Efficiency of an Artificial Intelligence-based Chatbot Support

for an IT-Awareness and Cybersecurity Learning Platform

Dominik Fanta, Farhan Sajid, Michael Masssoth and Lennart Kruck

Department of Computer Science

Hochschule Darmstadt (h_da) - University of Applied Sciences Darmstadt,

Darmstadt, Germany

e-mail: {dominik.fanta, farhan.sajid}@stud.h-da.de , {michael.massoth, lennart.kruck}@h-da.de

Abstract-The IT awareness learning platform with Artificial Intelligence (AI) learning chatbot imparts target group-specific expert knowledge on the topics of IT awareness and cybersecurity. The user interactively controls the AI chatbot by making selections and asking questions. There is also the option that the AI chatbot questions the user and the user has to answer the questions. The AI chatbot is an expert in 23 IT security topics, including malware, but also in the areas of sexting or catfishing. The goal is to provide a fully comprehensive IT awareness and cybersecurity learning platform. In order to best adapt the AI chatbot to the needs of the users, it was important to conduct surveys with the target group in order to best recognize the respective spelling of the users so that there are no problems with the recognition of the input at the beginning. IT awareness knowledge is imparted by means of the AI chatbot through efficient dialog-based learning in a low-threshold, mobile way, "in small bites", and "for in between".

Keywords— Artificial Intelligence; chatbot; it-awareness; learning platform; chat flow; ecosystem security.

I. INTRODUCTION

Due to the SARS-CoV2-pandemic, the threat situation in the digital space is intensifying. Employees are operating in their home offices, in some cases outside the company's own protected IT infrastructures.

IT infrastructures, and mobile devices are increasingly being used. Criminals are exploiting the global pandemic situation technically and, above all, as a thematic starting point for social engineering and other attacks.

The Proofpoint Human Factor Report 2019 proves, "more than 99 percent of cyberattacks rely on a human interaction in the process, making the individual user the last line of defense." The report shows that more than 99 percent of observed threats required a human interaction, whether it was activating a macro, opening a file, clicking a link or opening a document. To significantly reduce risk, organizations need a holistic approach to cybersecurity that focuses on the individual employee. Essential to this is the sensitization of all people in the company as well as effective security awareness training.

Through AI-based IT awareness training and education, companies and government agencies are strengthening the digital defenses of the entire workforce. AI chatbots enable efficient conversational learning. Learning with AI chatbots is thus comparable to learning through discussion rounds. As a rule, people remember content more easily when it is conveyed during a dialogue, rather than through a frontal presentation. AI chatbots make it possible to convey IT awareness knowledge in a short, mobile and interactive way.

This project aims to improve the aforementioned efficiency of AI-based learning chatbots in the context of IT knowledge training.

This paper is organized as follows:

Section II reviews the relevant terminology and advantages of AI chatbots. Section III describes the current state of the art considering related works. Section IV describes the IT awareness chatbot approach. In Section V, the implementation and structure of an AI learning chatbot. In Section VI, initial test results of a user testing are disclosed. Section VII deals with the efficiency of learning chatbots and the learning gains that can be achieved with them.

II. BACKGROUND

IT and cybersecurity awareness [Definition]: IT and cybersecurity awareness mean problem awareness and secure behavior. In everyday dealings with IT systems, awareness is an elementary security measure. First, this means creating an awareness of the problem of cyber security attacks and threats. Building on this, it is possible to achieve a change in behavior toward secure digital use. Security awareness measures are successful if they empower the target groups and motivate individuals to improve their cyber security. It is important to develop awareness at eye level and in a practical manner [1].

AI learning chatbot [Definition]: An AI learning chatbot is a computer program that uses Artificial Intelligence (AI) and Natural Language Processing (NLP) to understand learners' questions and automate responses to them, simulating human conversation. Users can ask questions to which the system responds in natural language [2].

Advantages of an AI chatbot: AI chatbots in use for IT awareness can help:

• Reduce costs. AI chatbots can support processes through automation and thus reduce process costs. Here specifically

the costs for necessary awareness measures and presence training.

• Relieve employees. AI chatbots are able to take on uncomplicated cases in the call center or self-services. This can significantly reduce the workload of employees; and they are given the opportunity to focus fully on the critical IT security cases where they are really needed.

• Improve the user experience through efficient dialog-based learning.

All advantages of AI chatbots at a glance:
• Chatbots are available 24/7
• Chatbots never drop out due to illness or vacation
• Chatbots learn constantly and get better the longer they are deployed
• Chatbots eliminate waiting time for learners and users
• Chatbots are fast and effective
• Chatbots are scalable

Benefits for around 150,000 employees in the state of Hesse:
In Hesse alone, there are around 150,000 employees (full-time equivalents) at the state level who can be users of IT awareness training with AI chatbots.

III. RELATED WORK AND RESEARCH QUESTION

State of research and technology:
If we take a closer look at the topic of chatbots, we can see that it has become increasingly important in recent years. It has therefore also been shown in several studies that it is possible to learn with a chatbot. The authors in [8] have shown in their study that it is possible to learn with a chatbot. For this purpose, they took 2 study courses with once 167 and once 124 students. Of the 167 and 124 students, 121 and 87 passed respectively. At the end of the semester, the students who had passed were able to fill out a questionnaire in which 187 had responded. The analysis of the questionnaires showed that 133 times (71.13%) the chatbot provided correct suggestions. In 30(16.04%) cases, the chatbot has the correct suggestion but not suitable for the students' needs. Only in 24 (12.83%) cases, the chatbot provided wrong suggestion.

In order to make learning with a chatbot more interesting, the authors in [7] showed that it is necessary to come up with a suitable gamification strategy to make users learn longer with it. Badges, different levels, quests, countdown, rule and reward or leaderboards are mentioned here as possible approaches, all of which should be considered when designing a AI learning chatbot.

However, good chances of success or a good gamification concept are only secondary for chatbots; it is much more important that the users can interact with the chatbot. Yin-Chun Fung and Lap-Kei Lee [6] conducted a survey with 20 participants to test an AI chatbot for cybersecurity awareness in their survey, it was found that 75% of the respondents know how to use an AI chatbot. It was also found that using a cybersecurity awareness chatbot can increase cybersecurity awareness, so 75% of the respondents agreed and the remaining 25% were neutral.

An extensive literature search has not yet been able to find any studies or research results on the use and effectiveness of AI chatbots in IT awareness training. IBM Germany also informed the project manager that Darmstadt University of Applied Sciences is conducting the first project in the area of AI learning chatbots for IT awareness in Germany [as of 01/2022]. The objective of the project goes beyond the current state of research and does real pioneering work.

Research questions and objectives: It is investigated how the existing knowledge about IT awareness and cybersecurity can be increased in a target group-specific way by using an AI chatbot. Target groups are especially users without detailed knowledge about information security, as well as executives and IT administrators. The goal of the research project is to determine the effectiveness and efficiency of an AI chatbot for raising awareness among employees of the Hessian state administration and government in a target group-specific manner. The AI-based learning chatbot will be tested and optimized on selected target groups.

IV. IDEA AND APPROACH

An IT awareness learning platform with AI chatbot:
An AI-based learning chatbot is an intelligent, voice-respectively text-based dialog system that allows chatting with an Artificial Intelligence. Such an AI-based learning chatbot is to be used and tested for the first time as part of an IT awareness training for basic sensitization of employees.
The AI chatbot conveys the most relevant learning content on the topic of IT awareness to the learner in a simple, and in some cases even playful, dialog. In the process, AI chatbots divide the knowledge into small "morsels" and send them to the user one by one.

Solution: The IT awareness learning platform with AI chatbots imparts expert knowledge about IT awareness and cyber security to specific target groups: Low-threshold, "in small bites", "for in between".

The user controls the AI learning chatbot through his questions/choices/selections.

The following **specialist topics** are already included in the current IT awareness learning platform with AI chatbots and optimized for **detection rates of over 75%.**

TABLE I.   SUBJECT MATERIALS

Malware	Phishing	Secure handling on the web	Good and secure passwords
Social engineering	Data protection on the web	Blackmail Trojan	Computer viruses
Spying on data	Botnets and DDoS attacks	Cyber and computer crime	Voice assistants
Hacking - my online bank data on the web	Industrial and commercial espionage	Cyberbullying and cyberstalking	Fake stores, fraud, subscription traps
Skimming	ICT criminal law	Sexting on the web	Catfishing

The **AI-based IT awareness training** starts with a **self-assessment** of the user and a **placement test** and is then based on the knowledge level of the individual participants. In this way, the strengths and weaknesses, as well as the individual learning type of the employee are taken into account and a training adapted to the respective person is guaranteed.

V. STRUCTURE OF THE AI CHATBOT

Learning scenario 1:
Answering questions from learners
The AI-based learning chatbot shall be able to answer frequently asked questions, a precise analysis of the most frequently asked questions per subject had to be carried out first. Based on this analysis, a knowledge base was then developed for the AI chatbot answers. If the AI chatbot detects a similarity between a new question and a question in the knowledge database, it outputs the corresponding answer.

Important success factor:
Helping users to ask questions
With an A/B/C-usability test it was conducted in which the participants were to test the learning platform by asking the chatbot questions. Group A was given no additional tools on the learning webpage, group B was given a mind map diagram as an additional tool to ask questions, and group C was given an additional info-video (but no mind map). As result of the A/B/C-usability test, it turned out, that group B achieved the greatest success, in which they were able to achieve the greatest learning gain and asked the most amount of questions to the chatbot [3]. The example mind map diagram in Figure 1 is intended to give users who are not familiar with the topic some clues and ideas as to what they can ask the chatbot.
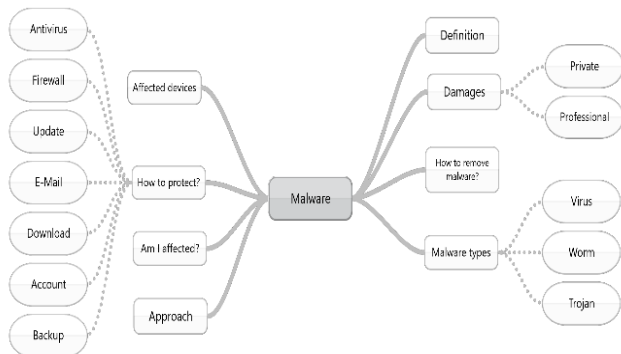

Figure 1.　　Example of a mind map diagram

Learning scenario 2:
Inquire about and deepen (prior) knowledge
The AI chatbot is used to determine the (prior) knowledge of a learner. To do this, the AI chatbot asks a series of predefined questions (**chat flow**) and evaluates the answers. Unlike multiple-choice tests, there are no predetermined answers. The AI chatbot can provide solution hints and feedback immediately after the answer. The prerequisite for such a dialog is that the test questions have been defined beforehand and the AI chatbot knows the correct answers. Using intent matching, the AI chatbot can estimate whether a correct or incorrect answer was given.

Test scenario:
Knowledge check to certify a training measure
The guided chat flow (from learning scenario 2) is used to test the knowledge of a learner. Here there are 3 different levels of difficulty (easy, medium, hard). The learner can collect 15 points per training unit. Once a certain number of points has been reached, a successful IT awareness training session can be certified.

A. Structure of the questioning chatbot

The chatbot is set up in such a way that the learner can prove his knowledge with the help of a quiz in the chatbot, where the chatbot asks the learner questions. By entering a keyword or trigger, such as "Malware Quiz", the chat flow in the chatbot is addressed and the quiz is started. The learner collects points by correctly answering the questions posed by the chatbot. The chatbot asks the learner five questions per difficulty level and topic. Depending on whether the learner answered the question correctly or incorrectly, he or she receives points and a short explanation of the correct answer.

1) Game method

There are 2 methods of play to successfully complete the quiz. The first method is based on the fact that the learner has already unlocked all difficulty levels at the beginning, whereas in the second method, the learner can only select the difficulty level at the beginning and unlock the other levels first. difficulty level at the beginning and has to unlock the other levels first. must first unlock the other levels.

a) Method 1: Difficulty level selectable

In the first method, the learner can choose any difficulty level, but the learner must play through all three difficulty levels for the chosen subject to be considered successful. For each question answered correctly, the learner receives one point. This means that the learner must achieve 15 points to successfully complete the quiz for the selected subject.

In the example, the chatbot was addressed with the trigger "test quiz" and the chatbot gives the learner the opportunity to select the difficulty level.

b) Method 2: Unlock difficulty level

In the second method of play, the learner must first successfully complete the easy difficulty to unlock the intermediate level, and then the learner must successfully complete this to unlock the hard difficulty.

This method gives the learner the feeling that he is in a game and must make progress to unlock the so-called "end level", the level difficult. In this method of playing, the learner does not have a free choice to select the difficulty level, but the learner can start the quiz or also read through the rules of the game.

2) Chat flows

To conduct the quizzes, so-called chat flows are used. Here there are connections that can be used to insert many branches into the chat flows. The learner can use these to navigate to a specific point. For example, in the quiz there are paths, depending on whether the learner's answer is correct or incorrect, the learner is forwarded to the particular branch. As a result of how many questions the learner answers correctly, he gets his points by advancing in the particular path. In this quiz, each correct answer directs the user down one level in the tree diagram and in the left direction; if an answer is incorrect, the branch at the bottom right is taken. On the whole, the chat flow is similar in structure to the normal Chat bot, in which the learner asks the chatbot questions, also a so-called Question and Answers. The special feature here, however, is that you can create a direct connection from one conversation to the next. In order not to put the performance of the chatbot under high load, a chat flow and a difficulty level has only five questions. By answering all the questions correctly, the node redirects the user to a new chat flow at the end, where he can continue with the quiz. This allows the learner to be guided through a multi-level dialogue, for example, to request several pieces of information or to define a problem in more detail. This function is also used, for example, to create a ticket for support. In Figure 2, you can see what the tree structure looks like with the various branches and how complex it can become, depending on the number of questions.
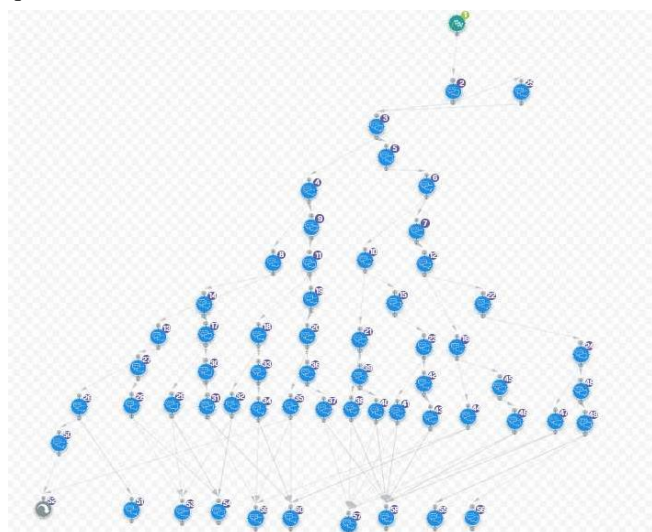

Figure 2.   Chatflow of a Multiple-Choice Quiz

3) Future outlook

To bring out the full potential of the AI-based learning chatbot, and for learners to achieve even better success, it is necessary to conduct surveys to find out the learning behavior of users. Therefore, some surveys about the learning behavior will take place in the coming weeks. On the one hand it will be tested if the learners prefer to learn via multiple choice or if they prefer a variant where they have to enter the complete answer manually. It will also be tested which of the above-mentioned game modes lead to a better game experience or to

an increased learning gain. In addition, it is still checked which requirements are optimal for the awarding of a certificate so that it has a relevant value. After completion of the surveys, the results will be evaluated and based on these, the chatbot will be further improved. In addition, a final test with subsequent certification will be implemented. In order for the certification to have a value that is recognized in society, an attempt will be made to accredit the complete IT awareness chatbot.

VI.   USER EXPERIENCE TESTING

A User Experience Questionnaire (UEQ) consists of 6 predefined UX factors: Attractiveness, Efficiency, Perspicuity, Dependability, Stimulation and Novelty. For many other products or applications, however, the above-mentioned UX factors are not really relevant. The extension of the User Experience Questionnaire (UEQ+) therefore does not consist of 6 predefined UX factors, but of a question catalogue consisting of 20 UX factors, which can be adapted to the needs of your product. Since each UX factor consists of 4 pairs of opposing characteristics and the importance of the UX factor is also asked, it is advisable not to use more than 5 or 6 of the 20 UX factors so that the length of the UEQ+ questionnaire is within a reasonable range. A user experience questionnaire is now conducted with a representative number of test persons in order to obtain values that are as accurate as possible. During the test, the test persons have to rate the pairs of opposites on the basis of a predefined question. As can be seen in Figure 3, the evaluation is done on a scale of 1 to 7, with the more negative characteristics on the left and the positive characteristics on the right [4].

Figure 3.   Example of a UEQ+ UX factor

After conducting the User Experience Questionnaire with a representative number of test persons, it can be analysed with an Excel table provided by UEQ+ and the mean value, standard deviation and confidence range for each individual UX factor are obtained. The confidence interval indicates the

range that includes the mean value of a distribution with a certain probability. For this purpose, the upper and lower limits of the confidence interval are additionally determined and presented in the evaluation. These are represented by black lines within the associated mean values of the respective UX factors.

There is also the option of displaying the importance of the individual UX factors, the evaluation is carried out as explained above. The aim is to get an overview of how well the respective UX factors are implemented and which factors need to be addressed.

A. User Experience Questionnaire+ for AI learning chatbots

Testing the user experience of an AI learning chatbot requires a good testing method. The UEQ+ is the best testing method for AI learning chatbots because it allows UX factors to be specifically tailored to the chatbot under test. However, since there are no studies yet on which UX factors are particularly well suited for an AI learning chatbot, a small study was conducted with 30 computer science students from the Darmstadt University of Applied Sciences as part of this project. The goal of the study was to find out which UX factors are particularly suitable for AI learning chatbots and to obtain initial user feedback on the existing AI learning chatbot. For the study, the 30 subjects filled out a user experience questionnaire with 18 of the 20 UX factors. The UX factors haptics and acoustics were deliberately neglected, as our AI learning chatbot does not generally communicate acoustically and cannot be touched. Then, the mean values of each UX factor were measured and the best 6 factors were selected based on the result. Figure 4 shows that it is especially important for a learning AI chatbot to be a reputable source that is good to learn with. After the best 6 UX factors were collected, they were then evaluated. Figure 5 shows that the learning AI chatbot already performs very well in many of the 6 relevant UX factors.
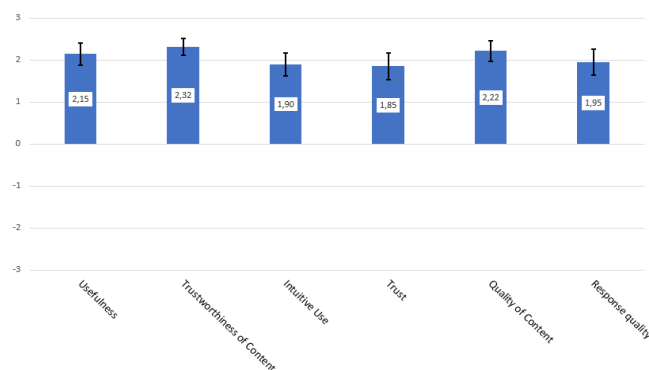
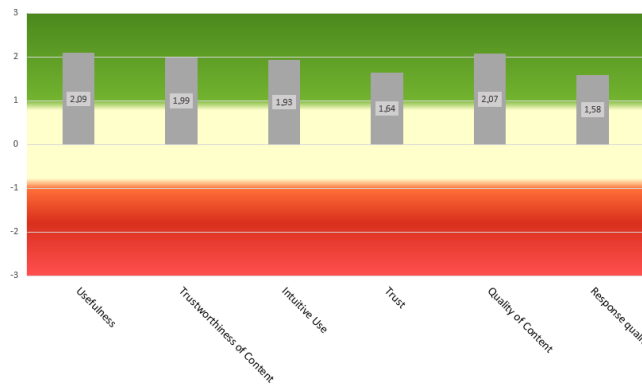Figure 4.   Importance Rating of an AI learning Chatbot

Figure 5.   General evaluation of the AI chatbot

VII. RESULTS

Initial user experience tests on the AI chatbot yielded the following results:

- The AI chatbot was very well received by test persons
- Subjects found it very enjoyable to use
- Easy use of the chatbot
- High recommendation rate

In order to measure the efficiency of an AI learning chatbot, learning growth was measured in addition to the UEQ+ mentioned above. For this purpose, a study was conducted with 30 computer science students from Darmstadt University of Applied Sciences, in which they were able to interact and learn with the AI learning chatbot. The study was structured in such a way that the subjects first had to complete the entrance test on a specialized topic (Table 1) and then ask questions to the chatbot in the learning area based on a mind map (Figure 1). In the next step, the subjects had to be questioned by the chatbot to verify the previously learned knowledge. Finally, the subjects had to complete the final test, which contained the same questions as the initial test. At the end, the points achieved in the initial test were subtracted from the points in the final test to measure the learning progress. The subjects had to complete this run for all subject topics. As can be seen in Figure 6, a learning gain of 15.73 % was achieved, even though the test subjects were computer science students who are at least in their 4th semester and who already have prior knowledge in the area of cybersecurity due to their studies.

Figure 6.   Learning Growth

Percentile:

Of all the valid tests for the individual subjects, the scores achieved on the entrance tests were used to calculate percentiles. In total, the results of 266 entrance tests were considered. Depending on the prior knowledge of the test subjects, between 0 and 100 points could be achieved on the entrance test. Table 2 shows that half of the test subjects (median) already scored 70 points or more on the entrance test. The best 10% of the test persons even achieved 90 points or more in the entrance test. The results in Table 2 clearly show that our test group had sound prior knowledge of all the specialist topics of IT awareness and IT security and cannot be regarded as beginners or laypersons.

TABLE II.   PERCENTILES OF 266 ENTRANCE TEST

Percentile	Value (points) [Up to max. 100]	Meaning and discussion
5 percent percentiles	20	95% of the testers scored at least 20 points or more on the entrance test
10 percent percentiles	20	See line above (5 percent percentiles).
50 percent percentiles	70	50% of the testers scored at least 70 points or more on the entrance test
90 percent percentiles	90	The best 10% of the testers already achieve entrance test score 90 points or more
95 percent percentiles	100	The top 5% of testers already achieved the maximum possible entrance test the maximum possible 100 points

REFERENCES

[1] Federal Office for Information Security (BSI), Germany; https://www.bsi.bund.de/EN/Home/home_node.html; last accessed on 2022-06-12

[2] IBM Chatbots: https://www.ibm.com/cloud/learn/chatbots-explained; last accessed on 2022-06-12

[3] A. D. S. Fernandes, " Implementation, evaluation and optimization of the user experience and IT security of an IT awareness learning platform with AI chatbots. ", Bachelor thesis 2021 at Darmstadt University of Applied Sciences at the Department of Computer Science

[4] UEQ+_Handbook_V2: ueq-research.org

[5] D. Bahcecioglu, "Development and optimization of an IT awareness learning platform with AI chatbots with regard to quality assurance through UX testing.", Bachelor thesis 2022 at Darmstadt University of Applied Sciences at the Department of Computer Science

[6] Y. C. Fung and L. K. Lee, "A Chatbot for Promoting Cybersecurity Awareness", Cyber Security, Privacy and Networking, 2022 - Springer

[7] I. Hidayatulloh, S. Pambudi, H. D. Surjono and T. Sukardiyono, "Gamification on Chatbot-Based Learning Media: a Review and Challenges", ELINVO (Electronics, Informatics, and Vocational Education), Mei 2021; vol 6 (1):71-80, ISSN 2580-6424 (printed), ISSN 2477-2399 (online,) DOI: 10.21831/ elinvo.v6i1.4370

[8] F. Colace, M. D. Santo, M. Lombardi, F. Pascale and A. Pietrosanto, "Chatbot for E-Learning: A Case of Study", International Journal of Mechanical Engineering and Robotics Research Vol. 7, No. 5, September 2018.