# Gamification in Information Security

Developing a Mobile App - Final Report

**Nikita Antonov**
Faculty of Computer Science
University of Vienna
Austria
a01348746@univie.ac.at

**Luise Bergold**
Faculty of Computer Science
University of Vienna
Austria
a01638598@univie.ac.at

**Melina Rudneva**
Faculty of Computer Science
University of Vienna
Austria
a01448509@univie.ac.at

## ABSTRACT

Computer science is constantly taking more room in our society. As such, also the subject of information security is gaining relevance. To protect public organizations from cyber-attacks, education of the employees is essential. With this project we want to provide an effective learning method of basic knowledge in information security. Gamification is a useful and well-established strategy to increase motivation and as such learning efficacy. In the process of the app development, we analyzed potential users, did a task and context analysis, created low-fidelity prototypes, developed our product and finally, evaluated it to detect strengths and weaknesses. Evaluation revealed that we succeeded in creating a functional product and in designing an appealing user interface.

## KEYWORDS

Gamification; Information Security; Cyber Security; App Development; App Evaluation

**ACM Reference format:**
Antonov, N., Bergold, L., & Rudneva, M. (2019). Gamification in Cyber Security. VU Human Computer Interaction, University of Vienna, Austria.



## MOTIVATION

In the context of a steadily more digitalized world, computer science is gaining more and more importance and relevance. As a result, the number of criminal activities in the cyber world such as phishing and hacking is increasing. Enterprises and organisations must find ways and develop methods to stay protected against cyber-attacks. As most attacks are aiming at the computers of the employees, the education and sensibilisation of employees in cyber security is necessary. The aim of this study was to conduct a new method to educate employees in organisations in basic concepts of information security. To increase motivation and learning effect we chose Gamification strategies. User analysis revealed our target group as employees in public organisations between the age of 25 and 50 years, being experienced in the use of computers but having no or little knowledge about information security. Anti-Virus-Software is preinstalled but still employees must be aware of how to recognise Phishing E-Mails, Virus via hardware, dispose physical and digital data and other potential risks to protect the integrity of the organisation.

Secondary users are all persons who use their private computer in everyday life for work and private matters. Their motivation is to protect personal data and not the subject of information security itself. As a result, the gamification approach is essential to keep up motivation.

The result of our task analysis with two primary personas is the following table. The most important tasks are marked grey.

## TASK ANALYSIS

| TASK | Persona 1 | Persona 2 |
|---|---|---|
| Learn basic terms in information security | +++ | +++ |
| Learn advanced terms in information security | ++ | + |
| Use with children | + | + |
| Play | + | ++ |
| Develop new scenaria | + | + |
| Teach terms | ++ | ++ |
| Learn how to handle information in a secure way | +++ | +++ |
| Use at home | + | + |

**Table 1: Task analysis regarding primary personas**

## RELATED WORK

To get an overview of the problem and possible solutions we did literature search and evaluated similar work. During literature search we found articles proofing the efficacy of gamification strategies [1;2;3] in learning information security. The competition described in an article about the Indian Capture the Flag gave us the idea to implement a ranking so that the game would be competitive and increase motivation.

Similar products that were inspiring for our app were the websites "Your medical practice" [5], "Sicher im Internet" [6] and the app "Enter IT security game" [10]. We incorporated the organisation of the content into several levels. At the beginning, only Level 1 is unlocked and solving it will unlock Level 2 etc. We adopted the division of one level into different parts like a game, an input, tips, and questions. We also liked the idea of a virtual office with real life cases where security risks are displayed and one can interact with the objects in the office. Due to our limited programming skills the interactive aspect was difficult to implement but we included a task with a displayed office and security risks. All investigated products illustrated the importance of good design, simple user interfaces and easy language.

A different approach is learning information security from the perspective of a criminal, trying to find security risks and use information against the organization, as in the App "Enter IT Security game". Although this approach is fun to play, we decided to stick to the classic view from employees as we were concerned about training criminal intentions.

## DESIGN

Our goal regarding design was keeping it simple and creating a self-explanatory and intuitive usable user interface. We chose a slightly grey background, grey buttons and a green bar at the top.

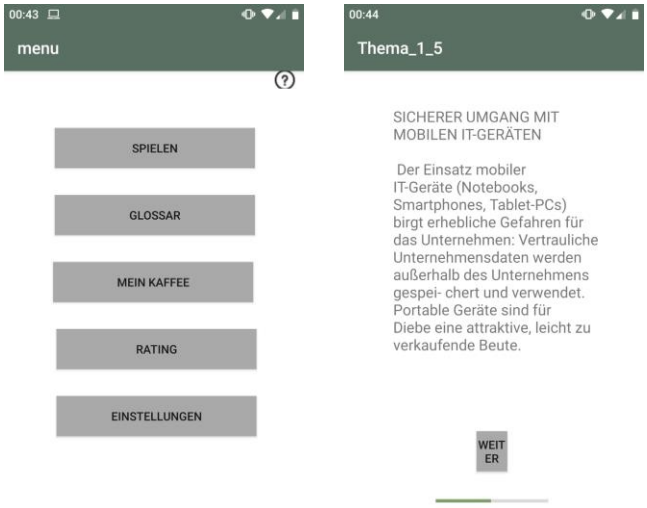


**Figure 1: Design of the user interface**

## IMPLEMENTATION

We used Android Studio as IDE. The programming language was standard java and java.android and we did not use any extern libraries or frameworks. Our app has the Android version API 15. We used Pixel 2 with API 26 as emulator.

A challenge we encountered was implementing the virtual office. The idea was to detect security risks by touching them but this was too difficult to implement. Instead users are required to name the risks and type them into a text field.

## EVALUATION – USABILITY STUDY

### Aims and procedure

To evaluate our app regarding functionality and design choices we did a usability study. In a qualitative approach we interviewed six potential app users who are representing our primary target group. The mean age of the sample was 24 years and four were female, two male. All were working in organizations and had no or little knowledge about information security. In preparation phase we created a script including a

questionnaire with instructions for the interviewer, including a warm up phase, four test items, and a cool down phase. In the script the questions are defined precisely so that no biases due to different expression of the questions would occur and to keep up a certain level of standardization. The structure of the interviews was as following:
In the warm up phase the interviewer is explaining the main aims of the study, gives basic information about our app, ensures anonymization etc. In the test phase four tasks are given and the test person is asked to speak out his or her thoughts aloud. The first task was logging in. Secondly the three of the test persons were asked to play Level 1, the other three Level 2. The third task was to find out what Phishing is followed by the last task, finding out if the player already earned a free coffee. Regarding the behavior of the interviewer it is important to express the questions in a non-suggestive way. The interviewer is writing down how the proband is solving the tasks as well as observing behavior and facial expressions. After every task the proband is asked what he found easy and what difficult when solving the task. In the cool down phase probands are supposed to state what their general impression of the app is, what they liked and disliked and express ideas for improvement.
The script is shown below.

**Recruitment of probands**
We mainly interviewed friends that were interested in the study. Inclusion criteria was being working in an organization so that the sample would be representative for the target group. Most probands were working 20 hours a week or less besides studying.

**RESULTS**

**General impression**
In general, the probands described our app as appealing and interesting. The structure is intuitive and easy to understand even for first time users. The start screen is well arranged and logical. Also, the gamification is fulfilling its purpose in motivating to play and engage with the content. The length of the levels is appropriate.

**Design of the interface**
Although the simple design of the user interface received positive feedback, it was sometimes perceived as too reduced and monotonous. Adding more colors for salient information was proposed. The way of naming the overview ("Thema_1_1") was criticized as being not appealing.
Some of the chosen icons are pixelated and placed irritatingly. The padlocks symbolizing that a level is unlocked differ only slightly from the locked ones. The white writing in the green bar at the top is not ideally legible.

**Functionality**

Looking at the functionality one could say that the app in general fulfills its function. The combination of theoretical input and small games results in motivation and a learning effect.
However, in Level 1 during the theoretical input, probands got tired after about five of the seven topics and stated that the text passages were too long. Some said that a progress bar displaying how many inputs still have to be read would be useful. The Glossary fulfilled its function as well but should rather be interactive so that one does not have to scroll all the way down to a certain term. The terms are described in an easily comprehensive way.
Starting Level 2 with an interesting fun fact was arousing interest in the upcoming input and making people identify with the presented topic. The ticking boxes during the process of creating an own password were not completely clear. After a level is completed, besides showing the earned points, we could refer to the coffee bonus as in "Congratulation! You just earned a coffee!".
An interesting suggestion was implementing a mascot that is accompanying the player through the game and showing up at several points (in the glossary, giving Tipps, congratulating at the end of a level etc.).

**Text**
A few inconsistencies were detected regarding the chosen language: "Password" and "menu" although everything else is written in German. Also, some grammar mistakes occurred. The information in general is presented in a good and easy way.

**Strengths and weaknesses**
We learned about our app that we achieved a clear and logical structure. Also, we succeeded in presenting rather boring content for most of the primary users in a motivating and interesting way.

On a basis of the results of this usability study we further improved the app. We changed the color of the bar at the top to a darker green and chose different padlock icons. We also corrected the language inconsistencies and grammar mistakes. We implemented a progress bar in the levels.

## REFLECTION

We divided the work of this entire project between all three of us.
For the first milestone we all did literature research and analyzed previous work. Luise did the context and user analyses, Nikita the task analysis, and Nikita and Melina created primary, secondary and negative personas. Melina did the project management. During the second milestone we met and did brainstorming to come up with many and diverse ideas. Then each of us created a low fidelity prototype and did an interview to detect strengths and weaknesses.
These were the foundation for milestone three. We summarized the findings of our interviews and developed the structure of the app. All three of us were involved in design decisions. Luise wrote the texts and Nikita and Melina implemented the app.
In Milestone four we evaluated our product. Nikita and Melina created the script for the usability study including test items and questions before and after. Each of us interviewed two persons and we then carried our findings together. Based on these, we made new design decisions which Nikita and Melina implemented. Finally, we discussed our experiences and motivation during this process and Luise wrote the final report.

For each of us, this project was an interesting and at the same time challenging experience. We learned that developing an app is not just programming but and includes a long preparation period. According to this, the importance of project management must not be underestimated. Also, the interdisciplinarity in our group was opening interesting perspectives, as our group consisted of two computer scientists as well as one psychologist.

## CONCLUSIONS AND FUTURE WORK

In summary, strengths of our approach are the task and user orientation. Looking at implementation, we succeeded in creating an app that is easy to use and functional. Also, the gamification strategy holds the potential to motivate people even though the learning content might not be that interesting for everybody. Room for improvement is implementing more complex games and thus increase the gamification factor but advanced programming skills will be necessary.

Future work could investigate the short- and long-term learning effect by testing the knowledge about information security after having used the app.

## REFERENCES


[1] Schreuders, Z. and Butterfield, E. (2019). Gamification for Teaching and Learning Computer Security in Higher Education. [online] Usenix.org. Available at: https://www.usenix.org/conference/ase16/workshop-program/presentation/schreuders [Accessed 24 Mar. 2019].

[2] Boopathi K., Sreejith, S., Bithin, A. (2015). Learning Cyber Security Through Gamification. [online] Available at: http://www.indjst.org/index.php/indjst/article/view/67760 [Accessed 24 Mar. 2019].

[3] University of San Diego. (2019). Bringing Gamification to Cyber Security Awareness Training. [online] Available at: https://onlinedegrees.sandiego.edu/bringing-gamification-to-cyber-security-training/ [Accessed 24 Mar. 2019].

[4] PulseLearning. (2019). Gamification in Corporate Training - Infographic. [online] Available at: https://www.pulselearning.com/blog/gamification-infographic/), [Accessed 24 Mar. 2019].

**Websites:**

[5] **https://www.healthit.gov/sites/default/files/cybersecure/cyber-ecure/** (Accessed 13th of March, 2019)

[6] **https://www.sichere-identitaet-bb.de/sicheriminternet/8**(Accessed 8th of March, 2019)

[7] **htttps://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzAbout/ITGrundschutzSchulung/WebkursITGrundschutz/WarumITGrundschutz/WarumSicherheit/Gefahrenpotenziale/gefahrenpotenziale_node.html** (Accessed 3rd of May, 2019)

[8] **https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzAbout/ITGrundschutzSchulung/WebkursITGrundschutz/WarumITGrundschutz/WarumSicherheit/Sicherheitsmaengel/sicherheitsmaengel_node.html;jsessionid=3AC162E5778D742E0B64117DAD27DBAF.1_cid351** (Accessed 3rd of May, 2019)

[9] **https://www.wko.at/site/itsafe/mitarbeiter-handbuch.pdf (**Accessed 3rd of May, 2019)

**Mobile Apps:**

[10] Enter IT Game" (downloaded 9th of March, 2019)