachers, examiners, invigilators, or other responsible people that are corrupt or willing to help could also provide unfair assistance.

Remotely assistance can be provided through wireless communication through electronic devices such as laptops, mobile phones, earbuds, or using the bathroom to hide answers and cheat sheets. While local assistance shares the risk between student and assistant, remote assistance places almost all the risk on the student taking the exam. In the questionnaire conducted as a pre-study to this thesis, several students at NTNU who participated expressed explicitly that they believed hiding electronic devices in their pockets, and using it in the toilet to receive answers was completely risk free [9]. Whether this is true is up for discussion, but it might be an indication that this approach is less risky than other alternatives, and furthermore that students might be using this approach.

### **2.3.4 Using Unpermitted Aids**

Most exams have strict rules regarding which aids can be brought, and which are illegal to use. Such aids can include specified books, pamphlets, calculators, cheat sheets, notes with answers, electronic devices, smartphones, and smartwatches. Using unpermitted devices could give a student an unfair advantage and make them able to provide an improved answer, or answers they would not be able to provide ordinarily. If an exam has multiple permitted aids it may become more difficult to separate the allowed from disallowed aids, and enforce the rules properly. The risk of bringing unpermitted aids increases, when the amount of permitted aids decreases.

### **2.3.5 Unfair Time Advantage**

As exams have time limits, it might be advantageous for a student to get receive more time. This can be achieved by starting too early, i.e, before the exam starts, or not stopping when the time is up. This can be considered a low risk and a low reward way of cheating. It is considered to give low reward because the student is only able to write answers they already knew, but didn't have time to write down. If the student is able to get 10 more minutes of time, on a 4 hour exam, this would just be an increase of 4%. If this leads to a 4% better grade it is still very likely to be less, and at most one full grade improvement, by NTNU's grading scale system [20]. It is considered low risk, since students working on their tasks before the exam has begun, or after the exam has ended are very likely to be given a verbal warning, and no further punishment. It is also possible to claim that they were not working on their answers, but filling out necessary information that is required to write down before handing in the exam, e.g., room number, course code or date of the exam.

### **2.3.6 Lying to Get Unfair Advantages**

During the exam, if a student has any questions regarding the task, the numbers, or phrasing, the student is allowed to ask the teacher for assistance. However, asking teacher for unwarranted help can be a form of cheating and might give the students help they are not entitled to. This is also a low risk approach with unknown reward. If the teacher decides that the student is lying or exaggerating to get unwarranted assistance, they can just say that they can not help, and move on to other students with other questions. The reward of this type of cheating would be very difficult to predict as the teacher could do anything between not saying anything, and virtually saying how to solve the tasks and providing the right answer. Based on assumptions it could be predicted that the teacher most likely will at most give pointers toward the correct answer, but to a student with no clue on how to solve the tasks to begin

with, it will probably not be very helpful.

### 2.3.7 Attack Trees

Unpermitted aids and assistance, and combinations of these are the categories of main focus in this research. Therefore attack trees representing some of the most relevant ways of cheating and possible mitigation strategies for these categories have been created. Attack trees are conceptual diagrams showing the way an asset can be attacked. In this case, an attack represents a way of cheating on an exam. In the attack trees created, the red arrows shows possible courses of action to achieve a successful "attack". The green arrows shows possible mitigation options for each path. The computer icon shows where electronic technology is involved.

The type of cheating that is the focus of this research is cheating by receiving assistance from another person. This can be done both remotely and locally, where the remote assistance requires that the assistance receives the exam tasks, and then is able to provide the answers to the student. Possible approaches are shown in the attack trees below. As seen in Figure 2.1 no electronic devices or use of technology is involved, which leads to local assistance not being included in the experiment. Although this is a possible way of cheating, the main focus is exploring the possibilities that comes with technology. Some of these possibilities are shown in the attack trees in Figure 2.4, Figure 2.3 and Figure 2.4.

Furthermore, some of the mitigation alternatives would work, but may be impossible, or very difficult to implement for various reasons. For instance monitoring bathroom visits, might lead to invasion of privacy, and disallowing bathroom visits fully could be considered unethical since the duration of some exams is very long, and would make the exam difficult for the wrong reasons.

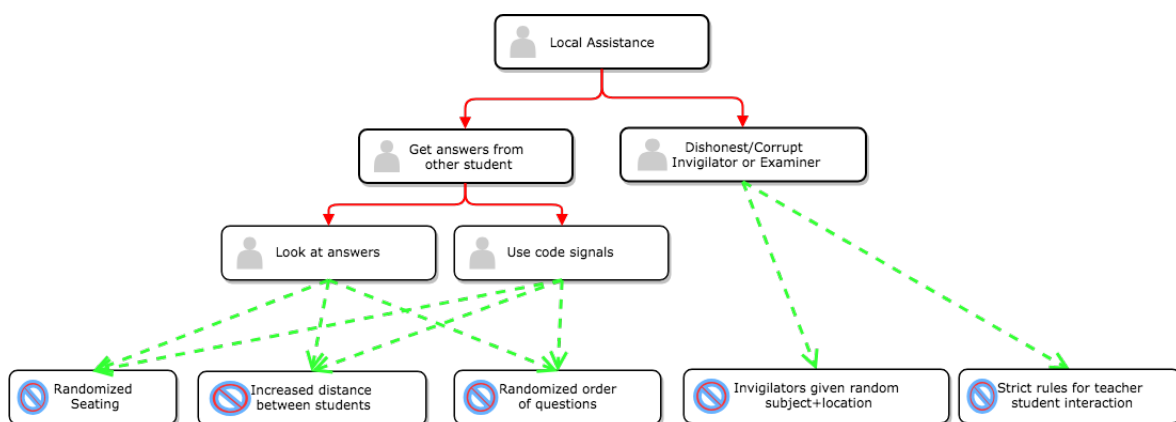


Figure 2.1: Attack tree of cheating by receiving local assistance without using technology or electronic devices

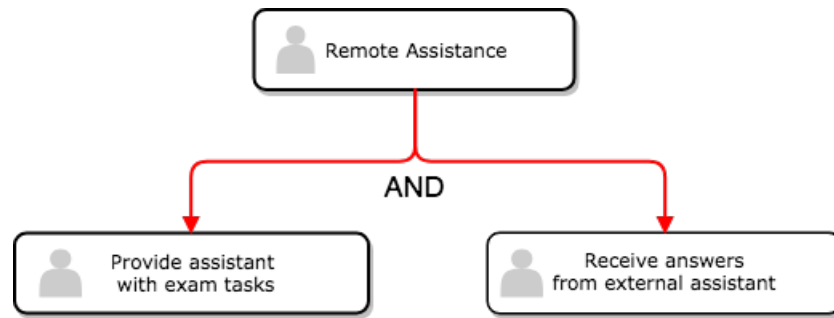


Figure 2.2: Top level of attack tree showing cheating by receiving remote assistance

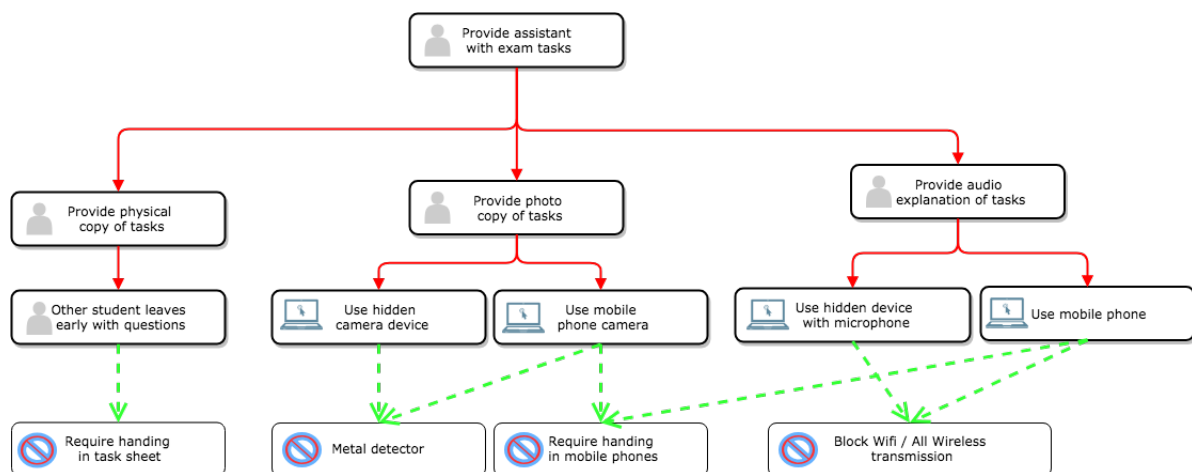


Figure 2.3: Attack tree showing ways of providing answers to assistant, required before receiving remote assistance

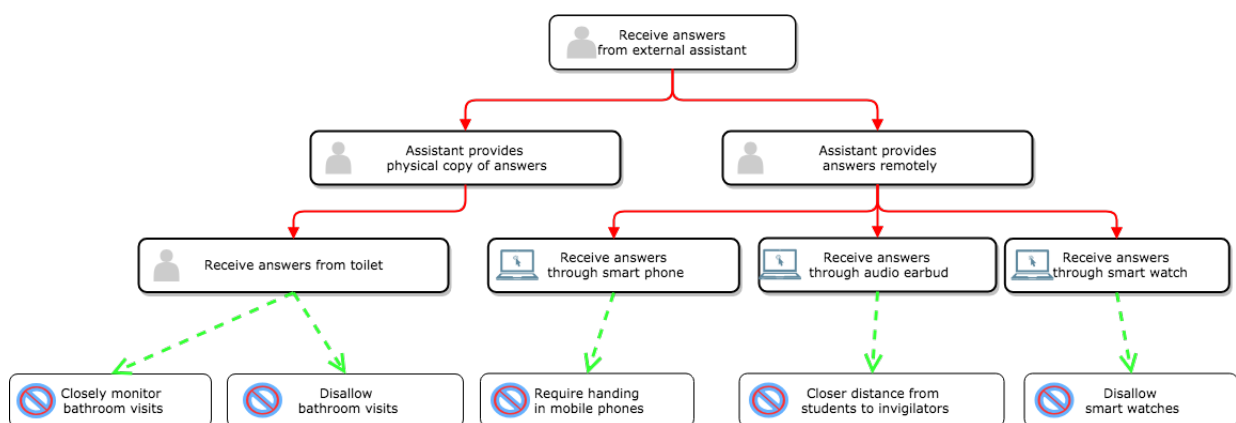


Figure 2.4: Attack tree showing ways of cheating by remote assistance receiving answers from assistant

### 2.3.8 Risk Assessment

The different types of cheating previously presented were ranked based on a risk assessment of likelihood and impact. The likelihood can be related to the inverse probability of getting



caught. This is based on an assumption where students are more likely to cheat when the chance of getting caught is small or insignificant. The impact score is related to how much a student could improve their grade or gain by using the specified type of cheating. This means that the “risk” in the risk matrix comes from the teachers or examiners point of view. It does not represent the risk of getting caught if a specific type of cheating is attempted. A high risk implies that it is something students are likely to try, and if they succeed, will greatly improve their grade.

In Table 2.1, a list of the types of cheating is provided. It contains the cheating type, an explanation of the specific way of cheating, the likelihood of students attempting it, the impact successfully doing it would have, along with an ID. The ID corresponds to the ID’s in the risk matrix in Table 2.2. The risk matrix shown in 2.2 indicates which types of cheating are most essential to mitigate, by highlighting the types of cheating has the highest reward, and lowest probability of being caught, i.e., the highest risk. These types of cheating are also the most interesting to test in the experiments. The different types of cheating are placed in squares based on their risk. The types of cheating ranked in the squares marked in red are the highest risk, while the yellow squares represents medium risk, and the green squares represents low risk.

The most important ways of cheating are the “quick wins”, i.e. types of cheating with high likelihood of students attempting it and high impacts. In addition, it is also important to notice the other alternatives with a higher likelihood of getting caught, but with a very high reward, which can almost guarantee a top grade. As the remote assistance is split into “provide” and “receive”, the impact scores have a somewhat different meaning for the two alternatives. For the types related to providing answers, the impact correlates to how easy the answers is to understand and use for the assistant. Incoherent, stuttering audio is more difficult to interpret and use than a high definition image. A low impact score implies that it will be difficult for the assistant to interpret and use what they receive.

Based on this risk assessment an evaluation of which cheating types that should be mitigated could be done. However, here it is also essential how much resources the mitigation itself requires. If the cheating is a quick win, but it requires a lot of people, time and money to mitigate it, it may not be possible. The risk assessment is shown in matrix (2.1).

Table 2.1: Risk Table

Cheating type	Explanation	Likelihood	Impact	ID
Local Assistance 1	Get answers from other student by looking at heir answers	3	1	LA1
Local Assistance 2	Get answers from other student using code signals	1	2	LA2
Local Assistance 3	Get answers from dishonest/corrupt Invigilator or Examiner	1	4	LA3
Remote Assistance Provide 1	Student leaves early with questions	4	4	RAP1
Remote Assistance Provide 2	Send photo using hidden camera	3	3	RAP2
Remote Assistance Provide 3	Send photo using mobile phone	2	4	RAP3
Remote Assistance Provide 4	Provide audio description of tasks using hidden microphone	2	2	RAP4
Remote Assistance Provide 5	Provide audio description of tasks using mobile phone	1	2	RAP5
Remote Assistance Receive 1	Receive answers from toilet	2	3	RAR1
Remote Assistance Receive 2	Receive answers through smart phone	2	3	RAR2
Remote Assistance Receive 3	Receive answers through airbud	4	4	RAR3
Remote Assistance Receive 4	Receive answers through smart watch	2	2	RAR4

Table 2.2: Risk Matrix

Likelihood → Impact ↓	1-Low	2-Medium	3-High	4-Very High
4-High	LA3	RAP3		RAP1, RAR3
3-Medium		RAR1, RAR2	RAP2	
2-Low	LA2, RAP5	RAP4, RAR4		
1-Insignificant			LA1	

# Chapter 3

## Research methods

This chapter introduces the research methods that were used in this thesis. The chapter also serves as an introduction to the theory behind experiment as a research strategy. Then, an explanation of how the research was set up and conducted is presented, with the two main parts of the research experiment, i.e, testing if it is possible to cheat, and evaluate the likelihood of getting caught.

### 3.1 Online Content Analysis/Mapping

Content analysis is a research method for finding useful information from studying documents, text, video, audio or other types of communication artifacts [21, 22]. In this research the communication artifacts analyzed were text, images and web pages, which means it can be called online content analysis. The most relevant approaches are explained below.

#### 3.1.1 Theory and Possible Approaches

As mentioned, there are multiple ways to conduct an online content analysis. The goal of the analysis was to explore and map potential vendors and the devices they provide. The three two main alternatives that were considered for this research were to use a web crawler, manual search, and netnography.

##### Web Crawler

As defined by Techopedia [23] a web crawler, also known as a “spider” is:

"an Internet bot which helps in Web indexing. They crawl one page at a time through a website until all pages have been indexed. Web crawlers help in collecting information about a website and the links related to them, and also help in validating the HTML code and hyperlinks."

This essentially means that an automated bot acts as a person exploring a website, by pressing all available links and stores the results, and doing so for all pages it reaches by pressing the links. This can be used for indexing, or to provide a map of websites and their sub domains. Advantages of this approach are that it can be used to create an exhaustive database of all web pages with devices and providers. A web crawler can find huge amounts of data in a very short time. This approach could be used to map everything that is for sale on a eCommerce website with hundreds of articles for sale, as the approach is quick and automated.

The disadvantages are that it would require extensive analysis and work to set up the crawler, and analyze the content it finds. This can result in overhead, and the approach is not very flexible, especially as the Internet and online marketplaces are very dynamic environments, constantly changing. In addition, a crawler constantly requesting information from web-pages can cause traffic similar to a denial of service attack to servers. This has led some websites to ban the use of crawlers. For instance the Norwegian football site [www.fotball.no](http://www.fotball.no) [24], states that no use of automated robots, crawlers, or spiders are allowed on their web-pages. The LinkedIn Terms of Services also contains rules that highly restrict the allowed use of crawlers on their websites [25] .

### Manual Search

Another alternative approach for conducting an online content analysis was using basic manual search. This includes using search engines, and manually providing queries assumed to provide results. An example of this approach could be using Google or another search engine, and searching for "*exam technology device cheating for sale*", and then evaluate the results".

The advantages of this approach are that it is highly flexible and modifiable, regarding the queries and search engines. There is also a low overhead related to this approach as it does not require any prior work, programming or resources. The method is very reliant on the person searching, knowing what to look for, but if done properly can provide quick and sufficient results. Another advantage is that it could reflect students looking for devices to cheat.

The main disadvantages include that it is time consuming, requires a lot of manual work, and is not necessarily a very rigorous approach. Going through every single item for sale

manually, on websites like eBay is not possible. In May 2018, there was more than 800,000 items in the electronics category on eBay alone [26]. This means that going through one article every minute, it would take more than a year to go through every item, and items are added daily.

### **Netnography**

Netnography is a type of Ethnographic research that is conducted online, or on the net. Netnographic research often focuses on social interaction and the people involved. In this thesis, netnography could involve reaching out to sellers and buyers of these type of devices, to understand their goals, motives and background. However, it might also mean shifting the focus somewhat away from finding ideal devices for the experiments lead to the decision of discarding the netnography approach.

#### **3.1.2 Selected Approach**

The main goal of the content analysis was not to map all devices and vendors that exists, nor determine motives or information about the people behind the websites. Instead, the goal was to establish an overview of available devices and vendors and then to select a representative collection to purchase and use in the experiments. Therefore, manual search was deemed most appropriate approach.

The manual search was conducted mainly through Google, by using appropriate and relevant keywords as queries that would lead to websites selling devices for cheating on exams and academic tests. Many combinations of search queries where used, and the most commonly used keywords in the searches are listed in Table 3.1. By looking at the results from searches, and potentially being linked to other sites that sell devices, several discoveries where made.

Keywords
Student, students
Cheat, cheating
Exam, test
Electronic
Device, gadget
Spy
Hidden, small, tiny
Earpiece, earbud, audio
Microphone, mic
Camera, cam
Cheap
Easy
Online
Buy, purchase, sale
Pen
Wifi, wireless transmission, IP
smartphone, compatible, iphone, android
Calculator, smart, storage, memory

Table 3.1: Most commonly used words in searches for relevant vendors and devices

Figure 3.1, Figure 3.2 and Figure 3.3 are examples of queries used to search for devices or vendors on Google. These figures show that both news paper articles and Youtube videos explaining how to cheat using technology was easily found. Also vendors such as eBay, Unseeeyn.us, and spystudent were among the first results from a Google search. By looking at these pages, seeing what they provided, and then evaluating new search queries several vendors and devices were found. A list of vendors along with the devices they provide, in addition to what were selected is presented in Chapter 5.


Google

Alle Bilder Videoer Nyheter Shopping Mer Innstillinger Verktøy

Omtrent 8 120 000 resultater (0,52 sekunder)

**Cheat Test: Gadgets & Other Electronics | eBay**  
<https://www.ebay.com/bhp/cheat-test> ▼ Oversett denne siden  
 Find great deals on eBay for Cheat Test in Surveillance Gadgets. Shop with confidence.

**Students are using 'smart' spy technology to cheat in exams**  
[theconversation.com/students-are-using-smart-spy-technology-to...](http://theconversation.com/students-are-using-smart-spy-technology-to...) ▼ Oversett denne siden  
 12. mai 2016 - Spy camera glasses used by the exam cheats. .... Many other **devices** are offered for covert cheating in exams through wireless audio ...

**7 Smart Gadgets For Cheating During Exams - YouTube**  
 <https://www.youtube.com/watch?v=05FtMkla85w> ▼  
 12. feb. 2017 - Lastet opp av YouFact EN  
 Forget about cheat sheets in your phone, and especially on scraps of paper, because today I will show you a ...

**More university students are using tech to cheat in exams | Education ...**  
<https://www.theguardian.com/.../more-university-students-are-using-tech-to-in-exams>  
 10. apr. 2017 - A growing number of UK university students are cheating in exams with the ... a quarter of all students caught cheating used **electronic devices**.

**12 Ways to Cheat on a Test Using Electronics - wikiHow**  
<https://www.wikihow.com/Cheat-on-a-Test-Using-Electronics> ▼ Oversett denne siden  
 ★★☆☆ Vurdering: 49 % - 348 stemmer  
 While taking a test, consult your cell phone, netbook, or other portable **device**. Using the Internet feature, find the answers to the questions you need. Make sure ...

**Bilder av electronic device cheat on exam**





Figure 3.1: Search Results Example 1

Google

Alle Bilder Videoer Nyheter Shopping Mer Innstillinger Verktøy

Omtrent 6 890 000 resultater (0,35 sekunder)

**Bilder av technology cheat exam student**



→ Flere bilder for technology cheat exam student Rapporter bilder

**More university students are using tech to cheat in exams | Education ...**  
<https://www.theguardian.com/.../more-university-students-are-using-tech-to-in-exams>  
 10. apr. 2017 - A growing number of UK university students are cheating in exams with the help of technological devices such as mobile phones, smart ...

**Students Are Using 'Smart' Spy Technology To Cheat In Exams ...**  
[www.iflscience.com/technology/students-are-using-smart-spy-tec...](http://www.iflscience.com/technology/students-are-using-smart-spy-tec...) ▼ Oversett denne siden  
 Students at a medical college in Thailand have been caught using spy cameras linked to smartwatches to cheat during exams. They used wireless spycams in ...

**4 Best Tech Gadgets for cheating in Exams - YouTube**  
<https://www.youtube.com/watch?v=64drGepw0B8>  
 1. okt. 2017 - Lastet opp av DroidWiki  
 4 Best Tech Gadgets for cheating in Exams Follow Me On Twitter : <https://goo.gl/RtNpEz> Top 5 Best ...

**Modern ways students cheat in exams | Daily Mail Online**  
[www.dailymail.co.uk/.../Sophisticated-ways-modern-students-CH...](http://www.dailymail.co.uk/.../Sophisticated-ways-modern-students-CH...) ▼ Oversett denne siden  
 11. mai 2016 - Exam season is here and modern teachers face new cheating techniques; A thread on Quora has seen teachers reveal the cheats they've seen ...

**University students are using technology to cheat in exams | Daily Mail ...**  
[www.dailymail.co.uk/sciencetech/.../University-students-using-tec...](http://www.dailymail.co.uk/sciencetech/.../University-students-using-tec...) - Oversett denne siden

Figure 3.2: Search Results Example 2



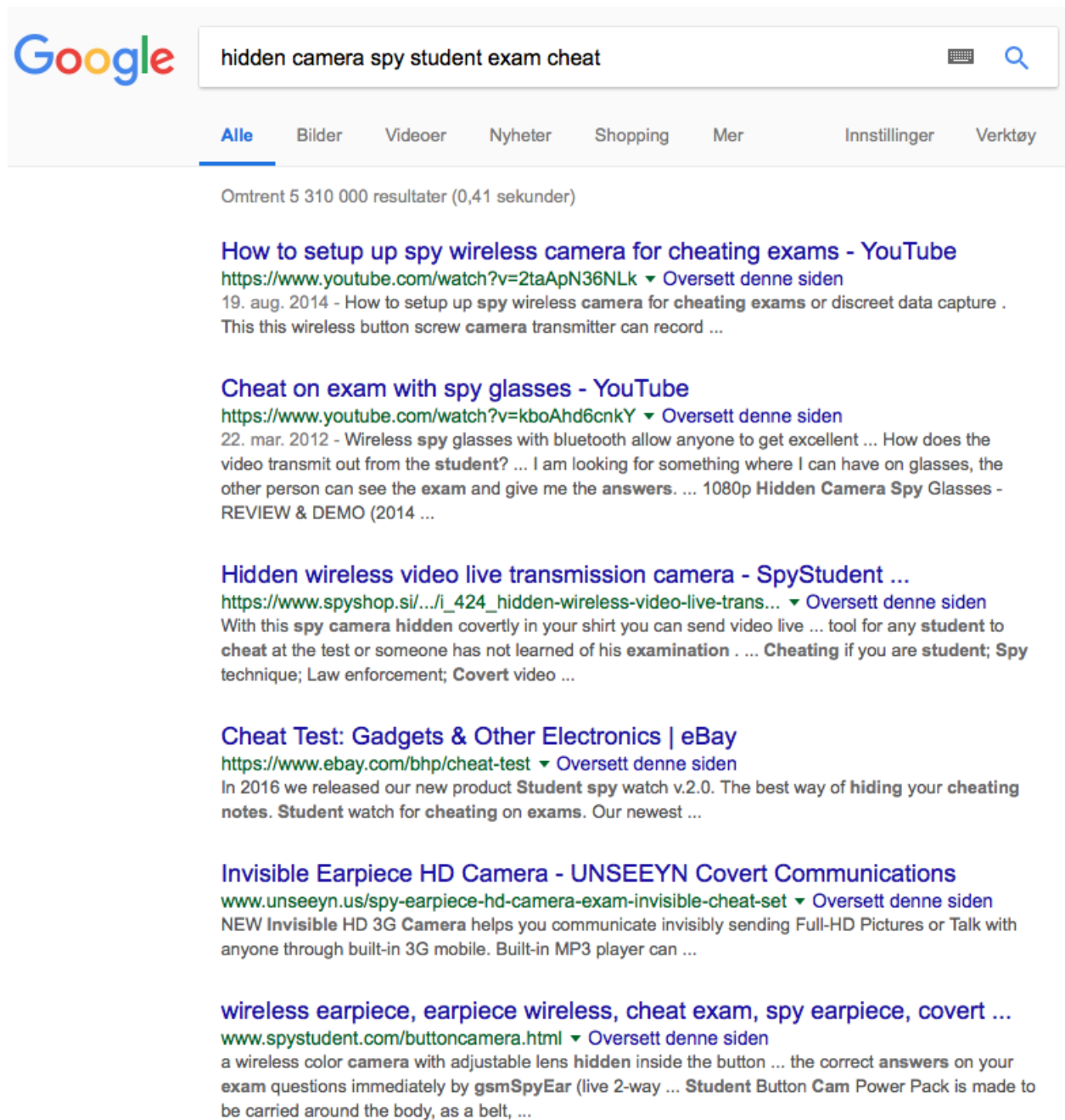


Figure 3.3: Search Results Example 3

## 3.2 Experiment with Devices

### 3.2.1 Experiment as Research Strategy

Before conducting an experiment there is relevant theory that must be known to conduct the experiment in a proper way and avoiding incorrect results and conclusions.

**Definition**

As mentioned in the book *Researching Information Systems and Computing* by Briony J. Oates, in everyday talk and experiment can be considered doing something, with the intention of finding out what happens [7]. This can be anything from changing between coffee and tea for breakfast to find out if there is a difference in how fast you are awake and concentrated in the morning, to going a different route to school and see if you get there quicker. A more formal way of defining experiments can be:

*"A scientific procedure undertaken to make a discovery, test a hypothesis, or demonstrate a known fact."*

as defined by the Oxford Dictionary.

**Process**

The experiment process often contains multiple steps. Some of the common steps in experiments are:

1. Observation and Measurement
2. Manipulation of Circumstances
3. Re-observation
4. Proving/Disproving relationship between factors involved and effects
5. Repetition

In step one of the experiment observations are made and measurements are taken. Examples include measuring how much time is spent on the experiments, how long each part took, and observing the final results. Then, in step two, changes are made to either the environment, the participants or the equipment. Such changes allows the possibility to conduct the experiment a second time, with further observation. The new results, can be compared with previous results, and be used to evaluate which factors caused the potential differences in results. Repetition is the last step and is important as it contributes to avoid arbitrary changes and to increase the certainty that the results were not caused by arbitrary factors, but were due to factors introduced on purpose in the experiment. How the steps were implemented in this thesis is explained in Section 3.2.5

**Validity**

It is important that the conclusion of an experiment has proper validity. Someone can make the hypothesis that they will be colder when they arrive at work if they run instead of walk to

work. They can try this once, and come to the conclusion that they are correct, but if this is caused by colder weather instead of changing from walking to running, the conclusion will not be valid. The two main parts to ensure validity is *internal validity*, and *external validity*, which will be explained in turn.

### **Internal Validity**

In his article on Evaluation Research, Paul M. Wortman explains that internal validity refers to the credibility between the implemented causes and factors in the experiment, and the effects [27]. Are the effects actually a result of the factors that were purposely introduced?

*History* is one of the threats to internal validity. As time goes by incidents may occur, and factors may affect the participants during the experiment. For instance if the experiment is about looking at stress levels of workers, death in family, learning you might get fired can have direct impact on stress levels. This can lead to affecting the experimental results.

*Maturity* is another threat to the internal validity. As the participants grow they can mature and learn from previous experiences. They can learn from the first test in the experiment, practice, or if the experiment has a large time-frame they can improve. This can cause the re-test to give more improved results than they were supposed to. Repetition in experiments can also cause boredom or fatigue or make them uninterested which can cause the re-test results to be worse than they should.

*Faulty instruments* can also be a factor that has unintended effects on the experiment. One time incidents that do not occur on a regular basis, such as network crashes or devices working improperly can also affect the results.

*Reaction to experiment setting* can also affect how the participants perform. The fact that participants are in an experimental setting where they are being tested can have a psychological effect on the participants and cause a difference in performance. B.J Oates, explains this by using an example of someone being tested for keyboard typing speed. Their regular typing speed may be higher in a normal real world scenario, but stress or other effects of being in a test setting can make the participant perform worse [7].

### **External Validity**

External validity is a measurement of how well the results can be generalized for other scenarios, people, situations. and locations. Are the results only valid for one specific group of people and situation or would the results still be the same if it was applied elsewhere?

*Specific participants* can lead to low external validity. If a study is meant to apply for students in general, only using students from one study program e.g., computer science students may not be an ideal choice. *Too few participants* may cause very low statistical significance, as they do not represent a large enough part of the study population. *Representative test participants and environment* is also essential, to properly reflect a real world scenario, and make

the results applicable to real exams.

### **Experimental Design**

There are several different experimental designs that could work for this research. The selected approach was using “one group”, with two different tests, without the “pre-test” and “post-test”. One group implies that the participants are the same for all repetitions and tests. Pre-test and post-test means that the participants will be allowed to attempt solving a task, then when new factors are introduced, they can do the test again. This way of conducting research allows fairly easy comparison of results, with introduction of new factors. In this research, where students were supposed to cheat on exams, the pre-test was not necessary. Instead of a pre-test and post-test alternative, a subject the participants did not know the answers to were selected. This meant there was no need to let them try the exam without cheating first, because the participants would most likely score 25% on a 4 option multiple choice exam. Instead they were allowed to cheat using different methods and devices.

### **Advantages and Disadvantages**

Advantages, and the reasons that this type of strategy was selected for this research was that it applied well to this scenario, and was possible to conduct. In addition, it is also a well established method, and seen as one of the most accepted and approved scientific methods according to B.J Oates [7].

The main disadvantage was that the test environment and scenario was not exactly like a real world alternative. Some factors may be different in the “laborator” setting than it is in the real world exam situation.

#### **3.2.2 Acquiring Devices**

Determining which devices to select to purchase was a difficult process. Without further research it was impossible to determine with 100% certainty what types of devices students might use. Purchasing all devices would be expensive, and testing all devices would be too time consuming considering the time limits of the research project. This meant that a selection of items deemed representative were chosen and evaluated.

As this research was limited to one semester, delivery and shipping times of the devices also had to be taken into consideration. Many of the vendors, especially on eBay, had long and unspecified shipping times. This meant items with more than four to six weeks of estimated shipping time were not eligible for selection because they would arrive too late. Another

problem regarding devices was that it was difficult to determine how much money students would be willing to spend to attempt cheating on exams research. As no research were available on this topic the only option was speculation, and going forward this research was based on the assumption that students are fairly poor and not willing to spend too much money on devices. This led to the most expensive alternatives of vendors and devices not being selected. Furthermore there were some alternatives available that did not look like serious actors. Vendors with poorly designed websites with no or poor customer reviews were also not selected.

Without further research it is also difficult to determine how much effort students are willing to put into the cheating process. Some devices require further purchases like Sim cards, adapters, certain types of mobile phones, cables or other parts, which are not included and may be difficult to acquire. Some devices requires a lot of practice and knowledge of how to use the devices properly, in addition to being expensive. Since it is difficult to gauge how much work, time and money students are willing to put into cheating, the biggest focus of this research ended up being on cheap but efficient devices; high reward devices that are fairly cheap and easy to use. Devices that requires a lot of practice before being able to use them properly were not prioritized. This set some restrictions on what devices to acquire.

The full list of devices that was purchased can be found in Section 5.4. However, of all purchased devices it was mainly audio earpieces connected either via a neck loop or bluetooth glasses, and a camera pen that transmitted video through wifi that were used in the experiment.

### **3.2.3 Preliminary Experiment Research**

Before the main experiment begun, some research was required to determine whether the devices worked at all, and if so, how well they worked. In order to test whether they could be used to cheat on exams, it was necessary to determine if they worked at all. Finding out how to use them, and what functionality they had available, along with their limitations was conducted as a preliminary part of the experiment.

#### **Range of Sound and Connectivity**

As the intended devices used some sort of Bluetooth or wifi wireless transmission, as well as small earbuds that transmit audio, evaluating the range of the devices was necessary.

To test the range of connectivity, one person wore the earbud, while another person that was connected to the earbud using voice call, provided a stream of audio by reading continuously

from a prepared arbitrary text. This meant that the person wearing the earbuds could begin with the earbud as close as possible to the transmitter, and then slowly move it further away. The threshold distances where the sound begins to differ in quality was measured and where sound completely disappeared. The participant was also assumed to have normal hearing, and there were no indications otherwise.

Sound noise from the earpieces were also a potential issue. This was tested similar to the test of the range of connectivity, where one person wore the earbud, while another person that was connected to the earbud using voice call, provided a stream of audio by reading continuously from a prepared arbitrary text. This time, a third person was involved, and started about 2 meters away from the person with the earbud. Then, the third person moved towards the earbud slowly until any sound was detected. However, as the volume was very low even though it was set to max, the third person was unable to detect any sound without practically hugging the person wearing the earbud, and placing their ears so close that they are touching, or 1 cm away from touching. Testing the volume from the earpiece while not in ear, it was required to be within less than 5-10 cm for any sound to be heard at all. This was tested similarly, except that person two did not wear the earpiece, but hold it in their hands.

From these tests, it was interesting to notice that that 5 cm is a very close distance - ear to ear this is close to giving somebody a hug. It would probably feel embarrassing for most people (e.g. invigilators, exam candidates) to be so close unless they are intimate with each other beforehand, which would rarely be the case. Hence, it is unlikely that an invigilator would be close enough to hear this "by chance". The only plausible cause for the invigilators to notice the sound might be if there is a very explicit instruction to do so, or if there is something suspicious about the candidate that triggers such an investigation. Moreover, if it was possible for the candidate to quickly adjust or mute the volume of the earbud, it might be argued that in most cases the candidate would see the invigilator coming before the distance is as short as 5 cm, and thus could avoid detection even if such embarrassing investigations were to take place.

In addition to a test of how easy it was to hear the earbud from outside, it was also performed a quick evaluation of how easy, or difficult, it was to see the earbud. Essentially: how close would the invigilator need to be to see it by chance, and how close to be able to see it if deliberately looking for it (e.g., if NTNU were to change the invigilator instructions, adding that they should be especially on watch about students using earbuds).

Since the earpieces are designed to be "in-ear" it was evaluated to be practically impossible to notice it while standing behind, in front, or facing the ear without the earpiece, of the student wearing it. This mean that the only way to see it was by standing on the side of the student with the ear with the earbud in it. Additionally, even though a person was standing

on the correct side, the earbud was very small, and skin colored, which made it hard to detect. Although it is hard to say with certainty, an invigilator would need to be approximately 3 meters away or closer to the student with the earpiece to notice it, if they are actively looking for it. And even though they could spot it, the student wearing it, could quite easily take the earbud out, and hide it, while they believe that an invigilator is in a position where the earbud could be seen. Since the earbud is small, and wireless, removing it, and placing it back in is an easy task, which can be done with raising suspicion. It could also be added that the likelihood of the earpiece being seen, is only relevant if students are required to openly display their ears. If the university allows students to have long hair outside the ears, or to wear hats, hijab, hoodies or in other ways block their ears, it will be impossible to see an earbud no matter how close you go.

The earbuds that connects to the Bluetooth glasses was one of the devices with most limited range. When the glasses were worn, and the earbuds was worn on the right ear, the connection was good. However, the range was very limited and moving the earbud more than 5-10cm away from the right side of the glasses resulted in stuttering or lack of sound. This resulted in that using the earbud in the left ear was not possible.

The earbuds that connects to the neck-loop had far better range. The neck-loop could be worn under clothes, either in a pocket, or around the neck as intended, and the earbud connected fine without stuttering or loss of sound. For this device the range was between 1-2 meters distance before stuttering and loss of audio started to occur.

The next device that was tested was the camera pen with wifi transmission. It contained a locally broadcast internal wifi, which a mobile could connect to. Then it was possible to view the footage through a mobile application specified to connect to wifi cameras. The range of this wifi was very limited, and at approximately 5-10 meters, depending on walls and other objects that help block the signal, the footage became poor. As the distance increased, the latency was increased significantly, the footage started to freeze on arbitrary frames, and the resolution and footage quality was lower. The best solution to this problem was to use another feature provided by the camera pen in combination with the mobile application. The camera pen could alternatively connect to an external wifi, as long as wifi only required password, and not username/password combinations etc. Connecting to an external wifi led to the signal being high quality as long as the wifi signal was sufficient. This meant the signal range was no longer dependant on the technology within the pen itself, but rather the router that broadcasts the wifi etc. While using shared wifi from a mobile device, the signal was properly transmitted and the footage acceptable at 10-15 meters range. Other ranges would depend on what internet is available and the hardware, e.g., router in use, but distances of approximately 50 meters is possible to achieve [28].

Unfortunately one of the devices, the suit button camera, did not work at all. It required a

specialized Usim-card, which none of the participants mobile carriers provides. Most common Norwegian mobile carriers, like OneCall, allows customers to get additional sim cards, but no U-simcards [29]. They provide additional data-only simcards, or extra regular sim-cards. Unfortunately the suit button camera did not work with either of these sim cards provided.

### 3.2.4 Test Environment

The second part of the experiment was creating a proper test environment. The main idea for the test environment was to reflect the exam situation as much as possible with regards to number of people, noise and visibility.

As mentioned in 2.1 exams are usually conducted in large halls with lots of students, and ideally cheating using these devices would be tested in these large halls, during a real exam. This is unfortunately very difficult due to rules, restrictions and ethics.

First, it would be difficult to get a permission to cheat without any repercussions for the participants if they got caught. Secondly, it might be disturbing for the other students that are actually taking the exam, and distract them or make them less focused. It could also require more attention and resources from the invigilators, since any noise or unusual actions would make them focus on the possible suspect, and take attention away from the other students who are actually taking the exam in a normal way.

In addition, it may be problematic due to lack of time, and scheduling issues. At NTNU exams are mostly scheduled late in the semester which would lead to insufficient time for analysis and evaluation of the results. If the exams are mostly conducted in May or June, this would lead to a too big work load in the final two months of the semester, and not enough work to distribute over the first four months of the semester.

Furthermore, testing the devices at a real exam might also be unethical towards the people that are given the assignment to make sure students are not cheating. As seen in the "instructions to invigilators" document provided by NTNU, the invigilators have several task, where looking for students who are potentially cheating, is just a small part of it [8]. They might feel that such an experiment is a test of their abilities to do their work properly. This is not the case, as the experiment is intended to test the possibilities of electronic devices, not abilities of invigilators. However, if it would cause less people to be interested in future jobs as invigilators it is not ideal. It would not be possible to conduct the exams if no one signed up for the job as invigilators.

This leads to the issue, which is creating a completely similar test environment. It was difficult since the exams are conducted in large halls with hundreds of students. Replicating



acoustics, sound decibel level, and distance from invigilators to students completely accurate would be almost impossible.

Moreover, it would be problematic if students, invigilators or other participants in the experiments know that the goal of the experiment is to cheat. The fact that it would not be a regular exam, but an experiment might make them more alert towards disallowed behaviour and more likely to detect cheating than during a regular exam.

The amount of students was hard to replicate since all participants in the experiment were volunteers. Getting more than 100 students to participate on a voluntary basis was not possible, so a smaller set of students were selected. However, an attempt was made to replicate the density of students and noise levels as much as possible.

Since it was not possible to conduct the experiment in these large halls, the solution was to conduct a fake exam in study halls at NTNU, where students study for exams, and work on their assignments and projects. These study halls fit between 20 and 100 desks, and are very similar to the exam situation, especially the continuation exams with regards to size and amount of students. These study halls also have approximately the same types of sounds and noise levels as the exams, although this was not tested or verified using scientific methods, but only based on the opinions of the volunteers and other students.

### **3.2.5 What Was Done**

#### **Participants**

All of the participants were approximately 25 year old male students, studying Computer Science at NTNU.

#### **Roles**

The idea was to conduct a "fake" exam, where participants play the different roles included in examinations. This meant some participants were to play the role as students, which their main task being solving an exam. One person was given the role as invigilator, and were given a set of instructions that are used at NTNU for invigilators [8]. This includes handing out tasks, checking whether the students have only brought permitted aids and calculators etc. In addition, they were told to write down a log containing information regarding possible cases of cheating. The document with instructions to invigilators, provided by NTNU, does not specify whether the invigilators should sit in one place, or walk around the exam hall [8]. Walking around too much, might distract the students, but sitting still in one place, could make it easier for students sitting furthest away to conduct unpermitted behaviour

unnoticed. In this experiment the person with the role as invigilator was instructed to sit close to the window, and approximately every 5-10 minutes take a walk around examination area. The final person were given the role of cheating assistant. This person plays the role of someone who is extremely competent in the subject, and has access to Google or other ways of finding the correct answers. In this experiment, they were given a set of solution manuals to the different exams. Once they received questions, they could go through the corresponding solution manual and provide the correct answer.

The tasks for the exam, along with the subject was kept secret for the participants to avoid them practicing and solving the tasks without cheating. The person who was supposed to cheat were given assistance from an outside person using a combination of the devices available. The idea was to find out if the students could get all the correct answer to e.g., a math exam without the correct math knowledge, by communicating the tasks to the outside person, and receiving the answers.

In practice, the students were first given devices to assist them. The combinations that were used was:

1. Glasses with microphone and earbud, in combination with mobile phone.
2. Earbud with neck-loop, and camera pen with mobile phone.

They were also given a sheet of paper with instructions for how to behave during the exam, and how to cheat. The invigilator were also given their set of instructions to follow, and exam tasks. Since the person assisting was not supposed to know the task answers, the invigilator was given 10 different exams, and was told to hand out one random exam.

### **The tasks**

The main focus was to solve an exam, where the selected subject was Technology Management. This subject has a multiple choice exam, with approximately 30 questions, with 4 alternatives per question, and one correct answer. Furthermore the participants were later told to attempt to solve a Discrete Mathematics exam. First, to evaluate whether it is possible to solve exams which are not multiple choice, but answers with text, formulas, and calculations etc. Secondly, if it was possible to solve the exam, evaluate if it was easier, or more difficult. Some of the participants has already taken these courses, but none had taken exams the last 2 years, and they admitted to currently having very little or no knowledge about the subjects.

### **Sending out questions**

The student taking the exam was required to communicate the exam tasks and exercises to the person assisting. While sending out the questions, the assistant was positioned in position 1. marked in 3.4. One of the students did this using the camera pen, which sent live video to the assisting person. The person with glasses had a microphone available. This microphone did not pick up sound very well, and it would require too much speaking, and mumbling. This led to the only alternative being taking a picture of the tasks with their mobile phone, and sending it to the person who was assisting. This was done by bringing the exam tasks and their mobile phone to the bathroom, where the pictures were taken and sent.

### **Receiving Answers**

Receiving the answers was done using the earpiece with audio. When the students attempted to receive answers, the assistant moved to position 2. in figure 3.4. Since the audio earpiece with voice call has a larger range than e.g., the camera pen, the assistant could sit further away, to make it less likely they were caught. However, as this was not a real exam, the assistant did not go out of the building, or to a completely different location. Since the only restrictions of the range was cellphone reception, it could be possible in a real scenario to be in a completely different building, but it was not deemed necessary in this scenario. The student with the glasses was required to keep the earpiece in the right ear for it to align with the bluetooth transmitter inside the glasses. The sound quality was not very good, and even though the volume was set to maximum, the sound level was very low. The answers were somewhat received anyway. As they had a microphone available, it was also easier to determine whether answers needed to be repeated or if they were understood.

For the person with the neckloop, the sound quality was a bit better, and the earbud could be worn in either ear as the transmitter in the neckloop had a stronger signal. This person did however, not have any way of letting the assistance person know whether the answers were understood or not. This meant the answers just had to be given and repeated several times in hope of being understood. The person taking the exam could however use the camera and video specific questions they did not get the answer to, or other improvising methods using the camera.

### **Detecting Cheating**

While the students were trying to solve the exam, the invigilator were among other things told to look for cheating, and log possible cases. They were told to write down what they saw, i.e., what was done, and what equipment was used, in addition to the time, and what they

think was done. If they saw someone using their phone, they were not told to intervene, but to write down the incident.

## Delivering answers

When the students felt they had the correct answers they were told to hand in their answers.

## Overview of the Test Environment

Below, figure 3.4 shows an approximate view of the test environment as seen from above. The squares represent desks, where students work on their tasks. The students marked with green are the participants in the experiment with role as student. The person in red has the role as invigilator. The person marked in blue has the role as cheating assistant. The other people are students who were present, but not actors in the experiment.

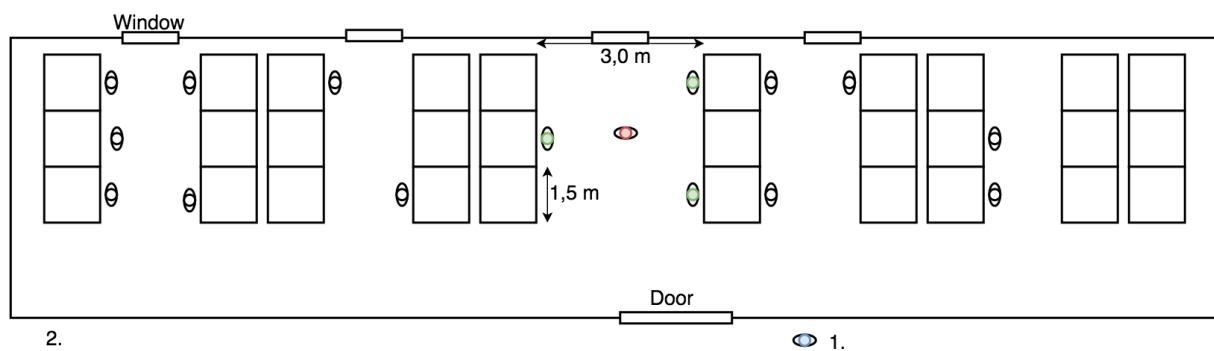


Figure 3.4: Overview of the test environment

### 3.3 Ethical Concerns

There are several ethical concerns related to this research. As mentioned earlier, a decision not to conduct the experiment during real exams, was made, partly due to ethical issues concerning the invigilators as well as other students. If the experiments were done during a real exam, other students from taking their exams, seated nearby might be distracted and receive a worse grade than they normally would. The invigilators, whose main task is not to detect cheating could feel that it was an attack on their personal abilities, and that they were doing their job poorly.

The most important ethical issue, was that this research might show students new ways to cheat, or work as a "how to cheat on exams"-tutorial. By finding new vendors, devices, prices, how the dives could be used, in addition to likely results it might make students more

likely to cheat. Students who were not aware of this type of cheating originally could learn new ways of cheating they could consider at a later exam. One of the main reasons this was still deemed acceptable is that most of the information presented in this research is already publicly available online. For instance, searching for "*exam cheat device*" on Youtube, presents videos of people using, or advertising for devices similar to the ones used in this experiment.

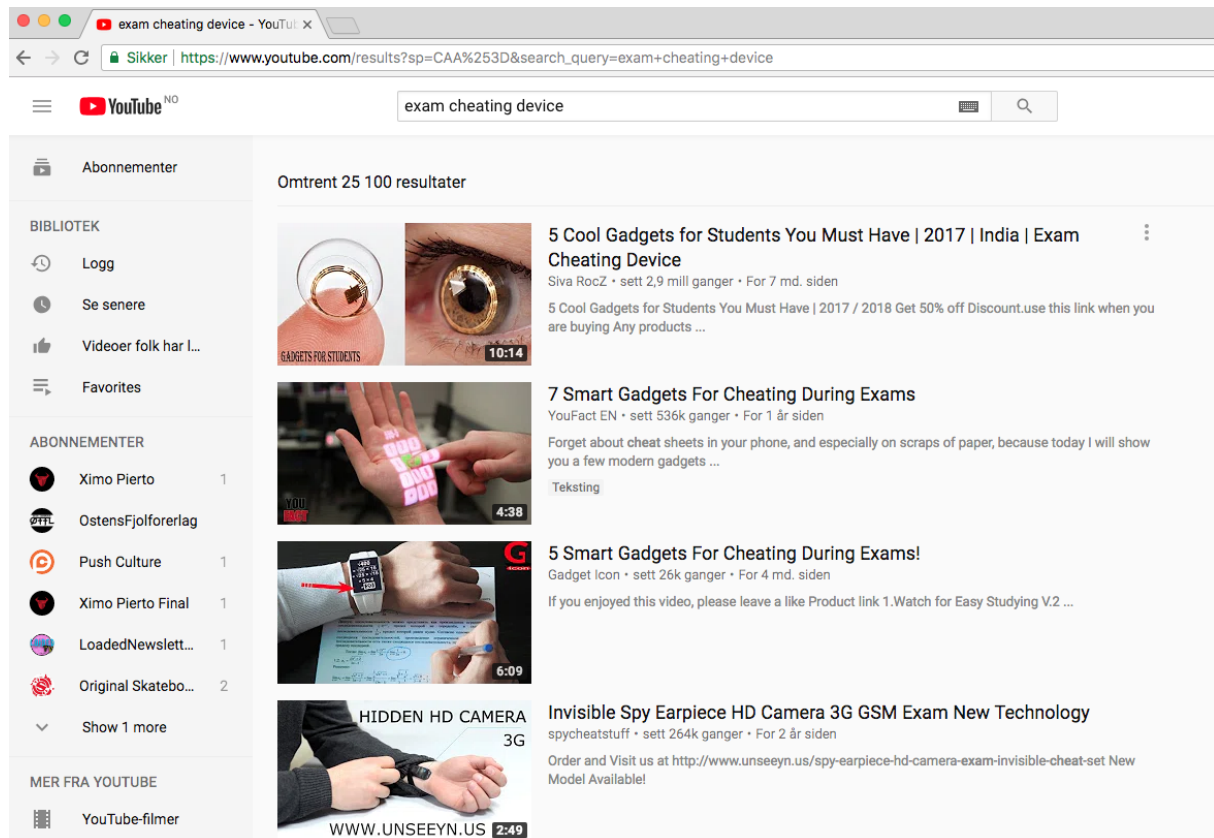


Figure 3.5: Search results on YouTube

Most of the devices were also acquired from stores most students are familiar with to begin with, like eBay, and if they tried would most likely be able to find everything presented in this research. Additionally, news reports are shown in section 4.1, from Sweden, England etc. which indicates that this type of technology is already familiar to students, and is being used. Therefore, it was evaluated to be more important to highlight the possibilities of this technology, and make university employees, examiners, and invigilators aware of these possibilities.

Furthermore, it would be positive that these threats were publicly known. If these types of threats are discussed openly and evaluated by invigilators, examiners and university employees they will probably be more capable of handling or mitigating the threat. In fact, knowledge about the technology and the possibilities that comes with it, is essential to avoid scenarios where students are exploiting it without being caught. If students believe that the

invigilators are not aware of this type of cheating, they would also perhaps be more inclined to try it. This means that exposing the threats and making all parties aware of the possibility, could decrease the number of students attempting to cheat this way.

# Chapter 4

## Related Work

This chapter contains articles and research similar to or related to the project.

### 4.1 Commonality of Cheating on Exams

Every year there are several instances where students get caught cheating. In Britain 40 000 students were disciplined for cheating in 2015 and 12 000 were deducted marks as a consequence according to the British newspaper The Guardian [30].

BBC also published an article with numbers from Ofqual (Office of Qualifications and Examinations Regulation) which stated that more British students got caught cheating in 2017 than in 2016. The increase was from approximately 2100 students penalized to 2700, where 40% were penalized due to bringing unpermitted items to the exam, mostly mobile phones.

The Norwegian newspaper Aftenposten published an article, using statistical data collected by ForskerForum, which states that cases where students get caught cheating at universities have risen substantially since 2011 [31]. Although some universities, like NTNU only has a few cases of people getting caught, 11 at NTNU in 2016, UiO and other universities have closer to 100 cases [32]. This is a very small amount of cases, considering the number of students in total at those universities, but the unrecorded cheating incidents can be very high. In fact a study done by Sentio Research Norge for Universitetsavisa showed that 5% of the 1001 students involved, admitted to previously having cheated on exams. If this was applied to NTNU, with 40 000 students, it would mean that the number of people who cheat could be approximately 2 000. As the number of students caught was less about 10 it implies there is a great possibility of cheating happening, but going undetected.

In Sweden, there was recently a case where the police have made multiple arrests and several people are charged with assisting students in cheating on exams by selling them cor-

rect answers to tests [33]. The Swedish Economic Crime Authority is a specialized authority within the public prosecution service, fighting economic crime in Sweden and coordinating responsibility for the activities of other agencies in this field [34]. They believe the network of people assisting students in cheating made up towards 170 000 SEK, per test, making up to 10 Million SEK, during the last four to five years. The logistics behind it and how the cheating was done in practice is not certain yet, but it is believed that the cheating was advertised through social media, and using a combination of students and examiners, they were able to transmit the correct answers using specialized earbuds [35].

## 4.2 Cheating Using Technology and Electronic Devices

In her article in Information Systems Education Journal, Liza Z. Bain writes about how students use technology to cheat, and what can be done to prevent it [36]. She states that many students are already using electronic devices, e.g. smartphones, to access unauthorized information and cheat on exams. She lists smartphones that can access internet, e-mail, documents and files etc., in addition to mp3 players, wireless earphones, cameras, and IM (Instant Messaging) devices, including IM enabled calculators as common devices. Any of these devices can give a student an unfair advantage on a test or exam by providing access to unauthorized material and information.

### 4.2.1 Incidents

The increased availability of these types of devices brings a massive opportunity for students to cheat on exams. In fact, there has been an increase of 42% in cheating using technology and gadgets, e.g. mobile or hidden earpiece since 2012, according to the British newspaper The Guardian[37].

In his article published in TheConversation Ritesh Chugh writes about how students cheat using technology [38]. He references among other, incidents of medical students in Thailand that were caught cheating on exams using glasses with hidden cameras connected to smart watches. This allowed them to transmit images and receive messages to get answers to exams.

Furthermore, the story about cheating on exams in Sweden in 4.1, also indicates that technological devices, i.e. specialized earbuds and computers, were used to cheat.



### 4.2.2 Related Studies

There has been very few studies directly on the possibility of cheating using different electronic devices, and evaluation of them. The most relevant and similar articles and their main findings are presented in this section.

### 4.2.3 Cheating using technology

Wong et al., published an article in the fall of 2017 on the usability of smartwatches for academic cheating on exams [39]. Their results showed that the usability was not very high for cheating using the smartwatches, however they found out it was easier to achieve a higher score on multiple choice tasks, than short written answer tasks using the smartwatches. These are interesting findings, but their research does not include any other type of devices. Their focus is only on smartwatches, which is not the main part of this thesis.

There has also been several studies regarding cheating on E-exams and Bring Your Own Device (BYOD) exams. Phillip Dawson published an article where he explained five different ways of "hacking or cheating" on BYOD examinations [40]. This is however also different from all electronic devices as it focuses on situations where students are supposed to bring their laptop, but use it in an illegal way.

Additionally, Thea Marie Søgaaard, researched different ways of cheating on BYOD exams at NTNU, and presented her findings in her specialization project and master thesis [41]. BYOD-related cheats were attempted, and multiple were successful, for instance to use Skype in spite of running Safe Exam Browser. This way, the cheater could achieve to get help from an outsider in a way similar to the GSM earbud approach. However, there could be different risk profiles. The Skype approach means to cheat via a network that the university controls (the network that they are running in the exam hall), so even though they are able to successfully fool the SEB, they might get caught if there is some additional surveillance of suspicious network traffic. A Skype conversation would probably transfer much more data than the submission of answers to the exam, along with other network irregular activity, which means the university could at least be able to detect that something suspicious is going on and decide to look into it. The GSM earbud on the other hand has the advantage that cheating takes place outside the infrastructure controlled by the university. On the other hand, a disadvantage may be that the earbud itself (and additional equipment on the body) will be very convincing evidence of cheating if the candidate is indeed caught red-handed, while the laptop was a legitimate piece of equipment and is thus no evidence of cheating in its own right. The research of T.M. Søgaaard, was also meant to detect whether there were flaws in the SEB environment, and if cheating was possible, not determining how well the unintended cheating functionality could be used to achieve a better result on an exam.

# Chapter 5

## Marketplaces and Devices

The content of Chapter contains information about the devices that are available for cheating. This includes the intended usage, as well as their features and possibilities, along with information regarding websites that sell them.

### 5.1 Usage

The idea for the devices was to cheat on an exam where the devices would enable an outside person to assist the student taking the exam. This could be done using a combination of items that provided one way or two way communication.

#### 5.1.1 Communication Possibilities

The first feature that was evaluated for the devices that was selected was whether they provided one way, or two way communication.

By one way communication it is meant that one person or device, can transmit an image/audio/text to another device, but not the other way around, e.g, device with one earbud and one microphone, can transmit from the microphone to the earbud, but the person using the earbud has no way giving feedback or transmitting their own messages.

Two way communication implies that both parties involved can both send and receive messages, e.g., a phone call.

Two way communication makes cheating easier as the student taking the exam can give feedback on the audio, or send an image of the exam tasks etc. It is still possible to cheat using only one way communication though this requires that the person assisting knows the tasks for the exam.

Cheating with no communication is also an option but this was not evaluated in this research due to two main reasons. The first reason is that bringing illegal material e.g., cheat sheets for instance using a calculator with storage memory, does not guaranty a good grade. Even though you bring all necessary materials to find the solutions to the tasks it may require to much time, and looking through every cheat sheet to find the right question and answer may not be possible. The other reason is that it requires to much effort. The person cheating would have to find all necessary material, learn how to find it, and how to apply it.

Since two way communication was evaluated to provide the best cheating results with minimum effort the preferred devices was a combination of that allowed the student taking the exam to send an image of the tasks and receive audio communication to get the results from the person assisting.

### **5.1.2 Ease of use**

The second most important feature was high usability, or ease of use. One of the main reasons for cheating on exams could be that students believe they would spend less time finding out how to cheat, than actually learning the necessary theory for the exam. This means that devices require

## **5.2 General eCommerce Vendors**

With the growth of internet purchasing something online has never been easier, and in fact more than 10 of the worlds 30 largest internet companies are eCommerce companies like Amazon, Rakuten, eBay, Alibaba etc. [42] Many of these companies provide online marketplaces that enables business-to-consumer (B2C), person-to-person (P2P) and business-to-business (B2B) sales and transactions.

### **5.2.1 eBay**

One of the most popular eCommerce sites available is eBay, with its revenue close to 9 billion USD. According to eBay they have more than one billion products available on their marketplace along with 170 million active buyers [43]. This allows for a large variety of available items. Their rules and restrictions regarding what items can be sold on eBay includes firearms, alcohol, blood etc., but there are no restrictions on items used to cheat on exams. This leads to a great variety of items aimed at students struggling with their academic tests.

### 5.2.2 dealExtreme

There are multiple eCommerce companies that provide websites where electronics are cheap and available. dealExtreme is a "small" company, on a global scale, but its website still provides a wide variety of cheap electronics available for purchase.

## 5.3 Vendors specializing on devices for cheating

There are also multiple vendors that specialize in selling gadgets and electronic devices for cheating at their websites.

### 5.3.1 Monorean

monorean.com mainly provides earpieces and some cameras. Their front page has the marketing slogan:

*"Cheat on tests with absolute discretion! The best wireless and invisible earpiece for cheating on tests: wireless communication without being caught. Finally, your nerdy classmates can tell you all the answers!"*

on their frontpage [44]. Their equipment seems serious as they provide lots of information regarding compatibility, how to use it, as well as warranties. Their devices are however very expensive with a price range from 350\$ - 550\$ USD.

### 5.3.2 Unseeyn

Unseeyn.us provides bluetooth earpieces, mp3 audio recorders, and hidden cameras intended for students having problems studying and trying to cheat on exams [45].

*"Having problems with study? No problem, we have a solution for you!"*

Their equipment is also fairly expensive as their bluetooth earpiece package is priced at 99\$, their mp3 player with bluetooth earpiece costs 89\$ and the hidden camera set costs 699\$.

### 5.3.3 Gsm-earpiece

Gsm-earpiece.com provides a variety of devices for passing exams without preparation [46]. Similarly to the other websites they sell a range of items including bluetooth earpieces and

cameras disguised as pens, watches and glasses etc. Their prices vary from approximately 180 \$ for mp3 bluetooth earpiece and 350\$ for a hidden camera set including bluetooth earpiece and camera with gsm 3G transmission.

## 5.4 Purchased devices

In this section the devices that was ordered online are presented along with their features, specifications, and images.

Due to students economical restrictions along with the financial limitations in this research most devices where purchased from eBay. Most of the items provided by the specialized vendors, where also available separately on eBay at cheaper prices. The devices that where selected along with their specifications and features are provided below.

### 5.4.1 List of purchased items

- Mini Spy Camera Pens USB 2.0 Hidden DVR Camcorder Video Recorder Full HD 1080P
- 960P 1.3MP Wi-Fi Ceiling Fan Hidden IP Camera, EU Plug - Golden + Black
- WCDMA 3G SIM GSM Button Spy Camera Hidden DVR Instant Video transmit Smart-phone
- Glasses Bluetooth Earpiece Spy Hidden Wireless Invisible Mini Covert Exam Test
- Mini 720P WIFI HD Spy DVR Hidden IP Camera Pen Wireless Videorecorder Cheat Exam
- Spy Earpiece Bluetooth Loop Invisible Micro Earphone Mini Wireless Covert Hidden

### 5.4.2 Camera Pen

The first item was a camera disguised as a ball point pen able to record video and take pictures.

<b>Item</b>	Spy Pen
<b>Price</b>	100 NOK
<b>Marketed as</b>	Mini Spy Camera Pens USB 2.0 Hidden DVR Camcorder Video Recorder Full HD 1080P
<b>Ordered from</b>	eBay
<b>Est. shipping time</b>	2 weeks
<b>Requirements</b>	Compatible smartphone, SD card, USB compatible device (e.g. laptop) to view recordings



((a)) label 1



((b)) label 2

Figure 5.1: Images from product page

This pen provides the user the opportunity to store images and video recordings on an SD card inside the pen. It does however, not provide any way to remotely access the recordings, e.g., online, which means that whoever wants to see the recordings needs to be in physical possession of the SD card with the footage.

### 5.4.3 Camera Pen with Wifi transmission

The second item was a camera that looks like a pen, that can record video and audio and transmit through wifi.

<b>Item</b>	Spy Pen
<b>Price</b>	400 NOK
<b>Marketed as</b>	Mini Spy Camera Pens USB 2.0 Hidden DVR Camcorder Video Recorder Full HD 1080P
<b>Ordered from</b>	eBay
<b>Est. shipping time</b>	2 weeks
<b>Requirements</b>	Compatible smartphone, app, wifi



Figure 5.2: Images from product page

Using a compatible smartphone the pen provides two ways of accessing the footage. The pen can broadcast its own wifi network which a user can connect to, and by using a designed mobile application the footage can be viewed both realtime, and as recordings. The second option of viewing the footage is by connecting the pen to another wifi network using the application on the phone. Then, after the pen has been connected, a user with a mobile phone connected to the same network can get access to the footage from the application. This also allows the user to view footage both realtime and as recordings.

#### 5.4.4 Suit button Camera

This item was a camera with 3G/wifi transmission disguised as a suit button.

<b>Item</b>	Suit button camera
<b>Price</b>	1400 NOK
<b>Marketed as</b>	Mini Spy Camera Pens USB 2.0 Hidden DVR Camcorder Video Recorder Full HD 1080P
<b>Ordered from</b>	eBay
<b>Est. shipping time</b>	4 weeks
<b>Requirements</b>	Compatible Mobile phone, 3G/GSM signal reception, USim-card, compatible mobile carrier

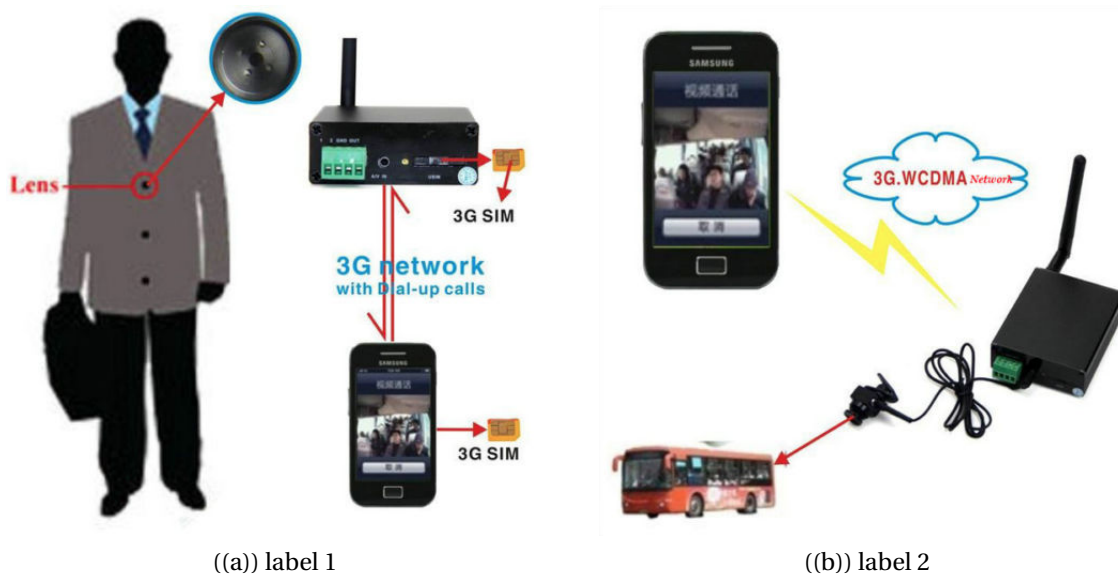


Figure 5.3: Images from product page

The suit button camera was one of the most promising devices, as it is properly hidden, and the GSM/3G connectivity provides a great range, compared to bluetooth. The downside with this item was that there was only one english manual, which was hard to understand, along with multiple requirements like the Usim card, and nessecary features that must be provided by your mobile carrier.

#### 5.4.5 Bluetooth Earpiece with Neck-loop

This item was a very small bluetooth earpiece that can be connected to a phone through a bluetooth signal with a neckloop for the transmitter and receiver. This allows you to receive audio messages undetected.



<b>Item</b>	Bluetooth earpiece
<b>Price</b>	600 NOK
<b>Marketed as</b>	Spy Earpiece Bluetooth Loop Invisible Micro Earphone Mini Wireless Covert Hidden.
<b>Ordered from</b>	eBay
<b>Est. shipping time</b>	2 weeks
<b>Requirements</b>	Mobile phone with bluetooth



((a)) label 1



((b)) label 2

Figure 5.4: Images from product page

#### 5.4.6 Bluetooth Earpiece with Glasses

Thus device has a similar earpiece to the previous one, but instead of receiving and transmitting the signal from a neck-loop, it uses electronics hidden in a pair of glasses.

<b>Item</b>	Spy Glasses
<b>Price</b>	100 NOK
<b>Marketed as</b>	Glasses Bluetooth Earpiece Spy Hidden Wireless Invisible Mini Covert Exam Test
<b>Ordered from</b>	eBay
<b>Est. shipping time</b>	3 weeks
<b>Requirements</b>	Mobile phone with bluetooth



((a)) label1



((b)) label 2

Figure 5.5: Images from product page

### 5.4.7 Wifi Camera

This item was a small wifi/Ip camera that could be hidden or placed in the area of the exam, and would provide video recording which is remotely accessible online.

<b>Item</b>	wifi camera
<b>Price</b>	700 NOK
<b>Marketed as</b>	960P 1.3MP Wi-Fi Ceiling Fan Hidden IP Camera, EU Plug - Golden + Black
<b>Ordered from</b>	eBay
<b>Est. shipping time</b>	2 weeks
<b>Requirements</b>	wifi, Internet connection



((a)) label1



((b)) label 2

Figure 5.6: Images from product page

After approximately 2-3 weeks of waiting, instead of the item arriving we received a message that the order had been cancelled and that the item was out of stock. This was somewhat unfortunate, as it is difficult to evaluate the quality of the product, but some conclusions can be drawn from the process nonetheless. The main takeaway is that some of these vendors are highly unpredictable. This instance shows that purchasing devices online comes with little or no guarantees regarding delivery time, quality, or getting your money back in case of unexpected incidents.

# Chapter 6

## Results

This chapter contains the main results, and findings from the experiments.

### 6.1 Device Usage Results

The camera pen worked quite well. The assistant was able to see all the questions, but the camera needed to be within 10 cm of the questions to read them easily. The closer and more thorough the questions for the exams were recorded on video, the more the chance of getting caught increases. When the distance between the assistant and the student was close to the limit, the video had a lot of stuttering and was not able to properly focus. The video needed to focus on the same questions for 10-15 seconds at the time for the camera to focus and stream in high definition quality to the mobile application. Fortunately seeing the answers was not very problematic, and the assistant could give audio messages to the student, informing which tasks they were not able to see properly.

The earbud with neck-loop worked quite well. The signal strength was good enough to keep the earpiece in either ear. The main issue with both earpieces were sound quality and volume. Although the volume was set to max, the sound was often too low for the student to hear properly. This led to some of the answers not being heard.

The microphone on the glasses was also of varying quality. It worked well enough to use it to communicate if an answer was heard, but not good enough to transmit normal voice speech.

## 6.2 Exam Results

On the first attempt, without repeating any answers, the student with the glasses were only able to get 7 correct answers out of 30. This was with the person assisting only saying the task, and the correct following answer. Once the person providing the answers repeated the answers two or three times, the correct answers was properly understood on approximately 50% of the answers, and after three rounds of providing answers all correct answers were recorded.

The person with glasses and neck-loop achieved better sound quality, but the volume was still low. The answers were heard and written down correctly on more than 66% on the first attempt, and by using the camera feed to show the questions they did not get correctly, the rest of the answers were provided and written down fairly quick.

In both of the types of cheating the exams were completed correctly in less than 90 minutes. Since exams at NTNU usually lasts at least 3 hours, with 4 hours being most common, this indicates that it should be more than sufficient time to communicate all answers. [10]

The table below shows the number of correct answers and time spent on each attempt for each student, with their respective combination of devices. C1 represents the Glasses with microphone and earbud, in combination with mobile phone, while C2 represents Earbud with neck-loop, and camera pen with mobile phone, as presented in 3.2.5.

Table 6.1: Exam Cheating Results

Attempt	Student 1, Glasses		Student 2, Glasses		Student 1, Pen		Student 2, Pen	
1	<b>Time spent:</b>	<b>Score:</b>	<b>Time spent:</b>	<b>Score:</b>	<b>Time spent:</b>	<b>Score::</b>	<b>Time spent:</b>	<b>Score:</b>
	0h 50m	7/30	1h 0m	11/30	1h 30m	30/30	1h 0m	30/30
2	<b>Time spent:</b>	<b>Score::</b>	<b>Time spent:</b>	<b>Score::</b>	<b>Time spent:</b>	<b>Score::</b>	<b>Time spent:</b>	<b>Score:</b>
	2h 42m	30/30	2h 10m	30/30	1h 10m	30/30	0h 50m	30/30

As seen in 6.1, the students using the combination of devices involving the glasses where mostly slower, and with less correct answers. This was mostly because the sound quality was worse, and that lower volume, compared to the earbud connected to the neckloop. This mean that the answers had to be repeated more times, for the student with glasses to comprehend what was being said.

## 6.3 Detecting Cheating

In this section the detection of cheating in the experiment is presented.

### 6.3.1 Providing Answers to Assistant

None of the participants who played the role as examiner did not catch the students sending images from mobile on the toilet or using the camera pen.

In addition, as mentioned in 2.3.8 the answers could easily be provided by another student signed up for the exam and leaving early. As Sindre et al. mentions in the comparison of Paper vs Digital cheating, NTNU has no rules or restrictions regarding students bringing the exam tasks with them when they leave [18]. However, students are not allowed to leave earlier than after 1 hour, which means the time to cheat and complete the answers would be shorter.

Regarding the glasses with microphone and audio earpiece, the examiners stated afterwards that they suspected something "fishy" was going on, because they had prior knowledge that the student wearing them, does not wear glasses regularly. They did not find out exactly what it was with the glasses, so they did not stop the student from wearing them.

### 6.3.2 Receiving Answers from Assistant

When receiving the answers, the earpiece belonging to the glasses where detected on both exams they where used. As mentioned in 6.3.1 the examiners where already aware of something suspicious going on related to the glasses, which can have helped them notice the earpieces.

The earpiece with the neckloop was not detected on any instances.

## 6.4 Threats on Validity

The theory explained in 3.2.1 suggests that same group, pre test, post test, and evaluate results is a decent approach. The same students were given the chance to solve an exam without preparation and assistance, and were later after receiving assistance on a later attempt given another chance. If the results when cheating were a great improvement on the previous results it is a fair assumption that the assistance lead to the improved results. By letting multiple students attempt the cheating process repetition is achieved, which increases the statistical significance.

as mentioned in 3.2.1, it is important to evaluate *internal validity* as well as *external validity*.

### 6.4.1 Internal Validity

The first factor mentioned in 3.2.1 is *history*. This did most likely not have any negative impact in this particular experiment. Neither of the participants had any specific events or occurrences that might affect how they performed in the experiment. Furthermore, the experiment took place in one day, which meant both history factor, as well as the *maturity*, did not have negative impacts. If the experiment was done over several days, or with some weeks in between the parts of the experiment it might have been relevant. In this case, the history and maturity can be considered insignificant.

One of the major threats on the validity is *Faulty Instruments*. As mentioned in 6.2, the sound from the earpieces was very low, and sometimes with stuttering. This could be due to low battery, or perhaps interference between a variety of wireless signals present. If multiple instances of each device were purchased a more thorough opinion could be made regarding the quality of the device. In this case it is hard to determine whether the quality of the device was just because of faults with a particular device, or if the type of device was of poor quality in general. There are also multiple potential problems that did not occur in the experiments, but might happen in a real scenario. For instance neither participants involved with earpiece phone calls, received a call from another person while the call was going on. What would happen in that case is not certain, but could cause problems for the students who are cheating.

Another factor of the internal validity is *reaction to the experiment setting*. As mentioned in 6.3.1 the participants noticed that the glasses looked weird, and that the student wearing them does not normally wear glasses. This might have been noticed due to being in an experiment setting, and might not have been noticed in a real world scenario.

The participants who cheated also knew that it was an experiment, which led them to behave in a very controlled and calm manner. If it was not an experiment, students might be stressed or show unusual behaviour because they are cheating, which might make the cheating more likely to be detected. Behaviour and reactions to stress etc. is however highly individual, and varies a lot from person to person, so no definite conclusions can be drawn.

In conclusion there were no major threats on the internal validity. This means that the correct results on the exams were highly likely to be only a result of the cheating techniques that were used.

### 6.4.2 External Validity

Regarding the external validity, and whether these results can be generalized to apply for all exams scenarios, different subjects, different students etc, is more questionable.

Of the threats to external validity is *specific participants*. All the students who participated in the experiments were computer science students. These could imply that they are more likely than other students to be familiar with new technology, and faster learners regarding electronics and the devices that were used. Even though they could be faster learners, they were not familiar with any of the devices before the experiment, and since they had no prior experience with such devices the participants were deemed acceptable.

Another threat is *too few, and limited participants and experiments*. To increase the statistical significance, and make it more likely to apply in different varied scenarios, it would be ideal to have a lot more participants, and different varied tests. There is a large uncertainty, regarding how well these cheating techniques would work in a different environment, for instance regarding the range of the wireless transmission.

In conclusion, the test environment was evaluated to be fairly similar, especially regarding sound and sound, but since exam scenarios are so varied it is not possible to say that because the cheating process worked well in this scenario, it is guaranteed to work well in every scenario.



# Chapter 7

## Discussion, Conclusion and Recommendations for Further Work

This final chapter summarizes the conducted work in this thesis and the results that have been achieved. The chapter also contains a discussion of the findings, and recommendations for further work.

### 7.1 Discussion

The goal of this research, as stated in Section 1.2 was to investigate electronic devices that can possibly be used by students to cheat on academic exams. In addition, the objective was split into three research questions. These research questions will in turn be addressed.

#### 7.1.1 RQ1: What devices are available?

As shown in Section 5.3 there are numerous vendors providing a huge variety of devices for cheating on exams. The most common alternatives are combinations that provides two way communication, allowing an ignorant and unknowledgeable student to transmit questions to an assistant, and receive answers without being detected. These combinations often feature some form of hidden camera device in combination with audio devices, like small ear-pieces.

The reason that this is the most common combination could be due to its difference from a cheat sheet or other aids. Using these combinations of devices could lead to a student with zero knowledge about a subject receiving a good grade. Other aids often require more effort and knowledge from the student taking the exam. These devices are small, difficult to recognize, and easy to use – making them ideal for cheating on specific types of exams.

Another reason could be that these electronic devices has become very cheap to produce over the years, meaning that vendors providing specialized “cheating device packages” could make huge profits. The devices that where sold separately, for instance on eBay, were relatively cheap. The same type of devices, sold in packages from specialized vendors were more than four times as expensive, which would imply that their profits are substantial.

Additionally, several of these devices are required to be used in combination with a smartphone. Based on the results from a survey by Kantar TNS, MedieNorge presents numbers indicating that more than 80% of the Norwegian population has a smartphone [47]. The use of devices in combination with smartphones increases the possible features and usages. The smartphone can be used through mobile applications and can provide features such as cameras, voice calls, and wireless communication.

### 7.1.2 RQ2: Is it a viable option to cheat using these types of devices?

Attempts to cheat on an academic exam were conducted in the experiments, and the conclusion was that it is certainly possible to cheat on exams with the tested devices. It was at the very least practically feasible. Cheating on multiple choice exams and math exams was easier than general essay-writing exams. On such exams it is definitely possible to pass, or even get a good grade even though the student has little knowledge about the exam subject.

The use of such devices does of course come with a risk of being caught, financial requirement to purchase the devices, and some effort to practice using them. Whether it is more convenient to study for an exam or purchase electronic devices to cheat, will first of all vary depending on how you define “convenient”, but nonetheless it will vary from individual to individual.

#### Determining viability

Although it can be concluded that it is practically feasible to cheat using these types of devices on specific types of exams, there is still a question of whether it is a viable solution. The word *viable* can for instance be interpreted to whether the cheating has an expected upside or value gain.

This can be explained by evaluating the cheating based on a formula to simply visualize the upside of cheating.

$$A \cdot p - B \cdot q > C \quad (7.1)$$

$A$  represents the value of the expected advantage gained by cheating and  $p$  represents the likelihood of successfully cheating.  $B$  represents the cost in case of getting caught cheat-

ing,  $q$  represents the likelihood of being caught, and  $C$  represents the cost of conducting the cheating process. Although this formula has no scientific basis, it can be used to show a possible way of evaluating whether the cheating is viable. If the left side, is larger than the right side of the equation, the cheating is viable, i.e., if the gain, accounted for risk of being caught, is larger than the cost.

In this case, both values of gain and cost can be partly concrete values like monetary value, time spent, and partly more abstract values. For instance, the student can be under the impression that improved grades is essential in order to get a job, even though this might not be the case. However, in general it is hard to calculate or estimate the monetary value. Determining the financial gain from receiving a better grade, e.g., a B instead of a C on an exam is almost impossible. Only in particular cases, for instance if a student is able to get a passing grade instead of failing a course, which leads to finishing the study program a semester earlier, it can be estimated that the cheating will have a clear monetary upside. In those types of scenarios, where finishing their degree half a year earlier makes them able to start in a job half a year earlier thus bringing concrete monetary value.

### **Rewards of cheating**

Another element of cheating is that the gain or upside can be other things than monetary value. For instance, the gain can be time saved. If the candidate is able to receive the same grade by cheating, as they otherwise could receive by studying more, the gain is that they are able to receive the same grade, through cheating, thus saving time. Furthermore, the gain or upside could also be better grades than they would normally be able to achieve. For some students the cheating could lead to a student performing better on the exam than they otherwise were intellectually capable of, even by spending a huge amount of time and effort on studying for the exam.

For the cheating to bring rewards, both realistically and in the long term, it is essential to have a situation where the grades themselves have a value, apart from the knowledge that a student is required to acquire to receive that grade on an exam. If the only value from receiving a good grade is the fact that this means the student possesses knowledge that it will need in future jobs or courses, a good grade in itself would be useless. In some scenarios this will not be the case, and a grade on its own can be useful. This could for instance be regarding the process of applying for a master's degree after finishing a bachelor's degree, or when applying for a PhD after a master's degree. It could also be in relation to applying for jobs, if the employers have an emphasis on good grades when selecting candidates, and the actual knowledge is not tested beyond the candidates abilities. Additionally some students might put a higher value on grades than they should, which means that the assumed value of cheating might be higher than the actual value.

### **Comparison with non-technology alternatives**

Another questions that needs to be answered in order to determine whether cheating using technology and electronic devices is a viable option for students, is whether it is more effective (higher potential and/or lower risk of getting caught) compared to other ways of cheating. One of the challenges related to answering this question is that this research was not comparative, and there was not made any comparisons between this type of cheating, related to other ways of cheating.

It is still possible to discuss this based on the results from the experiments combined with common sense. Throughout this thesis, the cheating process has been split into two parts. Sending the exam questions out to the assistant, and the assistant providing the answers to the student. Both of these parts can be done multiple ways both with and without the use of technological equipment.

As mentioned in the risk assessment in Section 2.3.8, one of the most effective and risk free ways of sending out answers, is by bringing the answers from a person leaving early from the exam. Since the only rule NTNU has on bringing the exam questions out is that the candidates can not leave the venue until one hour of has passed. This means that the only downside to this method of cheating is that the questions are not provided until one hour of the exam has passed. There is no risk of being caught, since the process of signing up for an exam, then leaving early with the questions is not illegal in itself. The person leaving early could be an accomplice with no intention of actually attempting to answer questions on the exam, or another student who is actually able to finish all the questions early. This way of sending out answers, compared to an electronic device approach e.g., camera pen, would have less risk of getting caught, higher chance of success, as the pen might not work and requires less work. There is however, no guarantee that using a spy pen would lead to every question being sent out before one hour has passed, but the possibility is definitely there.

Furthermore, when discussing the viability, it is important to consider the factors that affect the chance of getting caught. One of the first factors is the degree that the act of cheating itself is visible or noticeable. The more visible the action is, the more likely it is to be detected. The combination of sending out questions using camera pen, and receiving questions using earpiece has almost no visible actions. The questions are sent by pointing the camera pen towards the exam paper, which is a very insignificant movement from the student. The act of receiving audio was evaluated based on the experiment to be completely unnoticeable, as the student was not required to do anything in particular, except to listen carefully. Additionally, the audio was very low, and not possible to hear, even for nearby invigilators, unless they are well within touching distance. This is also very unlikely since the current instructions to invigilators state that are should sit quietly unless when they are performing specific tasks,

like handing out paper to students, or on toilet visits. Comparing with non-technological alternatives, for instance cheating by verbally communicating, or using code signals to get answers from other students is far more visible.

Another factor is whether the equipment tested was likely to be seen, and if invigilators will detect them. This factor is one of the main advantages of the small electronic devices. The hidden earbuds, were very small, hence the name “hidden”. The earbuds were evaluated to be highly difficult to spot, especially if the invigilators are not explicitly looking for it. The camera pen, looked like a normal pen, and even though if it were to be seen, invigilators would not be very likely to separate it from a normal pen. Compared to sending photos using a smartphone this is quite advantageous, as a mobile phone is easier to detect, due to its size and the fact that smartphones are among the unpermitted aids that students are explicitly told they are not allowed to use during the exam. Compared to receiving answers written on paper, for instance from the toilet, they are fairly similar on this factor. Paper is somewhat more likely to be seen by an invigilator than a camera pen, but likewise it is not necessarily evaluated to be illegal. Especially on paper-based written exams, it is completely natural that students have multiple sheets of paper with drafts and answers. In contrast, if a student is cheating by bringing answers from a book that is not allowed on the exam, they are more likely to get caught. They could either get caught since the action of looking through the book is noticeable, or by being in possession of illicit materials, as it could be difficult to hide a book from invigilators.

A third factor affecting the chances of getting caught is the extent that the action or device used to cheat is “out of place”, i.e., to what extent the action is not within what is considered normal behaviour or equipment in an examination scenario. An action or a piece of equipment does not need to look suspicious or gain attention if it is within normal behaviour during exams. For instance, using a pen to take photos of the exam tasks could seem perfectly normal on a paper based written exam. However, if a student continuously keeps pointing the pen at the computer screen on a digital exam, it might be more suspicious. Additionally, continuous communication is easier with electronic devices. For instance, if it is necessary with multiple rounds of communication between student and assistant, it could be suspicious with several trips to the bathroom within a few hours. Receiving messages through an earbud does not attract any more attention depending on the time spent and messages received. Using code signals or other ways to communicate answers, particularly on multiple choice might still be possible to do without doing anything out of place. Using sign language or other signals could be easy to detect, but scratching the back of the head or tapping a pencil are actions that students could very well be doing in an exam situation. That way the most limiting factor is not whether the code signal alternative is out of place, but whether it is sufficient to be able to actually understand the correct answers based on those signals.

### 7.1.3 RQ3: What countermeasures can be taken to make cheating less viable to students?

There are several countermeasures that could be implemented to lower the chance of students attempting to cheat, and decreasing the chance students cheating successfully. Unfortunately some rules are very hard to enforce, and some countermeasures could lead to privacy issues, or be too demanding of resources.

There are many different types of countermeasures that could be implemented, on different levels. Such types include technical countermeasures, organizational countermeasures and examination structural countermeasures, which will be further explained.

#### Technical Countermeasures

Possible technical countermeasures that could be implemented include surveillance of wireless communication, or attempting to jam wireless communication in the venue. Both of these could however have legal challenges, and potentially be illegal. Another technical countermeasure could be that every exam candidate has to walk through scanners, similarly to airport security checks. Unfortunately this would be quite expensive, and possibly feel like an invasion of privacy for students, where every student, also the innocent students would feel they were placed under suspicion. There also exists equipment that can detect hidden cameras, typically by scanning for reflections from the lenses, but equipment like this would be expensive, and might still not be able to detect these small spy pen cameras, because they would mostly face down towards the exam papers. These types of devices are only able to detect cameras if they are facing the correct angle [48]. This means that this type of equipment might actually just provide a false sense of security.

A potential technical countermeasure for digital exams could be to require that the candidates, as part of the exam infrastructure wears a headset with a microphone. Then, some tasks would ideally be given through audio, and some are provided by text, and some answers are supposed to be written down, and some given orally. This would vastly increase the burden of communicating tasks to an assistant. If the headset had two-way communication, and allowed the exam system to “hear” what the students hear, the possibility of cheating by using a hidden earbud would be almost completely eliminated. In essence, one of the main issues is that surveilling a large number of students taking an exam, manually, the way it is currently being done is incredibly difficult and ineffective. It requires a huge number of invigilators. The way it is currently being done, it is very limited how much the invigilators can focus on trying to detect attempts of cheating, as they have a wide number of equally important tasks, like providing paper to students, accompanying them on toilet breaks, checking identification when handing out the exam. The amount of time and focus they can spend on

detecting cheating becomes very limited, which means that the only types of cheating that are detected are the ones that are quite easy to detect, but cheating attempts that are carried out discretely is very likely to go unnoticed. On the other hand automatic surveillance, either using two-way communication headsets could be able to prevent cheating attempts using hidden microphones and earbuds.

Again, it could also be discussed whether this countermeasure makes candidates feel like they were unrightfully placed under suspicion. At the same time, exams are in general already a situation where all students will be placed under some sort of monitoring, e.g., by invigilators, which means that students might not find it any differently to be monitored by technology. It is also worth mentioning that most students perhaps should be positive towards all countermeasures to cheating. After all, the honest students are perhaps the biggest victims of cheating. The university does not have a lot of negative impact from students cheating, unless it leads to negative publicity once it is discovered that students are successfully cheating. The honest students, are in one way the most important victims of cheating. The honest students receive an unfair competitive disadvantage, and could receive a worse grade than they should, if exams are graded based on a normal distribution, and other students are cheating to receive better grades. This means that most students might actually be positive towards any type of countermeasure, unless they feel the countermeasure is an invasion of privacy, embarrassing, degrading, disturbing during the exam, or causes other similar problems.

### **Organizational Countermeasures**

The second category of countermeasures is organizational countermeasures. Potential actions within this category includes improved or changed instructions to the invigilators. This could for instance include that invigilators are intended to specifically look for hidden earpieces or earbuds. If this was implemented it would be very likely to increase the chance of someone cheating using earbuds being caught. The associated difficulty would be that this is almost impossible unless students are required to show their ears during the exams. The students could easily hide the earbuds by having long hair, wearing a hat or religious head wear like hijab. This could especially lead to controversies regarding religious head wear, where being forced to take it off could be considered as a violation of their right to choose and practice their own religion. Similarly, simple changes of instructions could also decrease the chance of students cheating through toilet visits successfully. By establishing a more thorough control sequence regarding toilet breaks, this type of cheating could possibly be prevented. Obviously, monitoring students during toilet breaks would be problematic regarding privacy, but making sure students do not bring illicit items in or out could be possible. If the invigilators were to be instructed to manually search, or at least look for mobile phones,

cheat sheets, or exam tasks when accompanying students on bathroom break a lot of cheating could be avoided. It could also be possible with clear instructions that candidates have to sit with their booth door open, would make it virtually impossible for the student cheat on the toilet, for instance by using their mobile phone, without the invigilator noticing. As mentioned in the survey conducted as the specialization project during the fall semester, some students at NTNU believe cheating during bathroom breaks, for instance searching for answers on Google with their smartphone in a booth, is a completely risk free and easy way to cheat [9]. Enforcing some sort of check before and after toilet visits, could be beneficial in two ways. Firstly, students could be more afraid of being caught, which might lead to less students attempting it. Secondly, it could actually lead to students that attempt to cheat this way get caught.

Moreover, a single invigilator could be assigned specifically to each bathroom. This invigilator could monitor the toilet booths between each student visit and make sure students do not hide or keep illicit material in the toilet booths. With regards to reducing the risk of students exchanging information with outsiders via the toilets, it would also be beneficial if the toilets were close to everyone except students taking the exam. This could also be enforced by the invigilator assigned to the bathroom. In practice, this might be difficult, especially if the venues is used by other people at the same time as the examination. Unless the venue has a very large capacity of toilets, restricting the toilets to students only might not be possible.

Another possible countermeasure is to require handing in mobile phones in prior to the exam. Unfortunately this would only stop the most lackluster cheaters, as bringing an additional phone is a quite simple solution from the cheaters point of view. Furthermore it could bring a lot of logistic issues regarding where to store each mobile phone, and who it belongs to. It could lead to theft or other problems, and if there are honest students who did not bring their phone they would need to be searched, or provide some sort of proof. This shows that a possible mitigation could actually cause a lot of issues.

### **Exam Design and Structure Countermeasures**

Regarding how the exam is structured and designed, most types of cheating are simplest to perform when all students are given exactly the same exam, with the same questions in the same order. This means that a candidate would not be required to send out their own individual questions, but that the assistant receives the questions from a student leaving after one hour would be sufficient. If the exam contains different questions for each student, or there are multiple versions of the exam that are distributed randomly to the students taking the exam, the student would be required to send out their own specific exam questions. This would also be troublesome for a person assisting multiple students simultaneously.



Especially on multiple choice exams it would make a huge difference if students were given scrambled questions and answers, compared to identical questions and answers. If the exam contains identical questions in the same order for every student, communicating the correct answers to multiple students would be a fairly simple task. If this was the case on a multiple choice exam with 50 questions, the answers could be communicated through a series of letter and number combinations, e.g., “1a” or “2c”, indicating that alternative a, and c is the correct on answers on question one and two. These type of answers could easily fit on a single sms text message, a post it note, or be read to the student through hidden microphone and earbud. If the exam were structured with scrambled order of questions and corresponding answer alternatives, this would no longer work. Then the assistant would be required to communicate unique keywords for each answer. Moreover, if each student was not given the same questions, but received a number of questions, randomly selected from a large base of questions, each students receiving assistance would need to send out their own questions. One set of exam questions would no longer be sufficient for the assistant, as each student would most likely, at least have some questions that were different.

In general, a potential countermeasures to reduce the possibility of cheating includes increasing the amount or frequency of communication that is required between students and assistants. To exemplify this: consider a student and an assistant intending to cheat using a mobile phone. If the entire set of questions is handed out at the beginning of the exam, a student could send a photo of the tasks, and the assistant could solve the questions, and send the answers. On the other hand, if the exam was structured to only provided one task at the time, and when the student has solved the first task, they receive the second task, it would be more troublesome. Then, the student and assistant would be required to communicate between every single task. This would highly increase the chance of getting caught, since the cheating act would have to be repeated multiple times.

## 7.2 Summary and Conclusions

In conclusion, there are several technology and electronic devices available online that can be used to cheat on academic exams. Many websites actually have students with intentions to cheat on exams as their main target group, but some vendors provides the equipment without solely focusing on devices for cheating. After a comprehensive analysis of available devices and vendors, the relatively cheap devices were selected for purchase to be used in experiments. The established overview of available devices and vendors can be used to increase awareness and knowledge for the organizers of exams. Through experiments it was found that the functionality of the devices were of surprisingly high quality. In experiments with a multiple choice exam and purchased cheating devices, the participants felt quite certain that they could successfully be able to cheat and receive a good grade on such an exam.

Whether they would get caught or not is uncertain, because of all the varying factors in exams. However, the electronic devices that were used were small, and are in general quite difficult to spot. In fact, most of the electronic cheating devices are at least equally difficult to detect, compared to non technology cheating alternatives, but will in some cases provide extended and better functionality and more possibilities. There are multiple countermeasures that can be implemented in order to mitigate this type of cheating, but unfortunately some of the most effective alternatives could lead to privacy issues, or be very demanding of resources. This research indicates that students can cheat in new ways, and presents possible countermeasures the university could evaluate. By being made aware of these new types of cheating the professors making exams, and invigilators overseeing them are more prepared to handle attempts of cheating. Considering that this is an under-researched field of study, more efforts should be made to investigate other technological devices for cheating and how universities can develop countermeasures to avoid cheating.

## **7.3 Recommendations for Further Work**

### **7.3.1 Test on Real Exams**

One of the most interesting parts of the further work that could be done is trying to cheat on real exams. For this research it was not possible due to the limited time, in combination with the difficulty of getting a permit to cheat without repercussions on official exams. Being able to try this would give answers with very high credibility and almost be able to determine with complete certainty whether this type of cheating is possible or not, and show if examiners would detect the cheating. This would probably have to be done on exams early in the semester, or by students who work on their master thesis for two semesters.

### **7.3.2 Purchase Devices From Specialized Vendors**

Another part of the further work that would be interesting is looking at the other vendors and the devices they provide. Even though there is no guarantee that the more expensive equipment would have higher quality there is often a correlation between price and quality. In this research the cheapest alternatives, mostly from eBay were selected, although other vendors provide more expensive variations of the same types of devices, as explained in 5.3.

### **7.3.3 Replicate Real Scenarios**

As mentioned in 4.1 students in Sweden were able to cheat on exams. It was not specified exactly how the cheating process was in that case, except that they used specialized earbuds to transmit the answers to the students taking the exams. Figuring out what they used, and testing the equipment they used would also be interesting as there is a strong indication it would work well. In the end, however, they got caught, but whether that was due to the electronic devices and earbuds not being of sufficient quality or due to other factors is uncertain.

### **7.3.4 Retest After a few Years**

Finally, in the long term it would be interesting to do an evaluation again in a couple of years as the different devices are refined and improved, and might make it even easier for students to cheat. If the time frame is too large other changes might be too significant. For instance if every exam becomes digital, the scenario is quite different. Conducting a similar test after three years could yield interesting results, that might also determine if this type of cheating will be more, or less viable as time goes by.

# Bibliography

- [1] Danielle Aker Bjørke. Innfører digital eksamen på ntnu. <https://dusken.no/artikkel/25288/innfrer-digital-eksamen-pa-ntnu/>, 2018. Accessed: 2018-28-3.
- [2] Department of Computer Science NTNU. Exams at ntnu. <https://innsida.ntnu.no/wiki/-/wiki/Norsk/Digital+eksamen>, 2017.
- [3] Hege Larsen. Økning i digitale eksamen. <https://khrono.no/campus/2016/04/stor-okning-digital-eksamen>, April 2016.
- [4] Ina Blau. Computers in human behavior. In *The ethical dissonance in digital and non-digital learning environments: Does technology promotes cheating among middle school students?*, volume 73, Amsterdam, The Netherlands, 2017. Elsevier Science Publishers B. V.
- [5] Gordon Moore. Moore's law. [https://en.wikipedia.org/wiki/Moore%27s\\_law](https://en.wikipedia.org/wiki/Moore%27s_law). Accessed: 2018-02-02.
- [6] smartInsights.com. ecommerce growth statistics. <https://www.smartinsights.com/digital-marketing-strategy/online-retail-sales-growth/>, 2017. Accessed: 2018-28-3.
- [7] Briony J Oates. *Researching Information Systems and Computing*. SAGE Publications, 2005. ISBN 978-1-4129-0224-3.
- [8] NTNU. Eksamensinspektørenes oppgaver. <https://innsida.ntnu.no/wiki/-/wiki/Norsk/Eksamensinpekt%C3%B8renes+oppgaver>, 2018. Accessed: 2018-01-5.
- [9] Matias Fehn Unsvåg. Student attitudes and preconceptions towards cheating on exams. *NTNU Specialization Project*, Fall, 2017. URL . . .
- [10] Atle Skretting. Ntnu tester ut digital eksamen. <https://www.tek.no/artikler/ntnu-tester-ut-digital-eksamen/113122>, September 2012. Accessed: 2017-12-01.
- [11] Universitetsavisa. Eksamen blir lagt til postterminalen. <https://www.universitetsavisa.no/student/2018/03/14/>

- Eksamen-blir-lagt-til-Postterminalen-72905.ece, 2018. Accessed: 2018-10-5.
- [12] NTNU. Special examination arrangements. <https://innsida.ntnu.no/wiki/-/wiki/English/Accommodations+during+exams+for+special+needs+students>, 2018. Accessed: 2018-28-4.
- [13] NTNU. Tilatte hjelpemidler. <https://innsida.ntnu.no/wiki/-/wiki/Norsk/tillatte+hjelpemidler>, Desember 2017. Accessed: 2017-12-01.
- [14] Department of Computer Science NTNU. Cheating examples by ntnu. <https://innsida.ntnu.no/wiki/-/wiki/English/Cheating+on+exams>, 2017.
- [15] Division of Student Affairs. University of california, berkeley. <http://sa.berkeley.edu/conduct/integrity/definition>, 2017. Accessed: 2017-12-01.
- [16] Manar Hosny and Shameem Fatima. Attitude of students towards cheating and plagiarism: University case study. 14, 08 2014.
- [17] Sara Shariffuddin and Richard J. Holmes. Cheating in examinations: A study of academic dishonesty in a malaysian college. 5:99–124, 12 2009.
- [18] Guttorm Sindre and Aparna Vegendla. E-exams versus paper exams: A comparative analysis of cheating-related security threats and countermeasures. 11 2015.
- [19] NTNU. Plagiarism control at ntnu. <https://innsida.ntnu.no/wiki/-/wiki/English/Plagiarism+control+at+NTNU>, 2018. Accessed: 2018-11-5.
- [20] NTNU. Grading scale using percentage points. <https://innsida.ntnu.no/wiki/-/wiki/English/Grading+scale+using+percentage+points>, 2018. Accessed: 2018-10-5.
- [21] K. Krippendorff. *Content Analysis: An Introduction to Its Methodology*. SAGE Publications, 2012. ISBN 9781483307039. URL <https://books.google.no/books?id=mZsgAQAAQBAJ>.
- [22] Wikipedia. Content analysis, wikipedia. [https://en.wikipedia.org/wiki/Content\\_analysis](https://en.wikipedia.org/wiki/Content_analysis), 2018. Accessed: 2018-10-5.
- [23] Techopedia. Web crawler, techopedia. <https://www.techopedia.com/definition/10008/web-crawler>, 2018. Accessed: 2018-10-5.
- [24] <https://www.fotball.no/>. <https://www.fotball.no/>. <https://www.fotball.no/>, 2018. Accessed: 2018-10-5.
- [25] LinkedIn. LinkedIn tos. <https://www.linkedin.com/legal/user-agreement>, 2018. Accessed: 2018-10-5.

- [26] eBay. Electronics ebay. [https://www.ebay.com/sch/Gadgets-Other-Electronics/14948/bn\\_1642007/i.html?\\_fsrp=1](https://www.ebay.com/sch/Gadgets-Other-Electronics/14948/bn_1642007/i.html?_fsrp=1), 2018. Accessed: 2018-16-5.
- [27] P M Wortman. Evaluation research: A methodological perspective. *Annual Review of Psychology*, 34(1):223–260, 1983. doi: 10.1146/annurev.ps.34.020183.001255. URL <https://doi.org/10.1146/annurev.ps.34.020183.001255>.
- [28] LifeWire. Typical range of wifi routers. <https://www.lifewire.com/range-of-typical-wifi-network-816564>, 2018. Accessed: 2018-01-5.
- [29] OneCall. Onecall extra sim-cards. <https://onecall.no/kundeservice/sim-kort/>, 2018. Accessed: 2018-01-5.
- [30] Richard Adams. 40 000 univeristy stundets diciplined for cheating. <https://www.theguardian.com/education/2015/jun/15/cheating-rife-in-uk-education-system-dispatches-investigation-shows>, 2015. Accessed: 2018-13-02.
- [31] Forskerforum. Flere tas i juks på høyskoler og universiteter. <https://www.forskerforum.no/slik-avslorer-de-studentene-som-jukser/>, 2017. Accessed: 2018-28-3.
- [32] Aftenposten. Flere tas i juks på høyskoler og universiteter. <https://www.aftenposten.no/norge/i/dEo11/Flere-tas-i-juks-pa-universiteter-og-hoyskoler>, 2017. Accessed: 2018-28-3.
- [33] Universitetsavisa.no. Svensk politi mener liga tjente ti millioner på eksamensjuks. <http://www.universitetsavisa.no/student/2018/04/17/Svensk-politi-mener-liga-tjente-ti-millioner-p%C3%A5-eksamensjuks-73755.ece>, 2018. Accessed: 2018-20-4.
- [34] Ekobrottsmyndigheten.no. About us, ekobrottsmyndigheten. <https://www.ekobrottsmyndigheten.se/en/about-us/>, 2018. Accessed: 2018-20-4.
- [35] Expressen.se. Liga drog in miljoner på fusk på högskoleprovet. <https://www.expressen.se/nyheter/liga-tog-100-000-kronor-for-fusket-pa-hogskoleprovet/>, 2018. Accessed: 2018-20-4.
- [36] Lisa Z. Bain. How students use technology to cheat and what faculty can do about it. *Information Systems Educational Journal*, 13(5), 2015.
- [37] Sarah Marsh. More university students are cheating using technology. <https://www.theguardian.com/education/2017/apr/10/>

- more-university-students-are-using-tech-to-in-exams, 2017. Accessed: 2018-13-02.
- [38] Ritesh Chugh. Students are using "smart" spy technology to cheat on exams. <https://theconversation.com/students-are-using-smart-spy-technology-to-cheat-in-exams-59241>, 2016. Accessed: 2018-07-02.
- [39] Stephanie Wong, Lillian Yang, Bernhard Riecke, Emily Cramer, and Carman Neustaedter. Assessing the usability of smartwatches for academic cheating during exams. In *Proceedings of the 19th International Conference on Human-Computer Interaction with Mobile Devices and Services*, MobileHCI '17, pages 31:1–31:11, New York, NY, USA, 2017. ACM. ISBN 978-1-4503-5075-4. doi: 10.1145/3098279.3098568. URL <http://doi.acm.org/10.1145/3098279.3098568>.
- [40] Phillip Dawson. Five ways to hack and cheat with bring-your-own-device electronic examinations. *British Journal of Educational Technology*, 47(4):592–600. doi: 10.1111/bjet.12246. URL <https://onlinelibrary.wiley.com/doi/abs/10.1111/bjet.12246>.
- [41] Thea Marie Søgaaard. Mitigation of Cheating Threats in Digital BYOD exams. Master's thesis, NTNU Groningen, Trondheim, Norway, 20016.
- [42] Wikipedia. List of largest internet companies. [https://en.wikipedia.org/wiki/List\\_of\\_largest\\_Internet\\_companies](https://en.wikipedia.org/wiki/List_of_largest_Internet_companies), 2018. Accessed: 2018-13-03.
- [43] eBay INC. Who we are. <https://www.ebayinc.com/our-company/who-we-are/>, 2018. Accessed: 2018-02-02.
- [44] Monorean. Monorean.com. <https://www.monorean.com/en>, 2018. Accessed: 2018-02-02.
- [45] unseeyn. unseeyn.us. <https://www.unseeyn.us/>, 2018. Accessed: 2018-10-3.
- [46] gsm earpiece.com. gsm-earpiece.com. <https://www.gsm-earpiece.com/>, 2018. Accessed: 2018-10-3.
- [47] MedieNorge. Andel som har smarttelefon i norge. <http://www.medienorge.uib.no/statistikk/medium/ikt/379>, 2018. Accessed: 2018-20-5.
- [48] techlicious. The secrets to finding hidden cameras. <https://www.techlicious.com/tip/the-secrets-to-finding-hidden-cameras/>, 2018. Accessed: 2018-01-6.

# **Appendix A**

## **NTNU – Exam Rules**

Exam rules as provided by NTNU on <<https://innsida.ntnu.no/wiki/-/wiki/English/Exam+rules>>

### **A.1 Arrival**

You must arrive at least 15 minutes before the examination starts. At digital examination you must arrive at least 30 minutes before the exam starts. Remember to bring a photo identification (e.g. driver's license, bank card or passport), which you must present before you sign the attendance list.

### **A.2 Calculators and other aids**

Find out which calculator you can use and other aids permitted for examinations.

### **A.3 During the examination**

All bags and personal belongings, including cell phones and other electronic aids which can be used for communication (e.g. smart watches), must be placed at designated places in the examination room. Cell phones must be switched off.

During the examination, any communication between candidates is prohibited, both on and off the premises. You must not leave your seat without the invigilator's permission, and you must follow the invigilator's instructions.



## **A.4 Terminated examination**

You may not terminate the examination during the first hour unless you are ill or for a similar reason. Candidates who terminate the examination must contact the invigilator to sign out before leaving the premises. A terminated examination counts as one examination attempt.

## **A.5 At the end of the examination**

You are responsible for submitting the answer paper to the head invigilator. The sheets of paper for writing your answers have a copy underneath that you tear off and keep. If you do not have enough time to write out a clean copy of your draft, you can submit any draft sheets that you have written. Include these draft sheets in the total number of submitted pages that you note on the cover. All unused paper must be handed in.

You are not allowed to bring paper out of the examination room before you have handed in your answer paper.

# Appendix B

## NTNU – Cheating On Exams

Exam rules as provided by NTNU on <<https://innsida.ntnu.no/wiki/-/wiki/English/Cheating+on+exams>>

### B.1 Examples of cheating

- Providing an answer taken from the Internet that is wholly or partly presented as your own answer.
- Providing an answer that was wholly or partly used by another person from a previous exam.
- Providing an answer that was wholly or partly prepared by another person.
- Providing an answer that was wholly or partly used by the student at a previous exam.
- Submitting practical or artistic work that was created by someone other than the student him- or herself.
- Copying quotes from textbooks or other academic sources, other people's theses, information taken from the Internet or the like which is supplied without stating the source of the information and without clear marking that it is not original work.
- Illegal aids that you take with you to the exam.

### B.2 Cheating on other assignments

Large obligatory assignments or reports that must be approved in order for the student to take the exam also fall under the same rules as for cheating on exams.

It is your responsibility to become familiar with the rules that apply to your work in terms of use of sources and references, as well as what kinds of aids are allowed in examinations or in the production of written or technical work. If you are uncertain about which rules apply, you should contact the responsible individuals in your academic discipline.

### **B.3 Checks for plagiarism**

NTNU has a system that enables documents and exams to be checked for plagiarism. All assignments, exams, theses and reports that are submitted can be checked for plagiarism.

NTNU's Central Appeals Board decides what kinds of sanctions will be levied in the case of plagiarism or cheating.

You can read more about this issue in the guidelines for handling cheating and attempts at cheating on exams at NTNU (pdf, in Norwegian). Cheating on exams can result in you being banned from university and having your examination results annulled.

# Appendix C

## NTNU – Instructions to invigilators

Exam rules as provided by NTNU on <<https://innsida.ntnu.no/wiki/-/wiki/English/Instructions+to+invigilators>>

### C.1 At the start

People who have agreed to be on invigilator duty must attend in person. Report absence in good time to the Student and Academic Division (see the additional list). The chief invigilator must have control over the exam question papers at all times before the start of the examination. Unless otherwise specified, written exams start at 9:00 am. Invigilators must arrive in good time, at least 30 minutes before the exam starts. Each invigilator must immediately report to the chief invigilator, and follow the instructions given. Candidates who report late for an exam must be referred to the Student and Academic Division at the exam location. If the invigilator does not find the candidate in the attendance lists, the chief invigilator must find out whether the candidate is in the wrong room. If the candidate has arrived at the wrong place, the chief invigilator must contact the Student and Academic Division if necessary. The candidate must normally be accompanied by the invigilator to the correct place. If the candidate is not on any of the attendance lists and must thus take the exam with reservations, the candidate must remain seated. The chief invigilator ensures that the form for exams with reservations is completed. The completed form for exams with reservations must be attached to the attendance lists. The candidate can be moved to another room if necessary. The invigilators ensure that the candidates bring only food, writing implements and permitted exam support material to their seats. Bags and personal belongings, including mobile phones and other electronic aids that could be used for communication, must be placed in the designated place at the exam venue. Mobile phones must be switched off. Permitted exam support material, as well as other relevant information, is listed on the cover

of the examination paper. All exam support material, calculators and dictionaries that candidates have brought with them must be inspected. The chief invigilator asks the candidates to present valid identification that includes a photo and their date of birth. If a candidate lacks valid papers, the invigilator informs his or her chief invigilator, who in turn contacts the Student and Academic Division for clarification. The chief invigilator informs the candidates of the time allowed for the exam. Permitted exam support material and the number of hours are listed on the cover of the examination paper.

## **C.2 During the exam**

If candidates have questions that concern the exam paper, these must immediately be reported to the responsible chief invigilator, who will then normally contact the course teacher. If a candidate discovers an error in the exam question paper, the Student and Academic Division must be contacted. The invigilators are responsible for ensuring quiet and order at the exam venue. All unnecessary conversation between the invigilators and everything that disturbs the candidates must be avoided. If any noise disturbance occurs during the exam, this must immediately be reported to the Student and Academic Division. Invigilators are not permitted to use mobile telephones or tablet computers, or to read newspapers, etc. Invigilators must be helpful and provide candidates with what they are entitled to as quickly as possible. An invigilator may only go out with one candidate at a time. The invigilator should not start a conversation with the candidate. It is up to the individual candidate to decide whether he or she would like to talk or prefers quietness and concentration. Any conversation about exam questions and exam subjects must be avoided. Candidates must not under any circumstances communicate with each other or with other external parties. This also applies to toilet visits. It is forbidden to take a candidate to a shop outside the exam premises or a phone/mobile phone. If a candidate wants to smoke, the invigilator must accompany him/her to a separate smoking area, away from entrances, windows, and air intakes. If there is a fire alarm, candidates and invigilators must immediately leave the exam room, and follow further instructions from the Student and Academic Division. Exam papers must not be taken out of the exam room. Give feedback to the Student and Academic Division if situations arise during an exam that could lead to complaints about procedural errors in the exam. These might include unnecessary noise, a cold exam venue, poor ventilation or other factors.

### **C.3 Suspicion of cheating**

If cheating is suspected, it is important that this be handled in a way that does not create unnecessary noise and disturbance at the exam venue. If an invigilator becomes aware or is made aware of activity that might cause suspicion of cheating, this information must be passed on to the chief invigilator. The chief invigilator immediately contacts the Student and Academic Division. The chief invigilator writes a report to the Student and Academic Division about the incident. The report must include the course code and course name, the exam date, the room in which the candidate sat, the time of confiscation, the candidate's name, the candidate number, and the invigilator's name and phone number. The invigilator confiscates exam support material that is not permitted and passes this on to the chief invigilator. The confiscated material is marked with the candidate's name or candidate number, as well as the course code. This is not limited to the use of illegal support material, but also applies if there is suspicion that candidates are communicating with each other or with others. The candidate is given the opportunity to continue with his or her examination paper.

### **C.4 At the end of the exam**

The chief invigilator announces when there is 1 hour left of the exam time and when there are 15 minutes left of the exam time. When the exam time is over, candidates have 15 minutes to prepare for handing in the paper. At this time, all writing on the answer paper must stop, and any violations must be pointed out by the invigilators. If the candidate still carries on writing, this must be reported to the chief invigilator. When a candidate is ready to hand in his or her answer paper, the invigilator must check that all sheets are numbered consecutively, marked with the date and the candidate number as well as the course code. In addition, the invigilator must check that the correct number of sheets and the correct candidate number are marked on the front of the cover. If there is not enough time to write out a clean copy, any rough drafts may be handed in. These draft sheets are then included in the total number of submitted pages noted on the cover. The inspector signs the cover page and ensures that the candidate hands in the answer paper to the chief invigilator. All unused paper must be collected and the answer sheets must be checked for any carbon copies. At the end of the exam, it must be as quiet as possible at the exam venue in consideration for other students. Submitted answer papers must be sorted by course and ascending candidate number, if applicable in relation to exam committee lists. Papers for each course are placed in envelopes labelled with:

- Course Code
- Examination Date

- Room
- Number of answer papers in the envelope
- Applicable candidate numbers
- Responsible invigilator's signature

The applicable candidate numbers can be recorded in two ways: Either only the first and the last candidate number for the answer papers in the envelope, or all the candidate numbers.

# Appendix D

## Questions and Solutions for the Exam Used in the Experiment

### D.1 Exam Spring 2015 TIØ4258 - Technology Management

#### D.1.1 Questions

Oppgaver fra entreprenørskapensumet:

**Oppgave 01:**

Hvilket av disse utsagnene er feil om «product-push»?

- a) Product-push er motstykket til Order-pull
- b) Product-push er normalt teknologidrevet fordi det tar utgangspunkt i nyutviklet teknologi
- c) Product-push tar ikke utgangspunkt i et eksisterende kundebehov
- d) Product-push er en ide om at produktet selger seg selv, vi trenger bare lage det

**Oppgave 02:**

Hva kan VRIO-rammeverket hjelpe deg med?

- a) Å skaffe finansiering til din oppstartsbedrift
- b) Å klargjøre kriterier for valg av organisasjonsstruktur
- c) Å analysere bedriftens ressursmessige forutsetninger for å oppnå konkurransekraft.
- d) Å sette sammen et godt team rundt forretningsideen

**Oppgave 03:**

Hvilket av disse utsagnene er feil om betydningen av verdikjeder for entreprenører?

- a) Verdikjeder sier noe om hvilke verdivalg andre bedrifter har gjort
- b) Verdikjeder gir oss en mulighet til å finne en «plass» i kjeden for vår bedrift
- c) Verdikjeder hjelper oss med å vurdere en fornuftig arbeidsdeling mellom vår bedrift og andre bedrifter
- d) Verdikjeder kan gjøres enda nyttigere ved å legge inn pengestrømmer for å konkretisere modellen

**Oppgave 04:**

Hvilken type oppstartsbedrift har vanligvis størst behov for tilgang på kapital?

- a) «Levebrødsbedrifter»
- b) «Portalbedrifter»
- c) «Vekstbedrifter»
- d) «Hobbybedrifter»

**Oppgave 05:**

Hvilken av utsagnene nedenfor er IKKE karakteristisk for Business Angels?

- a) De er private enkeltpersoner eller grupper
- b) De investerer normalt i bedrifter som interesserer dem
- c) De investerer normalt moderat med penger (100.000-2,5 mill)
- d) De venter normalt til etter at et venturekapitalfond har investert, slik at de vet at ideen er levedyktig.



### Oppgaver fra Organisasjonspensumet:

#### Oppgave 06:

Hvilke kjennetegn er IKKE beskrivende for en lærende organisasjon?

- a) Organisasjonen har en delt forståelse for visjon som en følge av en felles oppfattelse av hva som er viktig for organisasjonen.
- b) Organisasjonen har et samarbeidsorientert men utfordrende miljø som utnytter til fulle kreative spenninger, og som minimerer destruktive spenninger.

Side 3 av 7

- c) Organisasjonen har tydelige retningslinjer som gjør organisasjonen i stand til å identifisere lineære årsaker og virkninger.
- d) Organisasjonen har en systematisk tilnærming til komplekse organisatoriske dynamikker hvor handlinger og reaksjoner er forstått i lys av årsaksløkker.

#### Oppgave 07:

Hva er arbeidsdeling?

- a) Prosessen som etablerer og kontrollerer graden av spesialisering i organisasjonen.
- b) Fordelingen av ansvar og oppgaver mellom ledelse og ansatte
- c) Utfallet av interne klassekamper mellom ledelse og ansatte
- d) Prosessen som fordeler mennesker og ressurser i forhold til deres posisjon i organisasjonens hierarki

#### Oppgave 08:

Hvordan påvirker standardiseringsnivået graden av vertikal differensiering?

- a) Høy grad av standardisering reduserer ledelsens mulige kontrollspenn, noe som igjen sikrer en lavere grad av vertikal differensiering
- b) Høy grad av standardisering gjør det lettere for ledere på høyere nivå i hierarkiet å fungere bedre på grunn av mindre fokus på gjensidig tilpasning, og følgelig er det mulig å ha en større grad av vertikal differensiering
- c) En lav grad av standardisering gjør det lettere for ansatte og ledere som utfører komplekse og usikre oppgaver å basere seg mer på gjensidig tilpasning, og dette reduserer behovet for vertikal differensiering
- d) En lav grad av standardisering gjør det mulig for ledere å kontrollere flere hierarkiske nivå, siden de kan gripe inn og gi tilpassede retningslinjer for hver operasjon eller prosess som er påtatt

#### Oppgave 09:

Hva er fordelene med en matrise-struktur?

- a) Bruken av kryss-funksjonelle team reduserer funksjonelle barrierer og bidrar til å løse utfordringen med overdrevent subenhets-fokus
- b) Plasseringen av ansatte i kryss-funksjonelle team sikrer delt forståelse av individuelle oppgaver, noe som reduserer rolle-usikkerhet
- c) Et klart hierarki reduserer konflikt mellom produkt-team og funksjoner
- d) Produktteamenes selvstyre tillater en minimal intervensjon fra ledelsen

#### Oppgave 10:

Hva er kjernedimensjonene i jobb-karakteristika-modellen?

- a) Ferdighetsvariasjon, oppgave-identitet, oppgave-viktighet, autonomi og tilbakemeldinger
- b) Oppgave-identitet, motivasjon, oppgave-variasjon, utvikling av ferdigheter og tilbakemelding
- c) Motivasjon, tilbakemeldinger, ferdighets-viktighet og oppgave-identitet
- d) Ferdighets-viktighet, autonomi, ferdighets-variasjon, oppgave-viktighet og tilbakemeldinger

**Oppgaver fra økonomipensumet:****Oppgave 11:**

En bedrift har total kostnader gitt ved funksjonen  $TC(Q)$  der  $Q$  er mengden. Hva er da et korrekt uttrykk for marginalkostnaden?

- a)  $Q$
- b)  $dTC/dQ$
- c)  $Q \cdot dTC/dQ$
- d)  $TC(Q)/Q$

**Oppgave 12:**

En bedrift produserer en mengde slik at marginalkostnadene er lik gjennomsnittskostnadene. Hva er da sannsynligvis tilfellet?

- a) Marginalkostnadene er null.
- b) Gjennomsnittskostnadene er minimale.
- c) Variable kostnader er null.
- d) Variable kostnader er minimale.

**Oppgave 13:**

Etterspørselen til en bedrift er gitt ved funksjonen  $P(Q)$  der  $P$  er prisen og  $Q$  er mengden. Hva er da en korrekt tolkning av  $Q \cdot dP/dQ$ ?

- a) Marginalinntekt, dvs. ekstra inntekt ved salg av en ekstra enhet.
- b) Marginalprofitt, dvs. ekstra profitt ved salg av en ekstra enhet.
- c) Inntektstapet som følge av prisreduksjon med sikte på å selge en ekstra enhet.
- d) Økningen i solgt mengde per enhet prisreduksjon.

**Oppgave 14:**

En bedrift har tilpasset seg slik at marginalinntekten er positiv. Hva kan vi da generelt si om etterspørselen i tilpasningspunktet?

- a) Etterspørselen er elastisk.
- b) Etterspørselen er uelastisk.
- c) Etterspørsel elastisiteten er null.
- d) Tallverdien til etterspørsel elastisiteten er én.

**Oppgave 15:**

En bedrift i et frikonkurransemarked har marginalkostnader gitt ved  $MC = 0,2Q + 80$  der  $Q$  er mengden. Den har faste kostnader på 1 000. Dersom prisen i markedet er 120, hva blir optimal profitt for bedriften?

- a) 1 000
- b) 2 000
- c) 3 000
- d) 4 000

**Oppgave 16:**

Etter å ha analysert kostnader og etterspørsel finner ledelsen i et monopol ut at både marginalinntekt og marginalkostnad er positive tall, men marginalinntekten er mindre enn marginalkostnaden. Hva kan bedriften da gjøre for å øke profitten?

- a) Redusere mengden og øke prisen.
- b) Øke mengden og redusere prisen.
- c) Øke både pris og mengde.
- d) Redusere både pris og mengde.

**Oppgave 17:**

Etterspørselen i et duopolmarked der bedriftene opptrer i tråd med Cournot-modellen er gitt ved  $P = 100 - Q$  der  $P$  er prisen og  $Q$  er mengden. Begge bedriftene har marginalkostnader på 10. Mengdene til bedriftene er  $Q_i$  og  $Q_j$ . Reaksjonsfunksjoner uttrykker bedriftens beste svar på den andres strategivalg. Hva blir et korrekt uttrykk for reaksjonsfunksjonen til bedriftene?

- a)  $Q_i = (90 - Q_j)/2$
- b)  $Q_i = (100 - 10)/3$
- c)  $Q_i = (110 - Q_j)/2$
- d)  $Q_i = (90 + Q_j)/2$

**Oppgave 18:**

Etterspørselen i et duopolmarked der bedriftene opptrer i tråd med Cournot-modellen er gitt ved  $P = 100 - Q$  der  $P$  er prisen og  $Q$  er mengden. Begge bedriftene har marginalkostnader på 10. Hvilken mengde vil hver bedrift tilby ved likevekt?

- a) 20
- b) 30
- c) 40
- d) 50

**Oppgave 19:**

Egenkapitalen og gjelden til en bedrift har samme verdi. Hva kan vi da si om sammenhengen mellom gjeldsgrad og gjeldsandel?

- a) Ingenting egentlig – vi må kjenne total verdi av aktiva for å si noe om gjeldsandel.
- b) Gjeldsgrad er lik gjeldsandel.
- c) Gjeldsandelen er lik to ganger gjeldsgraden.
- d) Gjeldsgraden er lik to ganger gjeldsandelen.

**Oppgave 20:**

Se bort fra skatt. Hva kan vi si generelt om sammenhengen mellom total kapitalrentabilitet, egenkapitalrentabilitet og gjeldsavkastningen?

- a) Dersom total kapitalrentabiliteten er mindre enn gjeldsavkastningen, er egenkapitalrentabiliteten mindre enn null.
- b) Dersom total kapitalrentabiliteten er større enn null, er egenkapitalrentabiliteten større enn gjeldsavkastningen.
- c) Dersom total kapitalrentabiliteten er mindre enn gjeldsavkastningen, er egenkapitalrentabiliteten større enn total kapitalrentabiliteten.
- d) Dersom total kapitalrentabiliteten er større enn gjeldsavkastningen, er egenkapitalrentabiliteten større enn total kapitalrentabiliteten.

**Oppgave 21:**

Et investeringsprosjekt innebærer en investering nå på  $I$ . Forventet kontantstrøm i periode  $t$  i de  $N$  periodene prosjektet vil vare er  $k_t$ . Diskonteringsrenten for periode  $t$  er  $r_t$ . Hva blir et korrekt uttrykk for prosjektets nettonåverdi?

- a)  $-I + \sum_{t=1}^N \frac{k_t}{r_t}$   
 b)  $-I + \sum_{t=1}^N \frac{k_t}{(1+r_t)^t}$

Side 6 av 7

- c)  $-I + \sum_{t=1}^N \frac{k_t}{1+r_t^t}$   
 d)  $-I + \sum_{t=1}^N \frac{k_t}{(1+r_t)^2}$

**Oppgave 22:**

Hva er en korrekt definisjon på begrepet internrente?

- a) Internrenten er avkastningskravet til totalkapitalen etter skatt.  
 b) Internrenten er avkastningen til investeringene som er gjort internt i selskapet.  
 c) Internrenten er den diskonteringsrenten som gir nettonåverdi lik null.  
 d) Internrenten er renten på gjelden som er tatt opp internt i selskapet.

**Oppgave 23:**

Et investeringsprosjekt innebærer en investering nå på 100 000 000 og en forventet positiv kontantstrøm om fem år på 200 000 000. Dersom avkastningskravet er 10 % årlig, hva blir forventet nettonåverdi for prosjektet?

- a) 81 818 182  
 b) 50 262 960  
 c) 36 602 691  
 d) 24 184 265

**Oppgave 24:**

Et investeringsprosjekt vil kunne gi kontantstrøm i to år. Det er imidlertid usikkerhet knyttet til mulige kontantstrømmer. Bedriften regner med at det er 20 % sannsynlighet for at det går dårlig slik at det blir tap første år. Da blir det en negativ kontantstrøm på 2 000 000 og prosjektet avsluttes. Dersom det ikke går dårlig første året, er forventet positiv kontantstrøm om ett år 10 000 000 og prosjektet videreføres inn i det andre året. I så fall regner de med at det er like sannsynlig at det vil gi 0 som at det vil gi 10 000 000 to år fra nå. Hva er forventet nåverdi av kontantstrømmen når avkastningskravet er 10 % per år?

- a) 10 214 876  
 b) 11 404 959  
 c) 15 537 190  
 d) 18 545 455

**Oppgave 25:**

Hva er den mest korrekte definisjonen av alternativkostnaden til kapital i forbindelse med nettonåverdiberegninger knyttet til mulige investeringsprosjekter i bedrifter?

- a) Den forventede avkastningen i aksjemarkedet.  
 b) Den forventede avkastningen til selskapets totalkapital etter skatt.  
 c) Den forventede avkastningen eierne har på sine investeringsporteføljer.  
 d) Den beste alternative, forventede avkastningen eierne kan få i markedene med tilsvarende risiko som prosjektet.

**Oppgave 26:**

Hva kan vi si generelt om hvordan en risikoavers investor vil prioritere mellom alternative investeringer som kan tas inn i porteføljen?

Side 7 av 7

- a) Investoren vil alltid foretrekke investeringen med lavest mulig standardavvik.
- b) I valget mellom to investeringer med samme forventede avkastning og samme standardavvik, vil investoren foretrekke den med lavest korrelasjon med porteføljen.
- c) I valget mellom to investeringer med samme forventede avkastning og samme standardavvik, vil investoren foretrekke den med høyest korrelasjon med porteføljen.
- d) Investoren vil alltid foretrekke investeringen med høyest forventet avkastning.

**Oppgave 27:**

Hva er en korrekt definisjon av markedsrisikoen til en portefølje?

- a) Det er den delen av risikoen som ikke kan diversifiseres bort ved å legge til flere verdipapirer i porteføljen.
- b) Standardavviket til markedsavkastningen.
- c) Det er den risikoen investoren velger å ta fordi det koster for mye å diversifisere ytterligere.
- d) Forskjellen mellom forventet avkastning i markedet og risikofri rente.

**Oppgave 28:**

Beta til aksjen til et selskap er 3. Markedsrisikopremien er 5 % og risikofri rente er 2 %. Anta at Capital Asset Pricing Model, dvs. kapitalverdimodellen, er korrekt. Hva er da forventet avkastning til aksjen?

- a) 5 %
- b) 7 %
- c) 11 %
- d) 17 %

**Oppgave 29:**

La  $\beta_A$  være beta for selskapets aktiva, la  $\beta_E$  være beta for selskapets egenkapital og la  $\beta_D$  være beta for selskapets gjeld. Markedsverdien av selskapets gjeld er  $D$  og markedsverdien av selskapets egenkapital er  $E$ . Hva blir da et korrekt uttrykk for beta til selskapets aktiva?

- a)  $\beta_A = \frac{D}{D+E} \beta_D + \frac{E}{D+E} \beta_E$
- b)  $\beta_A = \frac{D}{D+E} \beta_D - \frac{E}{D+E} \beta_E$
- c)  $\beta_A = \frac{D}{E} \beta_D + \frac{E}{D} \beta_E$
- d)  $\beta_A = \frac{E}{D} \beta_D + \frac{D}{E} \beta_E$

**Oppgave 30:**

Avkastningen til et selskaps egenkapital er 8 %. Avkastningen til selskapets gjeld er 4 %. Gjeldsandelen er 40 %. Selskapsskattesatsen er 25 %. Hva blir avkastningskravet til totalkapitalen etter skatt, dvs. WACC?

- a) 4,0 %
- b) 5,5 %
- c) 6,0 %
- d) 8,0 %

## D.1.2 Solutions

Fasit for eksamen i TIØ4258 TEKNOLOGILEDELSE vår 2015

- 1) d, Product-push er en ide om at produktet selger seg selv, vi trenger bare lage det
- 2) c, Å analysere bedriftens ressursmessige forutsetninger for å oppnå konkurransekraft
- 3) a, verdikjeder sier noe om hvilke verdivalg andre bedrifter har gjort
- 4) c, «vekstbedrifter»
- 5) d, De venter normalt til etter at et venturekapitalfond har investert...
- 6) a og c aksepteres begge. Ordlyden i a kan tolkes på to måter (ordet delt kan tolkes som felles, men også som ulikt), så derfor blir begge godkjent.
- 7) a, Prosessen som etablerer og kontrollerer graden av spesialisering i organisasjonen
- 8) c, En lav grad av standardisering gjør det lettere for ansatte og ledere som utfører komplekse og usikre oppgaver...
- 9) a, Bruen av kryss-funksjonelle team reduserer funksjonelle barrierer...
- 10) a, Ferdighets-variasjon, oppgave-identitet, oppgave-viktighet, autonomi og tilbakemeldinger
- 11) b,  $dTC/dQ$
- 12) b, Gjennomsnittskostnadene er minimale.
- 13) c, Inntektstapet som følge av prisreduksjon med sikte på å selge en ekstra enhet.
- 14) a, Etterspørselen er elastisk.
- 15) c, 3 000
- 16) a, Redusere mengden og øke prisen.
- 17) a,  $Q_i = (90 - Q_j)/2$
- 18) b, 30
- 19) d, Gjeldsgraden er lik to ganger gjeldsandelen.
- 20) d, Dersom totalkapitalrentabiliteten er større enn gjeldsavkastningen, er egenkapitalrentabiliteten større enn totalkapitalrentabiliteten.
- 21) d,  $-I + \sum_{t=1}^N \frac{k_t}{(1+r_t)^t}$
- 22) c, Internrenten er den diskonteringsrenten som gir nettonåverdi lik null.
- 23) d, 24 184 265
- 24) a, 10 214 876
- 25) d, Den beste alternative, forventede avkastningen eierne kan få i markedene med tilsvarende risiko som prosjektet.
- 26) b, I valget mellom to investeringer med samme forventede avkastning og samme standardavvik, vil investoren foretrekke den med lavest korrelasjon med porteføljen.
- 27) a, Det er den delen av risikoen som ikke kan diversifiseres bort ved å legge til flere verdipapirer i porteføljen.
- 28) d, 17 %
- 29) a,  $\beta_A = \frac{D}{D+E}\beta_D + \frac{E}{D+E}\beta_E$
- 30) c, 6,0 %