Fachhochschule Nordwestschweiz
Hochschule für Technik

GEIGER Mobile Learning for Cyber Security

A cyber security mobile learning platform

Computer Science / iCompetence

IP6
Bachelor Thesis

by Ledermann, Turan
Mayer, Felix Markus

Coaches: Fricker, Samuel
Baumgartner, Louis

FHNW
University of Applied Sciences
School of Engineering

Windisch, 20. Aug. 2021

Abstract

In the following report we describe our research, concept and solution to the problem of cyber security education for SMEs. For SMEs, cyber security is instrumental as cyber attacks can be detrimental to the survival of an SME.
The goal of cyber security education should be to communicate cyber security knowledge and practises in a way that non-tech savvy employees can understand and implement them in their daily lives. However, often that is not the case.

To counter this problem research was conducted in the domain of cyber security and education, consulting the existing literature. Initial quantitative testing provided first insights into the users' learning behaviours and preferred communication services. Further qualitative user tests help us then to narrow down the optimal user experience with regards to learning.

It has shown throughout this project that the combination of different learning approaches in combination with user interaction and the provision of expert knowledge through the communication channel was an appropriate way to support users in the learning and application of cyber security concepts.

The prototype produced can be further improved upon or used as a template for future projects and research into new forms of cyber security education.
Through user tests our solution can be argued that such a learning approach can help SME employees to increase their awareness and counter personal vulnerabilities.

Acknowledgements

We would like to thank all that have participated in the project and helped us realise the GEIGER Mobile Learning project. First of all we thank Mr. Fricker and Mr. Baumgartner, our coaches, for their support during the whole project. Secondly we thank the internal project team members and developers for a good work relationship and their continuous support. Furthermore, we thank the whole GEIGER consortium for their time and cooperation as well. We also thank the FHNW for providing the opportunity to work on this project.

Declaration of Authenticity

We hereby declare that the contents of this report, unless otherwise stated, have been authored by the involved team members. All content from other sources has been declared as such in the bibliography. No parts have been directly copied from other authors, sources, or from papers previously submitted for assessment by other students, without declaring them.

Turan Ledermann

Felix Markus Mayer

Windisch, 20. Aug. 2021

Table of Contents

1. Introduction

1.1 Initial Situation

Cyber attacks pose a serious existential threat for small and medium-sized enterprises (SMEs) in Switzerland. Computers and various smart devices have become an integral part of business even in many non-tech enterprises and are used for various purposes. However, 62% of SMEs experience a cyber attack within a year and 60% of SMEs hit by a serious cyber attack are subsequently forced to go out of business.[1]

Coiffure Loredana is a typical SME. The business is owned by Loredana Bartels. She works in collaboration with "Coiffure Moustache, Ruth Fellino-Müller", a sole proprietorship.
As a small hairdresser business, they don't have much of an IT infrastructure, but still make use of some IT and smart devices such as smartphones, tablets, etc. and the internet in their daily business, using widespread apps like WhatsApp, Instagram, Facebook, Pinterest, Sumup, Outlook, Banana Accounting on devices such as Android smartphone, mini tablet, Windows PC and multiple routers.

Thus, Loredana is a potential target for cyber attacks. However, since hers is not an IT business and she's not trained in cyber security, it can be difficult for her to recognise and counteract such attacks. Cyber security workshops are a great way to learn more about cyber security, but they can be costly and are usually time-consuming, so they are often not an option for many businesses like Loredana that need to be open for most of the week.

1.2 The GEIGER project

GEIGER is a Horizon 2020 project that aims to aid non-IT SMEs and micro-enterprises in becoming aware of the risks associated with the internet and the IT devices in their infrastructure, helping them counteract and reduce their exposure to these risks.

As part of the GEIGER project, the GEIGER Toolbox is being developed, which provides a suite of tools that an SME owner can use to determine the state and quality of their IT infrastructure in terms of cyber security and in relation to current major cyber security threats e.g. phishing, malware and ransomware attacks. This project's GEIGER Mobile Learning application is an external app associated with the GEIGER Toolbox.

The GEIGER Toolbox allows a business to scan their IT infrastructure for potential cyber security risks according to currently circulating cyber security threats, particularly those affecting the business' industry. The overall security and risks within the business are evaluated and signalled by the GEIGER indicator. Recommended activities are then forwarded to the user of this project, the GEIGER Mobile Learning application. Users are notified about new learning recommendations. The application can then be directly started with the respective learning sequence.

[1] Percentages according to the description of the project "21FS_IIT24:GEIGER Mobile Learning für Cybersicherheit"

1.3 GEIGER Mobile Learning

The GEIGER Mobile Learning project aims to create an innovative, interactive mobile learning application for smartphones, inspired by the previous FHNW project CYSEC.

1.3.1 Motivation

The most common cyber attacks such as malware and phishing rely on the user's action, e.g. clicking a link, executing a file, etc., to work. Often, such attacks are identifiable by the language used or discrepancies with the sender's e-mail address or phone number, but a lack of awareness can lead to a user engaging with these messages regardless.

It can thus be suggested that raising the awareness of these major cyber attacks among SME owners and employees plays a significant part in the reduction of their impact.
However, as of now there is no accessible, verified and unified source for non-tech-savvy users to learn about cyber security. The need for such an educational platform is thus evident.

1.3.2 Concept

GEIGER Mobile Learning provides an educational element to the GEIGER Toolbox, that allows users like Loredana to undertake learning sequences with which they can learn about cyber security threats that are relevant to them and their business. A learning sequence is a structured learning experience in which a user learns about certain cyber security concepts, or how to do certain things, e.g. how to set up Google Backup on an Android phone, or how to recognise and handle, avoid and / or counteract certain cyber security threats such as phishing emails. In an initial step this is done by providing the learner with some text, images and external resources such as YouTube videos.

xAPI is used between the GEIGER Toolbox and Mobile Learning app to record the user's learning successes on the first and to trigger learning sequences on the latter. Learning sequences come preinstalled with the application and are thus locally available for all users of the software. For this project a basic set of learning sequences is provided.

The target demographic for the GEIGER Mobile Learning are employees from SMEs like Loredana that are non tech-savvy. Learning sequences are especially designed such that non-tech-savvy users can reasonably complete them on their own.

The other major element offered by GEIGER Mobile Learning is the dialogue between learners themselves and more experienced learners. To encourage reflection and to counteract potential barriers in understanding, users also have the ability to engage in discussion with other users with similar expertise and backgrounds and ask for support, or offer help as well. Such a channel for discussion is also a way in which learners can be motivated to return to a learning sequence after encountering difficulties. Design elements from chat applications and forums like WhatsApp and Stack Overflow are to be evaluated and implemented in the design of this feature.

The goal of GEIGER Mobile Learning is thus to provide a proof of concept implementation for

a learning app that helps users like Loredana learn about relevant cyber security threats using step-by-step instructions for countermeasures and allows them to communicate and support each other, and motivates them to continue learning.

Over the course of this project, the team has collaborated with Loredana and other users to ensure that the concept meets the needs of an average Swiss SME.

1.3.3 Project Goals

- Conduct research and provide an initial proof of concept for the GEIGER Mobile Learning application.
- Educate users about countermeasures against cyber security threats, according to their personal situation.
- Enable users to independently work through practical learning sequences with real world applications. Motivate them to continue completing learning sequences.
- Enable users to communicate and educate each other through a half-structured dialogue.

1.4 Limitations

GEIGER Mobile Learning in the scope of this project functions as a standalone tool and validates a proof of concept, namely the compatibility of a learning process and a half structured communication channel which enables users to enhance their learning experience by helping others or getting help from other learners and / or experts. The aim of this project is thus not the direct interoperability between GEIGER mobile learning and the GEIGER Toolbox. Nonetheless the project has to be built in a way that allows for this kind of scaling and makes integration easy.

The project does not aim to be production ready and will not, during the project, be released on the Google App Store nor the Apple Store.

Further limitations are within the styling of the proof of concept application. It is not a priority of this project to have an appealing design. This does not mean that the whole user experience will be neglected but neither is it in the center of this project.

1.5 Structure

In the following chapter 2 of this paper, the background for this project such as previous research, projects and literature will be reviewed.
In chapter 3, the requirements, solution concept and user stories that emerged from the review in chapter 2 and requirements elicitation are described.
Chapter 4 discusses the solution for the proof of concept, in terms of the architecture and technologies used as well as the implementation of various functionalities.
In chapter 5, the results and impressions from user tests are compiled and the findings and achievements of the concept subsequently discussed in chapter 6.
Finally, in chapter 7 the findings and conclusions of this project are summarised.

In the final part, the achievements of this project are evaluated and insights gained through the research and future steps for the project will be discussed.

1.6 Research concept

For this project the focus lies on how to deliver learning content such that a non-tech savvy SME owner or employee can complete lessons by themselves and is incentivised and motivated to learn and continue learning. Furthermore, we look at what kind of communication platform we have to provide in order to make the whole learning process more engaging and enable the users to help each other.
Research of existing educational applications is conducted to inform design decisions and synergise the aspects that work best.

1.7 Summary

In today's world the interconnectivity between businesses, the world wide web and other technologies has grown substantially. Digitalisation makes it that small to medium sized businesses with a smaller capital are even more vulnerable to cyber attacks, which can pose an existential threat to them.
GEIGER Mobile learning aims to prevent such attacks by fostering its users to become more knowledgeable and be less of a vulnerability themselves.
This is achieved through the integration of short and appealing lessons with a validation process at the end of each one of them. Learners are able to communicate with others as well as cybersecurity experts on the subject matter.
Aim of the project is to provide a concept for a mobile cyber security learning application which enables SME owners to learn how to protect their business from cyber threats.

2. Background

2.1 Cyber Security Threats

In the modern world people are surrounded by technology and use computers and various other devices connected to the internet every day. With the advent of smartphones and other smart devices particularly, access to the internet has become ubiquitous. In a survey conducted in 2018, it was found that 92% of all adults own a smartphone, of which 97% use their device daily. [Deloitte, 2018]
However, as constant access to the internet has become a normality, so have the risks associated with the internet become a threat which we are continually exposed to. Some of the most frequent and impactful cyber attacks include phishing and malware attacks, with malware representing the #1 top threat on the 2020 ENISA list of top threats, and phishing at #3. [ENISA, 2020]

Malware is short for “malicious software” and refers to software designed to cause damage to a single computer, server, or computer network. [Moir, 2009]

Phishing is a cyber attack using social engineering, which aims to trick a person into revealing sensitive information, e.g. passwords, financial account information and social security numbers, which can then later be used to the victim’s detriment. [Ramzan, 2010]

Common cyber attacks such as the aforementioned malware and phishing are no longer contained to the e-mail client on one’s personal computer, as the same fake e-mails can now reach a person at any time on their smartphone as well. In fact, phishing e-mails in particular are responsible for around 94% of all malware attacks. [Verizon, 2019]

The interconnected nature of the internet, social media and smart devices poses innumerable attack vectors that the average person is not necessarily aware of. Whereas a dubious e-mail on one’s personal computer or even on one’s smartphone may appear as an obvious phishing attempt, the same approach via a text message from a trusted phone number or contact may still get the user to respond in a way that an attacker wishes.

In fact, the vast majority of cyber security threats rely on some form of human interaction [Dark Reading, 2019], which usually involves clicking a link and running an executable or opening a document.

2.2 The Role of Human Traits in Cyber Security (Intentions)

Humans are often identified as the weakest link in cyber security, since any technical security solution is still prone to failures caused by human error. [Gratian et al., 2017]
Human factors such as individual differences, cognitive abilities and personality traits play a significant role in cyber security behaviour. [Parsons et al. 2010]

Thus, ensuring that a system is secure purely on a technical level is not enough to guarantee its security, since some manner of human interaction with the system is often required. Understanding the many factors that lead to human error in cyber security practises is vital to developing better ways to create awareness, educate and temper good cyber security practises by users.

The 2017 study conducted by Gratian et al. with 369 university students sought to correlate individual differences in human traits such as demographic factors, personality traits, risk-taking preferences and decision-making styles with four cyber security behaviour intentions.
To measure the students' cyber security behaviour intentions, the Security Behaviour Intention Scale (SeBIS) developed by Egelman and Peer (2015) was used, which measures a user's cyber security behaviour intentions of device securement, password generation, proactive awareness and updating using a set of 16 cyber security questions. [Egelman and Peer, 2015]

The students completed a survey in which they self-reported on personality traits, decision-making styles and risk-taking preferences, the results of which were correlated with the SeBIS to measure the impact of individual differences on the aforementioned cyber security behaviour intentions.

The study found that individual differences account for 5%-23% of the variance in reported cyber security behaviour intentions.
It particularly suggests that the cyber security behaviour intentions of password generation and proactive awareness are influenced by individual differences, particularly the personality trait of conscientiousness. Other findings suggest that a rational decision-making style influences good device securement and updating practices as well as proactive awareness.
Conversely, a spontaneous decision-making style seems to suggest poorer proactive awareness and updating practises. [Gratian et al., 2017]
Poor proactive awareness could suggest a vulnerability to social engineering and related cyber attacks such as phishing. A person with a spontaneous decision-making style might thus be more vulnerable to such an attack, as they may not check the URL of a fake website or closely examine the sender of a phishing e-mail.

In cyber security education, it is thus important to consider the wide variety of individual differences that people exhibit and circumstances they may be a part of, which may influence their cyber security behaviours.

2.3 The Mechanics of Risk Perception

Generally, when making behavioural decisions, individuals will often decide based on their estimates of the risks associated with the various options. Hence, the manner in which IT users perceive threats will influence their behavioural responses. [Parsons et al., 2010]

A person's level of knowledge or education in cyber security can greatly influence the perception of risks and thus - in the case that their cyber security education may be lacking - increase the threat that such risks pose.
To understand many cyber security threats and the magnitude or implications thereof, a certain level of technical knowledge may be required, which a user may not have.
The lack of such knowledge can affect effective decision-making and risk perception, resulting in users making decisions based on an inaccurate understanding of what being 'secure' means. [Parsons et al., 2010]

Such lack of knowledge can also lead to a lack of security motivation, as people may not understand the seriousness of the potential risk, and the associated need for security procedures. [Parsons et al., 2010]
Therefore, it is integral to educate IT users on security risks to cultivate awareness. However, although there have been many educational programmes regarding cyber security, they do not generally produce the desired long term results of better awareness and security practise.

2.4 Effect of Cyber Security Training Programmes

Cyber security awareness plays a significant role in the prevention of cyber attacks.
Particularly in the example of a phishing attempt, awareness can help the user to critically examine the information provided by e.g. a website, e-mail or text message.
However, for many IT users, such critical analysis of e.g. a website's URL or the sender of an e-mail or text message is not necessarily an instinctual action.

In many organisations, cyber security training programmes such as security awareness training are thus provided to teach good security practises in their employees. However, studies show that certainly in the long term, such training programmes do not tend to have the desired effect, e.g. creating cyber security awareness and changing staff behaviours in relation to cyber security. [Bada et al., 2019]

A 2016 survey by Axelos conducted in the UK examined the effectiveness of cyber security awareness training programmes, as perceived by 100 executives responsible for information security training in organisations with 500+ employees. [Axelos, 2016]
The results of the survey indicate that 99% believe security awareness training is important to minimise the risk of cyber security breaches and that 63% believe that minimising human error is important to their organisation's cyber security.
However, despite this, only 42% of the executives believed their awareness training was effective at providing general awareness of security risks. Only 33% believed their awareness training was effective in reducing the chance of an information security breach. Still only

28% believed that their training programme was effective at changing staff behaviours in relation to information security.
46% of organisations provide ongoing information security awareness training beyond new starter induction or annual e-learning courses.
The study also showed that 82% of organisations use computer-based training and e-learning for such programmes, rather than more modern approaches such as games, simulations and animations. [Axelos, 2016]

These findings suggest that cyber security awareness training within organisations is often a rare, if not one-time occurrence for most employees, rather than a continuous, engaging effort.
While such training programmes can encourage good practises in the short term, if they are not enforced throughout the organisation and training is not repeated, users may fall back into old patterns of poor cyber security behaviours in the long term, particularly when they encounter difficulties in applying the training in the real workplace.

When faced with the many cyber security threats that exist and the ambiguous warnings and complicated advice surrounding them, some individuals may choose to abandon all efforts for protection and ignore the threats altogether and deny the existence of a need for any security decision. [Bada et al. 2019]
This suggests that it is not necessarily that people are unaware of cyber security and the various threats they may encounter. In fact, people know the answers to awareness questions, but do not act according to cyber security guidelines regardless.
It is the stress and difficulties that people encounter when interacting with IT security systems that prohibit them from further pursuing better cyber security practises.
The difficulties that a normal IT user may encounter thus need to be factored into the design of such an IT system from the beginning [Bada et al. 2019], and users must be trained in its usage, as well as educated about cyber security practises in relation to that system.

However, most cyber security training programmes are generic in design [Parsons et al., 2010], such that anything that that users may learn may not actually translate into their IT usage in their daily lives.
Thus, to be effective in the first place, the content of a training programme has to be relevant to the needs of the staff as well as interesting, current and simple enough to be followed. It must provide feedback and immediate results to the user. [Parsons et al., 2010] [Bada et al. 2019]
Moreover, any training programme must be repeated, to reinforce the importance of the security messages and practises, and so that users can internalise the lessons learnt. Alternative methods for learning using various media can also help users better retain cyber security awareness and good cyber security practises.

2.5 Motivation and Adaptive Help Seeking in Education

Within education, it has been observed that many factors outside of the material being discussed itself play a role with regard to an individual's willingness and motivation to pursue academic success and the ways in which they do so.
In this chapter, the work of Richard S. Newman concerning the adaptive help seeking behaviours of students is reviewed.

Newman states that particularly during the learning process, it is often necessary to ask questions about material one does not understand. Moreover, because people do not always have the means or previous knowledge to master a challenge - academic or not - it is important for them to be willing to depend on someone else for help.
This process is referred to as adaptive help seeking, which allows a person to engage with others to solve a problem and gain an understanding for it, enabling the person to solve the problem on their own in the future.
Adaptive help seeking is thus a social process, whereby a learner understands that they require assistance from someone more knowledgeable than them and proceeds to ask for support. [Newman, 2008]
Though 'other-regulation' - that is, depending on another person to help solve a problem - may appear to be different from or perhaps stand in direct opposition to autonomy and self-regulation, it is in truth an integral part of self-regulation and self-efficacy. It requires an autonomous, self-regulated learner to recognise a gap in their knowledge and confidently ask for help to further their own intellectual development, without fear of judgment.

However, in contrast to the usefulness of this behaviour, people often fail to take the initiative to obtain help when they need it and instead exhibit other, maladaptive behaviours. Maladaptive behaviours include simply not asking for help and not resolving the problem at all, or asking for help when it is not necessary, e.g, when the individual has not attempted to resolve the problem on their own yet.

Several factors can lead to a person avoiding to employ adaptive help seeking:

Firstly, a person's disposition towards learning and the goals they aim to achieve e.g. the goal and value of learning versus the goal of simply performing well; the self-beliefs they hold which influence their self-efficacy, perceived competence and tolerance of challenges and finally, emotions that can affect self-esteem, which allows a person to admit to others their limitations. [Newman, 2008]

Another factor is the type of the achievement goals being pursued through learning and whether learning goals are being pursued or not. Learning goals are a set of goals that a group - such as a class of students - aims to achieve collectively. Such goals stand in opposition to performance goals, where good performances - measured perhaps by tests and earned marks - are the goal that must be reached. Performance-oriented goals tend to have an adverse effect on learning [Newman, 2008], due to their competitive nature encouraging comparison between learners and because whether any actual understanding was gained does not matter as much as the performance that was achieved.

In addition, another factor is the risk associated with asking questions. An individual may not want to open up about a gap in their knowledge due to a fear of potential embarrassment or appearing incompetent in front of their peers. [Newman, 2008]
In groups where performance goals are emphasized, there may be more perceived risk associated with asking questions, since it may reveal that a person may be having difficulties and might be “underperforming” compared to others.

Finally, the relations and involvement between learner and the teacher or instructor is another factor. Ideally, the individual taking on the role of teacher is present, able to take on the learner’s perspective and willing to help in the case that a learner may have difficulties with the material or task. [Newman, 2008]
When a teacher emphasizes collective learning goals, encourages mutual support between learners and takes initiative to listen, ask questions and provide help, the perceived risks associated with asking for help can be mitigated and learners can be motivated to ask questions when necessary.
However, this is not just conducive to the learner’s learning experience. Newman suggests that there can be a reciprocal motivating effect on teachers as well. To take their role as a facilitator of adaptive help seeking seriously, teachers must be patient, listen to students’ questions, not rush to give a response, explain how to handle problems rather than simply supply answers, and value errors as diagnostic information [Newman, 2008], which is invaluable for the adjustment of their curriculum and teaching methods in the future.

In essence, it is important in any form of education to foster a supportive atmosphere where learning is the primary focus. This motivates learners and allows them to employ the adaptive help seeking strategy, to feel free to ask questions and engage with other learners on the same level. This type of engagement can also have positive effects on the teacher, validating their work and efforts, motivating them in turn to be attentive to the needs of the learner, and adjust their methods accordingly.

2.5.1 Meaning for Cyber Security Education

In the previous section, it was mentioned that many cyber security educators do not feel that their work is having a substantial effect on the overall awareness and security proficiency of learners.
It can be suggested that the methods employed in cyber security training programmes would benefit from using the aforementioned strategies. However, this requires cyber security education to be treated as any other form of education. If the individual traits and learning behaviours of people are not considered and good learning behaviours such as adaptive help seeking are not actively encouraged in the educational programme, it is likely that the results of such programmes may continue to remain unsatisfactory.

2.6 Review of Existing Solutions

2.6.1 Educational Applications

Many educational applications already exist, examples of which include SoloLearn, Duolingo and Coursera. While using them, certain design patterns quickly become apparent.
While Duolingo is focused exclusively on learning languages, SoloLearn is focused entirely on learning programming languages, whereas Coursera offers a wide variety of courses, ranging from language courses, programming and general IT courses, to art and personal development courses. With Coursera, many of the courses are conceptualised by lecturers from universities such as Yale University or the University of Michigan.

SoloLearn and Duolingo are similar in that they provide small and simple lessons which can be completed in relatively little time on a smartphone as well as on PC. Coursera is also available on PC and as a mobile application, though its courses are more substantial in scope, often estimating one to three hours per chapter.
During a lesson, the learner is always able to access a discussion forum in each of the three solutions, where they can ask questions or search for the answer in older threads.

2.6.2 Q&A Platforms and Forums

Examples for popular Q&A platforms and forums include StackExchange and Quora.

StackExchange offers many sub-sites dedicated to various topics, with some of its most popular sites being StackOverflow for programming questions and other sub-sites dedicated to the English language and mathematics.
Users can ask questions and receive answers, and each question or answer can receive comments for further discussion as well. All of these elements can be up- or downvoted as well, to indicate their overall relevance. The user who asked a question can choose the best answer, allowing future visitors of the page with the same question to easily find the answer.

Quora is also a Q&A platform, allowing a user to ask any type of question, although it is not necessary for the question to be about a specific topic as with a StackExchange. A user can create and select their particular interests (‘Spaces’) and ask questions and find related questions to answer.

2.6.3 Instant Messaging Applications

Among the most popular instant messaging applications are WhatsApp and Telegram. [Statista, 2021]
In these applications, messages including images, videos, documents, etc. can be rapidly exchanged. Users use their phone number to register and can choose a name and picture to represent themselves with. These message systems provide an unstructured approach in which a user can freely share information with whom he wants to. This approach of communication and its use are widespread, thus many users of smartphones are very familiar with it. This not only takes away the anxiety from using a particular service as its structure is known but also gives the user the possibility of opening up more and also speaking more directly. Further it has to be noted that response times in comparison with

structured solutions such as forums tend to be smaller and engagement among its users higher.

2.6.4 Gamification of Education

Educational systems now more often than ever use gamification of learning processes to enhance the learners participation and overall motivation. Gamification helps negate negative emotions associated with traditional learning. In gamification currency based tracking mechanisms serve several purposes, on one hand it provides a motivational aspect and on the other it helps the tracking the progress of individual learners. [Hsin-Yuan Huang, 2013]

2.7 Innovation Gap

Due to the many previously-mentioned complexities involved in cyber security education, there is as of yet no definitive solution to relay good practises and awareness to IT users. However, cyber security awareness campaigns and training programmes by countries and businesses fail to achieve the desired results.

Therefore, the need for better cyber security education is clear. Particularly non-IT-focused SMEs - which may be unable to afford cyber security training programmes of any sort - would benefit greatly from an easily accessible resource that offers a single source of truth, which they can consult for simple, actionable cyber security guides and learning programmes that offer unambiguous benefits and feedback to the learner.

Because the active intellectual exchange among learners can be a powerful tool to foster a deeper understanding of the material, a channel dedicated to cyber security, which allows learners to ask questions about cyber security subjects and engage in discussion with experts and other learners could prove greatly beneficial.

However, no equivalent platform like SoloLearn or Duolingo exists for cyber security as of yet and neither does a combination of such a platform and a dedicated discussion channel for IT users. Furthermore, all of the existing solutions mentioned implement their discussion channels using a structured approach with forums, while an approach using a similar design to instant messaging applications has not been attempted yet.

Since the vast majority of adults own a smartphone and use it daily, it seems natural to harness the reach of such devices and design a mobile solution that offers an educational experience focused on cyber security and allows autonomous and collaborative learning. This is a new approach to cyber security education that could augment the set of currently existing solutions for cyber security education and provide a model for future solutions.

2.8 Summary

Cyber attacks are increasing in frequency and severity and the consequences for people and their businesses can be an existential threat, with phishing and malware being two of the most prominent cyber attacks. Because humans are the weakest link in a security system and cyber attacks often require the user's input to work, it is important to understand the reasons why people behave such that they fall prey to these attacks. Human traits and differences such as a person's decision-making style can influence how they react to certain cyber attacks and how they perceive cyber security risks. To be able to assess cyber security risks accurately and make informed and confident decisions, people need to be properly educated about cyber security.
However, cyber security training and education programmes generally do not produce the desired results, as many instructors feel their work does not have a great effect in terms of changing the users' behaviours, because the content is usually generic and not targeted at the real situation users work in daily.
Therefore it is important for cyber security training and education to make use of what is already known in 'regular' education and take the needs of staff and individual differences of learners into account to better communicate their messages and practises and allow a motivating, empowering and collaborative learning experience.

Several applications offer learning experiences with more or less integrated communication channels for learners. As the topic of cyber security education is a complex and difficult one there are currently no sufficient equivalent solutions on the market. However, many aspects of the existing solutions certainly have value. The short length of individual lessons are ideal for a mobile application and lends itself well to work commutes or for short breaks. Gamification is another such aspect, which can help raise the overall engagement level of learners. The active intellectual exchange between learners and experts through a semi-structured communication channel, which users are familiar with due to its resemblance of an instant messaging application, in combination with the learning program tailored to the needs of non-tech savvy users, GEIGER Mobile Learning could fill an as of yet neglected gap in the cyber security space.

3. GEIGER Mobile Learning

3.1 Stakeholders

GEIGER Mobile Learning has three main stakeholders with different goals, namely:

Learning content creators, who create the learning sequences to be used in the application and completed by learners.
This stakeholder is well-versed in cyber security concepts and creates learning content aimed at IT users who do not possess much knowledge in the field.
Although this user does not necessarily interact directly with the final product, it is important that they be considered during its design, as any difficulties that may be inherent to the process of learning content creation could hamper the success of the application in the future. Thus, it is important to propose a data structure and workflow for the creation of learning sequences that is simple to work with and does not require much software design knowledge.

SME owners and employees, who complete lessons and engage in discussion with other learners and cyber security experts.
This stakeholder is the main target audience of the final product. They own a business and use IT devices in their daily operations. They possess little to no knowledge about cyber security and their schedule and budget does not allow for cyber security training courses. To protect their business, they want to learn more about cyber threats and their respective countermeasures.
In the application, they complete lessons to learn about cyber security concepts and how to solve related problems. If there are difficulties in understanding the material or executing a task and they want to ask questions, they can access the app's discussion platform and receive support from other learners and cyber security experts. To allow free discussion, users can choose to remain anonymous when they use this feature, so that the common fears associated with asking questions can be mitigated.

Cyber security experts, who offer advice and help to learners.
This user uses the discussion feature of the application to support learners during the learning process. They can provide answers to questions or engage in general discussion with learners. They can also use images e.g. to provide visual instructions on how to complete a task.

3.2 Proposed Concept

3.2.1 Lessons

Lessons represent the structured learning approach, whereby a learner receives information in a linear manner. A lesson offers simple and short information spread across multiple slides, so as to not overwhelm the learner and to allow short learning sessions during a commute or break. The learner can swipe through these slides, similarly to Instagram stories or other learning applications. An optional quiz at the end can test if the learner has understood the content of the lesson. The learner is then rewarded by a congratulation and points, which are added to their personal score, which serves as an indicator for their personal learning progress. A reminder date can be set by the learner so they are reminded to repeat the lesson in the future.

Because there are no previous example lessons to use as templates for the project, the application should be able to integrate new lessons as they are added. It should also be able to handle various media in lessons ranging from simple text and images to audio and video and links to websites to allow diversity in the lesson content.

Realised Goal: By taking and repeating lessons, a learner can increase their knowledge of cyber security concepts, as well as expand their skill set. This allows them to better protect themselves and their business from cyber threats in the future.

3.2.2 Communication Channel

The communication channel represents the semi-structured, supported learning approach, whereby a learner consults other learners and experts with a question after encountering difficulties with the learning material. This aspect is modelled with inspiration from instant messaging applications such as Telegram and WhatsApp, lending a familiar feel to the interaction. A communication channel exists for every lesson. The ability to use text chat and images allows users to illustrate a question or problem and experts to respond with an answer or visual guide on how to solve it.

Realised Goal: Receiving help from others aids the learner in better understanding the concepts presented in a lesson, again leading to the benefits mentioned in 3.2.1.

In the following context-diagram are the system boundaries of the project stated.

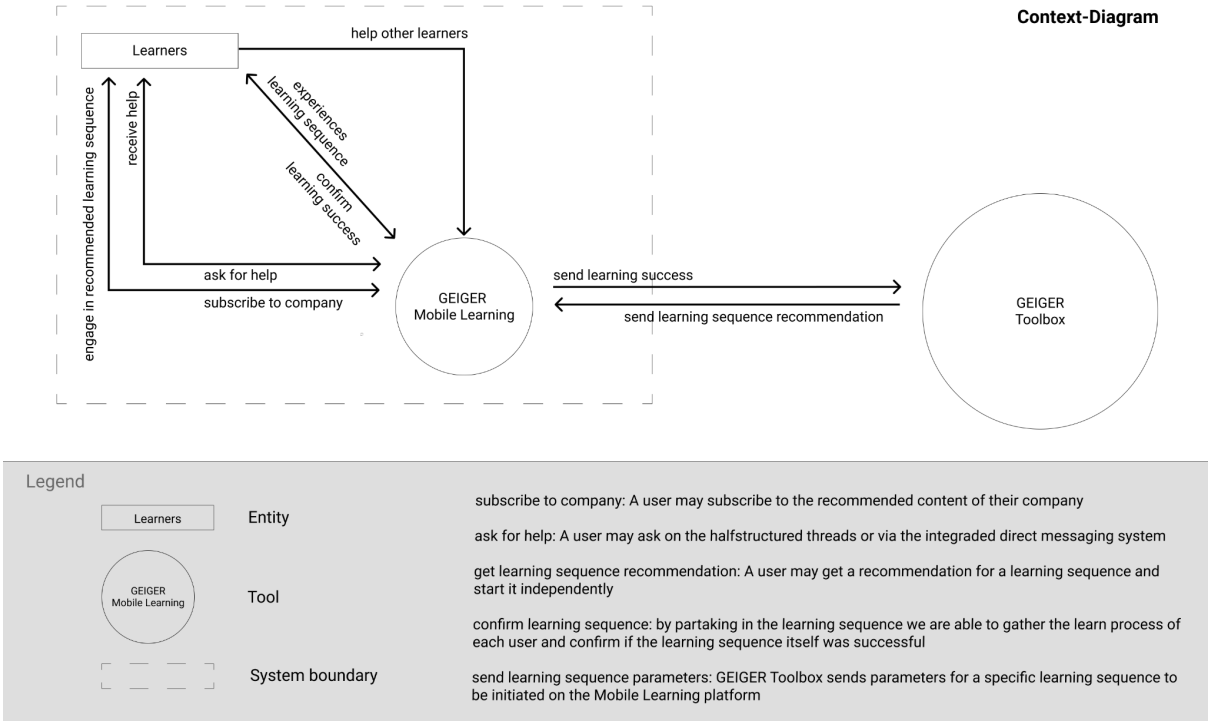


Fig. 1: Context-diagram of GEIGER Toolbox and GEIGER Mobile Learning

3.3 User Stories

Based on the stakeholder analysis, the following user stories were defined using Cohn's and Beck's User Stories [Cohn & Beck, 2004].

<u>as a learning content creator</u>
I want to create cyber security lessons for usage in the GEIGER Mobile Learning application.
I want to create lessons in as simple a way as possible.

<u>as an SME owner</u>
I want to learn how to protect myself and my business from cyber attacks.
I want to complete lessons to learn more about cyber security.
I want to ask questions about concepts I don't understand and tasks I can't complete on my own.
I want to receive help from cyber security experts.
I want other learners to benefit from the questions I ask.
I want to discuss cyber security with people who have a similar understanding of it.
IF I find it bothersome to ask a question, I want to remain completely anonymous when doing so.

as a cyber security expert
I want to support learners during the learning process.
I want to answer questions that learners may have.
I want to help learners with tasks they may have difficulties with.
I want to supply visual guides to learners.

3.4 Summary

Stakeholders
There are three main stakeholders in the project, namely the SME owner or employee which takes the role of a learner and is a content consumer, secondly the content producer which creates and provides the learn content and lastly the cyber security expert which is able to support learners over the semi-structured communication channel.

Proposed concept
The learner can take lessons, which are simple and short, linear learning experiences which can also have a quiz. Should they encounter difficulties in understanding the material, they can use the communication channel to ask other learners and cyber security experts questions, with the option to remain anonymous if they want to. By completing lessons and asking questions, a user can increase their knowledge about cyber security and better protect themselves and their business. Furthermore, gamification in the form of points rewards after completing a lesson offers another incentive to continue learning.
The learning content should be able to offer a diverse set of media to keep the learner engaged. Lessons will be created by a team of experts after initial development of the proof of concept. The application must therefore be able to integrate new lessons as they are added. To ensure efficiency, the content creation process should also be relatively simple.

4. Implementation

4.1 Evaluation of Technologies

4.1.1 Framework SDK

After an extensive analysis of different possible frameworks the most suitable one was narrowed down and decided upon based on a set of several criteria.

Flutter, a new, widely-supported framework by Google, that allows development of a cross platform (Android, iOS) solution, was chosen. Not only does it provide cross platform development support but has also the same codebase for both operating systems. It also supports older versions of the different operating systems which showed to be necessary for the target audience. Furthermore, it provides a stable UI, allowing for the MVC pattern and the look of the different elements are the same on all platforms. For all the aforementioned reasons and last but not least the fast performance of Flutter it was selected as the main framework for this project. Enabling fast prototyping and effective changes.

Evaluation summary

	platform support				development				performance			support			
SDK	Anroid	iOS	Web	desktop	plugins and libraries	dev features (hot reload)	time efficient prototyping	integrated testing	performant	stable UI	size	active community	reference material	IDE support	thought at the FHNW
Flutter	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	
Native (Java / Kotlin)	✓				✓				✓	✓	✓	✓	✓	✓	
React Native	✓	✓		✓	✓				✓			✓	✓	✓	
Jetpack Compose	✓						✓	✓	✓	✓	✓			✓	✓

Fig. 2: framework evaluation

At the time and for the major part of this project's duration, the GEIGER Toolbox project was being developed in TotalCross, a technology that also allows cross platform development for Android, iOS, Desktop, etc.
Support for external plugin applications developed using other technologies was planned, though due to concerns about compatibility issues that would possibly arise between the two technologies, a first attempt was made to develop the Mobile Learning application in TotalCross as well. Due to limited documentation and feature set however, severe difficulties were encountered during development and insufficient progress was made. Development of the Mobile Learning application was thus eventually restarted from scratch using Flutter, which enabled a much faster achievement of results.

4.1.2 Local storage

For the local storage implementation we evaluated several different approaches and came to the conclusion that a NoSQL database approach would be the best suited for a fast and responsive end user experience. This unstructured local storage solution enables a fast setup and up to 2636 ms faster reading speed for 1000 iterations and 14760 ms faster writing speed for 1000 iterations compared with SQL database solutions that are available for Flutter.[2] This improvement in speed comes with the downside of not having relational entries inside the database. However this downside was not meaningful for the amount of data the project is expected to store.

4.1.3 Communication Channel

During the project several communication solutions were assessed inside these three forum solutions, namely Discourse, Talkyard and NodeBB as well as a few chat solutions, namely StreamChat and Chat SDK. None of the aforementioned solutions fulfilled all the requirements given by the project. One of the key requirements was the security and control over the user communication, using third party implementations was thus not a viable option for the final product. Thus a custom semi-structured communication solution was implemented.

[2] https://pub.dev/packages/hive

4.2 Software Architecture

The context diagram shows the system boundaries of GEIGER mobile learning. Contrary to the initial concept a communication and implementation of GEIGER mobile learning with the GEIGER Toolbox was not possible as the Toolbox itself was in development and was in a volatile state. Thus we implemented our own backend server which handles all of our messaging traffic and user authentication.

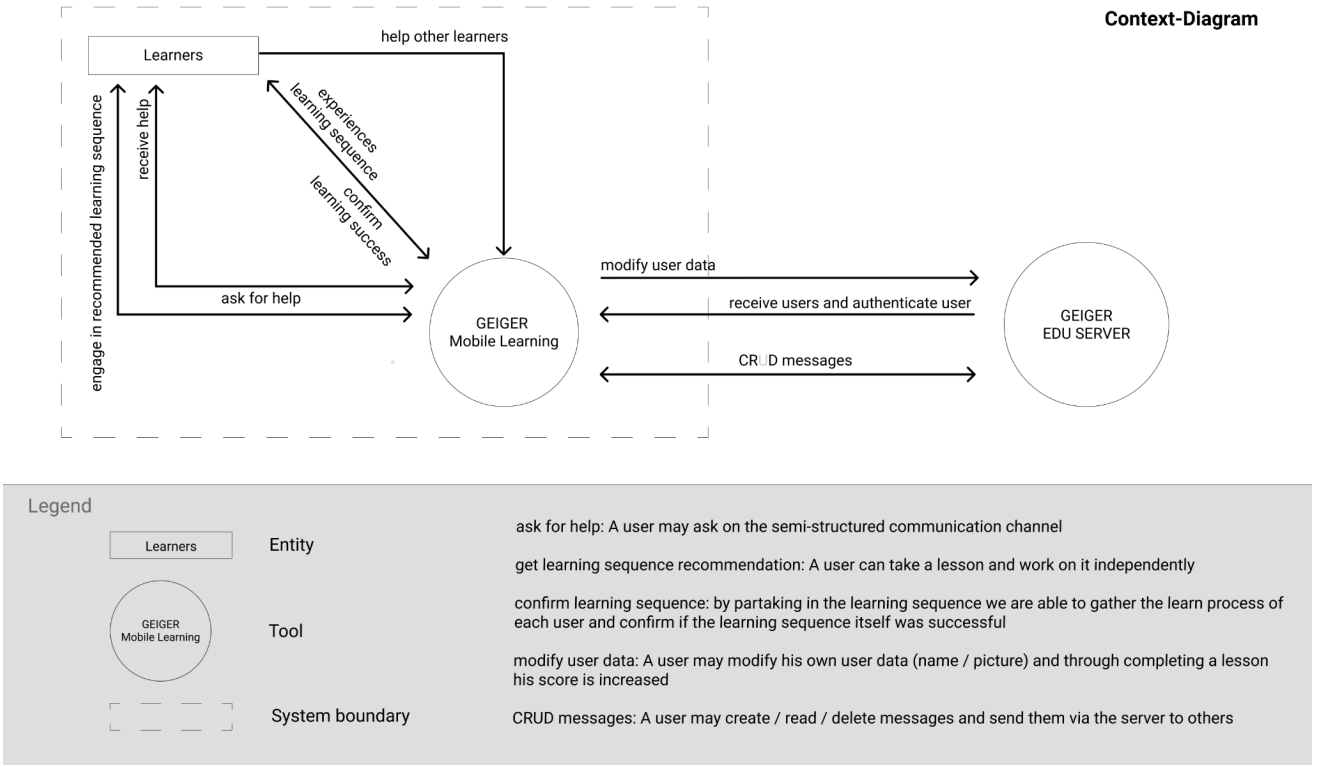


Fig. 3: software architecture context diagram

4.2.1 Design

From the beginning the final product had the aspiration to feel like an integral part of the visual language that the GEIGER Toolbox delivers. Thus the look and feel of the UI elements were derived from it. This helps to generate a consistent branding over a multitude of different applications and gives the user a sense of familiarity and trust in the product. The visual feel of the application was inspired from the various GEIGER Toolbox iterations in collaboration with the user experience designer of the GEIGER Toolbox team.

To iterate and have a firm validation of the design approach we applied the design thinking approach right from the start of the project. Regarding the product itself the design thinking approach is the most effective to support iterative work while focusing primarily on the need of the customer. Design Thinking sets the human in the center of innovation. First of all as a user but also as a valuable part of the team. It bolsters a creative culture and enables innovation. Ideas are experienced - Through the use of simple and fast prototypes it's possible to visualize ideas to build upon or disregard them. Furthermore the process of feedback generation through the use of prototypes is vastly enhanced.

Through the use of this approach the end users could be closely integrated right from the start of the project and were thus able to provide valuable feedback furthering the development of the user experience.

4.2.2 Interaction Design

Lesson Interface

The interaction with lessons was implemented according to the solution concept described in chapter 3.2.1 and based on Figma designs.

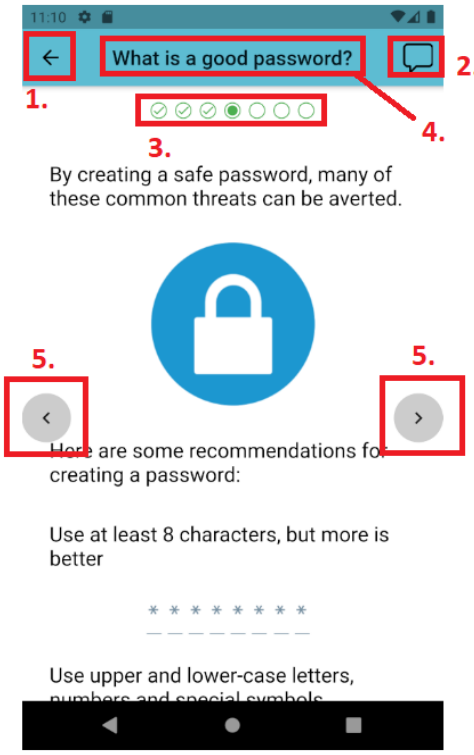


Fig 4: Slide from example lesson "Password Safety" with marked UI elements

In Fig. 4 an example of a slide from an example lesson can be seen, as well as various UI elements.

The UI elements in a lesson are:

1. Back Button:
   Navigates back to the previous screen.
2. Chat Button:
   Navigates to the current lesson's communication channel.
3. Progress Indicator:
   Indicates progress within the current lesson. The individual elements can be tapped to jump directly to a certain page. This element allows the learner to get a sense for how far they are into a lesson and to conveniently jump directly to any page.
4. Slide Title:
   The title of the current slide.
5. Slide Navigation Buttons:
   Navigate back and forth through a lesson's slides via tapping as an alternative to swiping.

Communication Channel User Interface

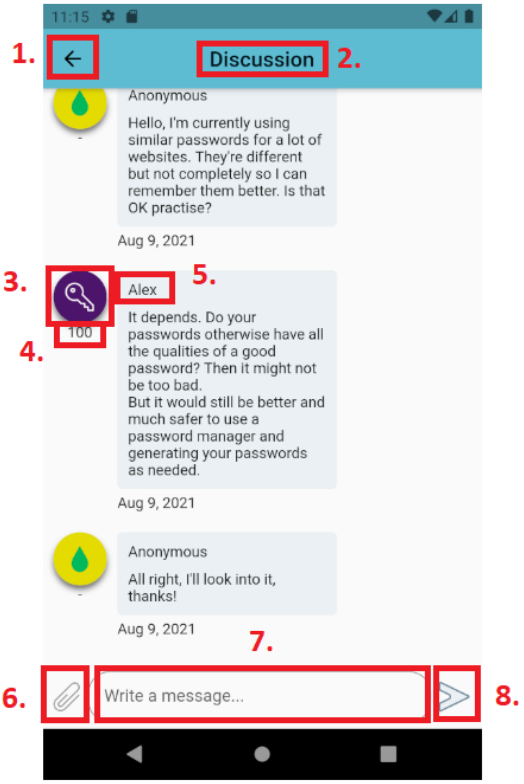


Fig. 5: Communication channel with marked UI elements

Shown in Fig. 5 is an example of such a communication channel, for the lesson “Password Safety”.

The UI elements in a communication channel are:

1. Back Button:
   Navigates back to the previous screen.
2. Screen Title
3. User Icon
4. User Learn Score
   Can also display as - if the user has set the respective anonymity setting.
5. Username:
   Can also display as ‘Anonymous’ if the user has set the respective anonymity setting.
6. Image Picker:
   Allows the user to select an image to send.
7. Message Field:
   Allows the user to write a text message.
8. Send Message Button:
   Sends the message.

Profile User Interface

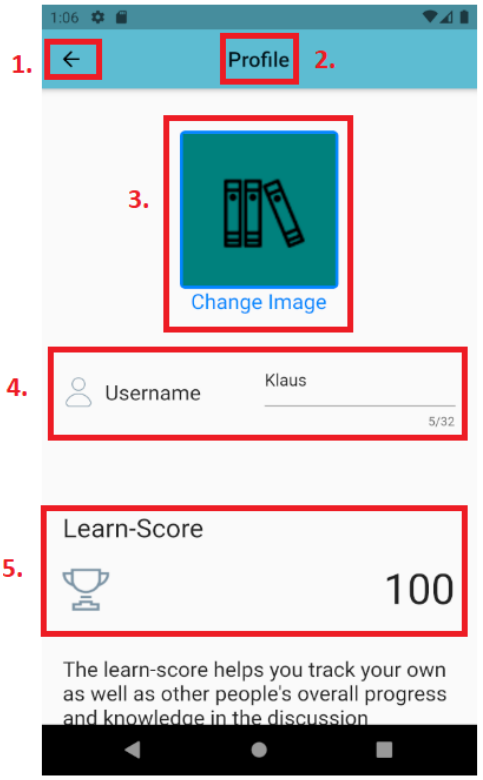


Fig. 6: Profile with marked UI elements

Shown in Fig.6 is the personal profile of a user, which enables the user to change their icon and username, with which they will appear in the communication channel.

The UI elements in the profile screen are:

1. Back Button:
   Navigates back to the previous screen.
2. Screen Title
3. User icon
   Allows a user to change his profile icon
4. User name text field
   Here a user may change his own username that is displayed in the chatroom when writing a comment
5. Learn score
   Allows a user to see his own learn score

Setting User Interface

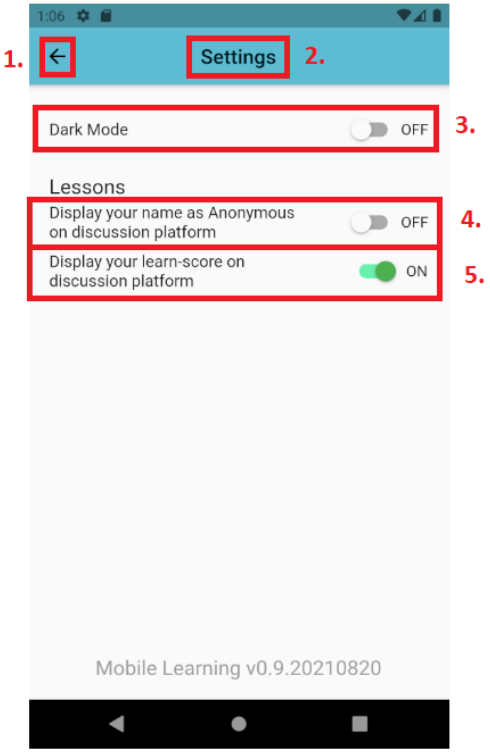


Fig. 7: Communication channel with marked UI elements

Shown in Fig. 7 is the settings screen, which enables the user to set anonymity settings as well as switch the visual theme of the application to a darker style.

The UI elements in the settings screen are:

1. Back Button:
   Navigates back to the previous screen.
2. Screen Title
3. Dark Mode Setting
   Switches Dark Mode setting on or off.
4. Name Anonymity Setting
   Switches name anonymity setting on or off.
   If set to On, the user's name will show up as 'Anonymous' in the communication channel.
5. Learn-Score Anonymity Setting
   Switches learn-score anonymity setting on or off.
   If set to Off, the user's learn-score will not be shown in the communication channel.

Comments User Interface

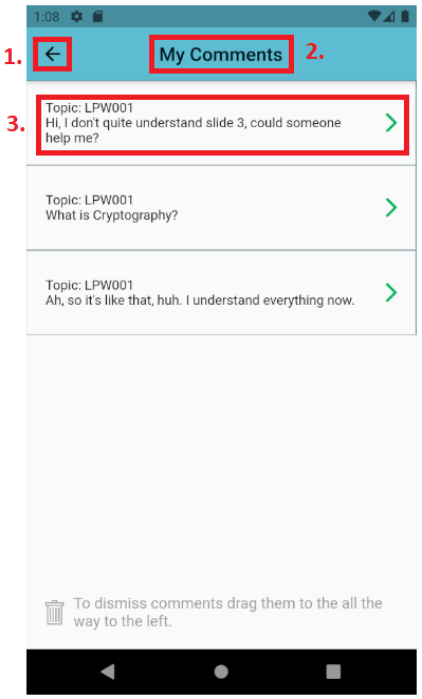


Fig. 8: Communication channel with marked UI elements

Shown in Fig. 8 is the comments screen, allowing the user to revisit the comments they posted in the various communication channels.

The UI elements in the comments screen are:

1. Back Button:
   Navigates back to the previous screen.
2. Screen Title
3. Comment
   A single comment that was sent in a communication channel. In this example, the comment was sent in the communication channel for the lesson with ID ‘LPW001’.

4.2.3 Lessons

Design and Creation Workflow

As mentioned in chapter 3.2.1, appropriate data structures needed to be chosen such that content creation would be as simple as possible, while allowing various media such as text, images and videos to be used. The application must be able to display the content accurately and the data structures have to be able to provide metadata e.g. lesson IDs, titles, etc. to save and display in the application.
The solution and workflow has been developed in cooperation with the University of Education Freiburg.

Aside from the set of lesson examples developed during the span of this project, the majority of the learning content will be created by experts of learning processes in cooperation with cyber security experts in the future. During the project, different solutions have been analysed. In a first iteration, a self-provided data structure was considered.
However, a custom data structure was perceived as too difficult, as learning a new data structure can be demanding, especially if the content creator does not have much programming experience.

This is solved by providing a simpler, more familiar solution in the form of the hypertext markup language (HTML) which also enables non-developers to easily provide lesson content in a structured form. Using HTML for the lesson content, a content provider can verify the intended structure through the use of a variety of editors and web browsers. The HTML editor BlueGriffon was particularly chosen for this workflow, since it offers a dual view where both the editor and the resulting page can be displayed and edited simultaneously.

Lessons therefore consist of multiple HTML files that represent the slides of a lesson, which the user can swipe through. In the application, the HTML files are hosted on a local server that is created on startup. The HTML files are then displayed using an internal web browser, which enables the use of CSS styling.

Lesson Folder Structure

The folder structure was designed such that a category directory is at the top level and its lessons are subdirectories. A lesson also contains multiple subdirectories according to the amount of supported languages. This allows a lesson to be available in multiple languages, with variations in content if necessary, as shown in Fig. 9.

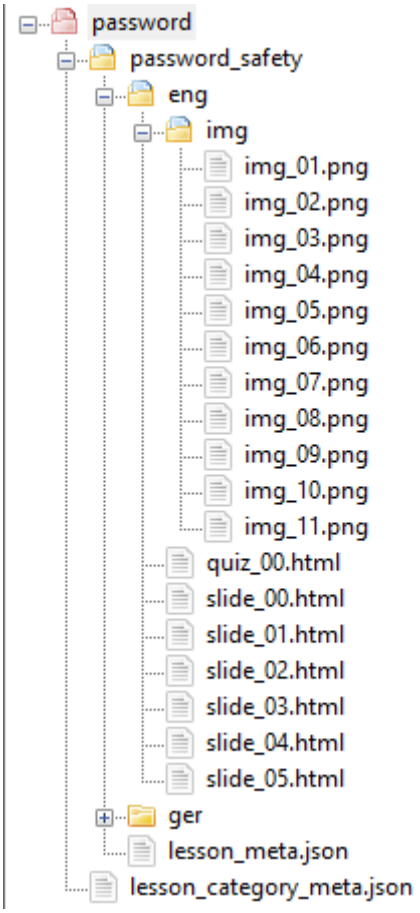


Fig. 9: data structure of a lesson

Lesson Category Metadata

Lessons each belong to an overarching category, e.g. a category “Passwords”, whose lessons focus on that particular subject. An example of a lesson category metadata JSON file is shown in Fig. 10.

```
{
  "lessonCategoryId": "CID001",
  "title": {
    "eng":"Passwords",
    "ger":"Passwörter"
  }
}
```

Fig. 10: structure of lesson category

Lesson Metadata

Lesson metadata is stored in JSON format due to its simplicity and its wide support.
It contains various general metadata about the lesson, which the application needs to save and display them during the lesson selection process. Using the data in this and the lesson category metadata objects, the application can display the various selectable categories and load the appropriate lessons once the category is selected. An example of such a lesson metadata file is shown in Fig. 11.

```
{
  "lessonId": "LPW001",
  "lessonCategoryId": "CID001",
  "title": {
    "eng": "Password Safety",
    "ger": "Passwortsicherheit"
  },
  "motivation": {
    "eng": "Improve your password security!",
    "ger": "Verbessere deine Passwortsicherheit!"
  },
  "duration": 3,
  "difficulty": 0,
  "hasQuiz": true
}
```


Fig. 11: structure of lesson metadata

Example Lesson Content

In this project a basic set of learning content was provided for the prototype itself to be able to be validated. The first lesson content for the "Password Safety" lesson was produced using various papers on the subject, so that the content itself is also based on the existing literature. Papers used for the first lesson were:

[Taha, 2013] On Password Strength Measurements: Password Entropy and Password Quality
[Komanduri, 2011] Of Passwords and People: Measuring the Effect of Password-Composition Policies
[Luevanos, 2017] Analysis on the Security and Use of Password Managers

4.2.4 Communication Channel

Design approach

As described in chapter 3.2.2, the communication channel for each lesson appears similar to well-known instant messaging applications to give the user a sense of familiarity in terms of its usage and to allow for a similarly quick interaction.

In the communication channel, the learner can write simple text messages to ask questions or discuss material that was not fully understood or problems with a task. They can also use images to illustrate the specific parts that were not understood or the problems encountered.
Cyber security experts and other learners can then respond using the same tools to offer guidance in the form of text and images to them as well.

4.2.5 MVC Design Pattern

Model View Controller (MVC) was used to get a separation of the business logic inside the application. This not only makes each individual file smaller and better to read as the different parts of the model, the view and the controller are separated but is also the de-facto standard of many complex software systems nowadays. [Gamma et. al, 2004]
This enables and improves the further development of GEIGER Mobile Learning in the future.

4.2.6 Communications Service

For the communication channel in the application, there was no existing infrastructure in place. A SwitchEngine server running Ubuntu Focal 20.04 was used to implement a server that can act as a central storage for the communication channels.
The server application and its REST API were implemented using Node.js, with a MongoDB serving as the database.
In the following part, the relevant aspects of the server application will be described.

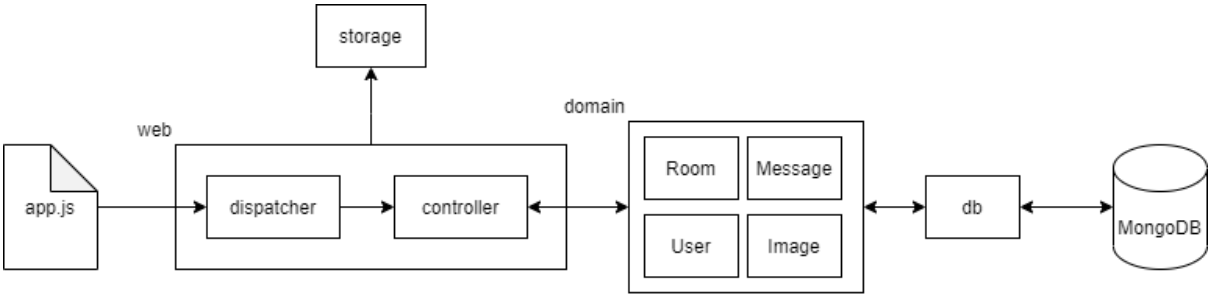


Fig. 12: communications server application schema

Package or File	Description
app.js	entrypoint for the application, where the middleware is loaded and the main route for the REST API is defined.
web	contains the dispatcher class which defines the REST API, as well as the controller class, which defines the functions called when a REST endpoint is accessed.
storage	contains functionality to upload images and store them locally.
domain	contains the domain model schemas used for the MongoDB, e.g. the User, Room, etc. models
db	contains the database handler, which uses the mongoose package to create the connection to the MongoDB and interact with it.
.env.defaults	file which contains default values that are loaded into the process.env variable on startup, e.g. the port for the server application and MongoDB host and database name.

Table 1: communications server application architecture

REST API

The REST API is accessible via the route /geiger-edu-chat. The various used endpoints are now described in the following table:

Endpoint	HTTP Method	Description
/users	POST	create user
/users/:userId	GET	get user
/users/:userId	PUT	update user
/users/:userId/messages	GET	get messages posted by user
/rooms/:roomId/messages	GET	get messages posted in a room
/rooms/:roomId/messages	POST	post message in room
/rooms/:roomId/images	POST	post image in room
/images/:imageId	GET	get image
/messages/:messageId	DELETE	delete message

Table 2: communications server REST API

xAPI

xAPI is a data structure that helps keeping track of a person's learning progress and learning behaviour. It was initially planned for GEIGER Mobile Learning to include and create xAPI-Statements. Due to time constraints and the GEIGER Toolbox being in development throughout the project, xAPI was only partially implemented. The Database structure to create xAPI elements is in place on the application although due to prioritisation not on the server thus the whole xAPI element has to be seen as not fully implemented.

MongoDB Schemas

In the MongoDB database, the users, discussion rooms, messages and images are stored. Model schemas were created and used in the server application to store and retrieve the objects.

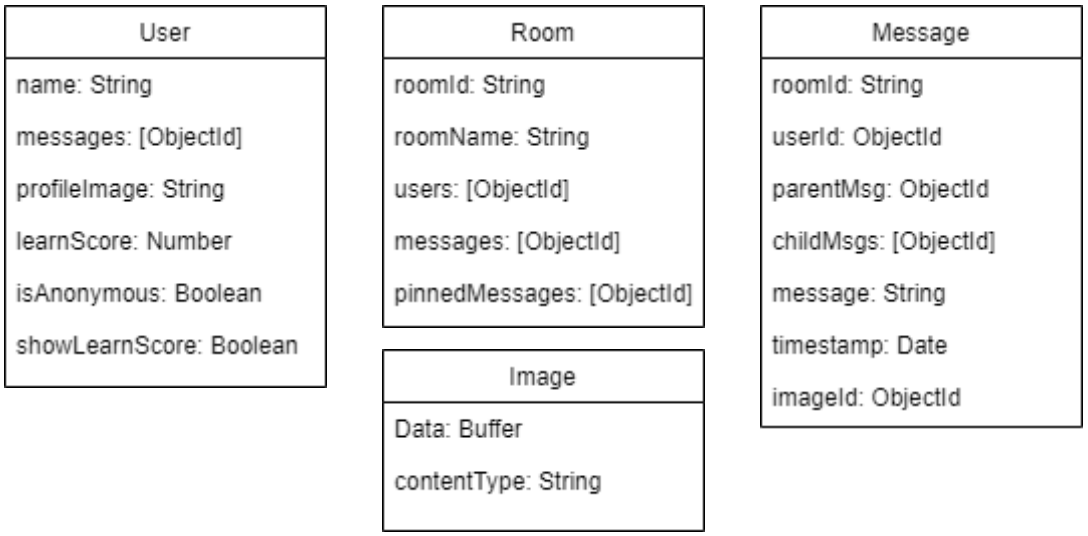


Fig. 13: MongoDB Schemas

User Authentification

When a user first engages with the GEIGER EDU server through the application, he is provided a unique identifier that enables an authentication process and user validation without the user having to create and maintain a login. This identifier is then saved locally on the user's device and used when a user sends / receives messages from / to a specific channel or modifies his userdata.

This authentication process increases the user experience and ensures that a user can only manipulate his own data.

4.2.7 Local Storage

Hive uses a key-value approach to store the data inside of so-called predefined boxes deriving their values from a plugin generated model class that itself points to the values defined in individual mvc-models. The different boxes that GEIGER mobile learning uses can be seen in the following database model:

Box	**Description**
userBox	Box containing all the user data Saves the user_ID received from the server upon first registration. Enables user authentication with the server.
settingsBox	Box containing all the app settings that a user can manipulate
commentBox	Box containing all the comments All messages received from the server are loaded in this box
lessonBox	Box containing all the lesson metadata received from the local JSON files
lessonCategoryBox	Box containing all the lesson categories To access the path of the lesson categories, so that the category data doesn't have to be loaded each time through the local JSON files

Table 3: HiveDB architecture

userBox	
key	**value**
default	User

settingBox	
key	**value**
default	Setting

commentBox	
key	**value**
comment_ID	Comment
. . .	. . .

lessonBox	
key	**value**
lesson_ID	Lesson
. . .	. . .

lessonCategoryBox	
key	**value**
lessonCategory_ID	LessonCategory
. . .	. . .

Fig. 14: NoSQL HiveDB Schemas

4.2.8 GetX

In this project, based on the recommendation of GEIGER software engineers that are familiar with Flutter, the plugin GetX[3] was used for easier state management and internationalisation support.

State Management
Flutter tends to use state to allow visual elements in the application to react and change according to user input. Programming these interactions can be a difficult process, as changes to values need to be reacted to immediately as they happen. GetX allows the simple decoupling of state from the visual elements.

Internationalisation
GetX was also used to implement internationalisation for the supported languages of English and German. The language is detected on startup of the application, according to the device's language settings. Using this setting, the lessons with the appropriate language are also selected. For the translations a key-value store is used.

[3] https://pub.dev/packages/get

4.3 4+1 Architectural View Model

Logical View

The following sequence diagram in Fig. 15 visualises the user interaction with the system when completing a lesson:

A user continues his lesson.
The user navigates through all slides.
The user receives the quiz that validates his knowledge.
The user successfully completes the quiz and his new lesson score gets added.
The user finishes the lesson.

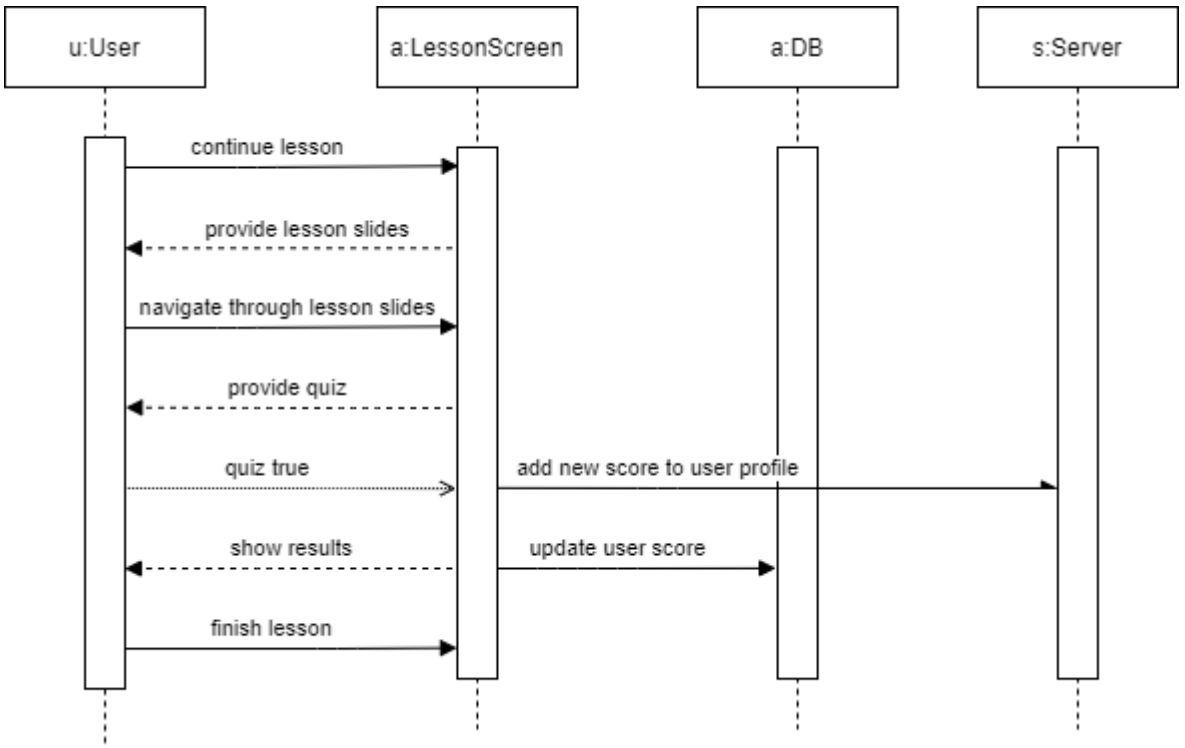


Fig. 15: Logical View for lesson completion process

Fig. 16 shows the logical view of the user interaction with the semi-structured communication channel:

A user opens the lesson screen and then the corresponding chat channel.
The user sees all the messages and sends a message himself.
The user deletes his message.

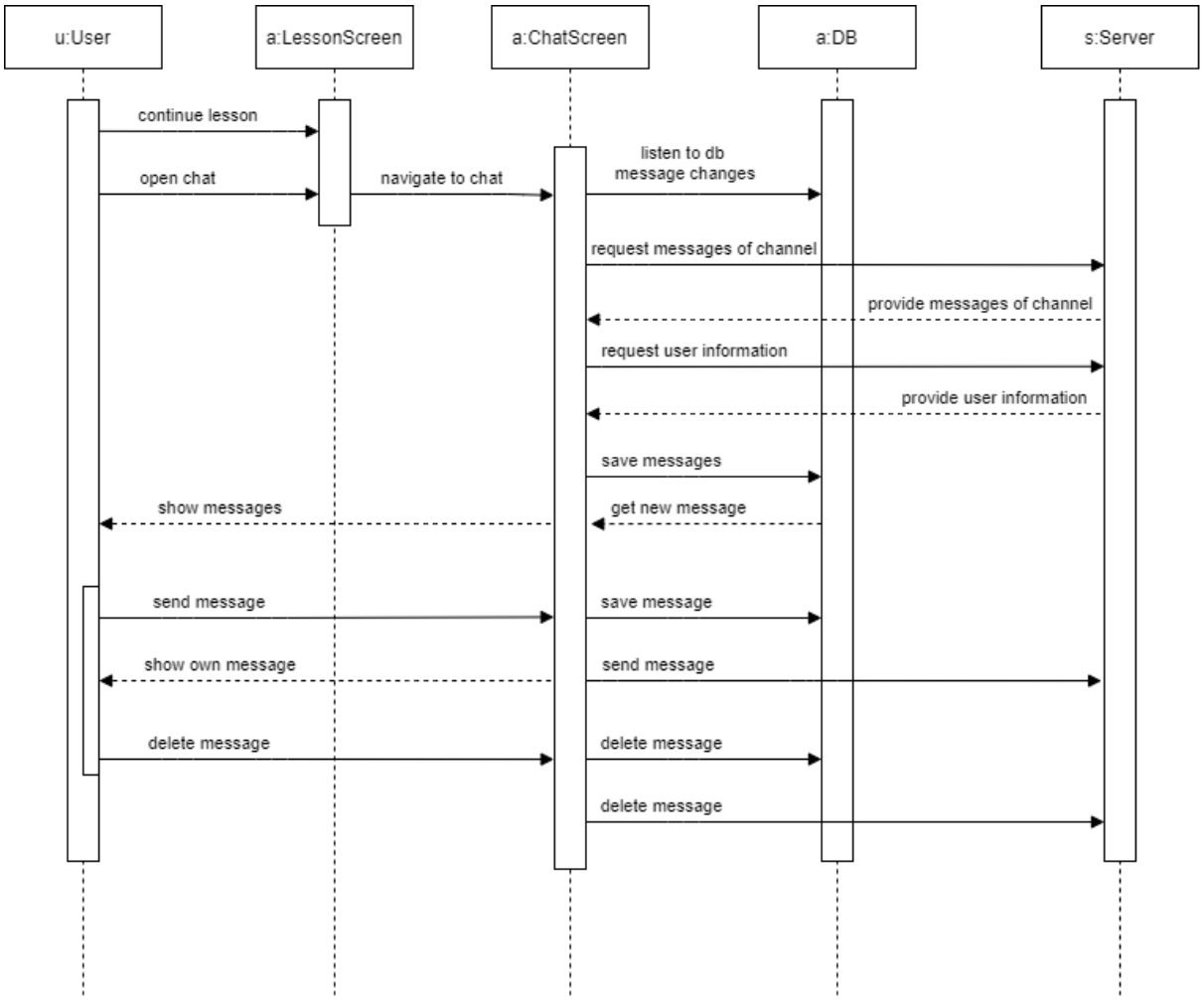


Fig. 16: Logical View

Process View

On application start, the database and local lesson server are sequentially initialised or loaded.

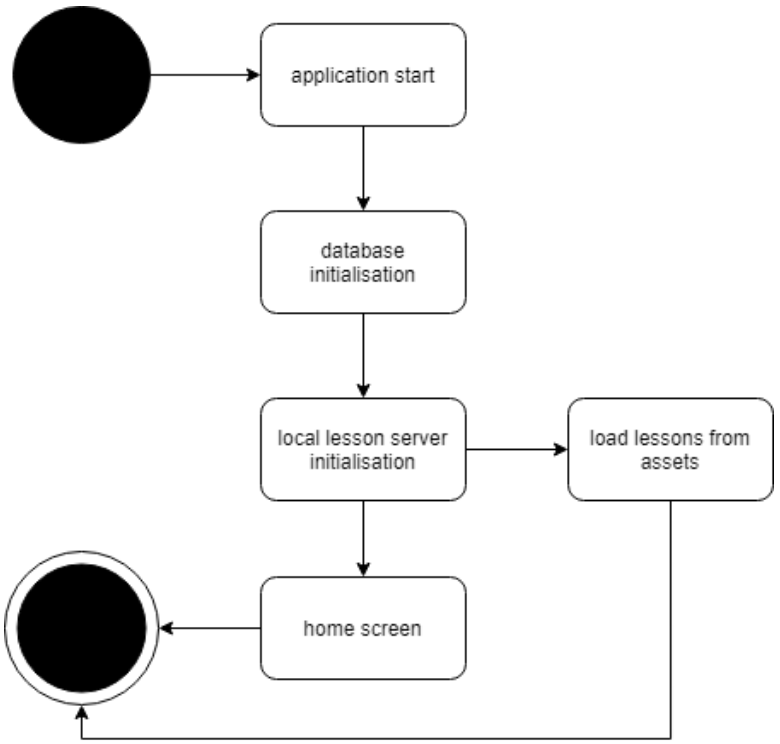


Fig. 17: Process View - Application start

On entering a communication channel the server is called and the messages are received synchronously.

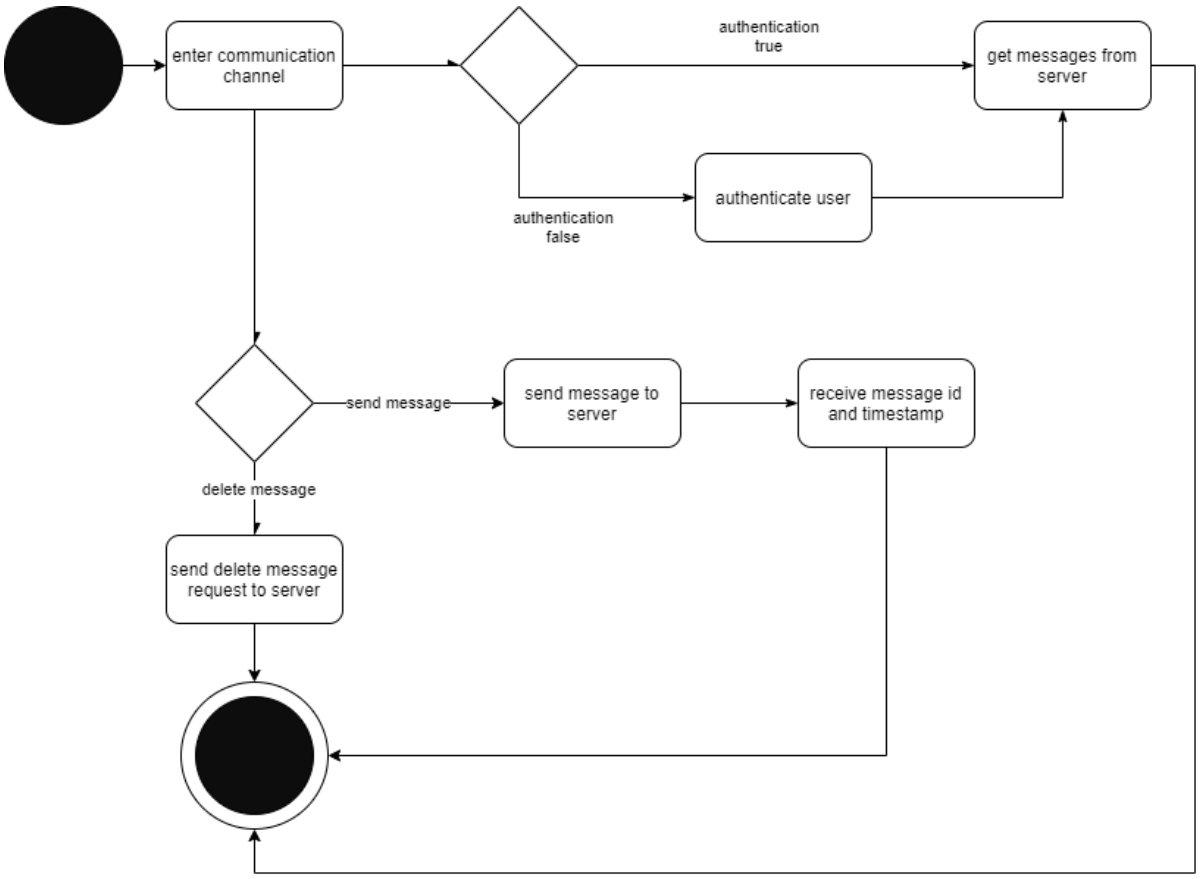


Fig. 18: Process View - Communication channel interactions

The following diagram shows an example on how data is persisted to the local database and the server accordingly.

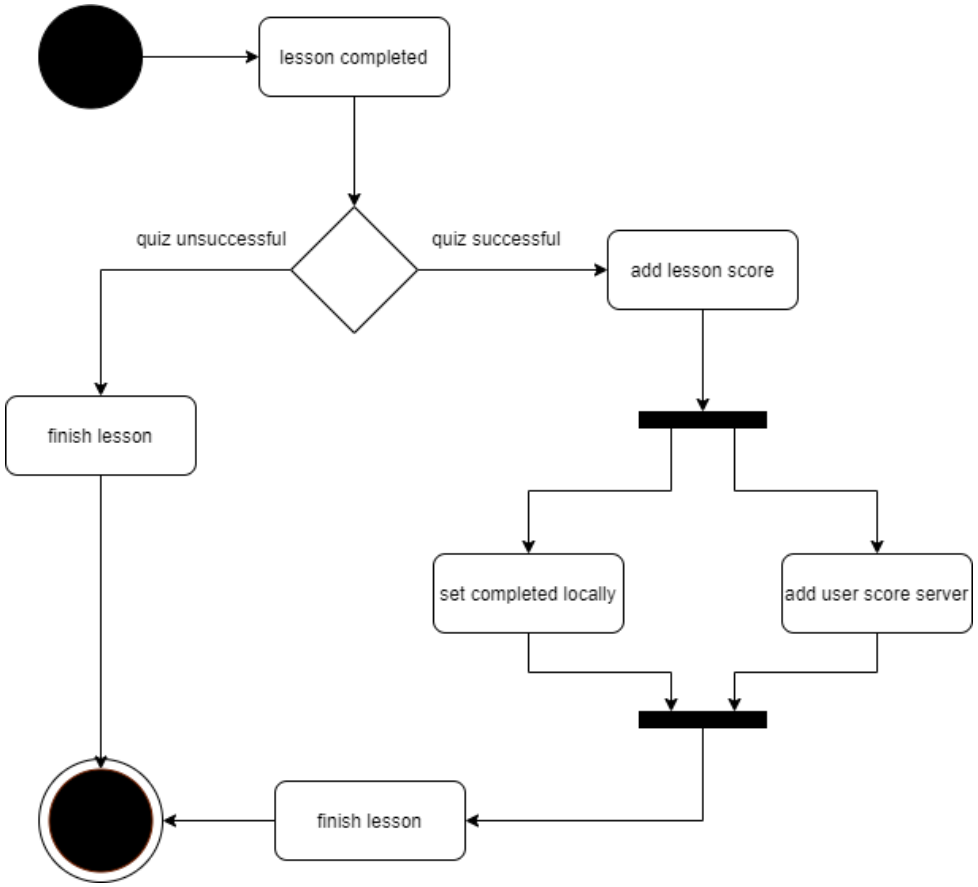


Fig. 19: Process View - Lesson completion

Development View

Flutter application structure:

Name	Type	Description
assets	package	contains assets used in the application, such as custom icons and lesson data
pubspec.yaml	configuration file	defines the project and the dependencies used by it, as well as the assets that are packaged with it
lib	package	contains all packages with the application classes
controller	package	contains classes that handle state and functionality for various parts of the app
model	package	contains model classes for the app, which can be saved to the Hive database and possess functions for the conversion to and from JSON for network transfer
providers	package	contains classes that only provide data and do not manipulate them.
screens	package	contains Flutter widget classes that define the screens which are navigated to and from during use of the application
services	package	contains calls that can provide data and manipulate them.
widgets	package	contains custom, reusable widgets for use in screen classes
main.dart	class file	entrypoint for the application, starts database and local server, creates controller instances, sets locale and language and initialises necessary values
route_generator.dart	class file	provides routes to each screen for simple navigation between screens across the application

Physical View

In this section the deployment view of the application and its communication server are displayed. It displays the different software components on their respective physical plane.

Device: Smartphone
Description: On the end user device the app and the HiveDB are deployed accordingly

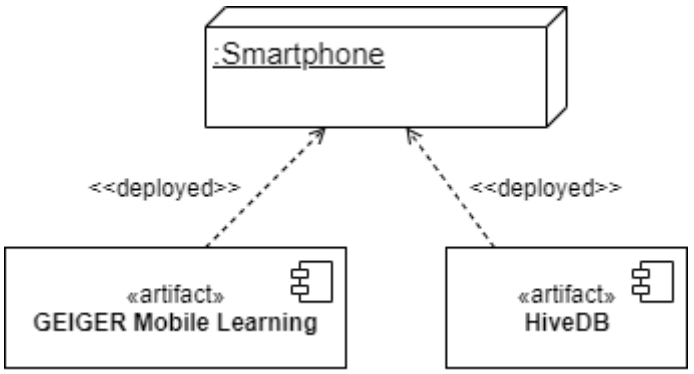


Fig. 20: Physical View for smartphone

Device: Communications Server
Description: For the communications server we use Node.js and Express in combination to form the backbone and the logic of the server. With MongoDB we have a fast NoSQL Database that works in conjunction with Node and Express accordingly.

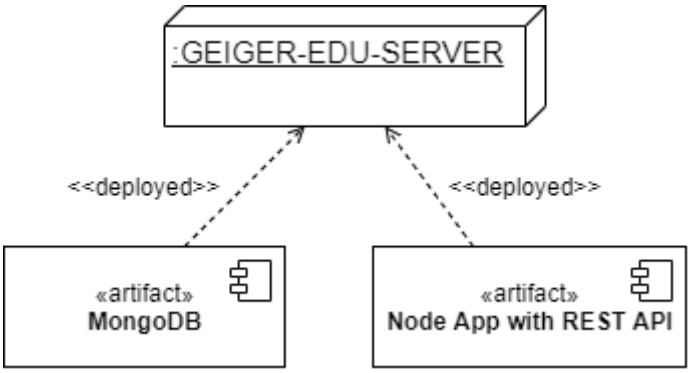


Fig. 21: Physical View for communications server

Scenarios

In this section the different use cases of the application are described using the UML standardisation.

System: Learning system
Type: Subsystem
Description: This use case describes the user interaction with the learning system.
Taking lessons and interacting with others, showing the structured lessons in combination with the semi-structured communication approach.

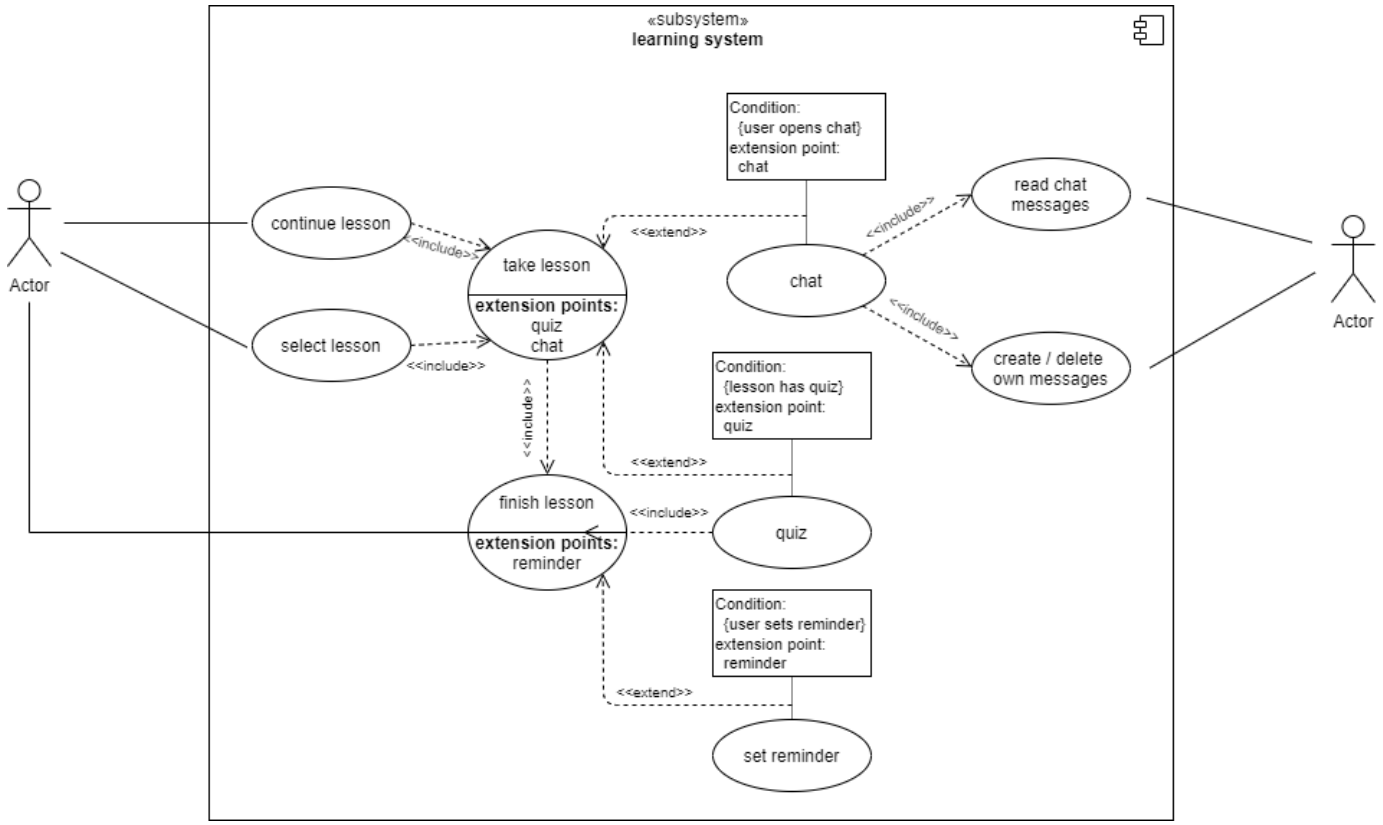


Fig. 22: Scenario for learning system

System: Comments system
Type: Subsystem
Description: This use case describes the user interaction with his previously posted comment using the comment management system of the application. Deleting comments and directly jumping back to the chat to see responses and continue the half-structured learning interaction.

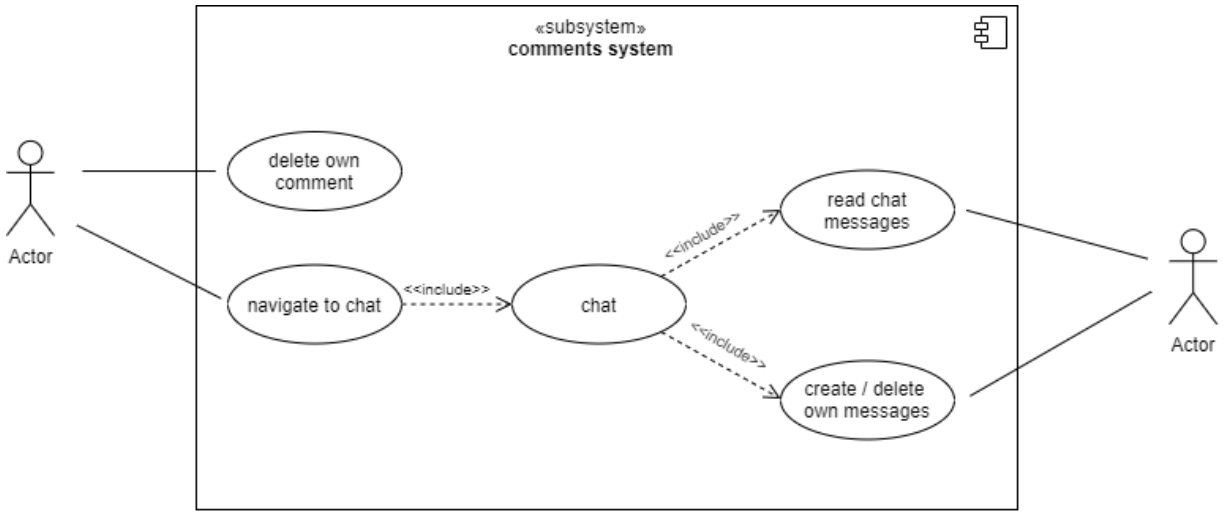


Fig. 23: Scenario for comments system

System: Profile system
Type: Subsystem
Description: This use case describes the user interaction with his profile data.

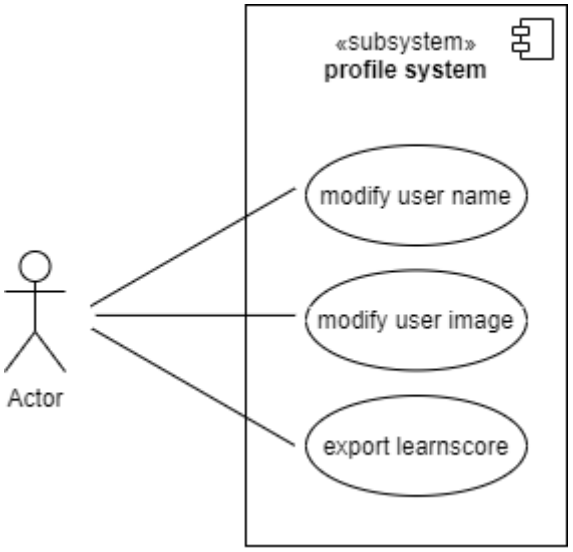


Fig. 24: Scenario for profile system

System: Settings system
Type: Subsystem
Description: This use case describes the user interaction with his application setting. Changing anonymity settings that can be relevant for the half-structured communication interaction and making changes to the application theme

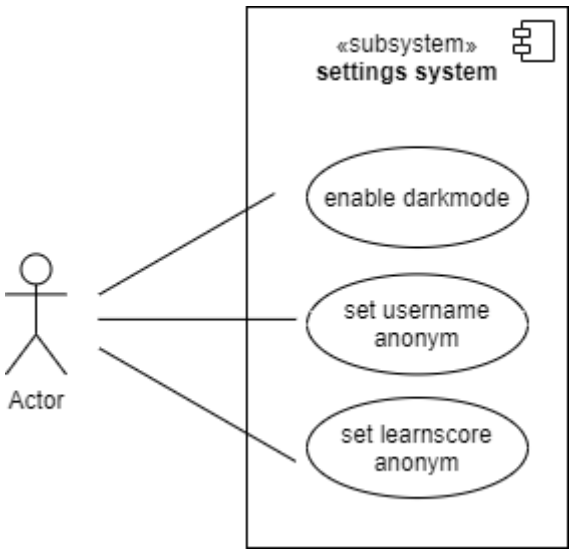


Fig. 25: Scenario for settings system

4.4 Summary

Evaluation of the different frameworks has shown that Flutter was the best approach for a prototype driven cross-platform development that mandates a fast development cycle and has multiple iteration phases. The concept as seen in chapter 3 was realised using this technology.
Through the use of various plugins, development speed was increased. A simple but effective state management solution was found in the GetX plugin, which also enabled the implementation of internationalisation, with the two languages German and English being supported as of the date of this paper.

The styling of the application was inspired by the designs for the GEIGER Toolbox to create a familiar feel over a multitude of related applications. The structural design was developed using the user feedback generated through user interviews and user tests.

The application itself uses the MVC pattern to allow for better flexibility and easier future extension.

A responsive local storage solution for user and lesson data was achieved using the NoSQL key-value-based database Hive, which integrates well into the overall framework of Flutter.

An initial set of lessons was created for the project while the workflow for lesson creation was designed. This workflow was developed in cooperation with the University of Education Freiburg to enable pedagogues and professionals in education and cyber security to be able to easily produce learning content that can be seamlessly integrated into the application as they are created.

Different existing communication solutions were analysed, but none of them proved to be a perfect match for the concept of GEIGER Mobile Learning to be realised. A custom user interface for the communication channel was thus developed, inspired by instant messaging applications such as Telegram and WhatsApp, allowing normal text messages and images to be sent by learners and experts, allowing learners to ask questions and discuss with other learners and expects.
Because the GEIGER Toolbox was also in development during this project, a custom backend solution was developed to store the data for the communication channels, namely the GEIGER EDU server, which was realised using the common tools Node.js, Express and MongoDB from the MEAN stack. In the future, it is possible that the GEIGER Toolbox storage infrastructure could handle this task instead.

5. Validation

5.1 Validation Process

Cyber security knowledge and software usage data
Early on, user data was collected through the use of a Google Forms questionnaire. This helped to gain a fundamental understanding on the uses of different technology channels in the target group.
In the questionnaire, various questions about learning behaviours, interaction with various applications and the use of communication channels were inquired, among others. The initial testing took the form of an online questionnaire which was shared with the students of the Berufsfachschule BBB and participating KMUs.

The results from this questionnaire showed that instant messaging applications like WhatsApp, Telegram, Signal and Threema are especially popular.
As for learning behaviours, the time spent learning at a time is evenly varied, 33% of interviewees tend to learn from 10 to 30 minutes or over an hour at a time, with 22% of people learning between 30 minutes to an hour.
100% of interviewees like to use online articles to learn new concepts, while 50% also like to use books and YouTube videos. 10% have also said that they like using the platforms Coursera, research articles, eBooks and O'Reilly Media and learning platforms such as Kaggle and Datacamp.
90% of interviewees prefer to learn alone, while 10% like to learn in pairs.
The most used Q&A platforms and forums are Reddit and StackOverflow.

Usability Tests
Over the course of the entire project user feedback was continuously obtained and used to inform the user experience.
First tests were conducted using a click-dummy created with Figma and had, due to the pandemic, been conducted remotely. Valuable feedback could be gathered during these first tests and improvements were made. These first user tests helped to validate the concept and further enhance the usability, so that development of a real prototype could begin.

Process of the usability tests
These user tests were conducted using a qualitative instead of a quantitative empirical approach, meaning that the focus during each of the tests was on meaningful user feedback and less on numerical data. During the multiple iterations of the prototype, users were guided by us through a story, the intention of the application and its aim were described and then tasks were assigned. Tasks included the completion of a lesson, asking a question in the communication channel, based around the story of a team learning together and discussing their learning progress at work. After each task all the traversed screens were discussed and feedback about the experience gathered. The results of these tests were then analyzed and measures to improve the solution were incorporated in the next iteration.

After these initial click-dummy tests, a first prototype was created. As the process used in the first iteration has shown insightful results the same process of user tests was reapplied

with the deviation that the tests were conducted physically in person under health security measures according to the BAG (Bundesamt für Gesundheit) recommendations.

Result of the usability tests

The results of these tests varied from integration of new elements to the prototype to changing navigation elements and rearranging UI elements in general to provide a more complete experience.

Some of these changes involve incorporating a motivational note at the start of each lesson, helping a user to see the aim of the lesson before stating it. Having a learning progress indicator on the main screen was found to be motivating for users, as they would want to see their progress increase. This feature, as well as a scoring feature provide a gamification aspect for the application and further increase the user interaction as described in chapter 2 .6.4 of this report.

5.2 Results

The usability tests showed us that users are able to use countermeasures against cyber security threats, according to their personal situation, after they completed a lesson accordingly. Not only could we validate that users understand the lesson content through the use of a quiz at the end of each lesson but as we used a task driven approach we were able to verify that a user is encouraged and capable of applying measures accordingly.

Prototype tests in person enabled us to see the user interaction with the application, and find uncertainties that arose when using different features of the application. Find, counter bugs and see the overall interaction not only with the application but also the physical device itself.

These prototypes enabled us further to verify the dialog between learners and experts. The use of the half structured communication approach was a success. In that it not only gives a user the freedom of structuring their experience themselves but also motivates through it being similar to frequently used chat applications, which further takes away anxiety from the user as the process of asking questions is familiar. This communication approach also showed the users need for anonymity if so desired.

Over the different iterations of the application it was seen that the user capability of working independently of a practical learning sequence was a success and users were motivated to not only complete learning sequences but also share their progress with their peers. In first iterations this was not the case as a user did not see the motivation to e.g. complete the password security lesson which prompted the integration of a motivation sentence at the start of each lesson.

5.3 Summary

Validation Process
Two main forms of user driven validation were used, initial empirical testing that provided a foundation for the initial click dummies and secondly remote user tests on the click dummy and physical tests with the users that further showed the device interaction. This second form of testing provided valuable information which was analysed, rated and iteratively incorporated in next generations of the prototype.

Results
The application proved to be accurately targeting people working in KMU with a small repertoire of information technology knowledge. This was verified through the questionnaire at the end of each lesson which was successfully completed by the test participants. After completing a learning sequence, the test subject was asked to apply the learned measures, which was shown to be successful.

6. Discussion

6.1 Success of Solution

With regards to the initial situation seen in chapter 1.1 it can be said that GEIGER Mobile Learning has shown to help users like Loredana to foster their knowledge about cybersecurity. With GEIGER Mobile Learning planning to release as an open source application costly and time consuming lessons in physical form ought to be a thing of the past. Having chosen a framework that allows multi-platform usage for the implementation of GEIGER mobile learning it enables a brought audience of smartphone users to partake in lessons independent of time, date and location. Furthermore helps the use of different learning channels, concepts and on top of that the use of gamification as a motivation to fully engage with the product.

6.2 Proof of Concept

As seen over the course of this document the proof of concept explained in chapter 1 could successfully be proven to work. The initial concept could not completely be realised as several parts of its proposition were not available, namely the GEIGER Toolbox itself. Regarding this matter a own substitution for this problem has been developed by us namely the GEIGER EDU Server. Simulating the interaction between an external system it validated that the concept is working. The lerneffekt could be validated through the user and even better right inside the application through the use of a quiz at the end of each lesson that validates the user's progress. This was also validated through the different usability tests as shown in chapter 5.1 and 5.2. The product is able to motivate user participation, although it has to be stated that long term studies could not be conducted as the project's duration does not allow for it.

6.3 Evaluation of Solution

GEIGER Mobile Learning was able to fill in the gap mentioned in chapter 2.7.
focus cyber, as it now provides a mobile application that has a strict focus and restriction to the whole domain of cybersecurity. Including a communication format that encourages participation through familiarity and that also enables cybersecurity experts to partake and support users of the application. As seen in chapter 5.2 the contribution of GEIGER Mobile Learning is a meaningful one with regards to the aforementioned problem statement.

6.4 Revelations of the Results and Future Steps

As our results have shown in chapter 5.2, the proof of concept was successful, meaning that the interoperability of a learning platform and a semi-structured communication approach provided an added benefit to non-tech-savvy users.

To further the developed application and iterate upon the findings and the whole of the concept we propose the following next steps in improving upon the final product of this thesis with the goal of making it production ready and marketable:

Content Production
As mentioned in section 4.2.2 the content production workflow, although validated to a certain extent, has to be further analysed and verified in a production environment.
It is recommended to base the learning content not only on personal knowledge but rather consolidate different papers as we did it for our set of example lessons. On the application side of things the possible implementation of multiple choice questions has to be accessed.

Traffic Encryption
The developed messaging system and overall interaction with the backend server is not encrypted as it was out of scope for this proof of concept. With encryption cyber security can not only be taught through the application but also practiced by it.

Platform-specific UI elements
As application navigation is different on the different platforms specific navigation elements can further improve the user experience.

Further Validation
We recommend further validating the user interaction with the semi-structured communication channel in combination with the learning experience and its effect on it. This especially in a scaled up production environment, where multiple users interact at the same time.

Backend Integration / GEIGER Toolbox
Backend Integration would be another vital part in making a complete ecosystem. As mentioned in chapter 4.2 the GEIGER Toolbox was itself in the early stages of development and thus our own backend had to be provisionally created. This step then opens the possibility to recommend lessons to a user, track progress (xAPI) and safety level resulting from learning progress and other factors (current threats, etc.).

Publish the Application
To finalise the application and enable production environment testing a publication to the different platform stores, e.g. Google Play Store and Apple Store, is recommended.

General Improvements
Last but not least some general improvements with focus on user experience are recommended, as user experience was not a focus during the project.
Implementing different quality of life features would finally round up the application, e.g. pinning messages to allow learners to refer back to previous given answers, editing messages, and the implementation of xAPI to track learning progress.

6.5 Summary

The proof of concept and its contribution to counter the problem statement seen in chapter 1.1 were a success. Through validation the proof of concept could be verified and it can after last improvements be marketable and as such fill the gap that we can see in today's market. The combination of the various features, different learning structures and the inclusion of experts, not only in the content production but also in the support of users through the communication platform revealed itself to be a triumph.

7. Summary and Conclusions

7.1 Summary of the Concept

Stakeholders
There are three main stakeholders in the project, namely the SME owner or employee which takes the role of a learner and is a content consumer, secondly the content producer which creates and provides the learn content and lastly the cyber security expert which is able to support learners over the semi-structured communication channel.

Proposed concept
The learner can take lessons, which are simple and short, linear learning experiences which can also have a quiz. Should they encounter difficulties in understanding the material, they can use the communication channel to ask other learners and cyber security experts questions, with the option to remain anonymous if they want to. By completing lessons and asking questions, a user can increase their knowledge about cyber security and better protect themselves and their business. Furthermore, gamification in the form of points rewards after completing a lesson offers another incentive to continue learning.
The learning content should be able to offer a diverse set of media to keep the learner engaged. Lessons will be created by a team of experts after initial development of the proof of concept. The application must therefore be able to integrate new lessons as they are added. To ensure efficiency, the content creation process should also be relatively simple.

7.2 Summary of the Software Architecture

Evaluation of the different frameworks has shown that Flutter was the best approach for a prototype driven cross-platform development that mandates a fast development cycle and has multiple iteration phases. The concept as seen in chapter 3 was realised using this technology.
Through the use of various plugins, development speed was increased. A simple but effective state management solution was found in the GetX plugin, which also enabled the implementation of internationalisation, with the two languages German and English being supported as of the date of this paper.

The styling of the application was inspired by the designs for the GEIGER Toolbox to create a familiar feel over a multitude of related applications. The structural design was developed using the user feedback generated through user interviews and user tests.

The application itself uses the MVC pattern to allow for better flexibility and easier future extension.

A responsive local storage solution for user and lesson data was achieved using the NoSQL key-value-based database Hive, which integrates well into the overall framework of Flutter.

An initial set of lessons was created for the project while the workflow for lesson creation was designed. This workflow was developed in cooperation with the University of Education Freiburg to enable pedagogues and professionals in education and cyber security to be able

to easily produce learning content that can be seamlessly integrated into the application as they are created.

Different existing communication solutions were analysed, but none of them proved to be a perfect match for the concept of GEIGER Mobile Learning to be realised. A custom user interface for the communication channel was thus developed, inspired by instant messaging applications such as Telegram and WhatsApp, allowing normal text messages and images to be sent by learners and experts, allowing learners to ask questions and discuss with other learners and expects.
Because the GEIGER Toolbox was also in development during this project, a custom backend solution was developed to store the data for the communication channels, namely the GEIGER EDU server, which was realised using the common tools Node.js, Express and MongoDB from the MEAN stack. In the future, it is possible that the GEIGER Toolbox storage infrastructure could handle this task instead.

7.3. Summary of the Validation

Validation Process
Two main forms of user driven validation were used, initial empirical testing that provided a foundation for the initial click dummies and secondly remote user tests on the click dummy and physical tests with the users that further showed the device interaction. This second form of testing provided valuable information which was analysed, rated and iteratively incorporated in next generations of the prototype.

Results
The application proved to be accurately targeting people working in KMU with a small repertoire of information technology knowledge. This was verified through the questionnaire at the end of each lesson which was successfully completed by the test participants. After completing a learning sequence, the test subject was asked to apply the learned measures, which was shown to be successful.

7.4. Summary of the Discussion

The proof of concept and its contribution to counter the problem statement seen in chapter 1.1 were a success. Through validation the proof of concept could be verified and it can after last improvements be marketable and as such fill the gap that we can see in today's market. The combination of the various features, different learning structures and the inclusion of experts, not only in the content production but also in the support of users through the communication platform revealed itself to be a triumph.

7.5. Conclusion

Cyber attacks continue to increase in frequency and severity for users and businesses alike. There is however a disconnect between what people are taught about cyber security, and how they live it. It has become apparent that there is a gap in cyber security education which needs to be considered, as conventional education methods are not affordable to many SMEs and they also do not produce the desired results.

Our work has shown that there is a way for SMEs to counter and mitigate these threats. A better understanding of how businesses and the people who work in them think and interact with IT systems is vital for cyber security education. Allowing people to collaborate and discuss cyber security matters using their own language can be much more conducive to furthering understanding than taking generic cyber security training.

GEIGER Mobile Learning thus combines various forms of learning experiences, namely a structured learning experience in the form of lessons and an semi-structured approach with the communication channels, where users interact with each other and experts to create an environment where collaborative learning is fostered.

With this project and prototype, a first step was taken in the direction of what near-future cyber security education could be, using the tried-and-true methods of other branches of education and the methods of the applications people use every day. Using this template, future work can explore further possibilities.

8. Bibliography

[Hsin-Yuan Huang, 2013] Wendy Hsin-Yuan Huang, Dilip Soman: A Practitioner's Guide To Gamification Of Education, 2013

[Newman, 2008] Richard S. Newman: The Motivational Role of Adaptive Help Seeking in Self-Regulated Learning, 2008

[Axelos, 2016] Bada, Maria, Angela M. Sasse, and Jason R. Nurse: Cyber Resilience: Are your people your most effective defence?, 2016

[Caldwell, 2016] Tracey Caldwell: Making security awareness training work, 2016

[Dark Reading, 2019] Dark Reading: More Than 99% of Cyberattacks Need Victims' Help, 2019

[Deloitte, 2018] Deloitte: "Smartphones are becoming the control centre of people's lives – only 8% of Swiss do not have one."

[Egelman, 2016] Egelman, Serge, Marian Harbach, and Eyal Peer: Behavior Ever Follows Intention?: A Validation of the Security Behavior Intentions Scale (SeBIS), 2016.

[Egelman, 2015] Egelman, Serge, and Eyal Peer: Scaling the Security Wall: Developing a Security Behavior Intentions Scale (SeBIS), 2015.

[ENISA, 2020] ENISA: List of top 15 threats, 2020.

[Gratian et al., 2017] Gratian, Margaret, Sruthi Bandi, Michel Cukier, Josiah Dykstra, and Amy Ginther: Correlating human traits and cyber security behavior intentions, 2017

[Moir, 2009] Moir, Robert: Defining Malware: FAQ, 2009

[Parsons et al., 2010] Parsons, Kathryn, Agata McCormac, Marcus Butavicius, and Lael Ferguson: Human Factors and Information Security: Individual, Culture and Security Environment, 2010

[Ramzan, 2010] Ramzan, Zulfikar: Phishing Attacks and Countermeasures, 2010

[Verizon, 2019] Verizon: 2019 Data Breach Investigations Report, 2019

[Cohn & Beck, 2004] Cohn, Mike, and Kent Beck: User Stories Applied: For Agile Software Development, 2004

[Gamma, 2004] Erich Gamma, Richard Helm, Ralph Johnson: Entwurfsmuster. Elemente wiederverwendbarer objektorientierter Software. 2. Auflage., 2004

9. Appendix

A1: Usability test template
A2: Quantitative Tests
A3: Figma

A.1 User-Test Template

GEIGER Mobile Learning - Begleiteter Usertest

User
Name:
Beruf:
Scenario:
Version:

Vorgang
Dem Benutzer wurde der Zweck der App erklärt. Der Ablauf war Task-Driven:

Task 1: Führe die erste Lektion zum Thema Passwortsicherheit durch
Task 2: Stelle eine Frage zum Thema Passwortsicherheit
Task 3: Lösche einen deiner Kommentare
Task 4: Ändere dein Profilbild
Task 5: Exportiere deinen Lernfortschritt

Feedback / Verbesserungsvorschläge

Dashboard:
-

Lektionsübersicht:
-

Lektions-Screens:
-

Diskussionsplattform:
-

Kommentarübersicht:
-

Profil:

-

Settings:

-

Task 1:

Task 2:

Task 3:

Task 4:

Task 5:

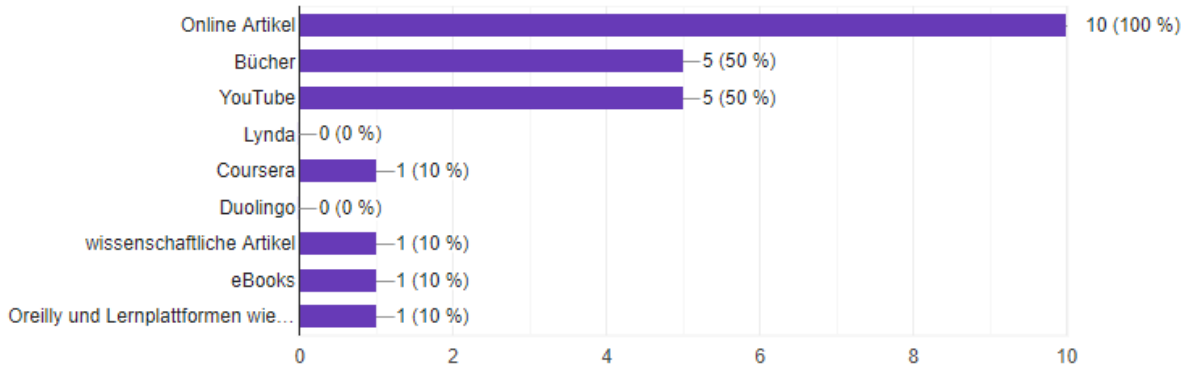
Schlussfolgerungen

-

A.2 Quantitative Tests: Google Forms Questionnaire

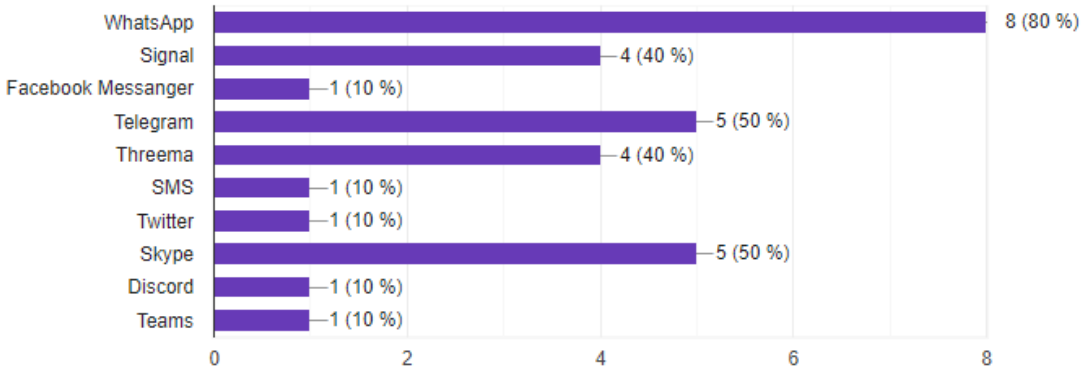
Wenn du etwas Neues lernen willst, welche digitale Plattform verwendest du?

10 Antworten



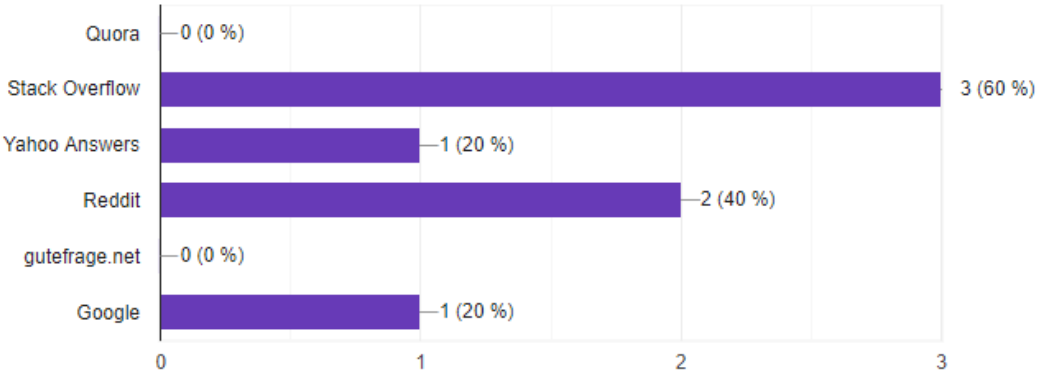
Mit welcher App kommunizierst du oft?

10 Antworten



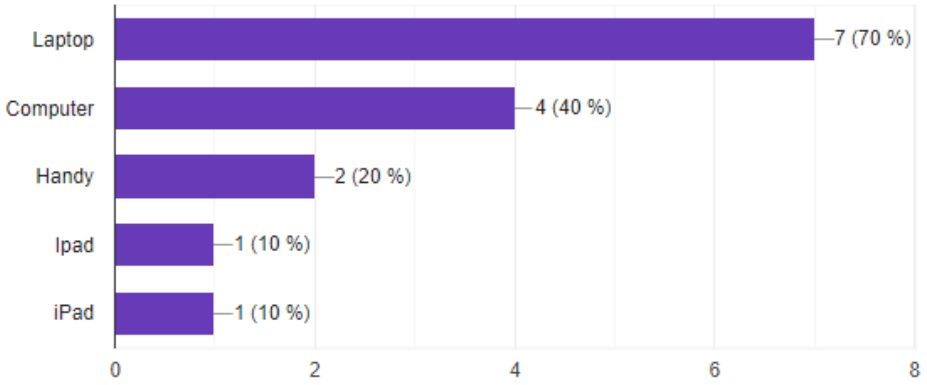
Hast du schon eine oder mehrere Frage/Antwort-Plattformen oder ein Forum verwendet? Wenn ja, welche?

5 Antworten



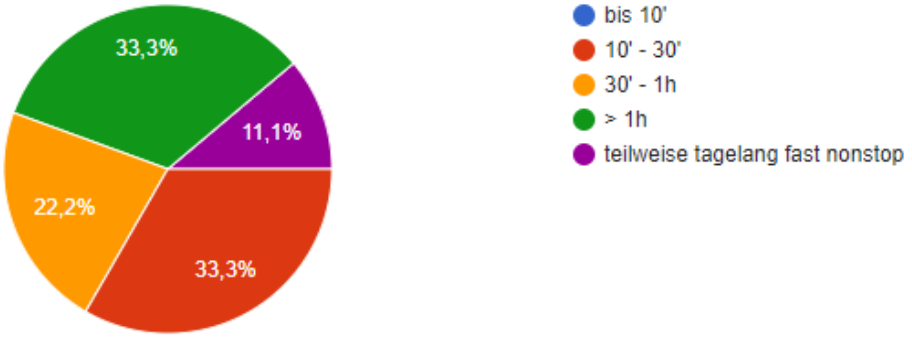
Mit welchem Gerät lernst du oft?

10 Antworten



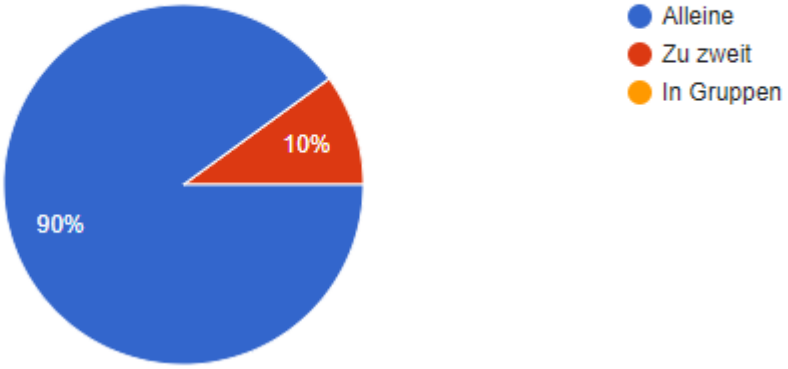
Wenn du etwas Neues lernst wie lange lernst du am Stück?

9 Antworten



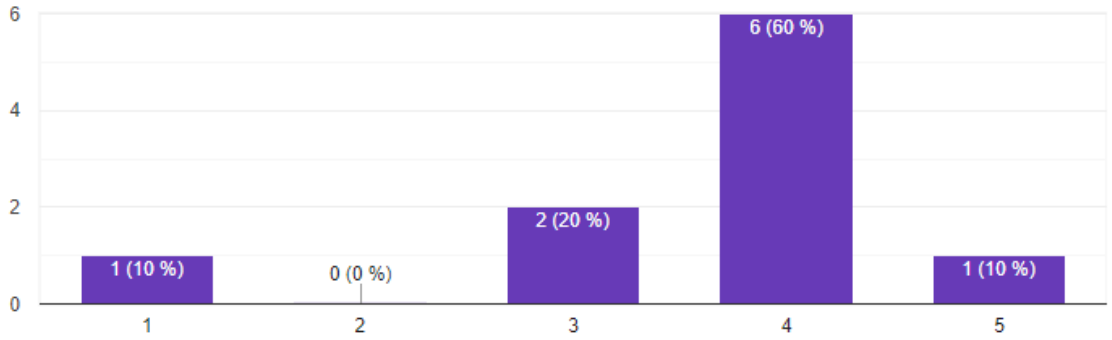
Wie lernst du am liebsten?

10 Antworten



Kennst du dich gut, bzw. befasst du dich mit deiner Sicherheit im Internet?

10 Antworten

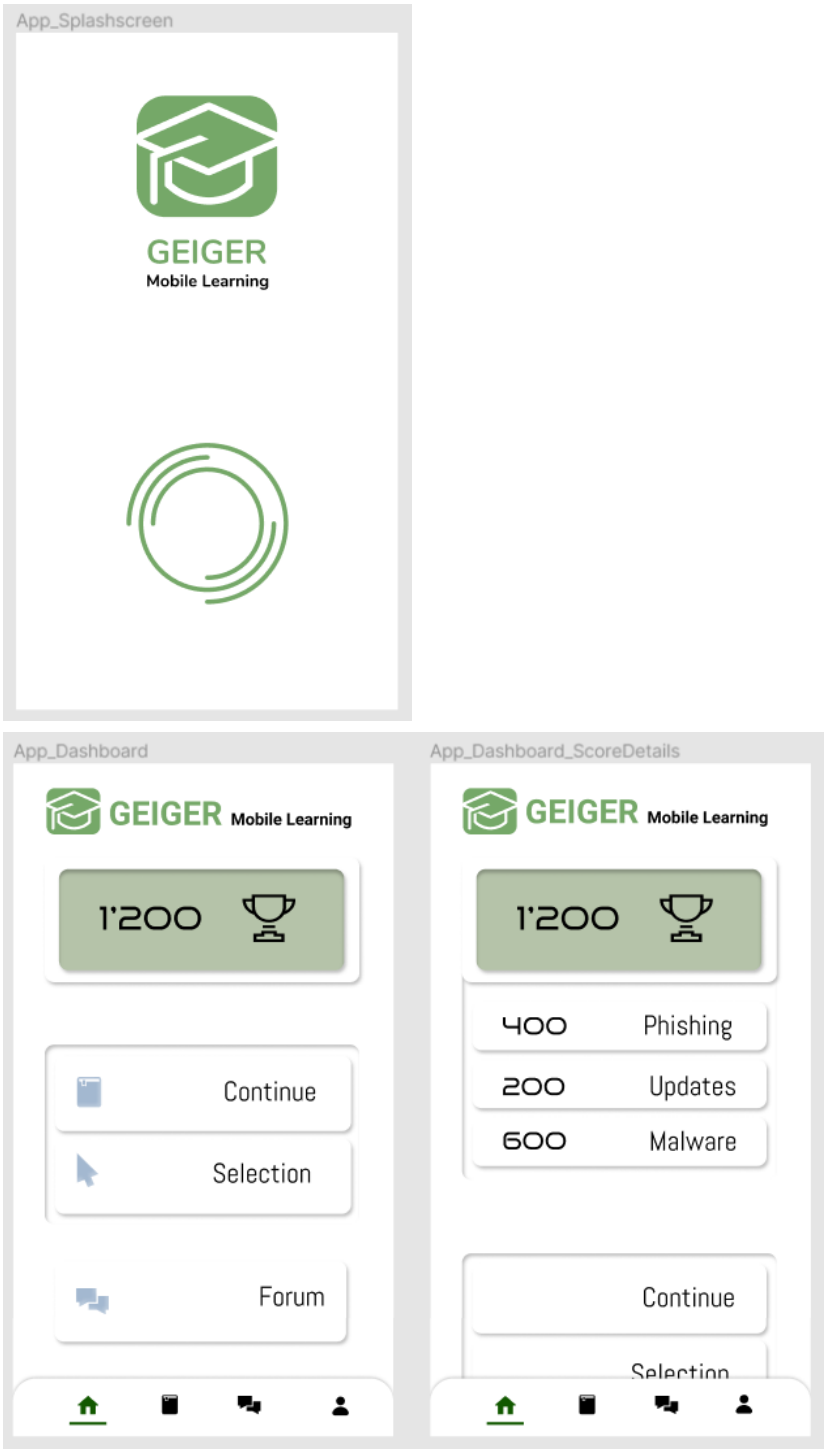


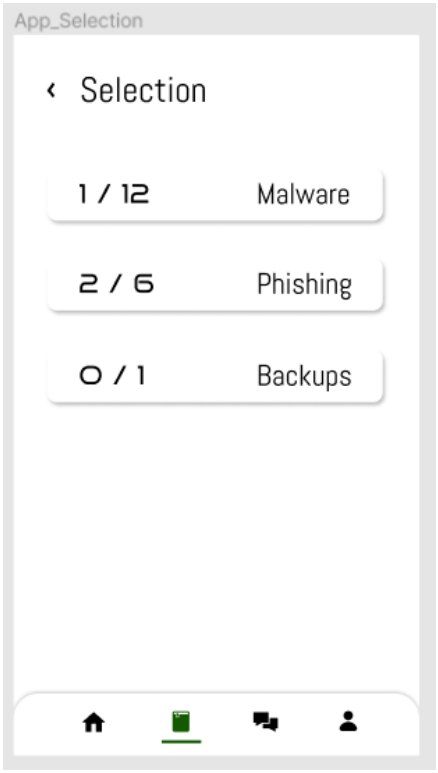
Sind Deine Antworten wahrheitsgetreu und können sie zur Analyse verwendet werden?

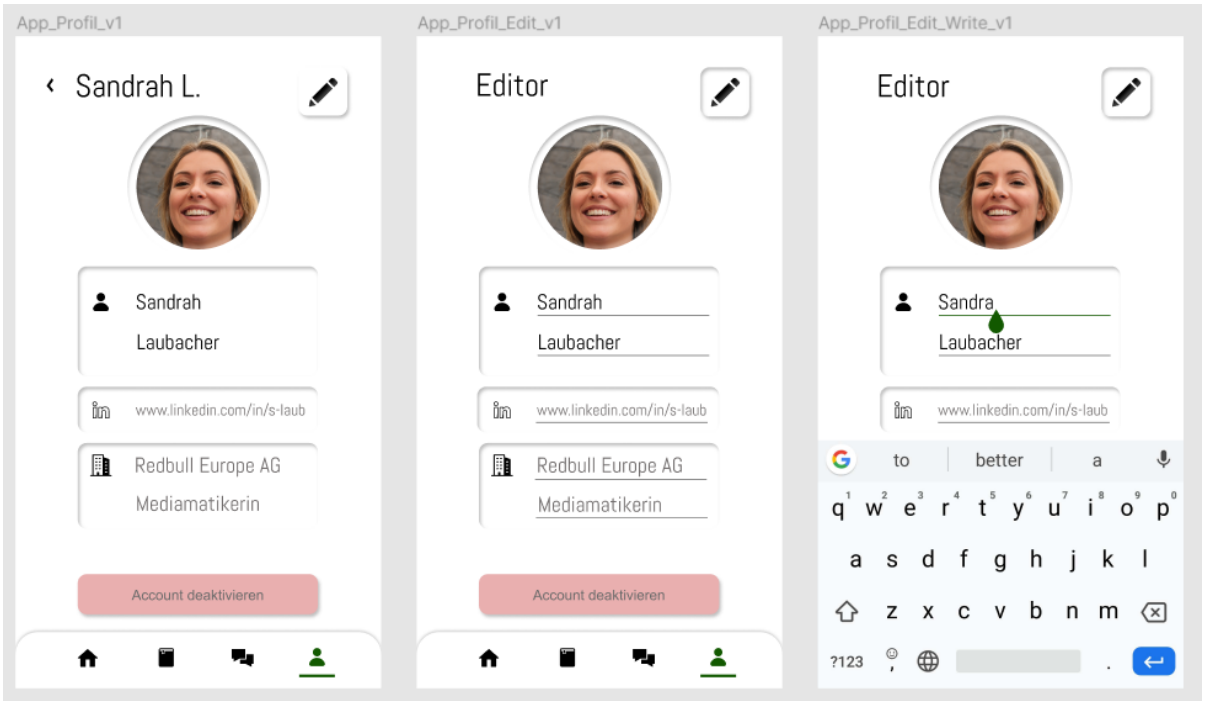
10 Antworten

A.3 Figma mockups

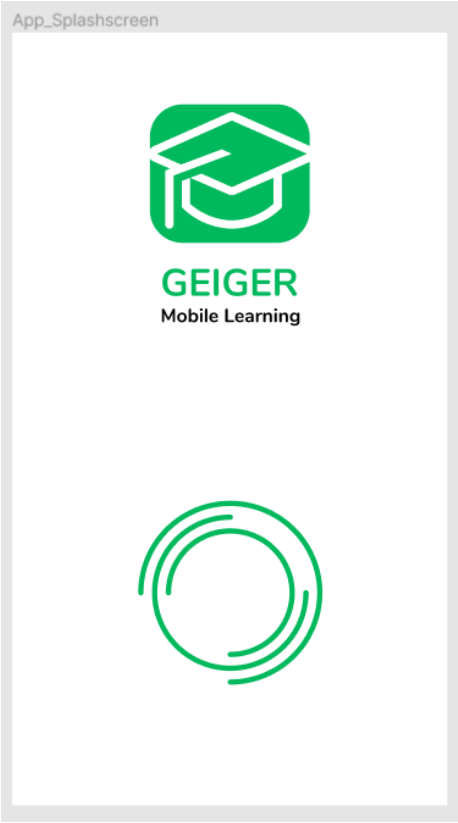
Iteration 3

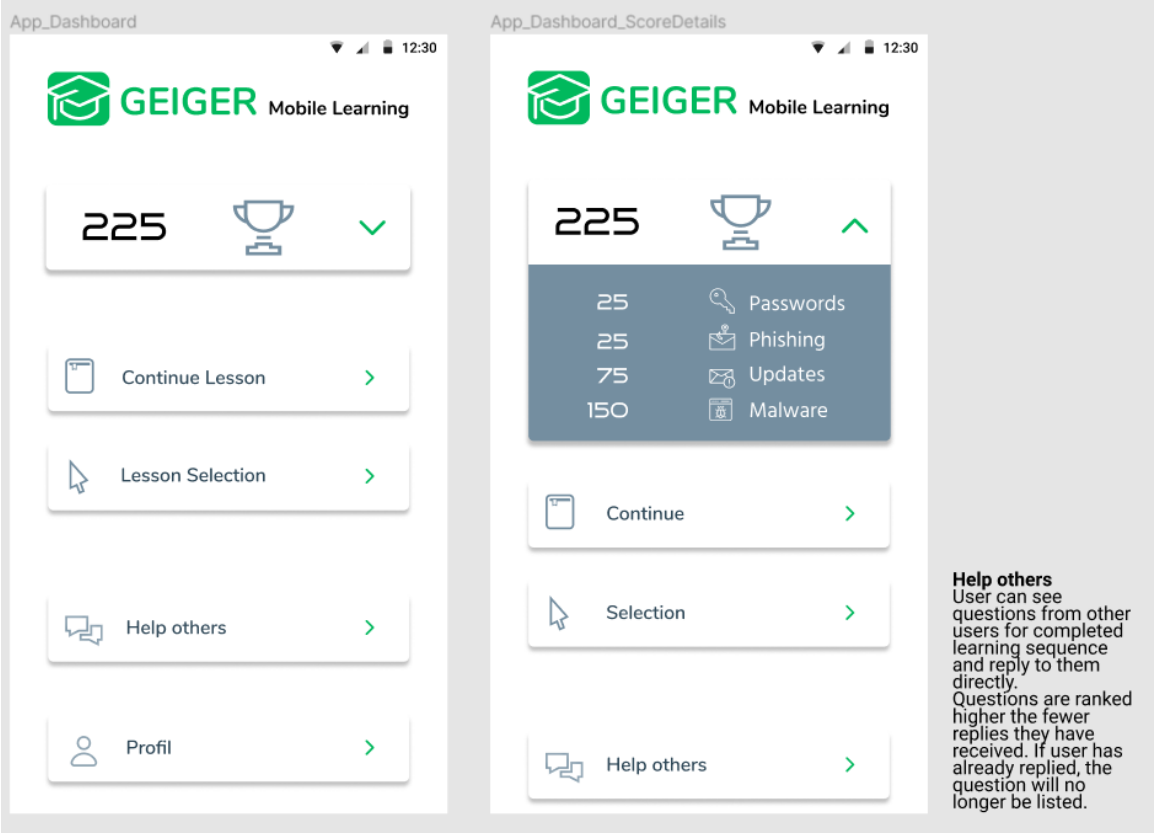


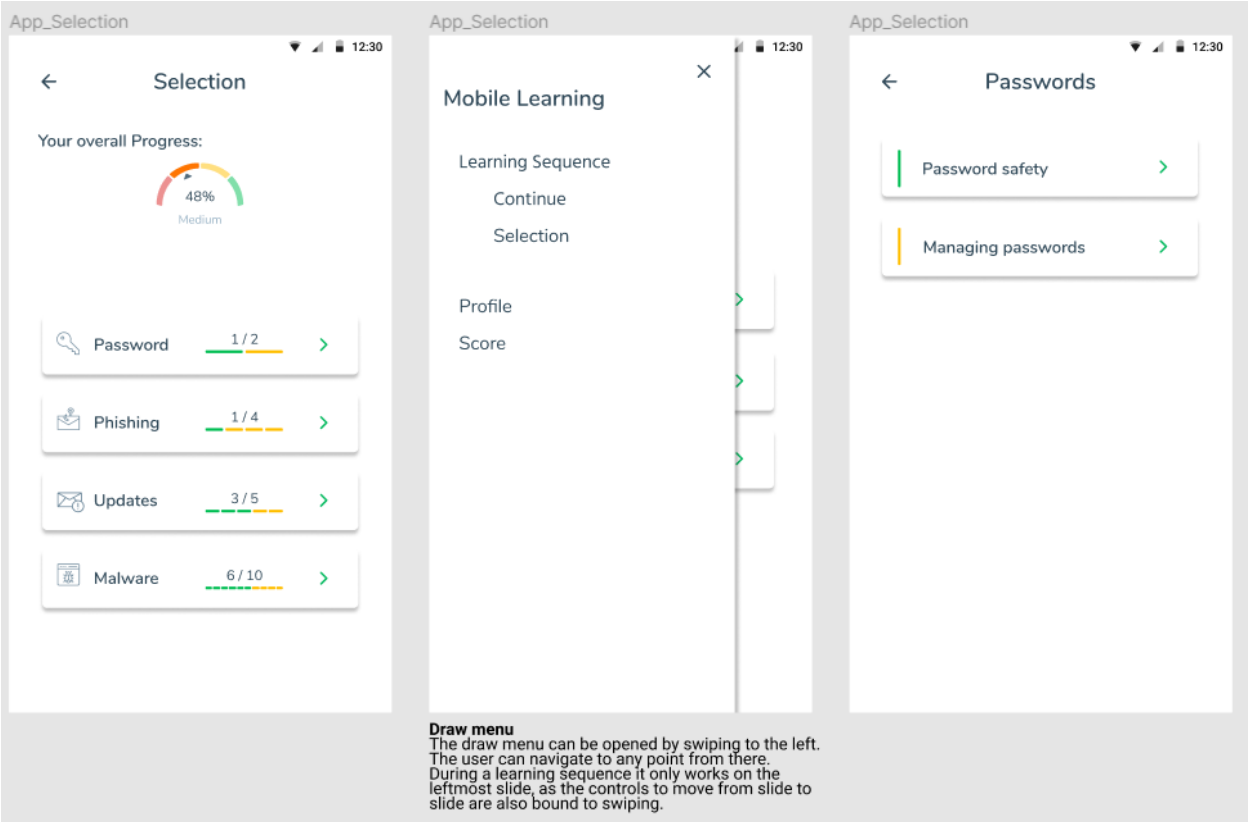

App_Selection
Selection
1 / 12
Malware
2 / 6
Phishing
0 / 1
Backups


App_Profil_v1
Sandrah L.
Sandrah
Laubacher
www.linkedin.com/in/s-laub
Redbull Europe AG
Mediamatikerin
Account deaktivieren
App_Profil_Edit_v1
Editor
Sandrah
Laubacher
www.linkedin.com/in/s-laub
Redbull Europe AG
Mediamatikerin
Account deaktivieren
App_Profil_Edit_Write_v1
Editor
Sandra
Laubacher
www.linkedin.com/in/s-laub
to
better
a

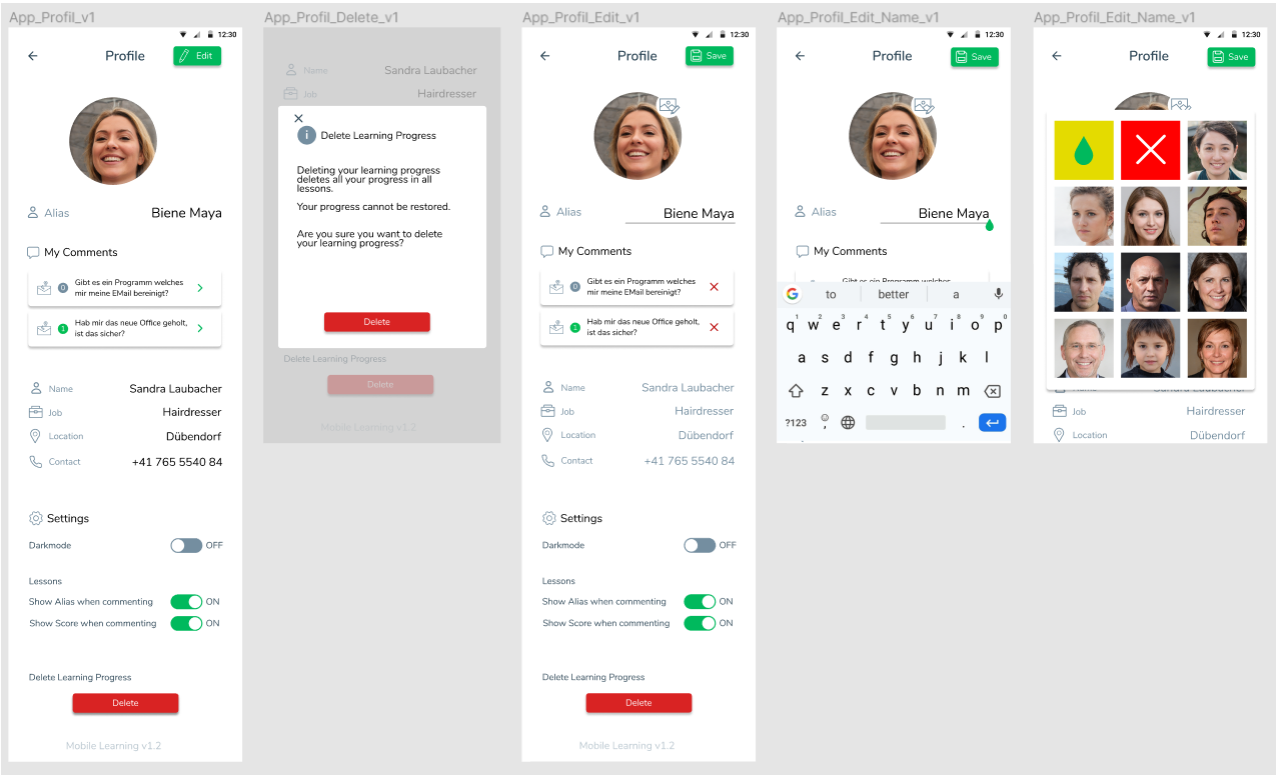
Iteration 4


App_Splashscreen
GEIGER
Mobile Learning


App_Dashboard
12:30
GEIGER Mobile Learning
225
Continue Lesson
Lesson Selection
Help others
Profil
App_Dashboard_ScoreDetails
12:30
GEIGER Mobile Learning
225
25 Passwords
25 Phishing
75 Updates
150 Malware
Continue
Selection
Help others
Help others
User can see questions from other users for completed learning sequence and reply to them directly.
Questions are ranked higher the fewer replies they have received. If user has already replied, the question will no longer be listed.

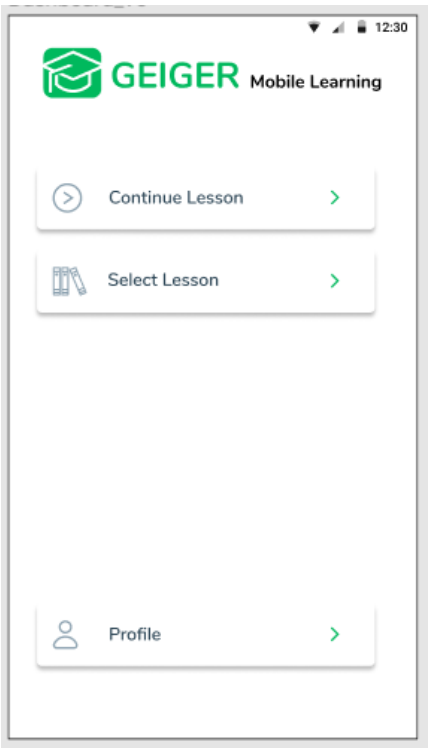


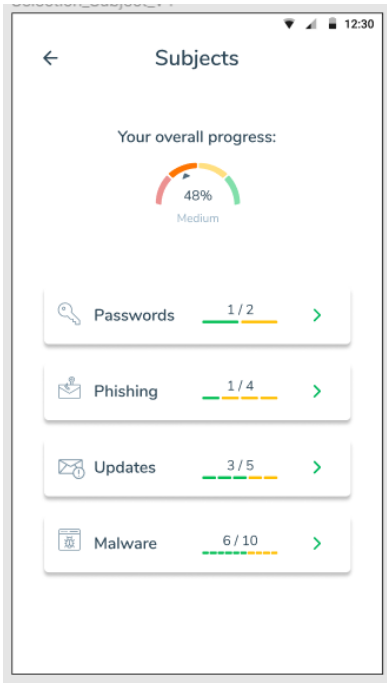
Draw menu
The draw menu can be opened by swiping to the left. The user can navigate to any point from there. During a learning sequence it only works on the leftmost slide, as the controls to move from slide to slide are also bound to swiping.

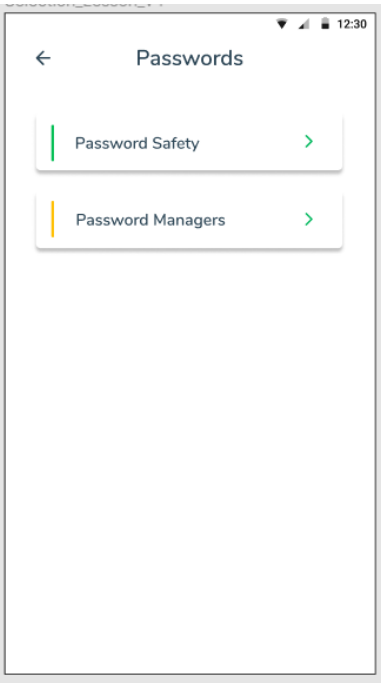


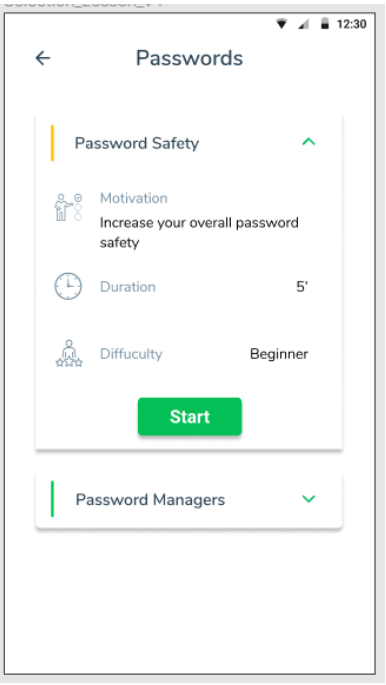
Iteration 5

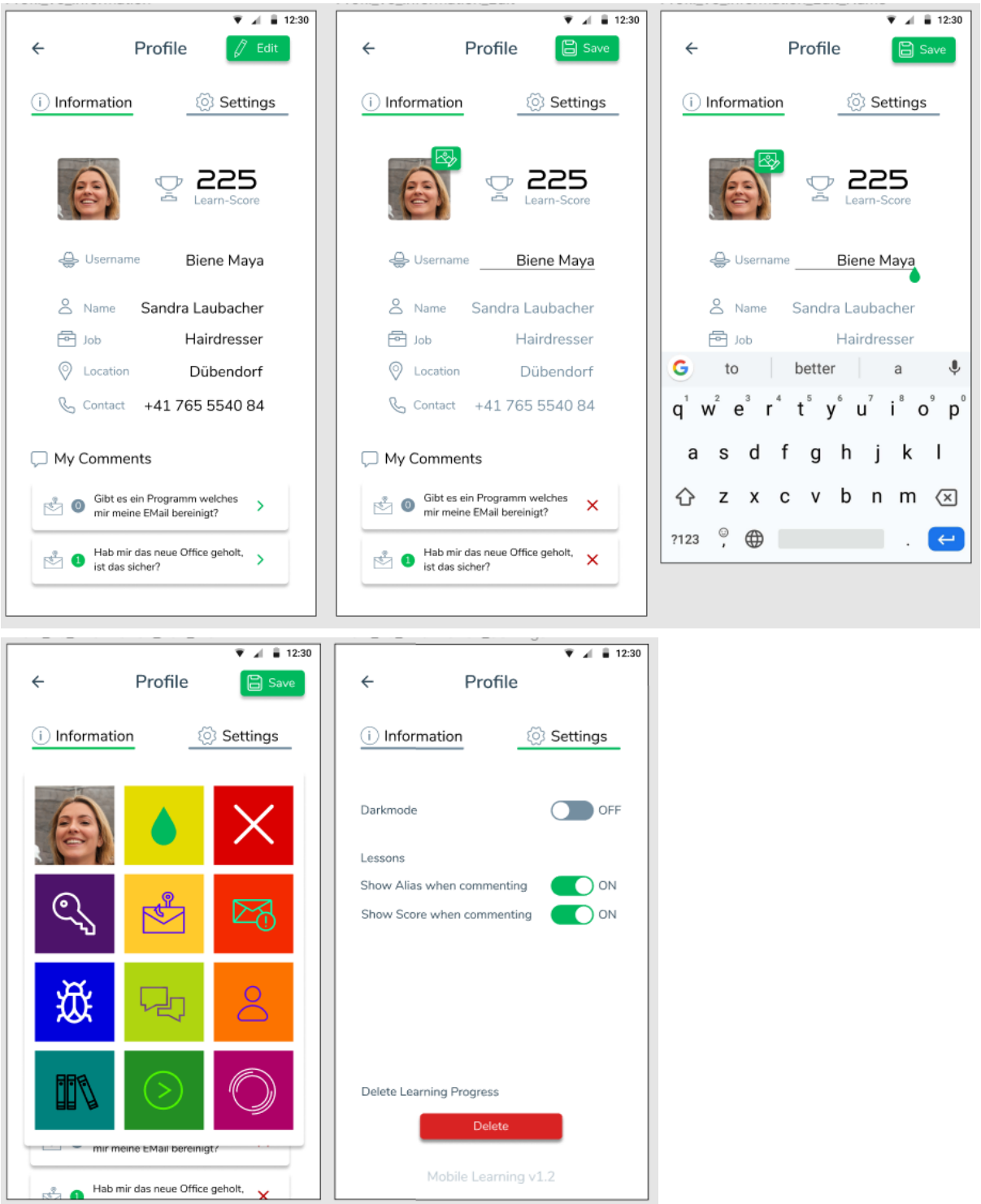

GEIGER
Mobile Learning


12:30
GEIGER Mobile Learning
Continue Lesson
Select Lesson
Profile


12:30
Subjects
Your overall progress:
48%
Medium
Passwords 1 / 2
Phishing 1 / 4
Updates 3 / 5
Malware 6 / 10

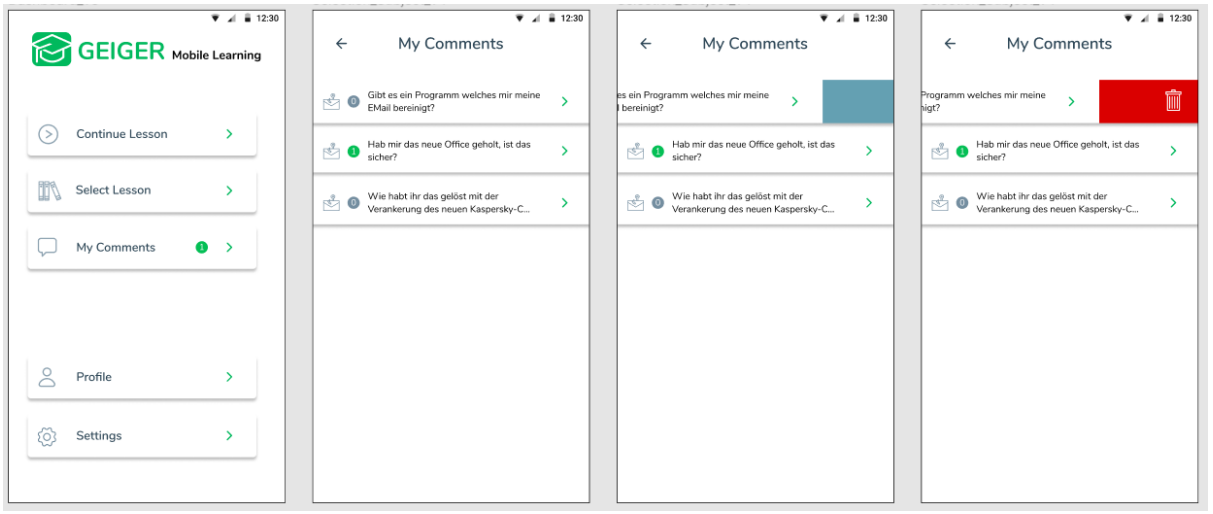

12:30
Passwords
Password Safety
Password Managers

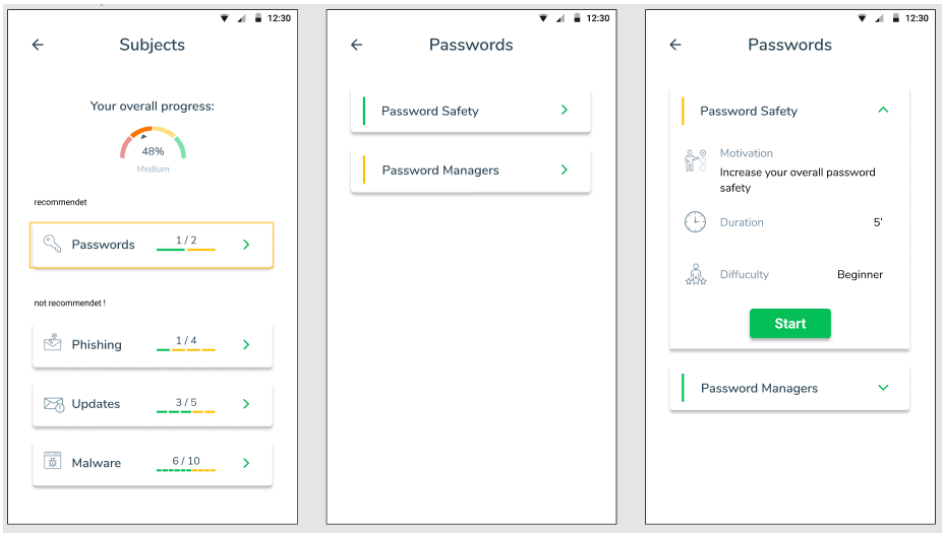

12:30
Passwords
Password Safety
Motivation
Increase your overall password safety
Duration 5'
Diffuculty Beginner
Start
Password Managers

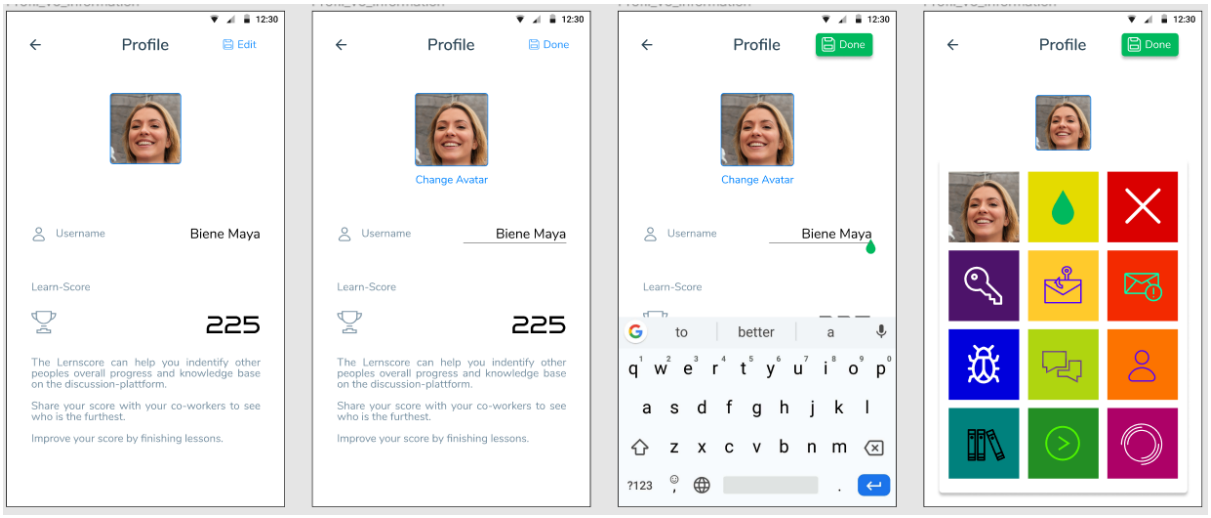

12:30
Profile
Edit
Information
Settings
225
Learn-Score
Username
Biene Maya
Name
Sandra Laubacher
Job
Hairdresser
Location
Dübendorf
Contact
+41 765 5540 84
My Comments
Gibt es ein Programm welches mir meine EMail bereinigt?
Hab mir das neue Office geholt, ist das sicher?
Save
to
better
a
Darkmode
OFF
Lessons
Show Alias when commenting
ON
Show Score when commenting
ON
Delete Learning Progress
Delete
Mobile Learning v1.2

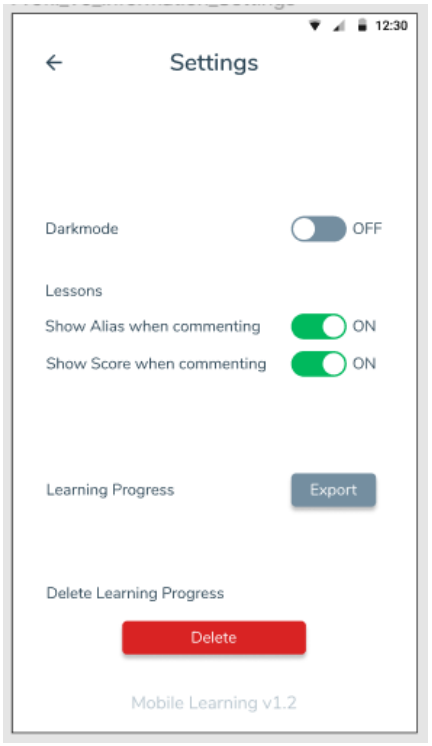
Iteration 6


GEIGER
Mobile Learning


GEIGER Mobile Learning
Continue Lesson
Select Lesson
My Comments
Profile
Settings
My Comments
Gibt es ein Programm welches mir meine EMail bereinigt?
Hab mir das neue Office geholt, ist das sicher?
Wie habt ihr das gelöst mit der Verankerung des neuen Kaspersky-C...

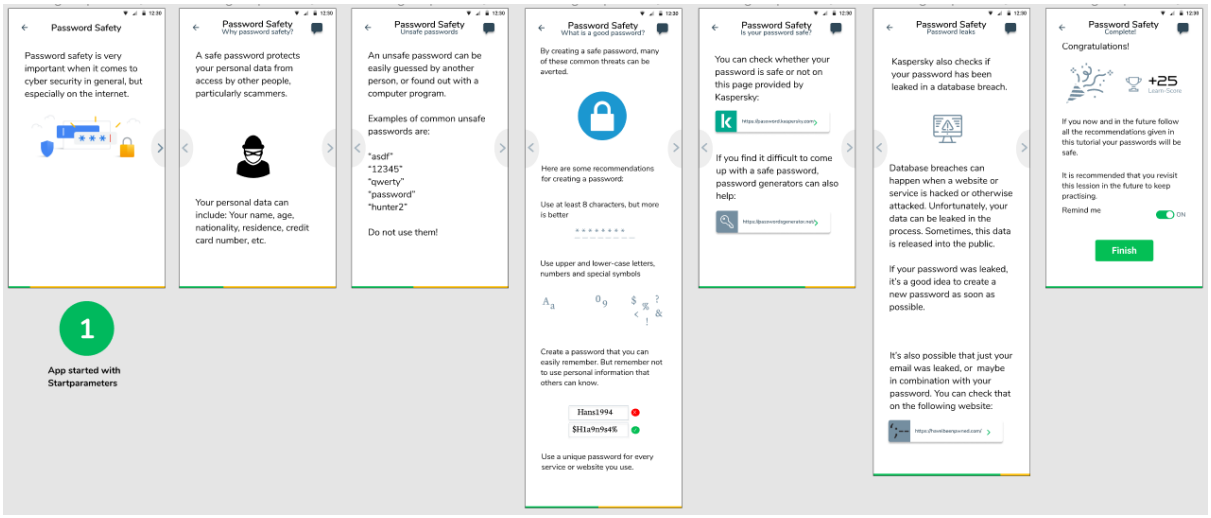

Subjects
Your overall progress:
48%
Medium
recommendet
Passwords 1 / 2
not recommendet !
Phishing 1 / 4
Updates 3 / 5
Malware 6 / 10
Passwords
Password Safety
Password Managers
Passwords
Password Safety
Motivation
Increase your overall password safety
Duration 5'
Diffuculty Beginner
Start
Password Managers


Profile
Edit
Done
Change Avatar
Username
Biene Maya
Learn-Score
225
The Lernscore can help you indentify other peoples overall progress and knowledge base on the discussion-plattform.
Share your score with your co-workers to see who is the furthest.
Improve your score by finishing lessons.

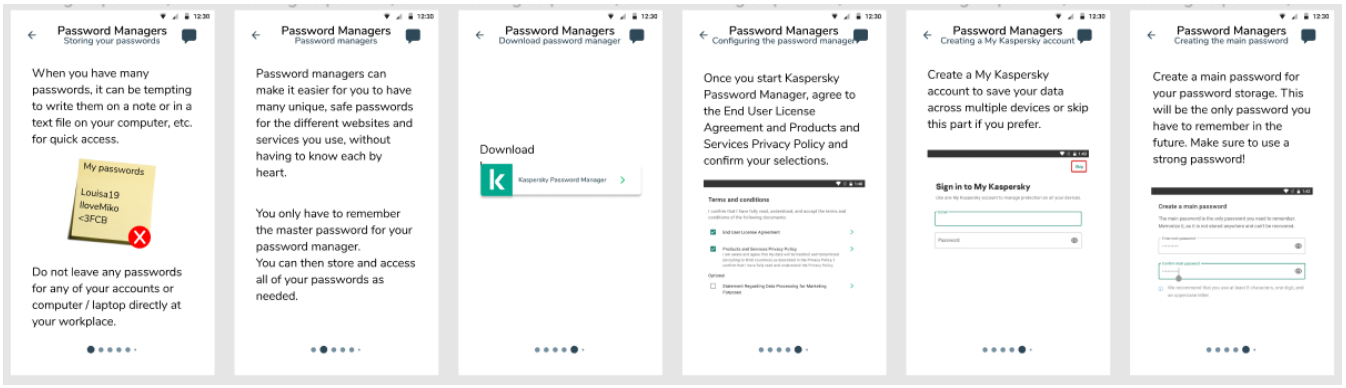

Settings
Darkmode
OFF
Lessons
Show Alias when commenting
ON
Show Score when commenting
ON
Learning Progress
Export
Delete Learning Progress
Delete
Mobile Learning v1.2

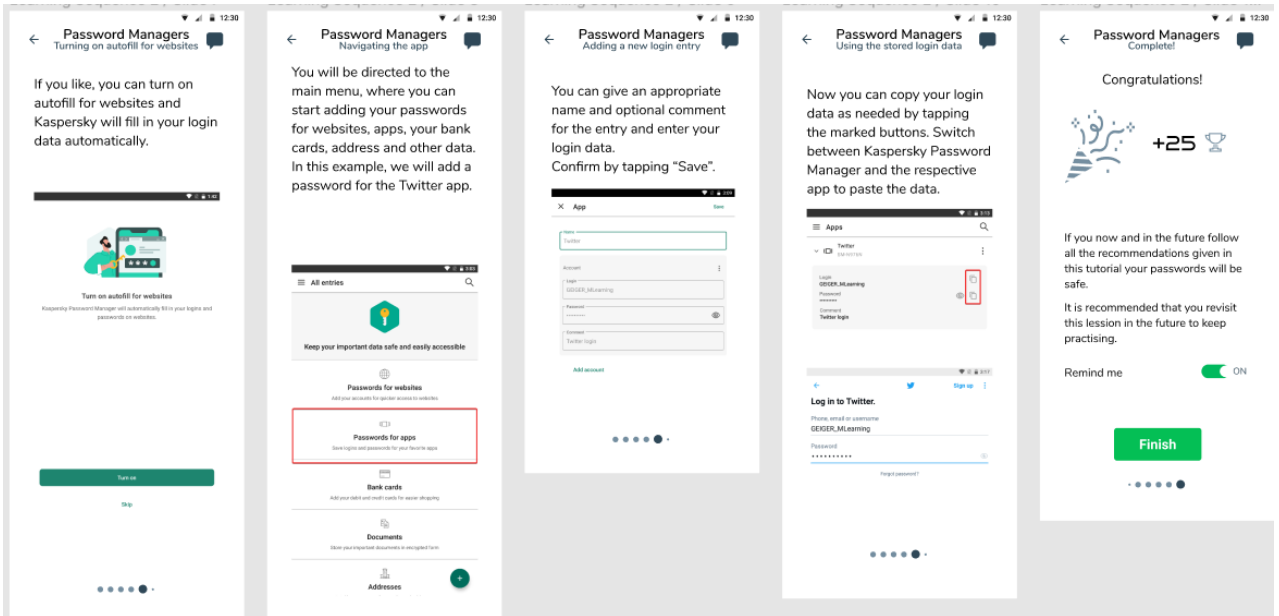
Lessons

Password Safety

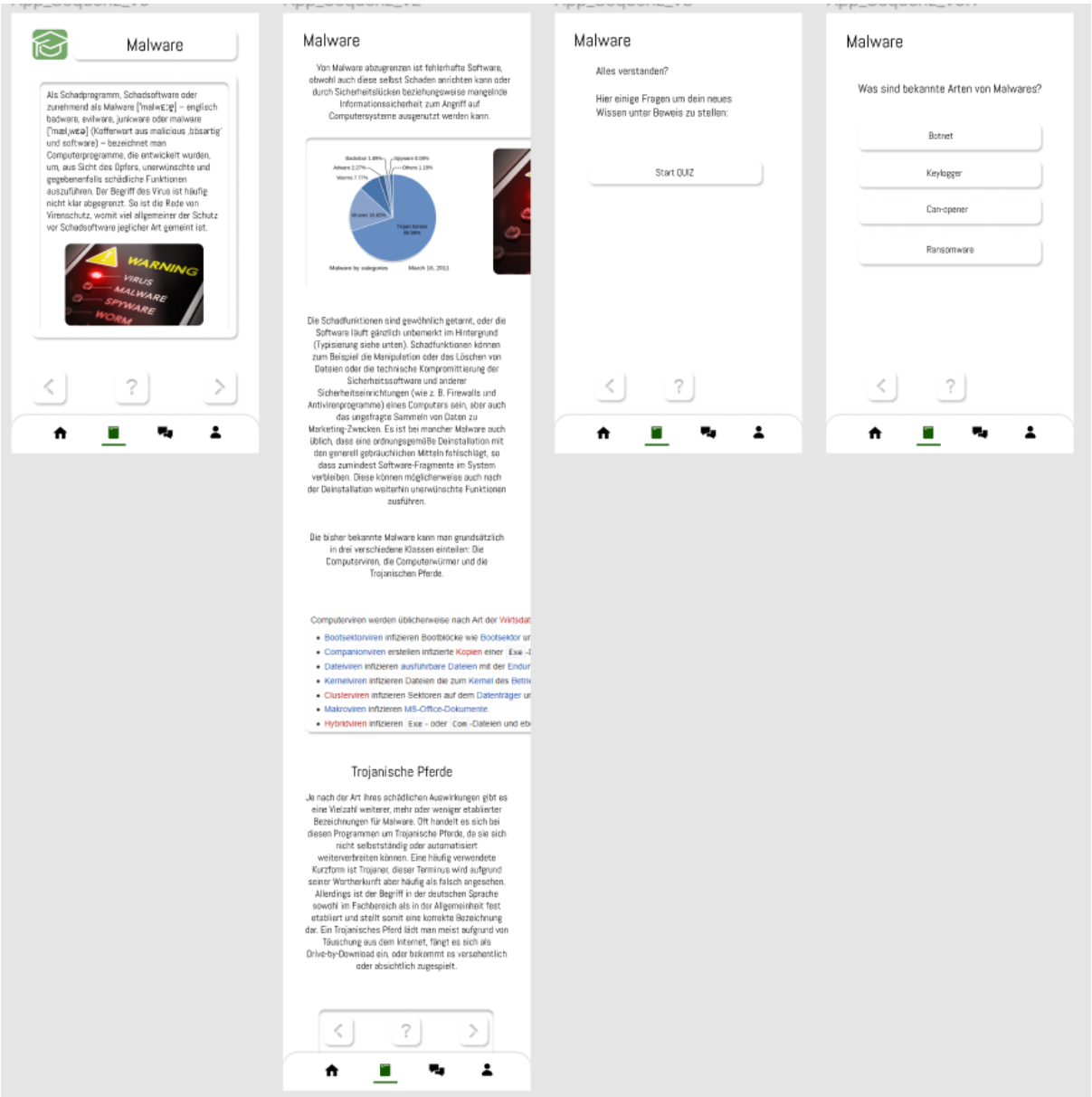


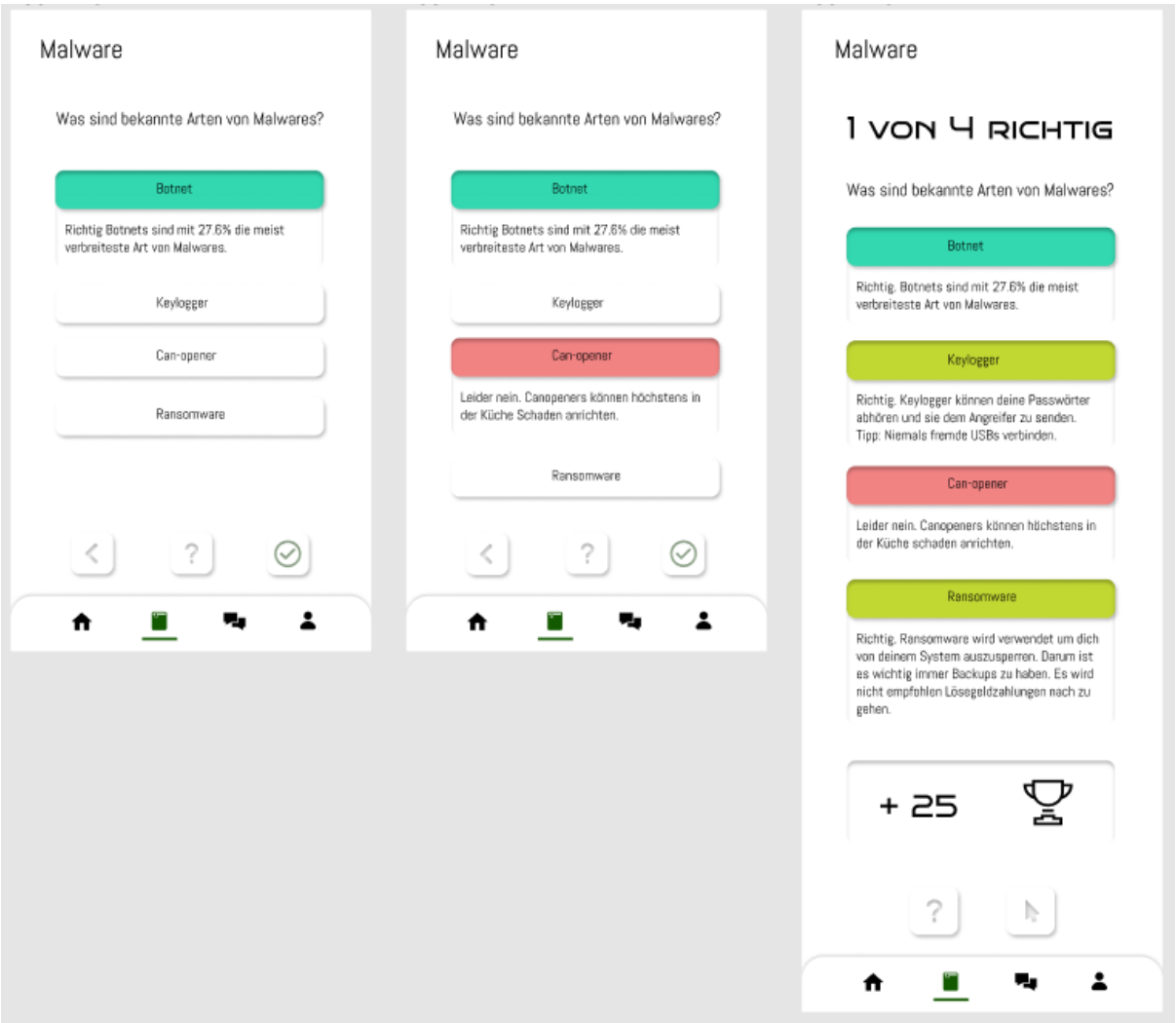
Password Managers



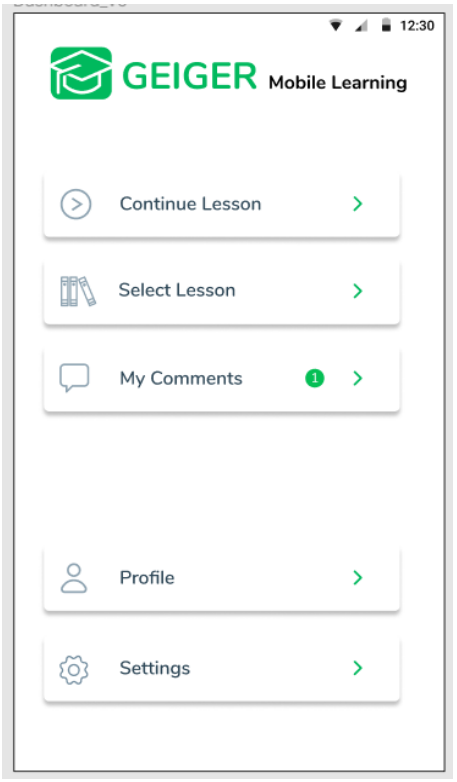


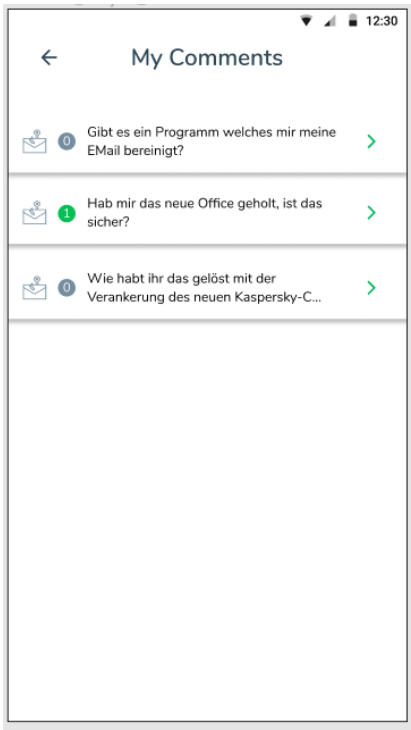
First Iteration of Lessons

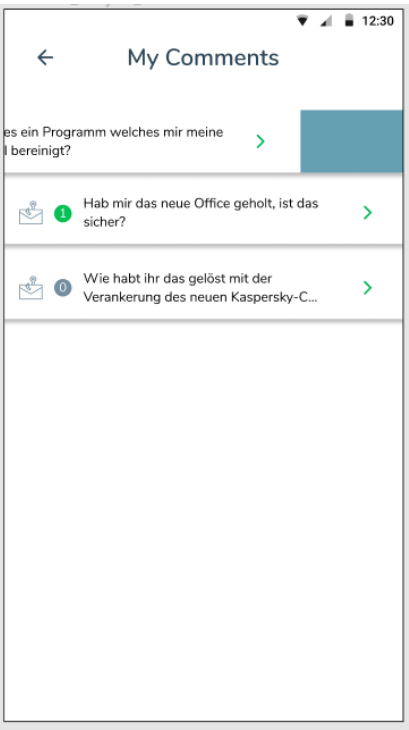


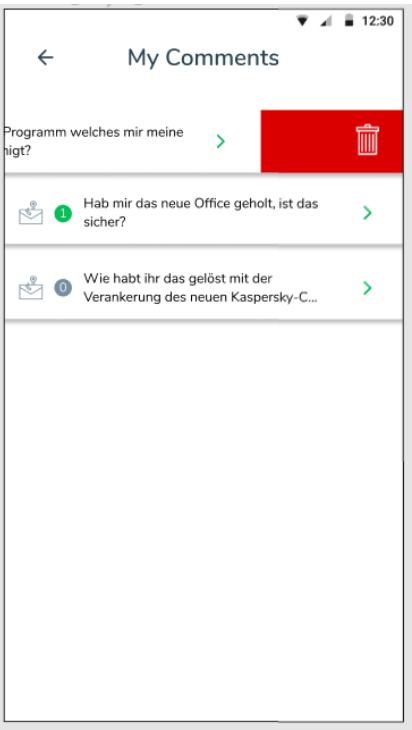

Malware
Was sind bekannte Arten von Malwares?
Botnet
Richtig Botnets sind mit 27.6% die meist verbreiteste Art von Malwares.
Keylogger
Can-opener
Ransomware
Malware
Was sind bekannte Arten von Malwares?
Botnet
Richtig Botnets sind mit 27.6% die meist verbreiteste Art von Malwares.
Keylogger
Can-opener
Leider nein. Canopeners können höchstens in der Küche Schaden anrichten.
Ransomware
Malware
1 VON 4 RICHTIG
Was sind bekannte Arten von Malwares?
Botnet
Richtig. Botnets sind mit 27.6% die meist verbreiteste Art von Malwares.
Keylogger
Richtig. Keylogger können deine Passwörter abhören und sie dem Angreifer zu senden. Tipp: Niemals fremde USBs verbinden.
Can-opener
Leider nein. Canopeners können höchstens in der Küche schaden anrichten.
Ransomware
Richtig. Ransomware wird verwendet um dich von deinem System auszusperren. Darum ist es wichtig immer Backups zu haben. Es wird nicht empfohlen Lösegeldzahlungen nach zu gehen.
+ 25

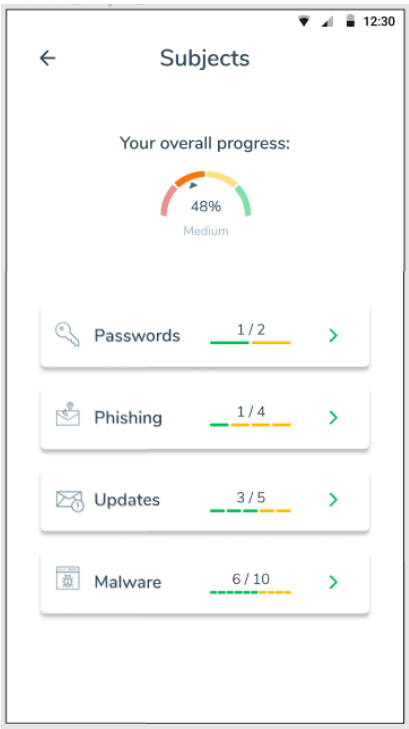
Final iteration of Mockups

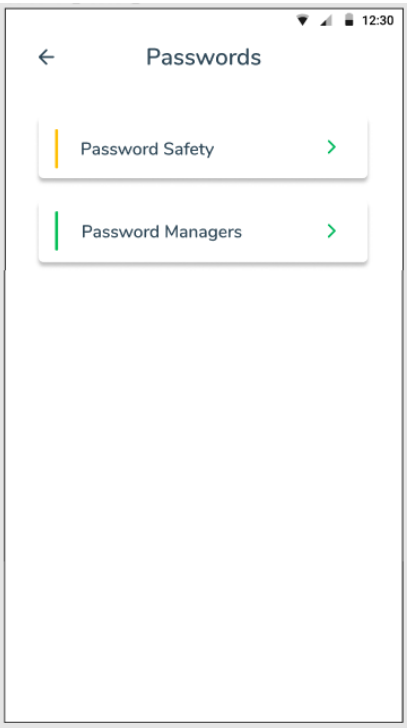


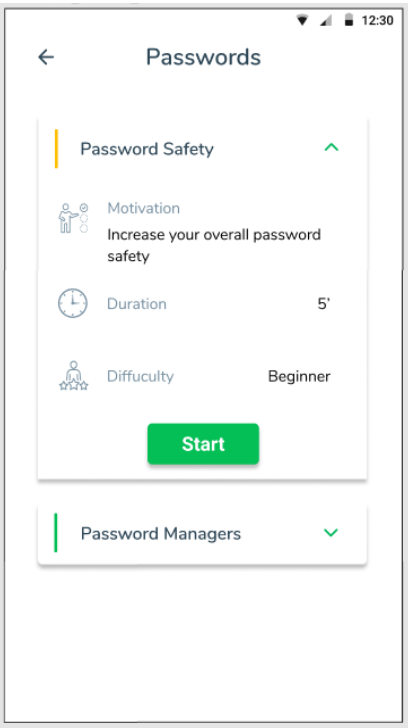


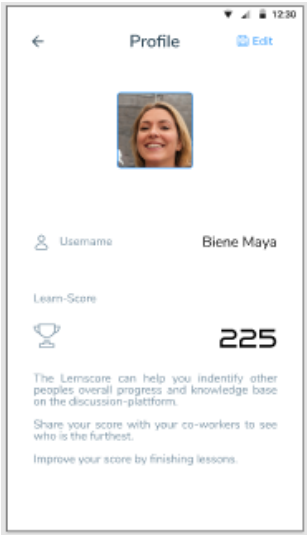


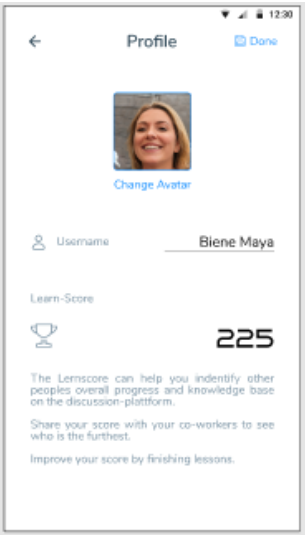


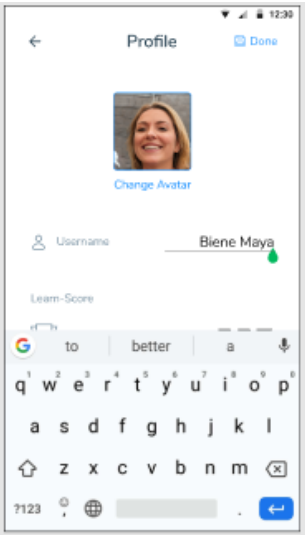

12:30
Subjects
Your overall progress:
48%
Medium
Passwords 1 / 2
Phishing 1 / 4
Updates 3 / 5
Malware 6 / 10

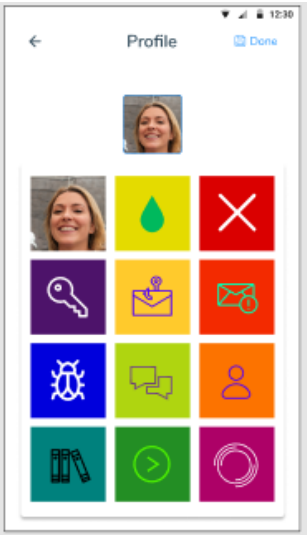

12:30
Passwords
Password Safety
Password Managers

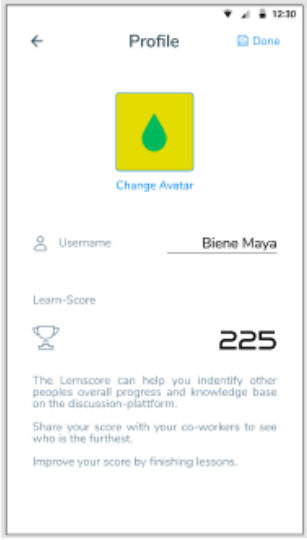

12:30
Passwords
Password Safety
Motivation
Increase your overall password safety
Duration 5'
Diffuculty Beginner
Start
Password Managers

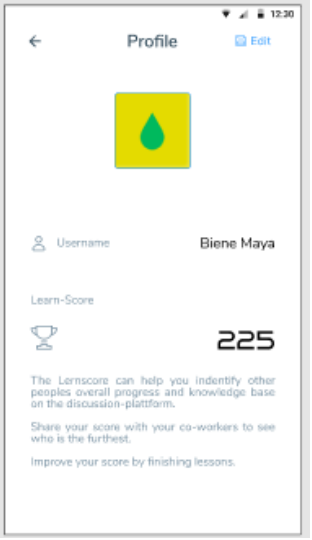

Profile
Edit
Username Biene Maya
Learn-Score
225
The Lernscore can help you indentify other peoples overall progress and knowledge base on the discussion-plattform.
Share your score with your co-workers to see who is the furthest.
Improve your score by finishing lessons.


Profile
Done
Change Avatar
Username Biene Maya
Learn-Score
225
The Lernscore can help you indentify other peoples overall progress and knowledge base on the discussion-plattform.
Share your score with your co-workers to see who is the furthest.
Improve your score by finishing lessons.


Profile
Done
Change Avatar
Username Biene Maya
Learn-Score


Profile
Done


Profile
Done
Change Avatar
Username Biene Maya
Learn-Score
225
The Lernscore can help you indentify other peoples overall progress and knowledge base on the discussion-plattform.
Share your score with your co-workers to see who is the furthest.
Improve your score by finishing lessons.


Profile
Edit
Username Biene Maya
Learn-Score
225
The Lernscore can help you indentify other peoples overall progress and knowledge base on the discussion-plattform.
Share your score with your co-workers to see who is the furthest.
Improve your score by finishing lessons.


Settings
Darkmode OFF
Lessons
Show Alias when commenting ON
Show Score when commenting ON
Learning Progress
Export
Delete Learning Progress
Delete
Mobile Learning v1.2