Design and Implementation of a Learning Application to Sensitize Senior Citizens for Internet Security

von / presented by
Nellesen, Marcel
292155

First Examiner: Prof. Dr. Ulrik Schroeder
Second Examiner: Prof. Dr. Jan Borchers

Aachen, July 24, 2019
## Contents

5.2. Structure .................................................. 31  
5.3. Additional Features ........................................ 33  
  5.3.1. Images ................................................ 33  
  5.3.2. Tutorial ............................................... 34  
  5.3.3. Creation of new Learning Materials .................... 35  
  5.3.4. Personalization Data .................................. 36  
  5.3.5. Logging ............................................... 38  
  5.3.6. Settings ............................................. 38  
5.4. Modules .................................................. 39  
  5.4.1. Passwords ............................................ 39  
  5.4.2. Information Security and Privacy ...................... 43  
  5.4.3. Additional Workshop Materials ....................... 45  

IV Evaluation and Discussion .................................. 47  

6. Evaluation .................................................. 48  
  6.1. Evaluation process ....................................... 48  
  6.2. Continuous Testing ...................................... 48  
  6.3. Study Preparation ........................................ 49  
    6.3.1. Study Group ......................................... 49  
    6.3.2. Consent Form ........................................ 50  
    6.3.3. Initial Survey ........................................ 50  
    6.3.4. Final Survey ......................................... 51  
    6.3.5. Task List ............................................ 52  
    6.3.6. Tools and Data Collection ............................. 52  
    6.3.7. Study Setup ......................................... 53  
    6.3.8. Study Procedure ..................................... 53  
    6.3.9. Pilot Study .......................................... 54  
  6.4. Study Conduction ......................................... 54  
  6.5. Study Results ........................................... 55  
    6.5.1. Analysis ............................................. 55  
    6.5.2. User Comments and Feature Requests ................ 64  

7. Discussion .................................................. 67  
  7.1. Discussion of the Design Goals ........................... 67  
  7.2. Interpretation of the Results ............................. 69  
  7.3. Limitations of the Results ............................... 70  

V Conclusion .................................................. 72  

8. Conclusion .................................................. 73  
  8.1. Summary ................................................ 73  
  8.2. Future Work ............................................. 74  

Appendix ...................................................... 75  

A. Bibliography ............................................... 76  

B. List of Figures ............................................ 81
Contents

C. Initial Survey 82
D. Final Survey 84
Abstract

The internet has become an important part of the everyday life of many people. Through tablets and smartphones, they can access information and communicate with each other anytime and anywhere. While these devices are especially popular with teenagers and young adults, they become increasingly common among senior citizens as well. The usage of mobile devices provides them with the ability to stay in contact with family members, take part in communities, and use internet services. While modern technology offers many possibilities for senior citizens, they are also seen as threatening by many; especially security concerns are common among senior citizens. This project aims at helping senior citizens to better understand and to securely use the internet, which enables them to keep their independence longer and reach out to others.

Within this thesis a learning application was developed for Android devices that can be either used within a workshop context or as a standalone application. Two learning modules were created that address the topics “secure passwords” and “information privacy and security”. The application was designed regarding the age-related impairments and specific requirements of senior citizens.

The developed application was systematically evaluated through a user study. The purpose of this study was to determine if the application can be successfully used to teach senior citizens. The user study was performed with ten participants. All were able to finish the learning module and the contained exercises. The System Usability Scale was used to gather information on the perceived usability. The usability of the application was rated good to excellent.
Part I

Introduction
Chapter 1: Introduction

In this chapter the motivation for the thesis is described. The goals for this thesis are discussed and a set of research questions are presented. The chapter is concluded by an overview of the structure of the thesis.

1.1. Motivation

Tablets and smartphones enable people to access information and services anytime and anywhere. The ability to communicate with each other and to use the internet made these devices an important part of the daily life of many people. In 2016, 96% of all German citizens of age 16 to 24 owned a smartphone [1]. The devices are not only popular with teenagers and young adults, the number of senior citizens that use a smartphone increases as well [1]. While in 2013 only 14% of all German citizens of age 55 and above owned a smartphone this percentage was 44% by the year of 2016 [1]. The usage of computers and mobile devices enables them to use different services in the internet; thereby increasing their independence and allowing them to stay in contact with family members and friends [2]. They can join communities and take part in the digital world [2]. While modern technology offers many possibilities for senior citizens, they are often concerned about using these technologies [2, 3].

The goal of this project is the creation of an eLearning application to teach senior citizens, this are all citizens of age 60 or above, basic knowledge and skills about computer science. Computer science is an important part in the education of children and young adults. By analyzing current curricula and standard for the education of school children, topics of interest were analyzed. These were used within a questionnaire to identify the topics senior citizens are interested in. Based on the results the following topics were selected for this thesis: secure passwords, information security and information privacy. The selected topics are of interest for the senior citizens and can often be found within German public media [2, 4].

The application will be created for Android mobile devices and can be used in existing workshop contexts or as a standalone application. The program and the learning materials will be designed in a way that makes them easy to use and understand by the senior citizens. Possible age-related impairments will be researched and regarded during the application development. The effectiveness of the application in teaching will be evaluated.

1.2. Research Question

This thesis aims at answering how basic knowledge in computer science, specifically secure passwords, information privacy and information security, can be taught to German
speaking senior citizens and adults with little or no prior experience in Information Technology (IT) Security, through a mobile application within a workshop context. To solve this problem the following questions must be answered:

- Which specific requirements and demands has the target group?
- How can the specific requirements and demands of the target group be considered within the application?
- What requirements must be fulfilled to use the application and the learning materials in a workshop?
- How does the usage of the application compare to a classical lecture design?

1.3. Structure

The work is structured in the following way: In Chapter 2, the necessary background information is provided: the possible age-related impairments of senior citizens are discussed and an overview about the learning content and technology enhanced learning processes is provided. Chapter 3 contains information about related work: current approaches for teaching senior citizens about computers and mobile devices are discussed and existing methods for IT Security education are analyzed. Research concerning the usage of computers and mobile devices by senior citizens and the usage of such devices within classrooms and workshops is presented. The specific concept of the learning modules is then discussed in chapter 4: a detailed concept of the learning application and the learning content is developed. Based on the concept, design goals and a basic structure for the application are described. In Chapter 5 the implementation is presented: after an explanation of the core functionality, specific features of the learning application are discussed in detail. The chapter ends with a presentation of the developed learning modules and the resources that are provided for the usage within a workshop context. Chapter 6 provides the evaluation of the application. The goal of the evaluation and a detailed description of the utilized tools and materials is given. The study conduction is described, and the results of the study are presented. In Chapter 7 the results of the evaluation and the benefit of the application are discussed. The design goals of the application are reviewed and analyzed. Chapter 8 concludes this thesis with a summary and a discussion of future work.
Part II

BACKGROUND AND RELATED WORK
Chapter 2: Background

Within this chapter the target group is specified. This is followed by a presentation of the learning content and its relevance for the target group. The chapter is concluded with a section about technology enhanced learning in which instructional design and the cognitive load theory are presented.

2.1. Specification of the Target Group

The target group consists of German senior citizens with little or no prior experience in Security. Multiple definitions of senior citizens exist, within this work senior citizens are all people of age 60 and above. Senior citizens as a group are often seen as both heterogeneous and homogeneous. Each senior citizen has an individual background. Some are academics while others have only received basic education. Therefore, senior citizens are regarded as a heterogeneous group. All senior citizens have a lifetime of experience and an increased likelihood of suffering from age related impairments. Because of this, senior citizens are also seen as a homogeneous group. In the following, the effects of old age, education, experiences and capabilities of the target group are presented. The section is concluded with a view on the learning motivation of the target group.

Aging is an individual process and two people which are of the same age can greatly differ in their age-related impairments. While the impairments do not occur at a specific age, the likelihood that a person suffers from an age-related impairment increases with age. In the following some common impairments are presented.

The reduction of eyesight is a side effect of the aging process. The ability to focus on near objects is closely linked to the ability of the eye lenses to bend. With an increase in age, the lenses lose their elasticity and become more solid. This effect is known as presbyopia 5. The ability of the eye to perceive colors is affected by the age, because the lenses change in color. This effect is largely countered by the visual system, though the perception of small color differences and the appearance of colors in the green spectrum remain affected 6.

One of the most common impairments associated with aging is a reduction in the ability to hear. Small hair cells in the inner ear are an important part for the hearing process. They adjust to the frequency of the perceived auditory signal to capture impulses, which are then processed in the brain. Aging or influences like exposure to extremely loud noises can impact these hair cells and reduce their abilities permanently 7. This can reduce the ability to hear sound with high frequencies 7. The same effect reduces the ability to notice acoustic signals which are very quiet 7.
In addition to limiting the range of sounds that can be perceived, concentrating on specific sounds is influenced by aging as well. Some of the hair cells are used to focus on specific sounds. When these cells lose their functionality, concentrating on specific sounds in the environment becomes more difficult. This has an impact exempli gratia (lt. for example) on following a conversation and can result in the senior citizens being more easily distracted [7].

Motoric functionality is the ability to move, as well as the speed and precision of the movements. With an increase in age the motoric functions decline. The reason for this is a decrease of muscle quality and muscle quantity [7]. This effect leads to a decreased mobility of the senior citizen. The decrease in mobility can result in less physical activities and thereby accelerate the reduction of muscle quantity [7]. The central nerve system is also affected by the aging process. In combination reduction in mobility the reaction time increases. The required time to perform actions increases as well. The hand-eye and foot-eye coordination becomes worse and movements are less precise [7].

The previously presented impairments focus on the physical changes of aging. However, cognitive capabilities are affected by the aging process as well [7]. The memory is typically divided into two types, the crystalized and the fluid memory [8]. The crystalized memory represents the stored knowledge and experience id est (lt. in other words) the long term memory, it remains functional even in high age [8].

The fluid memory, i.e., working memory, is responsible for the acquisition and processing of new information and skills. The capacity of the working memory is limited to 5-7 pieces of information that can be stored simultaneously. The working memory is affected by the aging process in several ways:

- Reduced capacity of the working memory [8].
- Increased processing time of the working memory [8].
- Reduction in the ability to filter irrelevant information [8].

The effects described above together have a significant effect on the cognitive capabilities of the senior citizen when compared to a younger person. This often results in difficulties during problem solving tasks and decision making.

Altogether, the impairments presented above have an influence on how the target group interacts with the environment and how it processes information. This has a direct impact on the capabilities to use a technical device such as a mobile phone or a tablet.

In addition to the possible impairments of the target group the education and experiences should be considered [9]. The education of the target group can vary strongly. A consequence is a very heterogeneous background for each individual member of the target group. The level of education also has an influence on the likelihood the target group will take part in non-formal learning programs [9]. Additionally, each individual in the target group has accumulated a lifetime of different experiences which further increases the differences between two people. This not only influences the expected technical understanding of the target group but the learning process as well.
2.2. Secure Passwords

The English language plays an important role in the internet as most resources found online are presented in English. Many teenagers and young adults encounter the English language on a regular basis, e.g. in school, hobbies, music or a work environment. However, the English language is not as omnipresent to senior citizens. Many of them have either never learned the language or they did not use it frequently. Therefore, they cannot be considered fluent in English. This limits the available resources for their education.

The motivation of the learner is a key component in education [9]. Senior citizens are often easier demotivated when learning something new [9]; therefore, they give up on learning a new skill more often and sooner than younger learners would [9]. The learning motivation of senior citizens is influenced by two factors [9]. The first factor is the expected gain of the knowledge or skill that would be acquired. The gain changes with the age of the participant [9]. For example, learning to type with 10 fingers at age 15 promises to be useful for a long period both in the personal and in the work life of a person. Acquiring the same skill at the age of 80 has a lesser impact on the life of the learner and can cause the learner to stop wanting to acquire this skill sooner [9]. The second factor is the estimated effort required to learn the new knowledge or skills. As described above acquiring new knowledge becomes increasingly difficult with age.

When considering the possible impairments, education, experiences, and capabilities of the target group, all the above factors can have an impact on the motivation of the target group and thereby on the success of the learning process [9]. An example: if a person suffers from reduced eyesight, reading a text size becomes more difficult. This will decrease the motivation, because the reading process requires more attention. Other tasks can become impossible due to a slow reaction time of the person interacting that interacts with the learning materials. To ensure that the target group can successfully use the learning materials the possible impairments and special requirements of the learners must be considered.

2.2. Secure Passwords

The internet connects people and services worldwide with each other. The physical distance to the person or service requires a form of identification and authentication that does not rely on a face to face interaction. To prove the user identity, a shared secret between the communicating parties is required [10]. One of the earliest and the most common forms of authentication in the internet is the usage of a password [10, 11, 12]. A password is a sequence of characters, which is used in combination with a username or an email-address [10, 11]. It usually consists out of letters (small and capital), numbers and special characters [10, 11].

To verify the identity of a user the password must be known to the service provider. To protect the passwords that are stored within a server, they are typically not saved as a plain text. Instead, a hash function is used to create a hash value of the password, then the hashed password is stored within the database [11, 12, 13].

Since passwords secure data and services, they are a frequent target of attacks [10, 11]. Attacks can be classified as either online or offline [14]. In case of an online attack, the attacker tries to gain access to a service directly. In an offline attack the attacker has access to several hashed passwords and tries to find a password that leads to a stored
2.2. Secure Passwords

hash value. Online attacks are not as common since many services limit the number of false login-attempts to a service. Whereas offline attacks cannot be regulated through such an approach and hence cannot be detected.

Several different attack vectors exist for hashed passwords. All passwords consist out of a combination of characters which are taken from a limited set. Therefore, one form of attack is to try every possible combination of characters until the correct password is found. This form of attack is called a brute force approach. The time required to find a matching password depends on the available computation power and the length of the password. Each additional character of the password results in a significant increase in the number of possible combinations.

The number of possible password combinations depends on the number of different characters that are allowed during the password creation: e.g. there are 1000 possible ways to combine three numbers from 0 to 9, when combining three characters that can be either a number from 0-9 or a small or capital character from a-z there are 238,328 possible combinations. Therefore, many services require the users to create a password that fulfills several additional criteria:

- The password contains letters (small and capital)
- The password contains numbers
- The password contains special characters (e.g. !,$, @)
- The password contains a predefined number of signs

However, people often use passwords which they can remember easily. This results in simple and weak passwords, like ‘Password123!’ or ‘Secret123!’ Since such passwords are very common, they can help an attacker to reduce the time to get a specific password. Common passwords could be tried first before trying every possible combination: e.g. Users tend to use the required characters for a password in a specific order. Many users just append these characters to their password. Therefore, the insertion of numbers and special characters does not increase the average password strength as significantly as expected. In fact, such a procedure makes attacking the passwords easier, since the likelihood that the last two characters of a password are a number and a special characters is high.

As described above a password becomes less secure when a pattern is used for the creation of the password. Even passwords that lock random can be weak if they use popular combinations of characters, e.g. the password “qwertzui” seems to be random, but since it is the first row of characters on a German keyboard it is a very weak password. Words that originate in the real-world language are also not suited for passwords. Ideally Passwords should have no connection to the real-world and to the person that created it. For example: while the own birthday or that of a person that is close to the user seems like a secret information, such data is often publicly available and could be used by an attacker to guess a password.

Many users create weak passwords that they can easily remember. Since such passwords are very common, attackers can create a dictionary by taking a list of common passwords and creating the corresponding hash values. When they want to attack a new
hashed password, they could first try to look up the hashed value in their dictionaries. Therefore, this type of attack is called a dictionary attack \[10\][11][13]. There are different methods to reduce the threat of such an attack \[11\][13] as well as many different attack vectors, however the usage of secure passwords can significantly increase the security of data and service.

Because the management and memorization of multiple secure passwords is seen as difficult, many people tend to use the same password for multiple accounts \[11\]. This is especially dangerous: if one account is compromised all other accounts can be affected. An example: if attackers have access to the email address and password used for a social media website, they could try the same credentials at a popular platform for online payment. This threat can be avoided through the usage of different passwords. These passwords must be completely different from each other. They should not contain any personal information or specific patterns \[14\], otherwise one leaked password could lead to the compromise of other passwords through the analysis of patterns and personal information.

There are many more possible attack vectors and difficulties with the usage of passwords. However, using strong passwords and using multiple passwords for different applications can help to secure the data of the users \[10\][11].

### 2.3. Information Security

From booksellers to movie providers, most businesses can be found in the internet. Business and user information are valuable goods which require protection \[12\]. Especially when sensitive user information, like financial or medical data, is considered. Information security means to secure the information that is handled or stored within a computer system. To achieve this, three goals must be fulfilled: confidentiality, integrity and availability of the stored data \[12\][16].

- **Confidentiality** means that only authorized personnel can get access to the information. The access must be protected from attackers and it must be ensured that only those users can access the data that have the required permissions. For example, the administrator of a bank’s \[11\] department should not be able to view the financial status of the customers.

- **Data integrity** means to ensure that the data is protected from changes or deletion. The changes could either be caused by malicious intent or through computer failures.

- **Availability** of the data means that the information must be stored in a safe way that even in the case of a Denial-of-Service (DoS) attack, which aims at overwhelming a server with requests \[12\], or an environmental accident, like an earthquake, it can be accessed at any time.

Utilizing services in the internet requires the users to trust the providers of these services to handle their data in a responsible way. However, users themselves must also consider the security of their own devices and information \[12\]. Frequent attacks on organizations and private persons result in the requirement to establish and evaluate security measures to protect their data \[12\].
2.4. Information Privacy

Information is a valuable good. By gathering data on a specific subject, it is possible to gain detailed information about it. Many systems collect extensive information about which users use the system and the interactions that are done. However, when information of users is gathered, their privacy can be harmed, as this data could be used to gain in-depth insight on them.

A prominent example is the tracking of user behavior in the internet. This allows to create detailed user profiles and could enable companies to show specific advertisements regarding the user’s preferences. This information can also be of interest for other institutions. Sharing or selling of user data can be profitable. When multiple data sources are combined, a more detailed user profile can be created.

The privacy of user data became an important issue and is a frequent topic in public news. While information privacy is a topic of interest for everyone, the laws regulating the privacy of user data vary greatly between nations. Within the United States of America only specific groups are protected by information privacy laws, the laws differ between different states and not many national laws exist. The member states of the European Union have released information privacy laws that are valid for all member states. However, even if information privacy laws exist, they can be difficult to enforce. Since the internet connects users and services worldwide, the privacy of user data can be problematic. Depending on the countries were the users and the services are located different rules can apply. Therefore, users should take measures to secure their privacy. While total information privacy does not exist, users can control the information they publish and which services they use. For example when using social media platforms, privacy options for the profile page can often be specified.

2.5. Technology Enhanced Learning

Technology enhanced learning, often also called eLearning, describes the usage of Information and Communication Technology (ICT) in the context of education. Many different forms of eLearning approaches exist, each with different strengths and weaknesses. The appropriate approach depends on the content, the scenario in which the technology is used, the available equipment, the teacher and finally the learner.

The conception and creation of learning materials is called Instructional Design (ID). The aim of the ID is the preparation of the learning materials and the environment in a way that is beneficial for the learning process. The learning process is split into the following nine events of instruction:

1. Gaining attention
2. Inform learners of objectives
3. Stimulating recall of prior knowledge
4. Presenting the new learning material
5. Providing learning guidance
6. Eliciting performance
2.5. Technology Enhanced Learning

7. Providing informative feedback
8. Assessing performance
9. Enhancing retention and transfer

Depending on the learning goals variations of this model are possible [18]. The model described above has often been revised to support the learning of complex skills, problem solving abilities and self-organized learning [18].

The creation of useful learning materials requires an understanding of the processes which are required to work with these materials. The Cognitive Load Theory (CLT) considers the processing of the learning material in the working memory [17]. The working memory of the human is seen as limiting factor for information that can be processed at the same time. Each task has an associated cognitive load. If the cognitive load of a task is too big, the learning process is harmed by the cognitive overload. The cognitive load consists of three components which each require a share of the working memory [17].

The intrinsic cognitive load depends on the difficulty of the task; therefore, it cannot be altered. The extraneous cognitive load is affected by the learning materials, for instance through type, structure and presentation. The third type is the germane cognitive load, which describes the amount of working memory that can be actively used to acquire new knowledge. To enhance the learning process, the available germane cognitive load should be increased by reducing the extraneous cognitive load [17]. There are a few methods to reduce the Extraneous Cognitive Load of the learning materials: The usage of worked examples helps to understand the problem-solving process. When using visual representations, the relevant textual explanations should be close to the materials to avoid splitting the attention of the learner.
Chapter 3: Related Work

Within this chapter related work is presented. In the first section existing approaches to teach computer science to senior citizens and current methods for teaching IT Security are analyzed. This is followed by a focus on the requirements and demands of senior citizens regarding the usage of mobile applications. The chapter is concluded with a view on benefits and limitations of using mobile devices in a workshop context.

3.1. Current State

The creation of a learning application for teaching basic concepts of secure passwords, information security and information privacy to senior citizens requires an analysis of currently existing approaches. Within this section the following areas will be regarded: computer courses for senior citizens, IT Security education in schools, existing mobile applications for IT Security education and IT Security games. After an analysis of the current approaches the section is finalized by a conclusion.

3.1.1. Computer Courses for Senior Citizens

A opportunity for senior citizens to learn about the usage of computers, tablets and smartphones are courses at local community colleges [19, 20]. These courses are offered on a regular basis and teach groups of participants basic skills and knowledge to use devices and programs. Some community colleges have special courses for senior citizens [19, 20]. These courses are often smaller, thereby improving the ratio of lecturers to participants. Such courses allow the participants to feel more at ease, since they are learning with people of their own age, that might have the same questions and problems as them. The difficulty of the learning materials is often adjusted within the courses for senior citizens.

There are many courses to teach senior citizens how to use a computer or a mobile device. These courses often focus teaching basic competences and skills to the senior citizens, e.g. how to write a mail or take pictures with the camera. The underlying principles, i.e. an understanding of the background in computer science is not addressed within these courses. The acquired knowledge is mostly focused on specific devices and programs and transferring this knowledge to other areas is difficult without a basic knowledge of computer science. While IT security is a topic the senior citizens are concerned about, it is not a primary topic within this courses, and is, if at all, only included as a side note.

When regarding all possible courses, there are also courses which target specific topics, e.g. security issues with mobile devices [19]. However, these courses are not designed for senior citizens and require prerequisite knowledge in computer science and the English
3.1. Current State

language [19, 20].

3.1.2. IT Security Education in Schools

An increasing number of schools in Germany is offering computer science classes. Within this classes the students learn basic skills for the usage of computers. Furthermore, the students are taught programming languages to design and create their own programs. Knowledge of underlying technologies, e.g. database design and interactions, is often part of the education as well.

Standards for the computer science education within schools have been introduced in Germany [21, 22] to define which topics should be part of the education. IT Security aspects are included within the standards and are described as an important part of the education. The topic is included in several books that are designed for the usage in schools. IT Security is often embedded into larger learning concepts. The goal is to provide a better understanding of the relevance and the interconnection with other topics [23, 24, 25, 26, 27]. However, these interconnection results either in a dependency upon previously acquired knowledge or include this knowledge into the learning materials [27]. To improve the learning process, the books often contain exercises which must be done in teams [23].

IT Security aspects have been identified as important aspect of computer science education in German schools. However, the topic is often not regarded in detail [23, 24, 25, 26, 27] and relevant security issues, like the danger of reusing passwords, are not considered [23, 24, 25, 26, 27]. The provided learning materials often require prior knowledge and are interconnected with other topics. Domain specific language or anglicism are used within many books [23, 25, 26, 27]. The writing style and the contained exercises are suited for a younger audience [23, 24, 25, 26, 27]. These characteristics make the learning materials unsuited for the education of senior citizens. Finally, while many books that are used in schools contain information on IT Security, this information only represents a small part of the contents, which reduces the benefit of buying enough books for an entire workshop.

3.1.3. IT Security Applications for Mobile Devices

The possibility to learn anytime and anywhere has inspired many different educational applications for mobile devices. Among these are some that focus on computer science and on IT Security [28, 29]. Most of these applications are designed for computer science students, which want to deepen their knowledge, or for high school students, with an interest in computer science. The presented learning material requires prerequisite knowledge in the field of computer science.

Course platforms like EdX [30] or Udemy [31] can also be used on mobile devices. In contrast to standalone applications these platforms offer many different courses and modules. Among these are also courses on IT security. The courses are often structured and organized. The registration for a course is either for free or requires a payment. Most of the courses are offered in English, the number of available courses in German is...
3.1. Current State

The existing applications and platforms are not suited for the usage by senior citizens or for the utilization within a workshop concept. Most of the applications or courses are only provided in English \[28, 30, 31\] and require in-depth knowledge of computer science. An additional problem is that the applications often do not regard the possible impairments of senior citizens, which makes them hard to use. Many of these applications and courses require fees or contain advertisements which makes them unusable within a workshop concept.

3.1.4. IT Security Games

**Purpose of Educational Games**

IT Security Games are a subgroup of educational games. By presenting the learning content in the form of a game the intrinsic motivation of the students should be utilized to improve the learning process. Various game elements are used, e.g., imbedding the learning content into a story, providing level-based challenges or including rewards for actions performed by the learners, to motivate the learners to keep learning and to improve their knowledge.

**Combination of IT Security and Games**

IT Security is a topic which can be found in several educational games, which are used to teach about the danger and the possibilities of attacks. The target group of these applications varies: some are designed for children, students, personal, managers and many more \[32\]. There are games for different aspects of IT Security, e.g., how to configure a firewall, detect spam mails or find vulnerabilities for Cross-Site-Scripting attacks \[33\]. Several of these applications focus on specific IT Security issues \[33\]. The duration of these games varies, some require only a few minutes \[34\] to complete while others take several hours \[35\]. Some IT Security games are played from the perspective of the attacker \[33, 35\] who has to find and exploit weaknesses to complete a challenge. This change of perspective is used to motivate the users and show them firsthand how dangerous and easy exploitable weaknesses could be.

While there are several IT Security games that are developed for end users without a background in computer science \[32\], many of these games fail to teach more than factual knowledge. The risks and threats of the presented security issues are often not explained \[32\]. This makes these games not suited for users with no prior experience in IT Security.

Most IT Security games focus on specific topics and are not customizable. This makes including the games within a workshop difficult. IT Security games that are only available in form of a website require an active Wireless Fidelity (Wi-Fi) network at the workshop location. Another disadvantage is that most IT games are only available in English, therefore they are unsuited for German senior citizens.

3.1.5. Conclusion

After analyzing the currently existing approaches to teach IT Security and reviewing computer courses for senior citizens, no approach did fulfill all the requirements of the target group. The most common and most severe limitations are discussed in this section.
3.2. Mobile Device Usage of Senior Citizens

- **Previous Knowledge**
  The presented learning material often requires previous knowledge in computer science, making them unsuited for the usage within a workshop with a limited time frame and a target group with little or no prior experience in Security.

- **Language**
  The learning materials are often only available in English. Since the target group often has no or only basic experience with the English language, this makes many learning materials unsuited.

- **Regarding individual requirements**
  When presented in the form of applications or learning games the programs often do not offer opportunities for customization, and therefore cannot be adjusted to the individual requirements of the users.

Most of the existing materials were not designed with senior citizens as the target group. Therefore, the specific requirements and demands of senior citizens are not regarded. To provide the target group with learning materials which are adequate for them and that can be customized to consider individual impairments a new application is required.

3.2. Mobile Device Usage of Senior Citizens

Consequences of Impairments and the Benefit of Mobile Applications

Senior citizens can face many different age-related impairments \[36, 37\], which often impact their ability to perceive and interact with the environment. This also influences the ability to use learning materials. For example, reading a text with a small font size is difficult or impossible for some people, if they have a reduced eyesight. This affects print media and digital media in the same way. However, mobile applications could help dealing with these challenges as individual needs of each learner can be considered, e.g., by displaying the text with a bigger font size; thereby, avoiding demotivation and increasing the success of the learning process.

When mobile phones are considered senior citizens in general prefer touch screens with a large display, a large font size and labeled buttons \[38\]. However, despite the fact that mobile devices are seen as user friendly, senior citizens often encounter problems while using mobile applications \[39\]. The usability of the designed application and its features is important and the diversity of the target group must be considered \[40\].

The usage of gestures for the interaction with applications is often seen as enjoyable by senior citizens \[41\]. Gestures can be trained to improve the performance of the participants \[41\]. The gestures must be intuitive for the users and should be indicated clearly through visual clues \[42\]. The application must be usable without gestures especially when the navigation is considered \[42\].

Small buttons and elements which are too close together, can reduce the success rate of the user interactions \[41, 43\]. This effect is especially notable during the typing process \[39\], it persists even after training with the application. To prevent frustration, every object used for interaction should have a width and height of at least 8 mm or 48 dpi \[41\]. In the case of buttons or other objects with text or images the success rate of actions can be increased by observing the point where the touch event occurs and to adjust the button accordingly. Humans tend to aim for the text in the object and try to touch it. However, inexperienced or unsure users often touch the device below the text of a
3.3. Usage of Mobile Devices in a Workshop Context

button. They want to be sure they touch the right object; therefore, they want to see the displayed texts as long as possible and aim for a point below the text. If the touch events are mostly registered in the lower third of the button, an adjustment of the text position can increase the precision of future touch events. Therefore, the text is displayed above the previous position. If the user still tries to touch the device below the text the touch event will now occur in the center of the button [43].

Other problems are caused by unwanted behavior, e.g. accidently leaving the application by pressing the "home" button on the device. Device configurations can also influence the usability, a small timeframe before the device switches into the standby mode is often seen as confusing by senior citizens [39-42]. The usage of advertisement within applications is also irritating for senior citizens as it can be difficult to distinguish between the application and the advertisement [42]. The usage of modal dialogs should also be avoid as the sudden break in the program flow and the changing visuals confuse senior citizens [42]. When complex interactions are required from the user, a detailed in place tutorial guides the user and increases the success rate of the process [44].

Diverse requirements and demands of the target group make a design that regards the individual user beneficial for the usability and the acceptance of an application. A personalization application could be used to gain insight on the specific requirements of each learner [43,45]. The data could be used to customize the application and thereby increasing its usability.

3.3. Usage of Mobile Devices in a Workshop Context

The usage of tablets and smartphones in a workshop has several advantages and disadvantages which are presented in this section. The devices can allow the teacher to include multimedia content, such as audio files, videos or animations into their lectures. This can benefit the learning process as it is easier to explain complex processes [46]. The usage of tablets and smartphones often has a positive effect on the learning process of the participants [46]. This effect can occur in a one-to-one scenario, where each participant receives one device, and in a many-to-one, with multiple participants sharing a device, scenario. When all participants of a workshop have their own device, electronic assessments are possible which could give the lecturers immediate feedback on the learning process of the participants. At the same time an electronic assessment reduces the time the lecturers need for the correction of the tests. Through assessments or a logging of the user interaction with the devices a detailed insight into the learning behaviors of the participants is possible [46]. This allows the lecturers to review the learning materials and improve them. Existing learning materials can be reused and adapted in different contexts.

All participants receives the multimedia learning materials on their own device, with which they can interact at their own pace [47]. This individual learning speed can improve the learning success, as the participants can process the learning materials at a comfortable speed [46]. The ability to interact with the learning materials, e.g. zoom in or out to see areas of interest in images, is another advantage.

As described in the previous section the usage of electronic devices allows to regard the specific requirements of all participants to aid them in the usage of the learning materials [46]. When exercises or assessments are used the participants gain immediate feedback.
3.3. Usage of Mobile Devices in a Workshop Context

to their answers without the need for a lecturer. The gain in competence is often similar when comparing the usage of mobile devices to a traditional paper-based workshop, however studies indicate that the usage of mobile devices can support the motivation of the learners.

Using tablets or smartphones within a workshop has the advantage that the devices are portable and often have a long-lasting battery [46]. The Lecturers are independent from the hardware equipment of a specific room and have full control over the devices they use for their course. Since the devices do not require external input devices, e.g. a mouse or keyboard, or contain movable components, like a monitor, they are more robust and often less expensive than a computer or a laptop [46].

The usage of mobile devices within a workshop setting has also disadvantages. Several mobile devices must be bought in order to supply a workshop. In addition to the initial costs, the devices need to be managed and require frequent maintenance. These costs can be reduced by allowing the participants to bring their own devices to the workshops. However, using these devices introduces potential errors as they might not be well maintained, can be outdated or could be from vendors that are incompatible with the used software.

Working with electronic devices requires that the lecturers have a basic understanding of the used technologies. They must be able to setup the devices and handle small problems on their own.
Part III

**DESIGN AND IMPLEMENTATION**
Chapter 4: Conceptual Approach

The previous chapters describe the requirements of an application teaching senior citizens the basic concepts of IT Security. These requirements are not fulfilled by current approaches. This chapter presents the design of a learning application regarding the special requirements and demands of senior citizens. At first the concept creation for learning modules including design guidelines is described. Afterwards the design goals for the application are formulated. The chapter ends with a presentation of the basic structure of the application.

4.1. Learning Module Concept

Within section the learning modules are described. The creation of the learning modules follows the Decision Oriented Instructional Design Model [17]. The model allows a systematic approach to the creation of multimedia learning applications. The basic structure of the model is depicted in figure 4.1 on page 21. As shown in the figure the model has a hierarchical structure. First the following goals of the learning platform are specified and analyzed:

- the learning goals
- the goals (of the platform)
- the target group (using the application)
- the content (of the application)
- the context (in which the application is used)

This is followed by a decision for a format for the learning application. The structure and sequencing of the learning content are planned. The multimedia components are designed. The selected media must be appropriate for the target group and the context. A layout for the is designed and a concept for the interactions with the application is developed. During these different steps the motivation of the learner is considered, therefore the planed features are analyzed regarding their motivational impact. The final design is implemented and evaluated.

The IT Security application will consists of two learning modules, whose design is presented in the following sections. Since these learning modules have several similarities they are described as one module in large parts of this section. Where the modules differ, or individual learning goals must be considered, the modules are described separately.
4.1. Learning Module Concept

4.1.1. Analysis

The IT Security application will be used to teach senior citizens with no prior experience in IT Security basic concepts and skill about safe passwords, information security and information privacy. The IT Security application must be usable in a workshop context and as a standalone application.

The target groups specific requirements and demands for using a learning application have been discussed in chapter 2 in section 2.1 and in chapter 3 in section 3.2. The learning application, that is developed within this thesis, is a part of a larger learning concept for senior citizens. It will be the fourth application within this concept. Therefore, the target group is expected to already have a basic understanding of smartphones or tablets from the previous applications. They are considered capable to use the following gestures: tapping, scrolling, swiping, zooming and drag and drop.

To use the IT Security application within a workshop only a minimal number of lecturers must be required. The lecturer must be able to use the application without knowledge in computer science. The presented learning content must be easily adaptable and extendable.

Android has the largest market share of all sold mobile devices Operating System (OS) and is the most commonly sold used OS. Therefore, the senior citizens might...
already be familiar with the operating system. Both device types can be supported by using a cross-platform developing software like Cordova [50], however supporting the specific requirements of the senior citizens is easier with an native application. The IT Security application needs to access the file system of the device in order to support existing applications and to export the logged user interactions. Other applications that were developed for senior citizens at the Lehr- und Forschungsgebiet Informatik 9 (Lufri9), e.g. a personalization application or a tutorial to install and deinstall applications from the Google Play store [28], are realized as native Android application. Developing the IT Security application as an native Android application as well eases the maintenance and makes interactions between the different applications easier. Therefore, the project will be realized as a native Android application. The IT Security application should be easy adaptable, hence all current Android versions must be supported.

To make the application easy to use under all circumstances it will be designed to not rely on an internet connection. Not every course room has an available Wi-Fi network. A direct connection between devices through Bluetooth or the installation of a local wireless network is be possible, but this creates overhead for the lecturers. Due to this and to reduce possible sources of errors, a communication between devices is not intended.

Workshops are typically divided into separate lessons. In Germany a lesson is usually 45 minutes long. This requires each learning module to be of the same length including introductions and discussions.

The workshop context influences the type of media that can be included as a learning material. While audio files and videos can be an asset in education, their benefit in a workshop context is limited. Playing several files at the same time leads to distraction of the participants. While the usage of headphones reduces this effect, the sense of community is reduced as well. Therefore, no features with auditory output are included within the application.

4.1.2. Learning Module Design

The format of a multimedia learning module describes the general interactions with the learning materials and the setting in which these materials are used. Several different formats of multimedia learning modules exist:

- Electronic compendiums (with a structure similar to classic lectures)
- Problem based learning scenarios
- Hybrid forms of both

The best approach depends on the learning content, learner and time frame. An electronic compendium features a strong instruction through either a lecturer or the learning system. This approach is beneficial for new or declarative learning content and communicating general knowledge about a topic. Since the target group has little to no prior experience about the learning content this format is suited best.
4.1. Learning Module Concept

The structure of the learning module will be organized in a deductive way, i.e., from an abstract point of view to special cases. A deductive approach supports the generation of fundamental knowledge. To improve the motivation of the topic a practical example can be given at the start of the lecture.

The process of segmentation and sequencing determines how the learners progress through the learning material. At first the learning material is segmented into small learning units. Learning units also depend on knowledge acquired within other units. However, different orderings or sequences of the learning units are possible. Considering the time frame of the workshop a linear successive sequencing of the learning units is suited best. A complex navigation between learning units can be considered overwhelming for the target group and leads to demotivation. To reduce the cognitive load, the content displayed at once is limited.

The learning goals influence the design of the exercises. The application will contain two separate learning modules with the following learning goals:

At first, within the **password learning module**, the learners are taught the following topics:

- What passwords are and why they are important.
- Generating secure passwords to protect devices and information.

Secondly, within the **information privacy and security learning module**, learners will be taught:

- Analyzing communication and data management in networked systems.
- Assessing these from the point of view of information privacy and information security.

The learning goals mentioned above, can be further specified for the target group. The senior citizens should be able to name and explain types of data they create while using computer systems. They should be able to explain why third parties could have interest in their data. They should be able to explain where their data is stored, e.g., when performing online banking transactions. The learner can explain terms information privacy and information security and give examples regarding a small network.

The presented learning goals mostly aim at providing factual knowledge about a topic the learners have little to no prior knowledge about. In addition to providing a basic conceptual understanding, skills are taught that are based upon the previous knowledge. To enhance the learning process repetition and frequent exercises should be used. Through examples and analogies, the relevance of the topics should be presented.

The design process of multimedia learning materials has a strong influence on the abilities of the learner to process these materials [17]. The efficiency of the developed materials depends on the learner, the setting, the structure of the materials and the quality of the learning material itself.
4.1. Learning Module Concept

Text is a main form of information transfer. Keeping the language simple helps reducing the extraneous cognitive load. Therefore, the prerequisite experience of the learner needs to be considered. The segmentation of text into smaller subsections improves the understanding of the content. To make these subsections easier to understand, plain language should be used. Important parts of the text can be highlighted by using bold text style to increase the attention. Short and structured sentences can be easier to process than long and nested sentences. The line length should not extend 80 characters per line, because long lines are harder to read. However, if the lines are to short the required eye movements breaks the reading flow. The optimal line length is between 60 and 80 characters.

A combination of text and images has a positive effect on the understanding process of the presented learning content. This benefit is dependent on the type of images. An excessive use of images to increase the optical appeal of the text hinders the learning effect. The images should be clear in their meaning to support the understanding process. When images are used in combination with text, e.g., labeling elements of an image, the text should be as close to the image as possible to avoid the splitting the attention of the learner. In general images can help the learning process through structuring the learning content, explaining complex principles or providing aid for transferring or memorizing the content.

The users interact with the application to manage their own learning process and solve tasks and exercises. The Human Computer Interaction (HCI) is determined by three factors: the user, the technology and the task to be solved. The goal is making the interaction with the computer as efficient and as user friendly as possible. To achieve this, the expected user behavior must be analyzed and guidelines for the designing of user interfaces must be followed. The following set design rules of graphical user interface was compiled by Shneiderman and should be considered [51].

1. Consistency of Procedures and Layout
2. Enable Shortcuts for experienced users
3. Feedback for every user interaction
4. Create closed processes
5. Include error prevention and methods for error solving
6. Allow users to undo actions
7. Let users feel in control of the system
8. Reduce cognitive load
4.1. Learning Module Concept

The interaction with the learning application can take different forms, but it should always be designed to support the learning process. Since the IT Security application will be used within a workshop context the possibilities for the learners to control their own learning process are limited as all learners should achieve the same learning goals within a limited time frame. The usage of tasks and exercises can benefit the learning process and can help memorizing and transferring the newly acquired knowledge and skills.

Assessments allow lecturer and learner alike to reflect on the learning process and gain insight on problematic areas. Questions used in assessments can be divided into three different groups: closed, semi-closed and open questions.

In **closed questions** the learner must select from predefined answers. **Semi-closed questions** require a specific answer which is known to the lecturer and can be evaluated. In contrast to the closed questions **open questions** do not have a unique solution. To allow automated assessments of the answers, the questions must either be closed or semi-closed. The learning application should be independent from other devices; therefore, the answers must be processed on the device of the learner.

The typing process on a tablet or smartphone might result in errors and could harm the motivation of the target group. Therefore, the questions and exercises should have a closed question format. If required, textual input is kept to a minimum.

Each exercise must provide helpful feedback to avoid possible misunderstandings or misconceptions. The learner must receive information about the quality. Additionally, information about the correct answer and a reasoning why it is correct should be provided. This is true even if the correct answer is chosen. It allows learners that were unsure or guessed an answer to improve their knowledge.

The adaptivity of a learning system describes the degree to which the learning system adjusts to the individual user. The purpose is to increase the learning process of the individual user. A platform that dynamically adjusts the difficulty of exercises and learning materials could be used to increase the performance of a learner. Such an approach is not suited for a learning module of the required duration. It could be a useful addition when the IT Security application is part of a larger standalone learning concept, where the learner has no time constraints.

The motivation of the learner is an important factor in the success of the learning process and must be considered in every step of the development of a learning system. Therefore, it interacts with the previously discussed designs. The main purposes of the motivational design are to keep the learners motivated and to avoid or reduce demotivating factors. Motivation is often categorized into four groups: Attention, Relevance, Confidence and Satisfaction. These motivational factors are contained in the Attention-Relevance-Confidence-Satisfaction-Model (**ARCS-Model**), which describes several methods to increase the motivation in a learning system. Depending on the conditions, i.e. the context, the time and the target group, under which the learning application should be used the following methods to maintain or improve the motivation of the learner can be applied.
The attention of the learner can be gained by making the learner curious about the learning materials. Unsolved questions that show possible implications or limitations of the learning materials can increase the motivation of the learner. This effect can be improved through variations in the presentation of information and the design of exercises. However, possible distractions must be reduced, because they have a negative impact on the attention of the learner.

The presented learning content must be relevant for the learner. Additionally, this relevance must be clarified for the learner, learning something that is envisioned to have a large impact on the everyday life of the learner can increase the motivation. This could be achieved through an explicit presentation of the learning goals to clarify what the learners can expect of this learning module. A description of the skills and knowledge which will be acquired during the learning module can be used to further clarify the relevance of the content. To show the relevance of the learning content during the learning module, examples and analogies can be taken from the field of expertise of the learner. Thereby, improving the learning process and showing the relevance of the learning content.

The probability to successfully finish the learning module and utilize the acquired skills and knowledge correctly describes the confidence of the learner. The confidence can be supported by clearly specifying the expected learning requirements. When exercises or tests are used the grading system must be obvious to the learners. If a task has a time constraint this must be explicitly stated. After exercises a detailed feedback is required to help the learner to reflect on their current capabilities and to emphasize new competences. The feedback should be detailed enough to support the motivation of the learner even in the case of mistakes.

The satisfaction of the learner describes the positive emotions connected to the learning process. It can be increased through exercises and tasks that allow utilizing the newly acquired knowledge and skills. Encouragement or praise after an exercise of adequate difficulty can increase the satisfaction of the learner. The satisfaction of the learner is also influenced by the consistency of the learning content. The advertised learning content must match the actual presented topic.

### 4.2. Design Goals

Within this section the goals for the design of the Security application are formulated and explained. These goals are based on the requirements of the target group, the mobile application usage of senior citizens and the learning module design.

**Usability**

Usability is a term describing the effectiveness, efficiency and satisfaction of a tool or application.

- The **effectiveness** determines the degree to which the application allows the users to achieve their goal.

- The **efficiency** is the amount of resources which are required to achieve these goals.
4.2. Design Goals

- The **satisfaction** describes the enjoyment of using the application.

All three aspects must be regarded to create an application that has a good usability.

In the previous chapters the requirements for the usage of applications through senior citizens have been formulated. To ensure that the IT Security application can be easily used a user-friendly design is required. Individual impairments of each user must be considered to provide an application which can be used by everyone. This requires personal information of the current user. This information can be gathered by a personalization application and is stored on the device. User interactions are analyzed, and suggestions are provided for the design of the user interface.

Exercises often require complex interactions of the user. Here the usability of the application is especially important. The forms of interactions must be intuitive and should be well described. The cognitive overhead for the interaction with the application must be minimal.

Since the IT Security application will be used by workshop lecturers and senior citizens it should be as stable as possible. Crashes and errors must be avoided as they have a strong impact on the motivation. Because the lectures might not have a background in IT Security fixing a device during a workshop is not an option.

**Quality of the Learning Materials**

The learning modules must be created regarding the prior knowledge and capabilities of the target group. All learning materials should be designed in a way that allows an efficient learning process without over- or underwhelming the learner. The created materials therefore should consider the cognitive load of the learner and must try to keep the extraneous cognitive load to a minimum. Used multimedia content should be beneficial for the learning process, otherwise it increases the extraneous cognitive load of the learner or is a distraction.

To avoid confusion and demotivation the learning modules must have clear structure. All materials should be easily accessible. To support the usage within a workshop the materials should be organized in a linear way. This makes monitoring of the progress of the learner easier and allows a better time management. To support the usage of the application as a standalone program a detailed description of the possible forms of user interaction is required. The application and the learning materials must be usable without guidance through a lecturer. When user interaction is required the tasks must be described clearly and the instructions must be detailed. During exercises and tests the underlying grading scheme should be transparent and fair. This helps avoiding demotivation. Additional motivational elements and features should be included in the design and development process early on.
4.3. Application Concept

Modularity

The IT Security application should be designed in a way that allows the exchange or alteration of existing features. Especially changes of the learning materials must be easy to handle. Therefore, the layout and the learning materials should be separated as much as possible from the core features of the application.

Created content must be reusable without too much effort. This allows the creation of new learning modules out of existing materials, for example for the creation of standalone and workshop lectures.

Support of existing Applications

The IT Security application must support two existing applications that are developed at the Lufgi9. The application supports the personalization of applications and the logging of user interactions.

The personalization application creates a text file within the external storage of the device. This file contains information e.g. about the required minimal button height, the relative text positions within buttons. The IT Security application must consider this personalization file to provide the users a graphical user interface that regards their individual capabilities and supports them in using the application.

The logging functionality is used to gather detailed information on the user interactions with the application. The IT Security application must support the logging of user interactions and must create logfiles with the same structure as provided by other applications developed by the Lufgi9.

Standalone vs. Workshop-Context

The resulting application should be usable both in a workshop-context and as a standalone application. Features that are used in a workshop should be disabled if they are not beneficial for the users which use the application on their own. All features and components of the application must be described in detail, since when used as a standalone application no additional external information can be provided.

4.3. Application Concept

Within this section the concept of the IT Security application is presented. At first the outline of the application is discussed then details of the concept are explained.

There are three different parties which all have an interest in the learning application:

- **Senior Citizens**
  The senior citizens want to learn about IT Security topics. They might have used a mobile device before. They want to use the application either within a workshop or on their own.

- **Lecturers**
  The Lectures want to use the application within a workshop. They only have a basic understanding of mobile devices and programming. They might want to alter the learning content or create new learning materials.
4.3. Application Concept

- **Researchers**
  
The researchers want to gather user data from the devices to gain insight on the way senior citizens use the devices and the learning materials. They want detailed information that can be automatically processed.

The application should be able to provide several different learning modules. This way it can be used in different courses and can provide a foundation for senior citizens that mainly learn at home. To reduce the cognitive overload for the senior citizens key features of the application should be consistent over all learning modules.

The navigation through the learning content must be easy to learn. Since the senior citizens might not be frequently using mobile devices or computers, the possible interactions with the learning application must be explained. To support users that have already used such devices the possible interactions and the resulting behavior should be consistent with other applications.

The creation of new learning modules or the alteration of currently existing modules must be possible. This allows Lecturers to extend the application. Therefore, the learning modules must be a modular component of the application as depicted in figure 4.2 on page 30. To modify an existing learning module, the modules themselves must consist of modular components that can be exchange with other components which is shown in figure 4.3 on page 30. This allows using existing components in multiple learning modules, e.g., some components can be used in a workshop environment and in a standalone application.

In order to achieve this modular structure, the learning components must be independent from each other, otherwise rearranging or reusing them is impossible. Therefore, the navigation between different learning components must be managed by the central application. To make the learning components as independent as possible and allow an easy creation of new learning components, other features e.g., should be managed by the central application as well.

These requirements result in the basic structure of the learning application that is depicted in figure 4.2 on page 30. As shown in the figure two types of components exists learning modules and utility modules. Both types of modules are managed by the central application. This application provides a basic framework, which contains e.g., the navigation between components.

This allows Lecturers to create materials without a detailed knowledge of the application. The components must therefore be included automatically into the learning materials wherever possible. However, a complete separation between learning modules and the basic functionality of the application is impossible. The logging of the user actions e.g., requires the usage of the logging functionality within the exercises to log exercise-specific events. Additionally, saving the application state cannot be completely separate, since the exercises need to persist their data themselves. Non-interactive learning materials however can be separated completely and require only minimal amounts of code to be included into the application.

As described within the design goals, the application must provide support for the logging of user interactions and the usage of a personalization file. In order to be consistent
4.3. Application Concept

with the modular design of the learning applications these functions should be usable an
easy exchangeable or customize able components. Therefore, they should be managed
by the central framework. They should only be active when the user wants to use this
functionality. The configuration of optional features should be placed within the settings
page.

The learning application must be usable in landscape and in portrait modus, depending
on the orientation of the device. If the senior citizens have used mobile devices before,
this allows them to use the learning application in the orientation, they are most com-
fortable with. Supporting multiple device orientations is an expected functionality. The
application must be equally usable in both orientations; therefore, the position of key
components and functions must be adjusted accordingly.
Chapter 5: Realization

Within this chapter the implementation of IT Security application is described. It is based upon the conceptual design presented in the previous chapter. This chapter begins with a presentation of the developed framework and its components. Then additional features of the application are discussed. The chapter is concluded with a detailed discussion of the created learning modules.

Within this chapter there are several images of the developed application. Since the language of the learning module is German these images are presented in German.

5.1. Overview

The IT Security application is realized as an application for the Android OS. Android has the largest market share of all sold mobile devices [48], therefore, the application can be utilized on many devices. An additional benefit is, that many participants are used to the device type and the OS. All Android applications have a corresponding Application Programming Interface (API) level. This level defines the minimal version number of the Android OS required to run this application. Since Android devices are often limited in the maximum Android OS version that can be installed on the device, the required API level has a direct influence the number of suitable devices for the IT Security application. The application is developed with a minimal API level of 15 which enables almost 100% of all Android devices to run the IT Security application.

The available resources, i.e. available Central Processing Unit (CPU), Random Access Memory (RAM) and storage, of the devices were considered in addition to the API level during the development of the IT Security application. Features that require too much resources were excluded to support older devices. The result is an application that is runnable on almost any Android tablet or smartphone, thereby allowing an easy adaption of the IT Security application for lecturers and senior citizens.

5.2. Structure

The structure of the main application is shown in the figure 5.1 on page 32. The application consists out of the application bar (top of 5.1a), a navigation bar (bottom of 5.1a) and the main section which contains the learning content (center of 5.1a). Applications on smartphones and tablets typically run either in portrait or in landscape orientation depending on how the device is held. This changes the display metrics, width and height, of the application. To support the user, the position of the navigation bar changes depending on the device orientation as depicted in figure 5.1b. This increases the available width of the application in the portrait orientation while increasing the available height in the landscape orientation, thereby allowing a comfortable presentation of learning.
5.2. Structure

materials. Additionally, through the positioning of the navigation bar on the side or on the lower end of the screen, the hand of the user is not blocking the line of view. To ensure that lefthanded user can comfortably use the application a left-handed mode can be activated in the settings. When this mode is active the navigation bar is displayed on the left side in landscape mode, this is shown in the figure 5.1b.

![Figure 5.1.](image)

(a) Portrait  
(b) Landscape with active lefthanded mode

Figure 5.1.: Structure of the application in different Device orientations

The navigation bar allows the learners to progress through the learning materials or to increase or decrease the font size of the presented content with a simple touch gesture. More advanced users can also use the swipe gesture to switch between pages. The ability to move between the learning materials can easily be altered for a specific fragment. Conditions can be specified which must be fulfilled before the learner can leave the fragment, e.g. to ensure the learner completes exercises or assessments before progressing towards the next fragment.

The readability of texts depends on the number of characters per line, as described within the previous chapter. To ensure that the provided texts are easy to read, the width of the main section scales with the current font sizes. The aim is to always provide an average number of 60 to 80 character per line. If the available screen size is too small to achieve this, the maximal available space is used. When a large device is used, the width of the main section is limited. The unused space is used as margin, i.e. an empty area at both sides of the main content. The background of the screen is intentionally set to a simple colored screen to avoid possible distractions, by shifting the focus away from the main content. Through choosing dark colors a strong contrast is created, which makes focusing on the learning content easier.
5.3. Additional Features

The basic structure of the IT Security application is designed in a modular way. It is simple to extend the application by creating new learning materials or new learning modules. This modularity is achieved through the creation of a framework which separates the learning content from the basic functionalities of the application. The framework contains all the utility functions and provides easy methods to alter the learning modules with only minimal changes to the source code.

The learning modules consist out of several different learning units that all implement the same interface. This allows to change existing learning modules and reuse created pages or elements within other learning modules. The learning units are completely independent from each other, therefore, a created learning unit can be used within a workshop context and in a standalone application.

While creating applications for Android devices the life cycle of the activity and its contents must be regarded. Changing the orientation of the device, e.g. rotating it from portrait mode to landscape mode, recreates the activity. Several other actions like switching towards another application, or exchanging the theme of the application, e.g. by using a zoom button on the navigation bar, have the same effect. To avoid confusion or frustration of the learner the current state of the application must be preserved. This is especially important for exercises and assessments. To achieve this all relevant information is stored, and during the recreation phase of the application and the fragment the data is used to recreate the previous state.

All text resources are saved in a centralized way; therefore, it is easier to maintain them. Adjustments can be made easily at a designated location. Using an external Extensible Markup Language (XML)-file for the language representation also allows an easy integration of new languages. When a new subfolder with a matching Strings.xml file is created, the language is automatically included and will be used if it is the current device language. The external storage allows an easy adaption of new languages because translators must work on only one file which enables them to do a quick and complete translation. Even partial translations are possible. All languages written from left to right and from top to bottom can be easily included into the IT Security application.

5.3.1. Images

The IT Security application contains many different pictures within the learning modules. Since the available space on the devices is limited, the size of the images is reduced to avoid too much scrolling. When users want to get a detailed view of an image, they can use a touch gesture. This results in a Fullscreen view of the picture. While in the Fullscreen view the users can interact with the images with the typically used gestures for image manipulation. The Fullscreen view allows zooming in and out of pictures.
5.3. Additional Features

and provides the opportunity to move the currently visible segment around the screen. The interaction with images in Fullscreen view aims at consistency with applications the users might be familiar with.

All images that are used within the application exist in two sizes. A small version that is included in the learning material and a large version that is used within the Fullscreen view mode. When tapping on a small image in the learning materials the large image is loaded instead. This reduces the amount of required RAM while working with the learning materials and at the same time provides users with high quality images when they switched to the Fullscreen mode to perceive details of the images.

5.3.2. Tutorial

A tutorial module has been created to support the users during their first usage of the application. The tutorial consists of multiple pages. Each page explains a specific form of interaction with the application. This is displayed in figure 5.2a, where elements of the navigation bar are explained. The tutorial module is automatically displayed at the start of every learning module. Experienced users can deactivate this functionality in the settings.

![Tutorial at the Start of the Application](image1)

![Manual for the Exercises](image2)

**Figure 5.2.** Tutorial for the application
5.3. Additional Features

The tutorial begins with welcoming the participants and explaining the purpose of the tutorial. Over the course of the tutorial the different ways to interact with the application are described. On each page there is a text indicating the end of this page and asking the user to press the “next”-button. At first the functionality to scroll through text is explained. After this the interaction with images is presented. As a precaution method all images that are used within the tutorial contain a description on how to return to the learning application when viewed in full screen mode. Then the navigation bar and its functions are presented in detail. If a functionality is not available all the time, the conditions are described under which it is available (see figure 5.2a on page 34). Thereby helping the user to analyze why a specific function might be disabled later. This reduces the amount of necessary in place explanation.

By using the tutorial module, the users receive all relevant information for the general interaction with the application. Specific interactions, i.e. for solving an exercise, must be explain in place so it is present when the user needs it. Figure 5.2b on page 34 shows the explanation of the drag & drop exercise. It contains information on the drag & drop gesture and presents a detailed step by step guide to use the gesture within the exercise.

5.3.3. Creation of new Learning Materials

All learning modules consists out of several small learning units. Each of this learning units corresponds to exactly one page in the final application. A learning unit contains at least one XML-File and one Java-Class file. The XML-File describes the general appearance of the learning unit and is displayed within the main content area of the learning application when the learning unit is displayed. Texts can either be displayed by including them directly into the XML-File or by binding them to specific elements of the file when the learning unit is created.

The following custom view elements were used to allow an easy usage of key components: a decorative headline and a text area with an automatic text flow around images. By using this custom view elements, new learning units can be created without consideration of the final display of the learning materials. The headline is automatically displayed with a larger font size and contains a decorative bar that stretches to both sides. The Texts areas with text flow support allow a combination of images and texts. The text is displayed automatically in a way that avoids the placed images. Line breaks are performed when there is not enough space. When possible, words are not split up, instead the sentence is divided at the closest whitespace character. The Text area considers the total available space and all possible obstacles. This is beneficial for the usage within the learning application, since the display size, the available text space and the image size can all change due to changing the orientation of the device or increasing or decreasing the selected font size. In addition the custom text areas allow formatting the displayed text by using HypertextMarkupLanguage (HTML)-Tags, e.g. to display text with a bold font style or ul to create and unordered list of objects. This enables the creators of learning materials to create new learning units with little knowledge about formatting the materials, while at the same time it allows them to include further elements for highlighting areas of interest or structuring the materials.
After creating an XML-File the Java-Class must be created. Every learning unit inherits the LectureFragment-Class. This class already contains features that each fragment must provide. When creating a new learning unit, the creator can use this default implementation without the need to write own code. In case the created learning unit should have specific features, e.g., the users must solve a specific task before switching to the next learning unit, this default implementations can be overwritten to define custom constraints. In addition to altering the behavior of the learning unit, the handling of images is defined within the Java-File. When an image should use the Fullscreen functionality a Listener can be defined and an image with a higher resolution can be linked with it.

After creating new learning units they can be included into existing learning modules within the LectureCreation-Class. Within this class the contents of learning modules can be altered, new learning units can be included, old units can be removed, and the ordering of the learning modules can be changed. Within the file new learning modules can be created as well, to use these modules they must also be registered within the MainActivity-Class.

When implementing a learning module, the exercise development is often especially time consuming. Several standard exercise types were developed within the thesis. These exercises were realized to allow an easy reusability. An abstract class was created that can be inherited. This class already contains several functionalities for a specific exercise type. To create, e.g., an exercise with multiple choice questions, the user must only provide a few lines of code to add the questions. Many other functions, e.g., displaying the questions, switching between question and feedback view, are already contained within the abstract class.

The creation of new learning materials is designed in a way that requires little previous knowledge from the user, while at the same time gives them the opportunity to create materials with different exercises to make their learning modules interactive.

5.3.4. Personalization Data

During previous workshops performed by the Lufgi9 user data was collected through the usage of a personalization application. The goal of this application is to gather data from the user and give estimations on optimal values for the minimal button size, the font size and many other components. The personalization data is stored in a predefined folder within the external storage of the device and is available to other applications. The personalization data supports individual user preferences.

To regard the user preferences in an appropriate way two possibilities, exist. The first is to create a generic page and adjust it accordingly to the required values. An example is to create a page as usual and the increase the font size of all displayed texts one after another. This approach allows a fine-grained consideration of the user preferences as the exact values can be considered. However, this means that every time a fragment is created it must be readjusted to the requested design.

The other alternative is the usage of themes. A theme consists of a predefined style which handles the representation of all elements. Themes can only be set at the startup of the
5.3. Additional Features

application and are immutable. This requires specifying themes for all combinations of style preferences (button height, text position within the buttons and the font size). This results in many themes as all combinations of the values must be considered. To keep the number of themes within reasonable bound, ranges of values can be combined. This reduces the granularity of the adjustments but allows an easy integration of the preferences without the need to adjust every element after creation.

Within the IT Security application the second approach was chosen, since it allows a better separation of the core functionalities and the learning materials. An additional benefit of this approach is the conservation of resources, since the representation must not be altered after creating it. Value ranges were used to determine the different settings. To determine the value ranges for the user preferences the data from previous workshops was collected and analyzed. The data set consisted out of 47 personalization files.

The effects of the personalization file are displayed in figure 5.3. The figure shows an exercise page without personalization file (figure 5.3a) and with the usage of a personalization file (figure 5.3b). The personalization file suggested the usage of larger buttons and an adjustment of the text position within the buttons. When directly comparing the two figures the buttons in the figure with personalization file are larger and the text is positioned above the center of the buttons. When no personalization file exists the text is positioned below the center of the buttons.
5.3. Additional Features

default representation is chosen.

5.3.5. Logging

Gathering user data from the target group can allow valuable insight on how the senior citizens are using the application and can be used to improve the application. To achieve this a detailed logging of user actions is required. Other application developed at the Lufgi9 use a predefined logging scheme for the storage of the user interactions. All actions are stored in a folder within the external storage of the device. Since the IT Security application should be usable in a workshop context and as a standalone application, the logging needs to be configurable. Therefore the IT Security application allows the alteration of the logging behavior.

The previously used logging application was replaced with a new component. The log data is stored within a Room database, an abstraction layer on top of an SQLite database system. SQLite is a small Structured Query Language (SQL) database, that often used within Android applications. The database is stored within the application; therefore, no access is required for the external storage. When an export is required the permissions can be requested. Instead of using a Text-File for the export, the IT Security application exports the SQLite database. This allows an easy integration of the captured user data from multiple devices within a central database. Additionally, log entries can be easier filtered and analyzed. Since the time is stored with each log entry the database can be configured to only keep the log data for a specified time period before erasing it.

The logging process itself was altered as well. The log files of seven applications, that were developed at the Lufgi9 were analyzed. The form, language and style of the different log files was very different. Therefore, a guideline was created for the logging process. It contains all information that should be logged and indicates which categories should be used for the different forms of log entries. Additionally, a range of predefined Logging functions was created that can be used for the logging of the position of all visible components of the currently displayed view. These functions improve the consistency of the created log files. If the log messages must be altered, they can be modified. The logging of user information is realized by the developed framework wherever possible, only special interactions during the usage of the exercises are not logged by the framework but must be logged by the exercises.

5.3.6. Settings

The IT Security application contains multiple options for customization of the application. Central feature like the support of the personalization data, the logging behavior, support for lefthanded users and many more can be activated or deactivated in the settings. Per default these features are deactivated. Therefore, the application only requires a minimal amount of permissions for the basic functionality. When features are activated that require additional permissions, writing to the external storage for the database export, the permissions are requested from the user.

The settings page also allows changing the currently selected learning module. When selecting a new module, it is automatically loaded in the background. Various learning
modules can be selected. This created content is reusable specific standalone, or workshop versions of learning module can be created and selected.

5.4. Modules

This section contains information about the developed learning modules. The content of each module is discussed, and highlights of each module are presented. The concept and the theoretical background of the exercises are explained.

5.4.1. Passwords

The learning module for the password creation follows a structured approach and has a linear ordering of the learning materials. The module begins with an introduction and motivation of the topic and a specification of the learning goals. Prerequisite knowledge is presented, and important concepts are briefly repeated.

The password module itself starts with an explanation of the idea of passwords and their use for authentication and identification in IT systems. This is followed by an official definition of the term password. Common criteria for password creation are explained. Then learners can deepen their knowledge in a short exercise (see below Password Creation Exercise). Common mistakes like the usage of patterns or using personal information for password creations are discussed. The threat of these mistakes is explained, and possible attacks are described.

After presenting how to create secure passwords the risks of reusing passwords are explained. An example is given to show a possible attack and the consequences. The different weaknesses of password are recapitulated in an exercises to help memorizing new information (see below Good vs. Bad Passwords Exercise). Since passwords are no object of the natural language people often have problems remembering them. A few methods to store passwords are presented and their weaknesses are discussed. The module is concluded by a summary of the presented topics and of the most important facts. After the summary the participants have to possibility to make a final exercise on the topic to test their knowledge (see below Final Exercise). After this an open discussion between the participants and the lecturer is encouraged. Several possible discussion topics (see below Discussion Topic) are provided to address questions the participants might have before the workshop. To compensate for the different speed at which the learners progress through the learning module, some questions are provided which the participants try to answer for themselves in preparation of the discussion.

As described above the password module aims at teaching basic concepts of the creation and usage of passwords. These concepts are motivated through examples to exemplify the threats and consequences of weak passwords or the reuse of passwords. The combination of new knowledge and exemplifying the relevance of this knowledge for IT Security can help the learners to actually use the acquired knowledge in their private life. Since this is a new field of expertise for the senior citizens, the aim of the exercises is to help memorizing the criteria for secure passwords and help identify common errors. Through repetition, highlighting the relevance of the topic and creating analogies the cognitive process of the knowledge acquisition is supported.
5.4. Modules

Password Creation Exercise

This exercise requires user to create a password which fulfills predefined requirements. A password must contain small, capital and special characters and numbers. A password must consist out of at least 8 characters. The users receive immediate feedback to the entered password. After each user input the current password is analyzed and possibly violated requirements are displayed. Most devices display the keyboard right below the entry field. Therefore, the feedback for the password quality is displayed above the entry field, this way it is always visible to the user. When an entered password fulfills the minimum requirements a color system is used to indicate the strength of the password. A password with more characters is perceived as more secure.

The password creation exercise requires special characters so that the user must find them on the displayed keyboard, since they are often only visible in a specific tab of the keyboard. In many online forms feedback on the security of the password is only visible after submitting. Within the password creation exercise the users receive feedback immediately. The feedback is detailed and lists every violated password condition. However, the password quality is estimated only by analyzing the types of characters used and the length of the password. Like most websites no semantic analysis of the password takes place for the quality estimation.

Good vs. Bad Passwords Exercise

Within this exercise the learners must evaluate a set of predefined passwords according to the rules they have learned before. The passwords can be evaluated by touching one of the buttons on the question page as depicted in figure 5.4a on page 41. Most of the passwords contain specific weakness which makes them less secure than expected. After categorizing a password, the users get feedback on their evaluation. The feedback page is shown in figure 5.4b. As shown in the figure the feedback contains information on the quality of the answer and it shows the correct answer. Furthermore, a detailed explanation for the correct answer is given.

While solving this exercise the learners must remember the rules and information for the creation of secure passwords. The passwords that are used during this exercise, highlight specific errors that users frequently make when creating passwords.

- Usage of dates
- Usage of real-world language
- Usage of keyboard patterns
- Usage of extremely common passwords

As described above the purpose of this exercise is not only to help the learners to memorize the learned content. It should help them to actively realize, that some types of passwords they have used before are unsecure.
Final Exercise

The secure password module is concluded by a final exercise. The purpose of this exercise is to recapitulate the acquired knowledge and skills and deepen the long-term understanding process. The exercise is realized as short test. The users must answer several multiple-choice questions.

An example question is shown in figure 5.5a on page 42. As shown in the figure for each question three possible answers are presented. An answer can be selected by touching it. The order of the answers is randomized. This creates a variation within the exercises and users must reread all answers if they take the test a second time. Additionally, when used within a workshop context, users can not imitate their neighbors, but are encouraged to solve the exercise on their own.

The exercise is envisioned to be more difficult than the previous exercise and requires a recapitulation of the newly acquired knowledge from the complete learning module. After an answer is selected a detailed feedback is given with an explanation of the correct answer. This feedback page is shown in figure 5.5b on page 42. As can be seen in the figure, the appearance of the feedback page is consistent to the previous exercise to reduce the cognitive load of the user.
Discussion Topic

When using the IT Security application within a workshop context a discussion between the participants is possible. The discussion allows the participants to use their newly acquired knowledge about passwords and transfer it to related topics. Additionally, social interaction and information exchange between participants is supported. The discussion can also be used to address questions of the participants.

Forgetting Passwords: Passwords are often long and complicated, what happens when a password is forgotten. In a discussion the lecturer can introduce the term security question. Security questions are often used to gain access to a password protected service, e.g., an email address, in case users forget their password. The questions often ask for personal information of the user: e.g., the favorite food or the maiden name of the mother. Within the group the consequences of these approaches should be discussed. Since these questions can often be answered by persons close to the user or people who did some research, they compromise the security of the password. Present alternative measures for password recovery can be discussed, e.g., providing a second email address at the password creation process which can be accessed to get the password back.
5.4. Modules

Two-Factor-Authentication: Is a password alone secure enough? How can the security be increased, and the authentication process secured? These questions can be discussed in a group, the solution is to ask for more than one information, a two-factor authentication [10]. Discuss methods how this can be achieved and name a popular example of a two-factor authentication method. Such an example is a cash card to withdraw money from your bank account. In order to withdraw money, the user has to have two things, the card and the corresponding PIN [10]. Discuss the danger of storing the two factors at the same place, e.g., keeping a note with the PIN in your wallet.

5.4.2. Information Security and Privacy

The learning module for the topics information security and information privacy is structured in a linear way. At first the topic is introduced, and the learning goals are presented together with a short motivation of the topic. Relevant knowledge from previous modules is presented to the participants and important concepts are briefly summarized. The different types of user data, e.g., personal information, user generated content and performed actions; are presented. They are explained with the example of a website to share recipes. Possible usage of this data is explained with the example of recommender systems and personalized advertisement. The interest of malicious third parties in the data is presented with the example of online banking. The knowledge about different types of user data and possible application for this data are tested within an exercise (see below My Data Exercise).

To prepare the explanation of the terms information privacy and information security a picture of a small network is shown and used to explain where the data of users is processed and stored. Different threats for user data are discussed and used to motivate the term of information security. Online banking is used as an example to explain the different threats, in addition to this each threat is provided with an example without IT support. The module continues with the presentation of the topic information privacy. Since these terms sound very similar in German, an exercise is used to help differentiate between information privacy and security (see below Ordering of terms Exercise). The module is concluded by a summary of the learning material and a final exercise (see below Final Exercise) to recapitulate the acquired knowledge. In analogy to the password module a discussion phase is included and several possible topics are provided (see below Discussion Topic).

The goal of the information privacy and security module is to teach basic knowledge of the types of data users create and the interest of third parties in this data. The terms information privacy and security are explained in detail. To support the learning process of the participants, analogies and examples are frequently used. The examples should help to memorize the new knowledge and connect it to already acquired wisdom. Especially the difference between the terms information privacy and information security are highlighted as the German terms for these concepts are very similar to each other, which can result in confusion. Through frequent repetition and exercises with detailed feedback the long-term memorization of the important concepts and terms should be enhanced.

My Data Exercise

This exercise is designed to help the user recapitulate the previously learned information: the different types of user data and the interest of third parties in this data. The aim of
5.4. Modules

This exercise is to support the memorization process and to deepen the understanding of the presented terms. The exercise itself consists of several different statements that the users must evaluate as either correct or incorrect. After giving an answer the users can see the correct answer classification and a detailed description on why this specific statement is correct or incorrect. The design of this exercise is similar to the design used within the Good vs. Bad Passwords Exercise. This consistency of the exercise design reduces the extraneous cognitive load of the exercise and helps users to focus on the exercise.

Ordering of terms Exercise

Within this exercise the users are given a list of several terms that must be sorted into the categories: information privacy and information security. The general layout of the exercise is depicted in 5.6a on page 45. At the start of the exercise all terms are placed within the box in the center of the screen. After analyzing a specific term, the users can move this term to a different category by using the drag and drop gesture. When an item is dragged its appearance changes, it becomes slightly transparent and follows the finger of the user, this is shown in figure 5.6b on page 45. Then it can be sorted in one of three boxes. The currently selected box is visually highlighted to help the users to see where they would place the item, indicated by a red border around the box. If a user tries to drop an item outside of the designated areas it is returned to the box where it was dragged from. All items can be moved between the boxes as often as the users want, even if they have already been placed within the correct box. The exercise is finished when all items are correctly placed within their designated box. To assist the users with their task a counter is placed above the boxes which indicates how many terms are currently assigned to a wrong box. Among the presented terms are some that do not specifically belong to the field of information privacy or security. The terms must not be sorted into other boxes but must stay in the neutral box. They serve as a distractor. The presence of such terms is explicitly stated within the exercise explanation. The explanation also contains a detailed description on how to drag and drop an item between the categories. By solving this exercise, the users improve their understanding of the terms information privacy and security and learn how to differentiate between these two topics.

Final Exercise

The final exercises within the information privacy and security module is designed in a similar way to the final exercise of the secure password learning module. The purpose of this is to maintain consistency over multiple learning modules. Therefore, all questions are multiple choice questions. For each question the users must choose one of three possible answers. Purpose of the presented questions is to help memorizing the learned concepts and to improve the differentiation between information privacy and information security.

Discussion Topics

In the following a few possible discussion topics are presented. The purpose of these topics is to increase the social interaction between the participants and confront them with new settings to which they can apply the newly acquired knowledge.
5.4. Modules

Search engines and Online Shops: Typically search engines and online shops save all search requests and all viewed or bought articles. Why do they do this? What is the benefit of this behavior? The collected data can be used to improve the services by recommending information or products that the user might be interested in. Gaining a detailed insight on the interests of the users can be useful in multiple contexts therefore such data could be sold.

Smart Homes: Many devices gather information about the environment to improve their services. An increasing number of devices can react to verbal commands to search for information, play music or offer other services. How do these devices work? Are the offered services worth the reduction in privacy?

Social Media: The world becomes interconnected and the social life of many people takes part online. Is this process positive or negative? Discuss the benefit and the risks of social media, regarding information privacy. Does social media improve the social behavior of people?

5.4.3. Additional Workshop Materials

To support the usage of the IT Security application within a workshop context, lecturers need information about the application and on the learning modules. Therefore, an information sheet was created that contains all important information about the...
application. The requirements for using the application are defined and a detailed description for the setup of the application and the selection of the learning module is given.

A short manual was created for each learning module that contains a summary of the presented learning content. The exercises are presented and problems, which the participants of a workshop can encounter, are described. A list of possible discussion topics is included, along with a short guideline for the discussion. The manual is concluded by a time schedule with the expected duration of the different parts of the learning module.

A handout sheet was created for every learning module. This can be given to all participants after they attended a course. The handout contains a short summary of the learning module and important facts that were presented. It supports the recapitulation of the course and the remembering of details. In case specific algorithms were presented during the learning module, e.g., the algorithm for creating secure passwords that can be easily memorized, the complete algorithm can be found on the handout. An example and a step by step explanation are included, thereby allowing the participants to follow the algorithm by them self. All handouts are created with a user-friendly font and use a large font size to ensure they can easily be read by every participant.
Part IV

EVALUATION AND DISCUSSION
Chapter 6: Evaluation

Within the previous chapters the design and the implementation of the IT Security application were described. To ensure that the developed application fulfills the requirements of the target group an evaluation is conducted. In the beginning of this chapter the basic process and the goals of the evaluation are presented. Then the continuous tests that were performed during the development phase are described. After this, all parts and tools that are used within the evaluation are presented and an explanation is given for their purpose. Next the study conduction is described. The chapter is concluded by a detailed analysis of the gathered data and the observations made during the evaluation.

6.1. Evaluation process

The purpose of an evaluation is to generate insight about a system or object under study. The generated knowledge can provide the basis for an assessment of the study subject and allows making profound decisions. Depending on the research question, an evaluation can be focused on specific criteria of the study subject.

While evaluations are frequently done, their quality and the usability of the results vary. To improve the evaluation process and generate results with a high quality, the Gesellschaft für Evaluation e.V. (DeGEval) created standards for evaluations. These contain information for their preparation, conduction and analysis. The standards formulated by the DeGEval are categorized into four groups: usefulness, conductivity, fairness and validity. These standards are regarded in the evaluation conducted within this thesis.

The standards that are proposed by the DeGEval aim at increasing the quality of evaluations in general. To ensure the quality of the evaluation, additional guidelines, that were specifically designed for the evaluation of multimedia learning applications, were followed.

Within the evaluation, different areas of the application will be analyzed: At first the usability of the application is evaluated, to ensure that the target group is capable to use the application as desired. Secondly the quality of the presented learning materials is studied, to show if they are well formulated and structured, and if the exercise tasks are precisely formulated.

6.2. Continuous Testing

Throughout the implementation of the IT Security application the functionality and usability of the application were regularly tested. The purpose of these tests was to determine if added features were functional and fit into the design of the application.
6.3. Study Preparation

The tests were done on multiple devices to ensure the application is usable with different screen sizes and Android versions.

In addition to functionality testing of the framework, the application and the learning modules were tested. The test candidates received a device with a preselected learning module. The test candidates were monitored while using the application. Feedback regarding the text materials and the exercise design was immediately recorded. After each testing session the overall feedback of the participants was collected in the form of an interview.

The continuous test resulted in various changes to the application. Several minor bugs were detected and fixed. In order to guide users during the first usage of the application a tutorial module was included. It explains all possible forms of interaction with the application in detail. In the early version of the application, dialog messages informed the user when they tried to perform unsupported actions, e.g. the try to increase the font size when the maximum font size was already selected. The dialog messages were removed since the sudden appearance of a dialog message confused the users; instead a visual indicator is now used to show that an action cannot be performed. The dialog message can be activated within the settings if a user requires more guidance.

The learning materials were revised, and unclear passages were extended to make them easier to understand. More line breaks were added to make the texts easier to read. Previously, all exercises contained a short explanation of the task. This explanation was separated from the exercises and is now displayed on the page before the exercise. The description of the task was extended and a short tutorial on the possible interactions with the exercise was included. The exercises themselves contain no further explanation, thereby maximizing the available space for displaying the contents of the exercise.

6.3. Study Preparation

The study preparation is an important part of an evaluation and can have a major impact on the quality of the generated results. In the following the conception of the user study is described.

6.3.1. Study Group

The users participating in the user study must come from the target group of the application. A specification of the partaking users is necessary to limit the number of variable factors and thereby increase the usefulness of the study. Therefore, the following participation requirements were set:

- All participants must be of age of 60 or above
- The participants must have used the Internet before
- The participants must have used a computer or a mobile device before
- The participants should not be experts in IT Security
The number of participants which take part in a user study has a strong impact on the usefulness of the results. While many participants can help determine influences and factors of the results in detail, the number of possible candidates is limited, and the conduction of a large-scale user study is a time-consuming task. Since parts on the evaluation are focused on the usability of the learning application, the number of necessary participants is derived from this: For usability studies of a small project the amount of necessary users is set between 5 [56, 57] and 7 [58]. This amount is estimated to find around 80% of all usability issues [56, 57].

Participants were recruited through personal contacts and by addressing organizations, clubs and communities that are frequented by the target group. A total of 15 potential candidates showed interest in the study. Out of these 2 dropped out because they did not answer further invitations. Another 3 could not participate in the study due to time conflicts. Therefore, the final study was conducted with 10 participants.

6.3.2. Consent Form

To be consistent with current law, a form of consent was created. This form contains basic information about the study in general. The different parts of the study were explained and the information that is gathered during each part is described. The rights of the participants are highlighted. In particular, the right of the user not to answer questions and the right to drop out of the study at any time were described. The last paragraph contains information about the stored data and the anonymity of the users. It was stated that the participants agreed to the consent form by taking part in the study after reading. Thereby no personal information or the need to sign the form is required.

6.3.3. Initial Survey

Before the start of the evaluation each participant must fill out a small survey. The initial survey that was developed for this user study can be found in the appendix C on page 82 of this thesis. The purpose of this survey is to gather demographic information about the participant and to gain insight on their previous experience with mobile devices and the internet. The following information were required from the participants:

- **Gender** [Male/Female]
- **Age** [Category: <60; 60-64; 65-69; 70-74; 75-79; 80-84; 85-89; 90+]
- **Computer Usage** [Never; once per month; once per week; multiple times per week; daily; multiple times per day]
- **Mobile Device Usage** [Never; once per month; once per week; multiple times per week; daily; multiple times per day]
- **Usage Context** [work; private]
- **What is a password?** [Free text]
- **What makes a password secure?** [Free text]
6.3. Study Preparation

- **How should passwords be stored?** [Free text]

The gender of the participants is requested to gain insight on the effect of the learning module on male or female participants. The age of the participants can give insight to differentiate between different ages within the target group. Although aging is an individual process, the likelihood and severity of impairments increase with age. The possible selection of the age is realized through blocks of 5 years. These age ranges are used to gather the relevant information from the participants without the need to fill in detailed personalized information.

The usage frequency of computers and mobile devices is required to determine how adapted the participants are in using these devices. Since the forms of interaction vary between these devices two questions are asked. The possible answers range from never to daily. The participants are asked to select the one that matches their device usage the best. To determine the motivation of the target group, the context in which the devices are used is requested. Multiple selections are possible.

The prior knowledge of the participants is gathered with free text questions in which the participants must answer questions about passwords and their security. The open answer format allows to gain detailed insight on the prior knowledge of the participants since they should give a short answer in their own words instead of checking a box.

### 6.3.4. Final Survey

The immediate feedback of the user is gathered with a feedback survey. The survey that was created to gather the feedback of the users can be found in the appendix D on page 84 of this thesis. It is based upon the System Usability Scale [SUS] [59]. An established usability survey is used to make the results comparable to other learning applications and to ensure that the participants are not biased by the phrasing of the question [60]. The SUS contains 10 statements about the usability of the system under study [60]. Each of these statements must be rated on a Likert scale [61] with five different checkboxes, ranging from strong disagreement to strong agreement with the statement. The questionnaire uses an odd number of responses; therefore, the participants can choose a neutral answer. Since the statements are formulated in a positive or negative way the participants need to read them carefully before rating them. After using the survey each rating is translated into a score from 0 to 4 point [59]. The total number of points is multiplied with the factor 2.5 and results in a SUS score with a value from 0 to 100 [59]. A high SUS score indicates a good estimated usability of the system [59, 60].

The SUS allows to receive feedback on the general usability of the program under study [60]; however, is cannot be used to identify a specific usability problem. Since only ten statements must be evaluated, the usage of the SUS does not require much time. This reduces the stress for the participants, which is beneficial for the target group. The statements are distinct from each other. The wording of the statements was slightly altered during the creation of the SUS questionnaire to make them easier to understand by the target group.

In addition to the questions of the standard SUS, two questions regarding the understandability of the texts and the complexity of the exercises were included. These questions...
used the same rating system as the previous questions and were formulated in the same way. Furthermore, three open questions were asked to gain information about things the participants liked, disliked or additional features they would like to have. This gives participants the opportunity to freely express their opinion on the application.

6.3.5. Task List

To ensure the participants understand how they can interact with the learning application the tutorial module was used. Here, the possible forms of interaction are presented and necessary information on the available controls are given. Then the participants were asked to study the learning module about secure password generation. Since the module utilizes a linear structure of the learning materials no further specification of the task was given. The participants could work with the materials at their own pace without any time constraints. The learning module on information privacy and security was not included in the task list since this would double the required time and might have a negative impact on the concentration and the cooperation of the participants in the interview and the discussion that follows the learning module usage.

6.3.6. Tools and Data Collection

Data was collected at three points from the participants of the user study. At the start of the study the users were asked to fill out the initial survey. The survey was realized as paper-based questionnaire with a large font size. The decision for a paper-based survey was made to reduce the possible stress on the participants, since they might not be as comfortable in filling out a survey on an electronic device. Additionally, possible problems by answering the free text question with a keyboard were avoided.

The learning application itself was used to log the interactions of the user. Viewed learning units, the time between page transitions, user input and user interactions with the device were logged by the application and stored within a database. The exercises within the application logged the given answers and the time required by the user to answer the questions.

Through capturing the user interactions and the timestamps it is possible to observe how long the users needed for each individual step through the learning module. By monitoring the progress within the exercises an analysis of the performance and the learning process is possible. Since every given answer was logged wrong answers can be analyzed to identify misunderstood concepts.

After the users had finished the learning module the final survey was done to gain insight on the general usability of the application. Finally, all participants took part in an interview. A set of questions was developed to guide the interviewer. However, the interviews were not performed in a structured procedure but instead as an open dialog. This allows the participants to freely express their thoughts and creates a more natural environment. When participants finished answering a question the guideline was used to ask questions that were still unanswered.
6.3. Study Preparation

6.3.7. Study Setup

Every participant received a fully charged tablet device of the same model. The tablets had a reflective display. No additional equipment was used in combination with the devices.

All devices were handed to the participants in landscape orientation. The participants were asked if they are lefthanded and if they were, they had the opportunity to receive a device with an active lefthanded mode. Every device had a new installation of the application to ensure that no influence by user generated data from previous users was possible. No personalization file was used to customize the learning application for an individual user. The required time for the personalization application would prolong the user study for each individual participant. The default settings of the application were set to the second highest font size.

6.3.8. Study Procedure

The procedure of the study was fixed to make sure the study was conducted on the same way with all participants. The duration of each task was estimated based on the times that were recorded during the pilot study. Additional buffer times where included to ensure that each participant has enough time to do the study at a comfortable pace. The result is the following study procedure:

- Preparation of the study materials
- Greeting of the participants and offering of refreshment
- Introduction and formalities (5 minutes)
- Initial survey (10 minutes)
- Usage of the learning module (35 minutes)
- Questionnaire and final interview (15 minutes)
- Discussion of the learning content and related topics
- Giving the handout to the participants
- Answering further questions from the participants about the study
- Thanking the participants for taking part in the evaluation
- Summarizing of notes
- Collection of user data from the device
6.3.9. Pilot Study

User studies are a time-consuming process and the number of eligible test candidates is limited. Therefore, a pilot study was conducted. The purpose of a pilot study is to find flaws and errors in the study design and to train the study leader for the actual user study. The results were analyzed, and the study setup was revised accordingly to ensure no avoidable problems occur during the actual user study.

Two pilot studies were made with a different focus. While the first study was done with computer science students the last pilot study was performed with a test candidate that matched almost all criteria of the study group. Each of the pilot studies followed the procedure that was prepared for the actual user study. The required time for each step of the user study was recorded. This time served as a basis for an approximation for the time required by the target group.

As a result of the first pilot study the password module was extended with a section on how to create passwords that are secure but still easy to remember. This is explained with an easy algorithm to create better passwords by using a short, memoizable sentence, a number and special characters. This algorithm is explained step by step with an example.

In addition to the extension of the learning content the existing texts were revised. The texts were reformatted, and the wording of the sentences was changed. The purpose of this alteration was to split the texts in smaller units that are easier to understand. Sentences that were too long or too complicated were split into multiple components.

The exercise description for the final exercise was slightly altered. The English word multiple choice was removed from the description after a test candidate stopped reading the text after encountering an unknown word, even though the word was explained in the next sentence. The feedback survey was slightly altered as well since the word “Inkonsistenzen” was confusing for a test candidate and needed further explanation. The word was exchanged for an easier understandable synonym and a short explanation was added.

6.4. Study Conduction

The study procedure followed the specific schedule. The valuation sessions were conducted over the course of two weeks. The evaluation was done with groups of people. It took place at the home of a participant of the evaluation session. This was done since many participants lived within proximity of each other. Also due to a reduced mobility of some participants conducting the study in rooms of the university would be impossible.

At first the participants were greeted; then a short introduction was done. Then the consent form was handed out and explained to the participants. After this, the initial survey was done. When all participants finished filling out the initial survey, the surveys were collected, and each participant received a tablet with the application. Lefthanded participants were asked if they wanted to use a left-handed version of the application. All participants worked through the learning application at their own speed. The progress of the participants was observed. Help was only offered if a participant closed the application or encountered problems with the build-in keyboard. After the participants finished the learning module, they were given the feedback survey. When the survey
was finished, additional refreshments were served. Once all participants of an evaluation session had finished the learning module and the feedback survey, additional feedback was collected by performing a short interview. Problems that had been observed during the trial were addressed within the interview. Then a discussion was started about the context of the learning module and related topics. The discussion was moderated, and impulses were given according to the discussion topic presented in chapter 5. All participants showed a strong interest and introduced own ideas and subtopics they were interested in. The related topics information privacy and information security were often mentioned as well, and participants explained a strong concern for these topics.

6.5. Study Results

Within this section the data gathered during the study is analyzed. After each study session, the new data was collected and compared to the previously acquired results. The learning modules and the materials used within the user study were all created in German, but for the discussion of the results of the user study an English translation of the collected feedback is used.

6.5.1. Analysis

At first, the data collected from the surveys and gathered by the devices was analyzed to gain insight on the overall usability of the application and to identify possible problem areas for the participants. Based on the initial surveys an analysis of the study group was performed. Then the required time for the learning module is considered and correlations between the time, the age and the prior experience with computers and mobile devices are regarded. The exercises are reviewed, and the performance of the participants is analyzed. The feedback questionnaires are discussed in detail and differences between the study groups are discussed.

Analysis of the study group

Within this section the study group is analyzed. The demographic information, the prior experience with computers and mobile devices and the prior knowledge about passwords are used to determine the capabilities of the study group. The data collected through the initial survey is used to gain insight on the following topics:

- Age distribution
- Gender distribution
- Distribution of prior computer usage
- Distribution of prior mobile device usage
- Usage context
- Prior knowledge about passwords
In total, 10 participants took part in the user study. Out of these there were four female and six male participants. The age of the participants is depicted in the figure 6.1. Except for the age range [65-69 years], all age categories were represented in the study. The average age of the female participants was 74.5 years. Thereby, it was slightly lower than the average age 76.16 of the male participants. The average age of all participants was 75.5 years. Since the survey used age ranges, the actual age of the participants is unknown. Therefore, the average age of each age category, e.g. 62 years for the age category from 60 to 64 years, was used for the calculations.

**Figure 6.1.: Age of the participants**

**Figure 6.2.: Computer and Mobile Device Usage of the Participants**
6.5. Study Results

Figure 6.2 on page 56 shows each participant’s prior experience with computers and mobile devices. Within this figure the participants are sorted ascendingly by the time they required for the learning module. All participants have used either computers or mobile devices before. All except one participant stated that they use one of these devices at least once per week. Seven of the participant use computers and/or mobile devices daily.

While almost all participants are frequently using computers and mobile devices, not every type of devices was equally used. The combined usage frequency of the device types is depicted in figure 6.3. The figure shows that 30% percent of the participants have little or no prior experience with mobile devices. From the 10 participants that filled out the initial survey all stated that they used computers and/or mobile devices in a private context. One participant was also using the devices in a working environment. This participant stated to use both, computers and mobile devices multiple times per day.

The prior knowledge about passwords was gathered through answering the following open questions:

- What is a password?
- What is a secure password?
- How should passwords be stored?
6.5. Study Results

For every question the number of received answers is gathered, then the answers are rated on their quality. All participants answered the first question; however, the quality of the answers differs greatly between the participants. While most participants gave a correct answer, some just wrote an example password. The second question was answered by eight participants. Two of these gave a bad or wrong answer. Only three participants gave an answer with a good quality that mentioned the requirements for numbers and special characters. Other requirements for secure passwords were not mentioned. Only five participants answered the third question. Among the answers there were two weak answers and only one answer with a good quality. The answers indicated, that most participants had a basic understanding of passwords in general. Advanced topics like the creation of secure passwords or good methods to store passwords were not as present.

The analysis of the initial survey shows that all participants that took part in the user study fulfilled the requirements and belong to the target group. The age and gender of the participants is evenly distributed. While many participants used computers and mobile devices daily, there were also users that rarely used such devices. In particular, some users had never used a mobile device before. The prior knowledge about secure passwords is basic, there are no IT Security experts among the study group.

Time

Within this section the total time the participants required for the completion of the learning module is analyzed. The demographic information of the participants and their prior experience with computers and mobile devices are compared to the required time to determine the following values:

- Average time required for the learning module
- Relations between required time and age
- Relations between required time and computer usage
- Relations between required time and mobile device usage

The time each participant required to finish the learning module is depicted in figure 6.4 on page 59. The participants are ordered by the time they required. The figure shows that most of the participants took between 20 and 32 minutes to finish the learning module. The average participant required 26 minutes. The fastest time to completion was 12 minutes while the slowest was 41 minutes. Since there is a large difference in the required time for some participants, possible reasons are analyzed below.

To identify the possible factors for the required time, the demographic data of the different participants were compared regarding differences between the participants that required less or more time than most of the other participants. The participant who required 41 minutes to finish the learning application was the only participant that used computers and mobile devices only once per month. Additionally, the participant had little prior knowledge about passwords and IT Security. The participants that finished the learning module in the shortest amount of time were all below 75 years old and were using computers and mobile devices daily.
Password Module: Required Time per Participant

![Required Time per Participant](image)

Figure 6.4.: Password Module: Required Time per Participant

Required time in correlation to age, the computer usage and the mobile device usage of the participants

![Required time and age](image-a)

(a) Required time and age of the participants

![Required time and computer usage](image-b)

(b) Required time and Computer Usage

![Required time and mobile usage](image-c)

(c) Required time and Mobile Device Usage

Figure 6.5.: Required time in correlation to age, the computer usage and the mobile device usage of the participants

Within the figure 6.5a, 6.5b and 6.5c on page 59, the required time is shown in correlation with the age, the prior computer usage and the prior mobile device usage of the participants. A regression graph is included within the figure to show the trends. As can be seen in figure 6.5a, the higher the age of the participants, the higher the required time. The figures 6.5b and 6.5c use a simple ordering of the prior knowledge on the x axis. A high x value indicates a frequent usage of the device. The figures indicate that a high usage frequency results in a lower required time.
6.5. Study Results

Performance

Within this section the performance of the users is analyzed. For every exercise within the learning module the following information is presented:

- Scores of each participant
- Failure rate for each question

Within the first exercise six passwords were presented to the participants that needed to be classified as good or bad. The presented passwords relate to the criteria that were presented in the learning application before. The number of correctly answered questions per participant is depicted in the figure 6.6a. As depicted in the figure most participants were able to correctly categorize the passwords. The lowest score was 50% correct answers the best scores were 100% correct answers. On average the participants managed to get 81.3% correct answers.

![Figure 6.6a: Number of correct answers per participant](image)

![Figure 6.6b: Percent of correct answers per question](image)

The chart [6.6a] shows the performance of the participants for each of the questions. All participants were able to correctly evaluate the last two passwords "14061951" and "ich-liebedich" as bad passwords. These passwords only contain a single character type and are not random combinations of characters. The password "qwertzui" was correctly as a bad password evaluated by 7 of the 10 participants. Even though this password only contains letters, it was evaluated as secure by three participants because the sequence of the characters seemed to be random, although it is part of the first row of characters on a German keyboard.

One participant stated to have evaluated the passwords not only on their security but also on how good they could be memorized. Therefore, the participant rated the passwords "i1p@27Oz!5BzhRib" and "5!gZe9vBa" as bad passwords.
6.5. Study Results

The final exercise was designed to test how good the participants understood the concepts of secure passwords. The test was designed as a multiple-choice test in which sentences must be completed by selecting one of three possible answers. The results of the tests are visualized in figure 6.7 on page 61. As shown in the figure 6.7a, the scores of the participants were lower than in the previous exercise. On average the participants received 1.7 out of 3 points during this exercise. This equals a success rate of 56.67%. Considering the percentage of correct answer per question, as depicted in figure 6.7b, it becomes obvious that most of the participants were able to answer the first and third question correctly. However, many participants had problems to finish the second statement: "A perfect (unbreakable) password..."

- does not exist. [Correct answer]
- contains numbers, letters and special characters [Distractor 1]
- consists out of at least 12 signs. [Distractor 2]

The answers of the participants were analyzed to determine if the participants guessed an answer or if one of the distractors was too strong. Out of all participants only three gave the correct answer. However, all other participants selected the answer "contains numbers, letters and special characters.". Thereby indicating that this distractor was selected because it contained important keywords that were part of the lecture.

![Figure 6.7: Password Module: Final Exercise](image)

Feedback questionnaire

Within this subsection the data gathered from the SUS survey is analyzed. The feedback survey used within the user study is found in the appendix D on page 84 of this thesis.

- Overall score
- Average score per question
After each evaluation session, the results of the questionnaires were analyzed. The results of the first evaluation session are depicted in figure 6.8. All answers are graded with a score from zero to four points. A score of zero indicates that the participant selected the answer that represents the worst possible usability, four points are for the best possible answer. The scores that are presented within this section are the average number of points that were given by the participants for each question. The scores all questions are summarized; the maximal achievable value is 40 points [59]. Finally, the total points are multiplied by the factor 2.5, this results in a SUS between 0% and 100% [59].

When analyzing the SUS questionnaires of the first evaluation session, the average score is 30.25 out of 40 points which equals a SUS of 75.625%. This score indicates a good usability of the system under study [60]. However, the results from the questionnaires highlight that using the system in general is too complicated. The following statements received a significantly lower score than the other statements:

- Statement 3: I think that I would need the support of a technical person to be able to use this program.
- Statement 8: I found the program very awkward to use.
- Statement 10: I needed to learn a lot of things before I could get going with this program.

This information was combined with the observed user behavior and the direct feedback of the participants. The exercises were perceived as being too difficult. This is also indicated by the additional questions on the SUS questionnaires. While the users rated the texts as very easy to understand with 3.75 of 4 possible points, the difficulty of the exercises was rated with 2.75 out of 4 possible points. Specifically, the password creation exercise was problematic for the participants.
To improve the overall usability of the application this exercise was further investigated. The feedback of the users was compared to the data logs and possible sources for errors were analyzed. The following tasks were especially difficult for the participants:

- **Usage of Special Characters**
  The participants often had problems when entering special characters, many inserted other special characters than the ones allowed in the exercise.

- **Unable to Identify Wrong Characters**
  While the exercise provides the user with feedback that is updated after every button press, the participants often entered the password they had in mind first and then looked at the feedback text. This led to users being unable to identify false characters since all characters other than the last entered one are masked. Therefore, the users deleted the complete password and started again.

This resulted in two alterations of the password creation exercise that took place between the first and the second evaluation session. The exercise was altered so that more special characters were accepted. While the exercise description already contained a list of allowed special characters the word “following” was changed to a bold font type to emphasize that only these characters should be used. Finally, the input field for the password creation was altered. Previously, all characters, except for the last entered one, were masked. Now the complete input is visible at all time.

After all other evaluations were done, the data gathered during the first session was compared with the data gathered from the rest of the evaluation. The values gathered by the evaluation are visualized in figure 6.9. Between the evaluations large differences in the values for statements 3 and 8 can be observed. This indicates that the changes that were made to the password creation exercise were beneficial to the overall usability of
6.5. Study Results

the application.

The figure 6.10 shows the data from all SUS questionnaires. Since all evaluation sessions were combined the score of the statements 3 and 8 is still lower than the average score of the other statements. The total SUS for the system is 33.8 out of 40 points or 84.5%. This indicates a good to excellent usability of the learning application [60]. The texts were perceived as being easy to understand with 3.8 out of 4 points. The difficulty of the exercises was rated with 3.3 out of 4 points.

6.5.2. User Comments and Feature Requests

Within this section the open questions on the feedback surveys are analyzed. Things the participants liked or disliked about the system are regarded and possible explanations are provided. The feedback is extended with the responses recorded during the interviews. The section is concluded with the feature requests of the participants.

Things the participants liked

After using the learning application, the participants mentioned several points they liked about the application:

- "It is easy to use the application."
  Four of the ten participants liked that the interaction with the application is easy. One of these participants also stated to like that there was a detailed explanation before each exercise.

- "The structure of the content is helpful."
  Three of the participants specifically mentioned the perceived helpful structure of the materials.

- "The texts are easy to understand."
  Three participants liked that the texts were easy to understand and did not contain much domain-specific language.
6.5. Study Results

Things the participants did not like

The feedback of the participants contained a few points they did not like about the application. The comments are presented below along with a description of the error and a possible solution.

• "The exercises are too difficult"
  Two participants within the first user study session stated that the exercises are too difficult. Both participants had problems with the password creation exercise. This problem was immediately addressed and was described in detail in the section above.

• "It is hard to see the display"
  One participant stated that the display was hard to see. All devices used within the user study had a reflecting screen. This results in problems seeing the display when the angle by which the participants look at the devices is similar to the angle between the light source and the device. A tablet holder with a variable angle can help to deal with this problem. Alternatively, a tablet with a non-reflective display could be used.

• "The buttons on the bottom of the screen are confusing"
  This comment was made by a participant that previously managed to leave the application by accidently pressing one of the hardware buttons on the tablet. The participant used the device in landscape orientation. The device was held with one or two hands on the bottom while the upper part of the device was resting on the edge of the table. By holding the tablet in this way, the fingers were close to the hardware buttons. When readjusting the device to use a function of the navigation bar the participant accidently pressed one of the hardware buttons. This problem could be solved, similar to the issue mentioned above, by using a tablet holder to see if the participants are comfortable with the device standing before them rather than holding it themselves. Alternatively, an explanation about the hardware buttons can be included that is either done before the participants receive the devices or is within the tutorial.

• "The keyboard is hard to use"
  During the second user study session there was one participant that had many problems using the keyboard of the tablets. The participant was using the device in landscape orientation. The device was held in the left hand and the participant tried to input characters with the right hand. Due to changes of the tablet position, the displayed keyboards were frequently switched, alternated between the keyboard layout for characters and the layouts for special characters and other symbols. Like the problems described above, the problem can be reduced if a holder for the tablets is used.

• "It is difficult to close the keyboard."
  Three participants mentioned that the functionality to close the keyboard was not obvious enough. The displayed keyboard can either be closed by pressing the "Finished"-Button on the keyboard layout itself or by using the "Back"-Hardware button on the mobile device.
Feature Requests and additional responses

There was no specific feature requested by multiple participants of the user study. Instead the participants gave several additional responses that include further usage of the application and express their interest in the topic. The responses were made:

- "I would like to learn more about..."
  Five of the participants explicitly stated that they would like to receive information on this or similar topics regularly.

- "I would like the application to be available online."
  A participant wrote that he or she would like to be able to download the application. The writer would like if more people would have the opportunity to improve or test their knowledge on the usage and the importance of secure passwords.

- "I would like to have such a program for my own use."
  One participant stated to want to use a similar program for the education of clients and colleagues at work.
Chapter 7: Discussion

Within this chapter the results of the evaluation are discussed. At first the design goals that were planned for the IT Security application are analyzed. This is followed by an interpretation of the results of the evaluation. Possible limitations of the results are discussed at the end of this chapter.

7.1. Discussion of the Design Goals

In Section 4.2 several design goals were introduced that the IT Security application should achieve. Within this section the design and the implementation of the IT Security application are analyzed to see if they were indeed fulfilled.

Usability

The main design goal for the creation of the IT Security application was to create an application that is easily usable by senior citizens. Since the users can suffer from different age-related impairments and have hence specific requirements, the application was created with the target group in mind.

The design and the realization of the developed application and the created learning modules were based upon guidelines for the creation of learning applications. Additionally, current research regarding the interaction of senior citizens with mobile devices was considered during the development process. The methods of interaction and the design of the application is consistent across the developed learning modules. Further methods for the customization of the application and the support of a personalization file were included. All included features were evaluated regarding their usage within a workshop context.

The conducted evaluation was systematically performed and used the SUS to determine the perceived usability. The application achieved a SUS of 84.5% which indicates a good to excellent usability [60]. Among the test candidates were participants that have never used a mobile device before, however they still were able to use the application and finished the learning module successfully.

Quality of the Learning Materials

The learning materials that are used within the modules were created specifically for the target group. Guidelines for the development of learning materials were used in the creation process. The learning goals and the skills that should be acquired were analyzed and appropriate learning materials were developed. The capabilities of the target group were considered during the development of the learning materials. Therefore, no time critical operations of materials were used during the learning module design. Text is
chosen as the main form of knowledge transfer; therefore, they were created to be easily understandable by the target group. All texts were written without using English terms or domain specific language. The sentences were mostly short and used simple language.

The participants of the user study rated the texts as being easy to understand. The exercises within the learning module have shown that the users were able to correctly judge passwords based on their security. The performance of the users was slightly worse for the second exercise. For the second exercise, whose questions were suited to deepen the understanding of the participants for the topic. All participants took actively part in the discussions and showed an interest in further topics related to secure passwords and IT security in general.

Modularity

As described within the previous chapters the application itself and each learning module were designed to be modular and easy extendable. The creation of new learning materials can be done with basic programming skills. Many features were designed in a way that allows a central management. For example, almost all log data is created in the core component of the application which allows an easy exchange of either the logging functionality or the learning materials. The materials themselves are not linked together but can be reordered at will.

Support of existing components

The developed application fully supports the personalization files that are created by the personalization application. However, while all data from the files is processed, not every value is used for the application. The most important features for the target group were analyzed and the corresponding values were considered. Special focus was put on the font size of the application. The user can easily control the desired font size at any time through the controls on the side of the screen.

The logging of the user interactions was realized after analyzing the logfiles from several other applications that were developed at the Lufgi9. Required information was filtered and the logging messages were altered to create a unified logging style. The categories that were used for the logging process were revised and do now provide a clear distinction between the different log events.

Standalone vs. Workshop-Context

The application was used in a workshop environment with 5 participants. The participants were able to complete the learning application on their own without introduction to the program by the lecturer. All participants were able to finish the course. After this the participants took part in a discussion about the contents of the learning module. The learning application itself is not dependent on the interaction between the participants. It can be done by a single participant as well. If a learning module should be used that is specifically made for the use as a standalone learning application this can be easily done. As discussed above the application is modular and learning units can be created or exchanged with basic knowledge of the program.

The usage as a standalone application can be difficult for users that have never used mobile devices before. During the evaluation some users without prior experience managed
7.2. Interpretation of the Results

Within this section the results of the user study are interpreted considering the research questions that motivated the thesis.

The developed application was used to teach senior citizens fundamental knowledge about the usage of secure passwords. The learning module was utilized within a workshop context. All participants were able to successfully use the application even if they had not used mobile devices before. The usability of the application was evaluated and received a good to excellent rating based on the SUS score of 84.5% [60].

The participants had varying prior knowledge of the topic. The analysis of the performed exercises has shown that the users were able to correctly classify passwords according to the criteria learned within the learning module. More complex knowledge of the topic was acquired as well. All participants showed a great interest in the topic after using the learning module.

During the preparation and the conduction of the user study, further observations were made regarding the usage of the learning application by senior citizens.

It is important to use a simple language when creating learning applications for senior citizens. Even English words that are frequently used within plain language, e.g. “multiple-choice”, can be unknown to senior citizens. When confronted with an unknown word, a senior citizen stopped using the application. Words that are not frequently used within common language should be avoided as well, e.g. “Inkonsistenzen”.

The exercise design can have a strong influence on the experienced usability of the learning application for senior citizens. When comparing the surveys of the first user study session with the other surveys, the effects of small changes to the password creation exercise were observed: the perceived usability of the application increased strongly.

Senior citizens that have never used a mobile device before had often problems with accidently pushing the hardware buttons on the devices. Since users without prior experience cannot differentiate between the functionality of the program and the functions of the device, they do not know how to return to the application on their own.

A high variation in the required time to finish the learning module was observed during the evaluation. Based on the demographic data and the usage frequency of computer and mobile devices possible influences were analyzed. Older participants required more time to finish the learning application. Similarly, participants that frequently use such devices required less time. When using the application in a workshop context, gathering this information can help to estimate the required time for the course.
7.3. Limitations of the Results

The study setup and the selection of participants can have an impact on the generalization of the user study. Within this section the limitations of the evaluation’s results are discussed.

- **Size of the Study Group**
The user study was conducted with 10 participants. This amount of people is sufficient for usability studies for a project of this size. The analysis of the collected data showed correlations between the age, the computer usage and the mobile device usage of the participants and the time they required to finish the learning module. However, due to the high variation in the required time this result cannot be generalized.

- **Capabilities of the Study Group**
All participants of the user study were still living on their own and did not require special assistance. Therefore, the results of the user study might not be comparable for senior citizens that live in retirement homes or similar institutions.

- **Nationality of the Study Group**
The study was performed with German senior citizens and the learning module was specifically created in German. Therefore, no knowledge was generated about the possible benefit of the application for senior citizens from other countries.

- **Study performed Locally**
All participants were recruited locally, within an area of approximately 150km. Therefore, the study group might not be an accurate representation of German senior citizens in general as education and the availability of technical equipment varies between different states.

- **Size of the Study Group compared to a Workshop**
The application was tested with small groups of people. The usage of the application was monitored, and a discussion took place in which the participants could express their opinions and concerns. Within computer courses for senior citizens the number of participants is typically bigger than within the user study. This makes the observation of the participants’ individual progress and difficulties harder and can hinder the equal participation of everyone within the discussion.

- **Long Term Memorization**
Each evaluation session took between 1 and 1.5 hours. There were no further tests with the participants after the evaluation session ended. Therefore, there is no information on the long-term memorization of the provided information.
7.3. Limitations of the Results

- **Change in User Behavior**
  The learning application provided the participants with detailed information about the usage of secure passwords. While the creation, storage and the danger of reusing passwords were discussed, no information was collected on how many participants changed their usage of passwords after taking part in the workshop.
Part V

CONCLUSION
Chapter 8: Conclusion

This chapter begins with a summary of the thesis and of the results obtained by the user study. A section on future work and future research concludes the thesis.

8.1. Summary

Computers and mobile devices have become an important part in the daily lives of most German citizens. These new technologies were quickly adopted by younger generations. Recently, senior citizens begin to use these technologies more frequently. The reasons for this vary: e.g., staying in contact with family members, taking part in communities, or use one of many services offered in the internet. While the internet offers many possibilities, there are many threats as well. In order to protect senior citizens a basic understanding of key features is important.

Within this thesis the special requirements and possible impairments due to old age of senior citizens were analyzed. Current approaches to teach senior citizens computer skills and currently existing forms to teach IT Security were analyzed. The approaches were unsuited for the education of senior citizens since they often required prior knowledge and were only offered in English. Furthermore, these approaches did not consider possible impairments due to old age. A new learning application was designed and developed that considers senior citizens as the target group. Research regarding the mobile device usage by senior citizens in general and specifically in classroom or workshop environments was considered during this process. The design and implementation of this learning application were presented within this thesis. Two learning modules were created: the secure passwords module and the data privacy and security module. During the design and development of the learning modules current guidelines for the creation of learning modules were considered. The finished application was evaluated through a user study. The study and the utilized tools were described in detail within this thesis.

The evaluation of the learning application show that it is useful for teaching senior citizens about the importance of secure passwords. The usability of the learning application was measured with the SUS and showed that the learning application was perceived as having a good to excellent usability by the target group. In particular, small changes to the program showed significant improvements in the perceived usability of the system, which in return shows the importance to consider the requirements of senior citizens in order to provide applications that can be easily used by them.
8.2. Future Work

Within this section possible future work and research is discussed. The topics are based upon the discussion of the evaluation results and the limitations of the user study.

The framework which was created for the IT Security application could be utilized to present other relevant concepts of computer science to senior citizens to further increase their knowledge. An adaption of the framework in other fields of education is also possible.

The IT Security application was created with German senior citizens as the target group. The developed framework and the learning content could be used for the education of senior citizens in other countries: additional languages can be included into the application through the provision of a Strings.xml file in the corresponding language. Further studies could then be performed with senior citizens of other countries, providing insight on the usage of the application as a standalone version for other countries.

The user study showed large variations in the time required to finish the learning module. While data indicated a correlation between the age of the participants, prior experience with computer and mobile devices, and the required time, the study group was not large enough to determine the effect of these factors. Further studies could be performed to estimate the required time. Such an estimation could either be used for the creation of workshop units or to adapt the learning contents to the capabilities of the learner by utilizing more difficult exercises or including additional, individual content for users that are faster than the average participant.

During this user study there was no data collected on the long-term effects of the learning materials. It can be beneficial to collect data on how well the participants are able to recapitulate the contents of the learning materials after an extended period. Since the best result of the secure password module would be a change in the behavior of the participants a study on the long-time effects of the learning materials is of interest. The participants of such a study could be contacted after a year and asked how many changed their password creation behavior.
## Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>API</strong></td>
<td>Application Programming Interface</td>
</tr>
<tr>
<td><strong>ARCS-Model</strong></td>
<td>Attention-Relevance-Confidence-Satisfaction-Model</td>
</tr>
<tr>
<td><strong>CLT</strong></td>
<td>Cognitive Load Theory</td>
</tr>
<tr>
<td><strong>CPU</strong></td>
<td>Central Processing Unit</td>
</tr>
<tr>
<td><strong>DeGEval</strong></td>
<td>Gesellschaft für Evaluation e.V.</td>
</tr>
<tr>
<td><strong>DoS</strong></td>
<td>Denial-of-Service</td>
</tr>
<tr>
<td><strong>e.g.</strong></td>
<td>exempli gratia (lt. for example)</td>
</tr>
<tr>
<td><strong>HCI</strong></td>
<td>Human Computer Interaction</td>
</tr>
<tr>
<td><strong>HTML</strong></td>
<td>Hypertext Markup Language</td>
</tr>
<tr>
<td><strong>ICT</strong></td>
<td>Information and Communication Technology</td>
</tr>
<tr>
<td><strong>ID</strong></td>
<td>Instructional Design</td>
</tr>
<tr>
<td><strong>i.e.</strong></td>
<td>id est (lt. in other words)</td>
</tr>
<tr>
<td><strong>IT</strong></td>
<td>Information Technology</td>
</tr>
<tr>
<td><strong>Lufgi9</strong></td>
<td>Lehr- und Forschungsgebiet Informatik 9</td>
</tr>
<tr>
<td><strong>OS</strong></td>
<td>Operating System</td>
</tr>
<tr>
<td><strong>RAM</strong></td>
<td>Random Access Memory</td>
</tr>
<tr>
<td><strong>SUS</strong></td>
<td>System Usability Scale</td>
</tr>
<tr>
<td><strong>SQL</strong></td>
<td>Structured Query Language</td>
</tr>
<tr>
<td><strong>Wi-Fi</strong></td>
<td>Wireless Fidelity</td>
</tr>
<tr>
<td><strong>XML</strong></td>
<td>Extensible Markup Language</td>
</tr>
</tbody>
</table>
Appendix A: Bibliography


A. Bibliography


A. Bibliography


A. Bibliography


A. Bibliography


# Appendix B: List of Figures

<table>
<thead>
<tr>
<th>Figure Number</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1</td>
<td>The Decision Oriented Instructional Design Model (Adapted and Redrawn from [17])</td>
<td>21</td>
</tr>
<tr>
<td>4.2</td>
<td>The structure of the application</td>
<td>30</td>
</tr>
<tr>
<td>4.3</td>
<td>The structure of a learning module</td>
<td>30</td>
</tr>
<tr>
<td>5.1</td>
<td>Structure of the application in different Device orientations</td>
<td>32</td>
</tr>
<tr>
<td>5.2</td>
<td>Tutorial for the application</td>
<td>34</td>
</tr>
<tr>
<td>5.3</td>
<td>Example Effects of the Personalization File</td>
<td>37</td>
</tr>
<tr>
<td>5.4</td>
<td>Password Module: Good and Bad Passwords</td>
<td>41</td>
</tr>
<tr>
<td>5.5</td>
<td>Password Module: Final Exercise</td>
<td>42</td>
</tr>
<tr>
<td>5.6</td>
<td>Information Privacy and Security: Drag and Drop Exercise</td>
<td>45</td>
</tr>
<tr>
<td>6.1</td>
<td>Age of the participants</td>
<td>56</td>
</tr>
<tr>
<td>6.2</td>
<td>Computer and Mobile Device Usage of the Participants</td>
<td>56</td>
</tr>
<tr>
<td>6.3</td>
<td>Usage Frequency of Computers and Mobile Devices</td>
<td>57</td>
</tr>
<tr>
<td>6.4</td>
<td>Password Module: Required Time per Participant</td>
<td>59</td>
</tr>
<tr>
<td>6.5</td>
<td>Required time in correlation to age, the computer usage and the mobile device usage of the participants</td>
<td>59</td>
</tr>
<tr>
<td>6.6</td>
<td>Exercise: Good and Bad Passwords</td>
<td>60</td>
</tr>
<tr>
<td>6.7</td>
<td>Password Module: Final Exercise</td>
<td>61</td>
</tr>
<tr>
<td>6.8</td>
<td>SUS of the first evaluation session</td>
<td>62</td>
</tr>
<tr>
<td>6.9</td>
<td>Comparison of the SUS Scale of the First and Second Evaluation Session</td>
<td>63</td>
</tr>
<tr>
<td>6.10</td>
<td>SUS of all evaluation sessions</td>
<td>64</td>
</tr>
</tbody>
</table>
Appendix C: Initial Survey

Fragebogen:
Geschlecht:
□ männlich    □ weiblich

Alter:
□ <60   □ 60-64  □ 65-69  □ 70-74
□ 75-79  □ 80-84  □ 85-89  □ 90+

Gebrauch von Computern:
□ Noch nie    □ Mehrmals pro Woche
□ Einmal pro Monat □ Täglich
□ Einmal pro Woche □ Mehrmals am Tag

Gebrauch von mobilen Geräten (Smartphones, Tablets o.ä.):
□ Noch nie    □ Mehrmals pro Woche
□ Einmal pro Monat □ Täglich
□ Einmal pro Woche □ Mehrmals am Tag

In welchem Zusammenhang benutzen Sie die Geräte
□ Beruflich    □ privat
Versuchen Sie die folgenden Fragen kurz in ein bis zwei Sätzen zu beantworten. Sollten Sie auf eine Frage keine Antwort wissen, können Sie das Feld leer lassen.

Was ist ein Passwort?

Was kennzeichnet ein sicheres Passwort?

Wie sollte man Passwörter speichern / aufbewahren?
Appendix D: Final Survey

**Fragebogen:**

Im Folgenden sehen sie einige Aussagen. Sie können diese bewerten indem Sie eines der Kästchen ankreuzen.

Vielen Dank für Ihre Unterstützung!

**Das Programm ist einfach zu benutzen.**

Lehne stark ab □ □ □ □ □ Stimme stark zu

**Ich finde das Programm unnötig komplex.**

Lehne stark ab □ □ □ □ □ Stimme stark zu

**Ich würde die Unterstützung einer erfahrenen Person brauchen, um in der Lage zu sein das Programm zu benutzen.**

Lehne stark ab □ □ □ □ □ Stimme stark zu

**Ich kann mir sehr gut vorstellen, das Programm regelmäßig zu nutzen.**

Lehne stark ab □ □ □ □ □ Stimme stark zu

**Ich finde, dass die verschiedenen Funktionen des Programms gut integriert sind.**

Lehne stark ab □ □ □ □ □ Stimme stark zu
Ich finde, dass es im Programm zu viele Unstimmigkeiten (unterschiedliche Darstellungen, Änderungen der Funktionsweise) gibt.

| Lehne stark ab | ☐ ☐ ☐ ☐ ☐ | Stimme stark zu |

Ich kann mir vorstellen, dass die meisten Leute sehr schnell lernen würden, mit diesem Programm umzugehen.

| Lehne stark ab | ☐ ☐ ☐ ☐ ☐ | Stimme stark zu |

Ich finde das Programm sehr schwerfällig im Gebrauch.

| Lehne stark ab | ☐ ☐ ☐ ☐ ☐ | Stimme stark zu |

Ich fühle mich sehr sicher bei der Benutzung des Programms.

| Lehne stark ab | ☐ ☐ ☐ ☐ ☐ | Stimme stark zu |

Ich musste eine Menge Dinge lernen, bevor ich mit dem Programm arbeiten konnte.

| Lehne stark ab | ☐ ☐ ☐ ☐ ☐ | Stimme stark zu |

Ich finde die Texte sind gut zu verstehen.

| Lehne stark ab | ☐ ☐ ☐ ☐ ☐ | Stimme stark zu |

Ich finde die Übungen zu kompliziert.

| Lehne stark ab | ☐ ☐ ☐ ☐ ☐ | Stimme stark zu |
Versuchen Sie die folgenden Fragen kurz in ein bis zwei Sätzen zu beantworten. Sollten Sie auf eine Frage keine Antwort wissen, können Sie das Feld leer lassen.

Mir hat gut gefallen, dass...

Mir hat nicht gefallen, dass...

Ich fände es gut, wenn...
Eidesstattliche Versicherung

Nellesen, Marcel 292155

Name, Vorname Matrikelnummer (freiwillige Angabe)

Ich versichere hiermit an Eides Statt, dass ich die vorliegende Arbeit/Bachelorarbeit/Masterarbeit* mit dem Titel

Design and Implementation of a Learning Application to Sensitize Senior Citizens for Internet Security

selbstständig und ohne unzulässige Hilfe erbracht habe. Ich habe keine anderen als die angegebenen Quellen und Hilfsmittel benutzt. Für den Fall, dass die Arbeit zusätz-lich auf einem Datenträger eingereicht wird, erkläre ich, dass die schriftliche und die elektronische Form vollständig übereinstimmen. Die Arbeit hat in gleicher oder ähnlicher Form noch keiner Prüfungsbehörde vorgelegen.

Aachen, July 24, 2019

Ort, Datum Unterschrift

*Nichtzutreffendes bitte streichen

Belehrung:

§ 156 StGB: Falsche Versicherung an Eides Statt
Wer vor einer zur Abnahme einer Versicherung an Eides Statt zuständigen Behörde eine solche Versicherung falsch abgibt oder unter Berufung auf eine solche Versicherung falsch aussagt, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

§ 161 StGB: Fahrlässiger Falscheid; fahrlässige falsche Versicherung an Eides Statt
(1) Wenn eine der in den §§ 154 bis 156 bezeichneten Handlungen aus Fahrlässigkeit begangen worden ist, so tritt Freiheitsstrafe bis zu einem Jahr oder Geldstrafe ein.
(2) Straflosigkeit tritt ein, wenn der Täter die falsche Angabe rechtzeitig berichtigt. Die Vorschriften des § 158 Abs. 2 und 3 gelten entsprechend.

Die vorstehende Belehrung habe ich zur Kenntnis genommen:

Aachen, July 24, 2019

Ort, Datum Unterschrift