A Chatbot for Promoting Cybersecurity Awareness

Yin-Chun Fung and Lap-Kei Lee

Abstract Cybersecurity is one of the hot topics nowadays. However, not many Internet users know the cyber risks around them. To promote cybersecurity awareness, this paper presents a chatbot that is a cybersecurity expert. It aims to let its users learn more about cybersecurity. It relies on Google Dialogflow, which is a natural language understanding platform. Our chatbot contains a knowledge base on cybersecurity knowledge. Users can make queries to the chatbot to learn definitions and concepts of different cybersecurity terms. Our chatbot also provides self-quizzes for users to test their knowledge on different cybersecurity topics. It also provides suggestions to users on cybersecurity issues such as how to identify and handle phishing emails. In a survey of twenty users, the majority of the users agreed that our chatbot is easy to use and can increase their awareness of cybersecurity issues.

Keywords Chatbot · Cybersecurity awareness · Natural language processing

1 Introduction

The term "cybersecurity" started to be famous in 2009 when US President Barack Obama called upon the citizens to recognize the importance of cybersecurity [1]. Cybersecurity awareness is still an important topic around the world, like assessing the awareness of university students [2] and a systematic review of multimedia tools [3]. Yet many cyber users are still unaware of possible cyber risks around them in the cyber world [4]. It is essential to promote awareness of cybersecurity issues in society.

Y.-C. Fung (✉) · L.-K. Lee
School of Science and Technology, Hong Kong Metropolitan University, Ho Man Tin, Kowloon, Hong Kong SAR, China
e-mail: Chinaycfung@study.ouhk.edu.hk

L.-K. Lee
e-mail: lklee@ouhk.edu.hk

D. P. Agrawal et al. (eds.), *Cyber Security, Privacy and Networking*, Lecture Notes in Networks and Systems 370, https://doi.org/10.1007/978-981-16-8664-1_33

Among the many ways to increase the awareness of cybersecurity, game is one of the popular ways. Pape et al. [5] conceptualized a cybersecurity awareness quiz as a serious game, where the players have to answer questions concerning a social engineering attack, which is one of the common cyber risks. The serious game lets the players think more about security issues in real life. Alqahtani and Kavakli-Thorne [6] developed a game for players to learn cybersecurity using the technology of augmented reality.

Chatbots are artificially intelligent computer software that can chat with humans, which have many applications in the cybersecurity field [7]. One of the applications is the detection of cyber criminals [8], where the chatbot can interact with suspects to profile their interest in online child sexual abuse. The Cyber Helpline[1] in the UK is a chatbot that gathers information about cybercrime incidents and identifies the attack in real time. Artemis is another chatbot example that assists cybersecurity experts, which was developed by Filar et al. [9]. Chatbots can also provide cybersecurity guidelines to users. Gulenko [10] showed a chatbot that can teach the users how to appropriately set the privacy settings on a social media platform and how to set a good password.

Apart from cybercrime detection and analysis, chatbots can be used in education. Nenkov et al. [11] demonstrated how to use a chatbot in Facebook Messenger to let students answer questions of an online test. Lee et al. [12] presented a chatbot for instantly answering students' questions for a university course, and the chatbot supports multiple social platforms commonly used by students, including Telegram, Facebook Messenger and Line. Clarizia et al. [13] also developed a chatbot for supporting students in learning cultural heritage contexts. Some chatbots [14, 15] train one's cybersecurity awareness, but they may not be up to date for fulfilling the cyber environment nowadays.

This paper presents the design of a chatbot to users' awareness of cybersecurity. Our chatbot contains a knowledge base on cybersecurity knowledge. Users can make queries to the chatbot to learn definitions and concepts of different cybersecurity terms. Our chatbot also provides self-quizzes for users to test their knowledge on different cybersecurity topics. It also provides suggestions to users on cybersecurity issues such as how to identify and handle phishing emails. A survey on twenty users from different age groups showed that our chatbot is easy to use and can increase users' awareness of cybersecurity issues.

Organization of the Paper. Section 2 gives the detailed design of our chatbot. Section 3 presents a preliminary evaluation of the chatbot on twenty users. Section 4 concludes the paper and proposes some future work directions.

[1] https://www.thecyberhelpline.com.

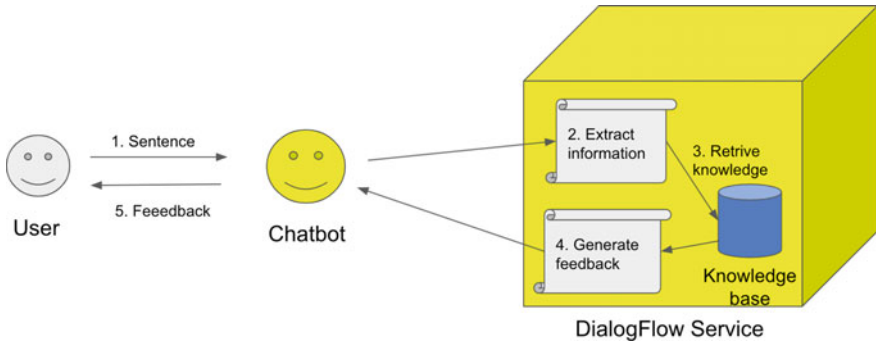

Fig. 1 Architecture of our chatbot

2 Design of the Chatbot

2.1 Architecture

Our chatbot relies on the Google Dialogflow platform,[2] which is a natural language understanding cloud service. The Google Dialogflow platform contains an inference engine that helps to extract information, including intents and the relevant entities, from messages of the users during a conversation. Figure 1 shows the architecture of the chatbot. When a user message is received, it will be passed to the Dialogflow service to extract the intent and entities of that message. Our chatbot contains a knowledge base on cybersecurity knowledge such that relevant knowledge will be retrieved according to the intent of the message and feedback in English will be generated as the reply to the user.

Dialogflow provides basic features to build a chatbot. First, we need to set up the set of intents and entities such that the chatbot can identify the topics that it needs to handle. Next, the chatbot will be trained using some carefully designed training phrases so that it can correctly identify the intents from different user messages. We can also set up some default responses to different intents. Dialogflow provides a convenient interface for constructing the knowledge base of the chatbot from properly formatted data prepared by us such that the chatbot can retrieve cybersecurity terms and other knowledge and respond to the user queries appropriately.

2.2 Message Handling

Like other chatbots in the market, our chatbot can handle input in different forms.

[2] https://cloud.google.com/dialogflow.

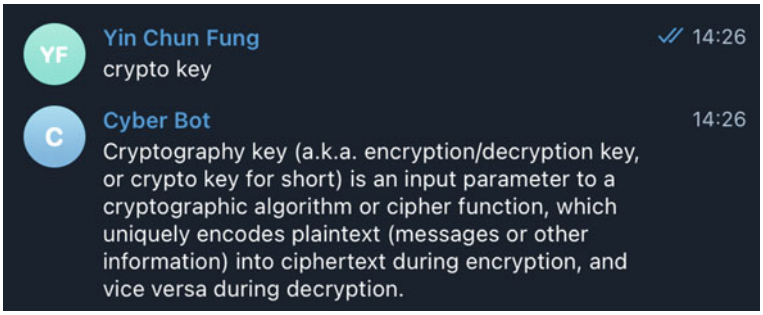

Fig. 2 Example of handling messages in the form of a term

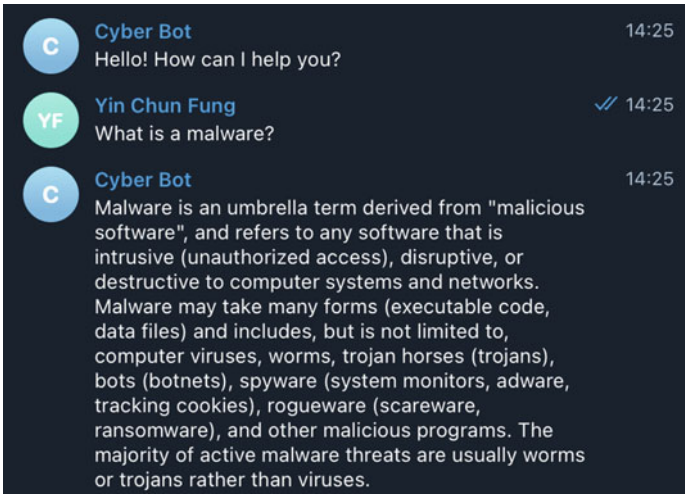

Fig. 3 Example of handling a natural language sentence

Term. Users can input a single term to the chatbot. The chatbot will respond appropriately according to its knowledge base. As shown in Fig. 2, the chatbot obtains the definition of "crypto key" in its knowledge base and response to the user.

Natural Language. Users can input a complete sentence, and the chatbot will analyze the meaning of it. In Fig. 3, with the help of Dialogflow's inference engine, the chatbot realizes that the user wants to know the definition of malware. It obtains the meaning of the term and then responds to the user.

Command. There are pre-defined commands, which start with a slash ("/"), built in the chatbot. Users can input them, and the chatbot will perform corresponding tasks. For example, in Fig. 4, if the user inputs the command "/quiz," a self-quiz will be started.

Fig. 4 Example of handling a command

Button. Sometimes the chatbot may require some pre-defined replies from the user. Like that in a quiz shown in Fig. 5, the user should respond in one out of the five choices of a multiple choice question. The buttons are the expected replies from users. Users are not required to input the answer themselves in the chatbox. The buttons also help the chatbot easily trigger feedback from the users. These buttons can also be hyperlinks that link the users to other web pages.

2.3 Supported Features

Term Definition. The knowledge base stores several cybersecurity terms. Users can ask the chatbot about the definition of a term. The chatbot can retrieve the explanation from the knowledge base as shown in Figs. 2 and 3. If the chatbot cannot find a particular term, it will tell users that it does not know the term (Fig. 5).

Self-quiz. User can test their understanding of cybersecurity in a self-test. In a self-test, the chatbot will randomly choose one multiple choice question from the knowledge base to ask the user. If the answer is incorrect, the chatbot will tell the user that the selected answer is incorrect (see Fig. 4 for an example). Users can answer the questions again until the correct answer is chosen. The chatbot will provide a detailed explanation when the answer is correct (Fig. 6).

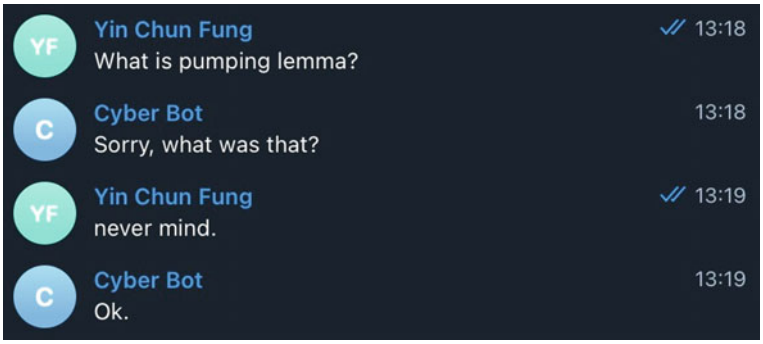

Fig. 5 Example of responses to a term outside the knowledge base

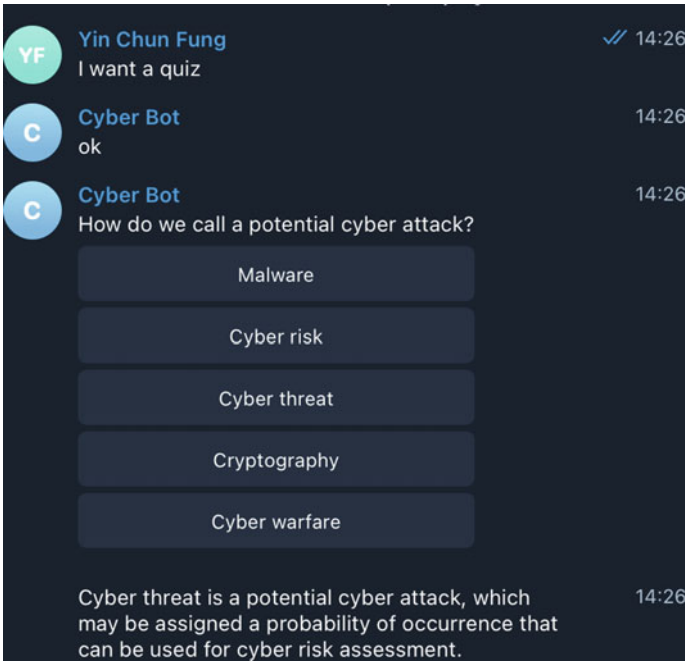

Fig. 6 Example of a self-quiz question

Workflow Structure. The chatbot provides some workflow to help the user with cybersecurity issues. One of the workflows is to help users determine whether an email is a phish. It will ask the users questions and follow the decision flow in Fig. 7. According to the responses from users, the chatbot can tell what the user should do regarding the email (Fig. 8).

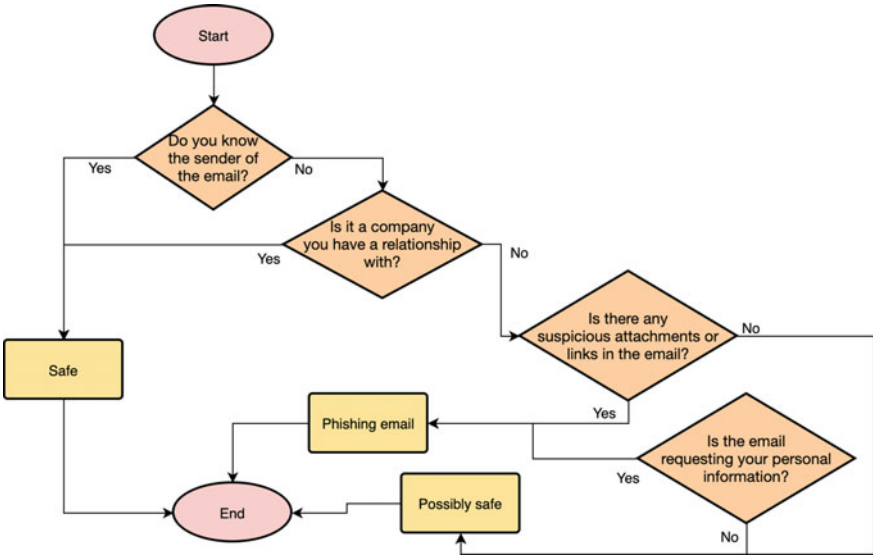

Fig. 7 Decision flow of the identification of phishing emails

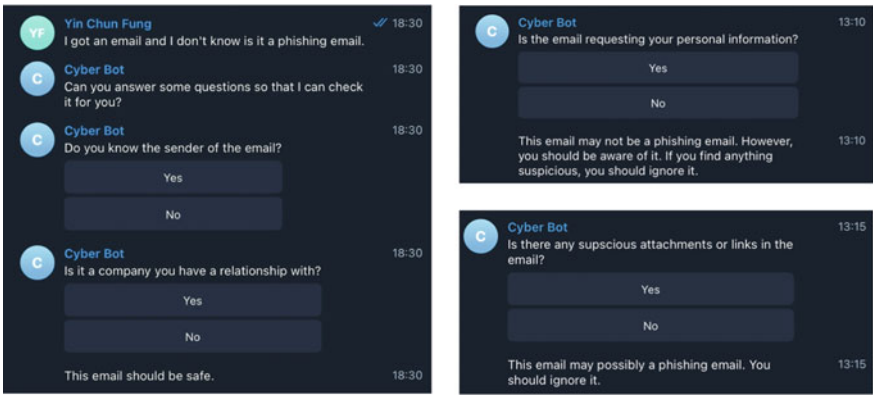

Fig. 8 Example on how to identify a phishing email

3 Preliminary Evaluation

We invited 20 participants from the Internet to chat with our chatbot and complete a survey. They are of different industries and have different backgrounds in cybersecurity. The survey consists of seven questions on a 5-point Likert scale (1: disagree, 2: partially disagree, 3: neutral, 4: partially agree, 5: agree) and one open-ended question to give some comment in the text about the chatbot. Table 1 shows the survey results.

Table 1 Survey result

Item	1	2	3	4	5
The chatbot is easy to use (%)	0	0	25	70	5
The chatbot can answer questions correctly (%)	0	0	30	60	10
The content given by the chatbot is easy to understand (%)	0	15	30	50	5
The chatbot is a quick tool for checking cybersecurity terms (%)	0	0	15	80	5
The quiz by the chatbot is useful (%)	0	10	65	15	10
The answer to the quiz by the chatbot is accurate (%)	0	0	0	95	5
The chatbot can make me more aware of cybersecurity (%)	0	0	25	60	15

In the evaluation, Question 1 reflects the ease of use of the chatbot. 75% of users agree that the chatbot is easy to use. 25% of users think it is neutral. They suggest that the list of commands and their usage is not clear.

Questions 2–4 correspond to the question answering of cybersecurity knowledge. More than half of the respondents think that the chatbot gives a satisfactory response. However, some users report that they cannot get the definition of networking terms like TCP/IP which they think is related to cybersecurity and the chatbot should be able to give a brief explanation on it.

Questions 5–6 concern the self-quiz given by the chatbot. Users think it will be great to have regular quizzes with more questions. A scoreboard can be used to record users' scores to make the quiz more competitive.

Question 7 asks the user if the chatbot makes them more aware of cybersecurity issue. 75% of them agree that it is true that our chatbot increases their awareness of cybersecurity.

Some users also think that the chatbot can provide more functionality like suggesting the strength of a password and remind them to change passwords at a period regularly. They also suggest that the bot can give some cybersecurity reading daily to keep their awareness.

4 Conclusion and Future Work

Cybersecurity awareness is an important topic in nowadays society. This paper presented a chatbot to promote cybersecurity awareness. It contains a knowledge base with cybersecurity terms. It can explain terms to users. Users can take self-quizzes to test their understanding of cybersecurity knowledge and revise the knowledge they learned from the chatbot. It also provides workflows to assist the user in some cybersecurity issues such as determining a phishing email. In the evaluation, majority of the respondent agrees that the chatbot makes them more aware of cybersecurity.

There are still a lot of improvements to the chatbot. The chatbot should provide more functionality and provide more workflows to assist users in multiple aspects.

The chatbot can be implemented into personal assistant apps to remain the users about potential threats of cybersecurity. The chatbot should also fill up with terms that are less relating to cybersecurity but are important when learning terms in cybersecurity into its knowledge base. These will be our future works.

References

1. Sanger DE, Markoff J (2009) Obama outlines coordinated cyber-security plan. The New York Times, p 29
2. Alharbi T, Tassaddiq A (2021) Assessment of cybersecurity awareness among students of Majmaah University. Big Data Cogn Comput 5(2):23
3. Zhang-Kennedy L, Chiasson S (2021) A systematic review of multimedia tools for cybersecurity awareness and education. ACM Comput Surv 54(1):1–39
4. Nagyfejeo E, von Solms B (2020) Why do national cybersecurity awareness programmes often fail?
5. Pape S, Goeke L, Quintanar A, Beckers K (2020) Conceptualization of a cybersecurity awareness quiz. In: International workshop on model-driven simulation and training environments for cybersecurity, Sept 2020. Springer, Cham, pp 61–76
6. Alqahtani H, Kavakli-Thorne M (2020) Design and evaluation of an augmented reality game for cybersecurity awareness (CybAR). Information 11(2):121
7. Mármol FG, Pérez MG, Pérez GM (2016) I don't trust ICT: research challenges in cyber security. In: IFIP international conference on trust management, July 2016. Springer, Cham, pp 129–136
8. Rodríguez JI, Durán SR, Díaz-López D, Pastor-Galindo J, Mármol FG (2020) C3-sex: a conversational agent to detect online sex offenders. Electronics 9:1779
9. Filar B, Seymour R, Park M (2017) Ask me anything: a conversational interface to augment information security workers. In: SOUPS 3rd workshop on security information workers (WSIW 2017), July 2017
10. Gulenko I (2014) Chatbot for IT security training: using motivational interviewing to improve security behaviour. In: AIST (supplement), pp 7–16
11. Nenkov N, Dimitrov G, Dyachenko Y, Koeva K (2016) Artificial intelligence technologies for personnel learning management systems. In: 2016 IEEE 8th international conference on intelligent systems (IS), Sept 2016. IEEE, pp 189–195
12. Lee LK, Fung YC, Pun YW, Wong KK, Yu MTY, Wu NI (2020) Using a multiplatform chatbot as an online tutor in a university course. In: 2020 international symposium on educational technology (ISET). IEEE, pp 53–56
13. Clarizia F, Colace F, Lombardi M, Santaniello D (2020) A chatbot for supporting users in cultural heritage contexts
14. Al Sabbagh B, Ameen M, Wätterstam T, Kowalski S (2012) A prototype for HI^{2}Ping information security culture and awareness training. In: 2012 international conference on E-learning and E-technologies in education (ICEEE), Sept 2012. IEEE, pp 32–36
15. Kowalski S, Pavlovska K, Goldstein M (2013) Two case studies in using chatbots for security training. In: Information assurance and security education and training. Springer, Berlin, Heidelberg, pp 265–272