Chatbot for IT Security Training: Using Motivational Interviewing to Improve Security Behaviour

Iwan Gulenko

Technical University of Munich, Munich, Germany
ivrosh@ymail.com

Abstract. We conduct a pre-study with 25 participants on Mechanical Turk to find out which security behavioural problems are most important for online users. These questions are based on motivational interviewing (MI), an evidence-based treatment methodology that enables to train people about different kinds of behavioural changes. Based on that the chatbot is developed using Artificial Intelligence Markup Language (AIML). The chatbot is trained to speak about three topics: passwords, privacy and secure browsing. These three topics were 'most-wanted' by the users of the pre-study. With the chatbot three training sessions with people are conducted.

Keywords: IT-security education, chatbots, Artificial Intelligence Markup Language, natural language processing.

1 Introduction

We strongly believe that one should refrain from stress users with education about security behaviour, if there is a technical solution. As long as there is no technical solution, security training is a necessary evil and has its place both in research and practice.

Motivational interviewing (MI) is an evidence-based treatment methodology that enables to train people about different kinds of behavioural changes [1]. It assumes that humans are willing to change for the better but often they are not capable to do so; the main reason is that they have conflicting thoughts about the change; they are not resistant but rather ambivalent. MI was already used in various fields. One example is e-therapy - smokers were able to break addiction to cigarettes when treated with MI techniques [2].

Also, chatbots were used for security education [3]: Positive attitudes of users are leveraged, when chatbots were used in an e-learning setting about security behaviour. We build on this research and combine MI with chatbots to improve users security behaviour. For this we use Artificial Intelligence Markup Language (AIML) – a basic method to simplify natural language processing[1].

[1] http://www.pandorabots.com/pandora/pics/wallaceaimltutorial.html

2 Previous work

Motivational interviewing (MI) is a way of talking to people about change. It has been used for a variety of problems including addictions, medication adherence, smoking cessation and overeating. The underlying theory assumes that often decisions are not blocked by resistance but rather by ambivalence. Often weeks or months are between knowing that a change is needed and making the change. In this period, people are in an state of ambivalence in which they want to change and do not want to change at the same time – this makes them procrastinate. MI is rooted in Self-determination theory (SDT) which is about motivation about people's growth tendencies. It presumes that people can make choices without any external influence. Research suggests that if people think they have decided to engage in a certain behaviour, they are more likely to stick to it.

The generic structure of MI can be easily adapted to security behaviour. The interviewer tries to lead the conversation from the problem, which the client wants to solve towards 'change talk' – ideas, plans and intentions to change behaviour coming from the client. In MI only this content matters, since this is most likely to be implemented by the client. A typical MI talk is a semi-structured interview divided into four phases: open questions, affirmations, reflections, and summaries. In our case asking open questions would be about typical security behaviour – for instance: *What do you do to secure computer practice or his identity online?* Instead of lecturing about some security violations, open questions enable the conversation to go into the direction of what the client really needs. The interviewer gives information or advice only when asked directly for it. Using affirmations the interviewer highlights the qualities of the client and how he managed to overcome issues in the past to engage in some desired behaviour; e.g., how the client already changed some Facebook privacy settings and is therefore capable of doing more. This should be followed by reflective listening: the interviewer tries to "guess" what the client is really thinking. It is more than just repeating what the client said; it is giving qualified guesses about what the client actually wants to say. At the end of the process the interviewer gives selective summaries of what was said. Obviously, he chooses to summarize only content that deals with 'change talk' – information coming from the client that points towards the desired behaviour [1].

Not all these facts about MI can be implemented by a chatbot. However, we believe that the first two phases, the open questions and the affirmations can be simulated by a computer. In the next section we describe in a pre-study how the first two phases of security behaviour interview MI can be conducted online.

3 Pre-study

We gathered 25 responses from Mechanical Turk (MTurk) using three basic MI questions. Through this it was feasible to get abstract information about what actually bothers internet users. The participants were paid 50 Dollar-cents per response. The survey consisted of basic questions about demographics, followed by the MI questions. We used the following wording for the questions:

– What would you like to change in your computer security behaviour?
– What hinders you to start engaging in the described behaviour?
– What would be the next steps to start engaging in the described behaviour?

We had 25 replies; the data is represented in table 1. The demographics suggest that we represent the internet user population with a small bias towards 35-54. Male and females are represented equally and the education level seems to be also representing the U.S population. In general this shows that the gathered sample has no extremes; yet we have to get more data to compare this to some bigger population. Generally, our survey results seem reliable, which confirms Buhrmeister 2011 [4]. We choose ten most substantial answers out of the 25 to give the reader a taste of the high quality of the responses (regardless of the 50 Dollar-cents payment).

The replies had mostly to do with passwords. Thirteen replies dealt with the fact that they want to improve their passwords habits. Eleven people talked about protecting their privacy online and secure browsing (protecting against malicious websites, logging out of websites, shutting down facebook. Three replies had to do with the fact that he or she wants to use better software or install an anti-virus software,. Therefore, online users (at least in our sample) mostly want to learn about passwords, privacy, secure browsing.

In the following section we develop our chatbot based on our pre-study.

4 Chatbot

The goal of a chatbot is to appear as human as possible and keep the user interested. Therefore, entertainment-wise a chatbot might be superior to traditional IT-security awareness campaigns such as posters, leaflets, mass mailings. From the viewpoint of efficancy an online trainer is much cheaper for big organizations, where the requirement is to train thousands of employees at the same time.

We develop a chatbot using pandorabots.com, a hosting platform for chatbots; it is also suits as an AIML interpreter. AIML (Artificial Intelligence Markup Language) is the state-of-the-art XML-based programming language for chatbots. Chatbots were already used in manifold contexts such as marketing, entertainment, help on smoking cessation and countless other areas. Interestingly, chatbots were also used for security education [3]: Positive attitudes of users are leveraged, when chatbots were used in an e-learning setting about security behaviour. However, Kowalski [3] does not clarify how the chatbot is programmed, which hinders us to replicate the study and forces us to build our chatbot based on questions from our pre-study, and to use MI techniques.

We briefly describe the basics of chatbots that are based on AIML. The markup language is based on XML and there are three types of tags: *patterns*, *templates* and *that*. Patterns are substrings of strings entered by the user. Patterns are nodes in a graph and edges are decisions. The chatbot traverses through a search- tree to find a path which fits the pattern. The template is at the end of a path and is the output of the chatbot. A tag called 'that' refers to the most recent output of the chatbot.

Table 1. Ten most substantial replies out of the sample of 25 participants

No.	Wanted change	Perceived hindrance	First steps
1	Protect data online, solid passwords	Lack of skills	Take class on computer security
2	Log-out of websites if not using the computer	Log-out of all websites is time-consuming	Log-out of websites after use
3	Use different passwords for different websites, figure out Facebook privacy settings.	Memorizing different passwords is hard, laziness hinders to check Facebook privacy settings	Change passwords of most-visited websites. Reading forums and Facebook FAQ.
4	Change personal data	Laziness	Take time to learn security, use antivirus for Mac
5	Use better passwords	Lack of knowledge what a good password is, many passwords	Websites should standardize password requirements
6	Buy better computer anti-virus, anti-malware, firewall to secure browsing	High cost of security software	Save money, install software
7	Use more secure browsers that do not track surfing behaviour	Inability to find such a browser	Find a browser that has a good reputation for security
8	Remember and change many passwords	Complexity of passwords (special characters, numbers)	Make complex passwords, and change suffix for different platforms
9	Change weak passwords, change them often, scan for viruses more often, change Facebook for privacy	Procrastination, nothing happened so far, virus-scan scan makes internet slow, does not care about certain logins, does not know how to adjust Facebook privacy	Acquire knowledge
10	Be less reckless, wants more protections	Money to buy security software	Get more money

We use bitlbee, an irc server, to fetch text from and send text to the chatbot. With bitlbee we can connect our chatbot to any common platform that has a chat function – e.g., Yahoo, Skype, ICQ, Facebook, Twitter. We choose Yahoo Messenger to interact with bitlbee, because of "Yahoo! Pandorabot", an open source project that seamlessly connects bitlbee with our chatbot.

We use the chat-database of *Dr. Richard S. Wallace bot 2002*. It represents a chatbot that has common knowledge that imitates a real human being. So if Dr. Wallace's bot is asked what his name is, how old he is and how he feels, he gives a reasonable answer. Additionally to this boilerplate-personality we add conversation patterns dealing with (1) passwords, (2) privacy and (3) secure browsing – exactly the requirements that we elicited in the pre-study.

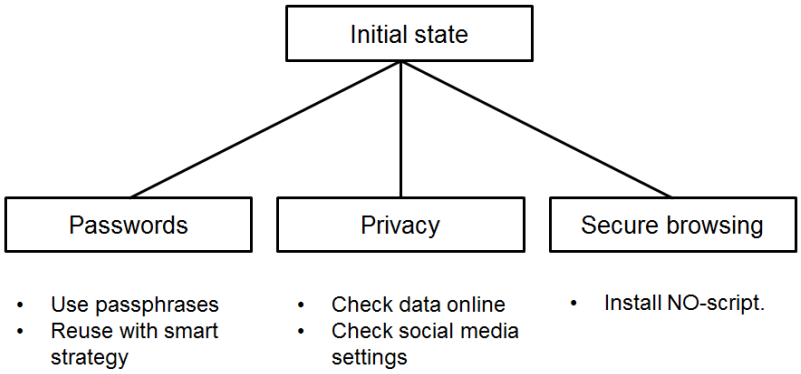

Fig. 1. Chatbot chooses the topic based on user's input and is then able to talk about different aspects of that topic

We present three sample-conversations with the chatbot. The XML pattern files that led to this conversations can be downloaded. Below we show three screenshots of the chatbot talking to clients about different topics of it-security behavioural change.

5 Conclusion

We believe that our chatbot is ideal to be used especially in big organizations, where face-to-face training of every employee is infeasible. An other way to continue the research is to use cognitive thesauri that can be used as an input for the chatbot and thus optimize its functionality. For future research, we need to test the chatbot in more usecases and how users engange into using it.

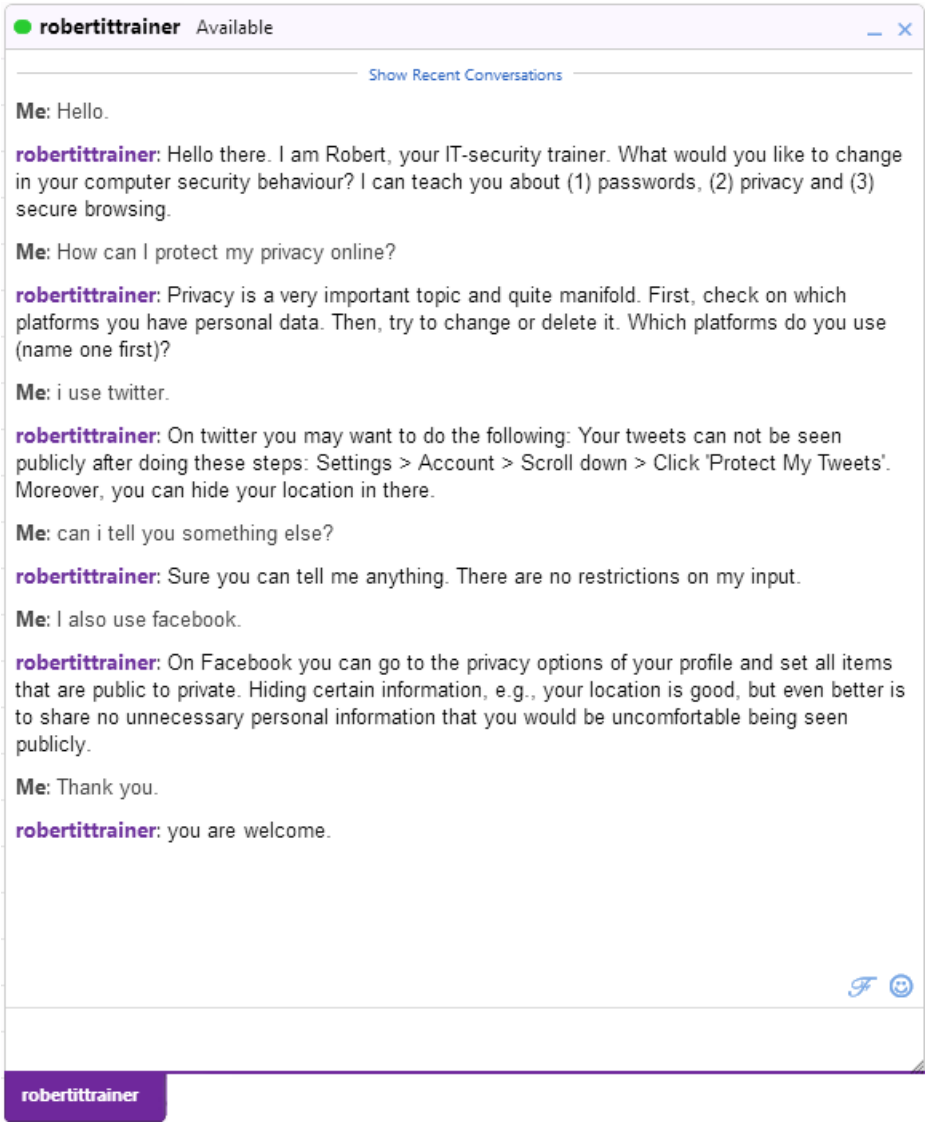

Fig. 2. Chatbot talking about privacy

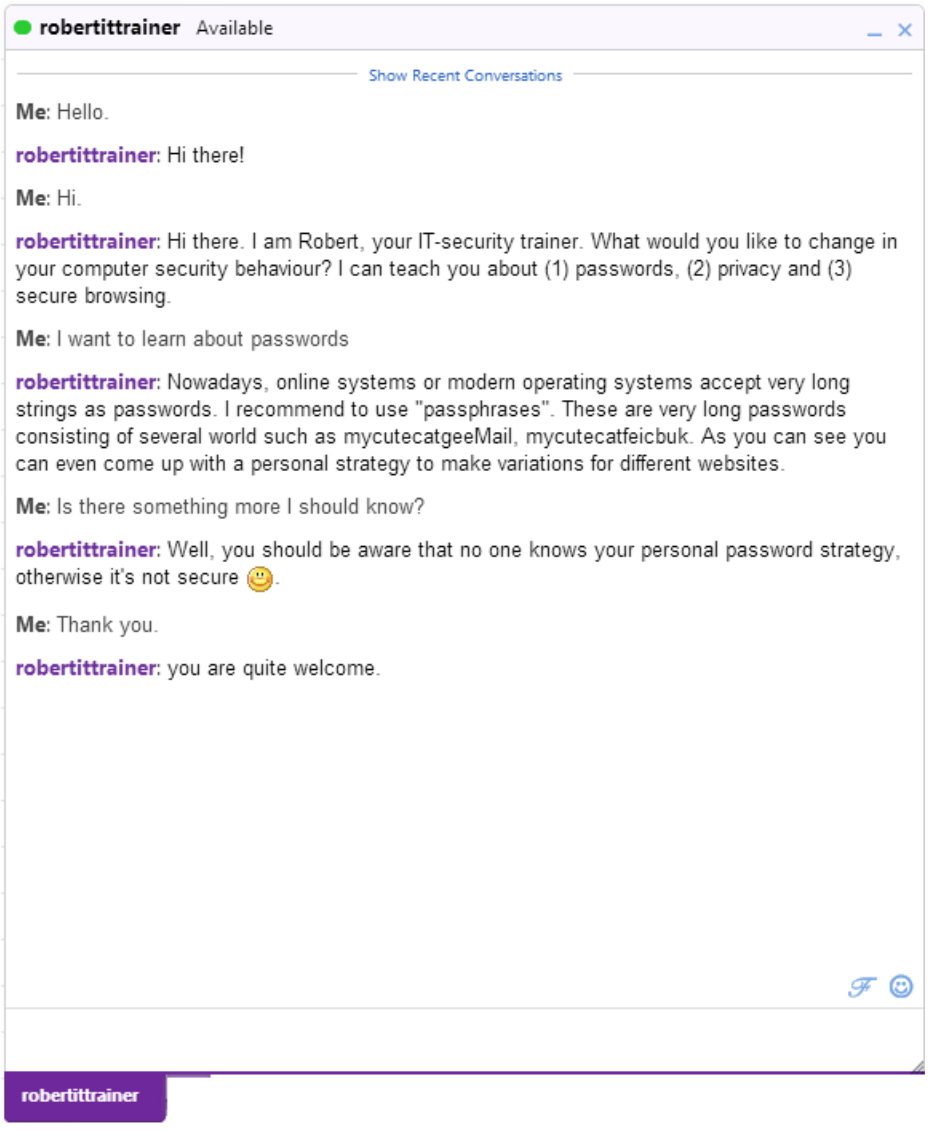

Fig. 3. Chatbot talking about passwords

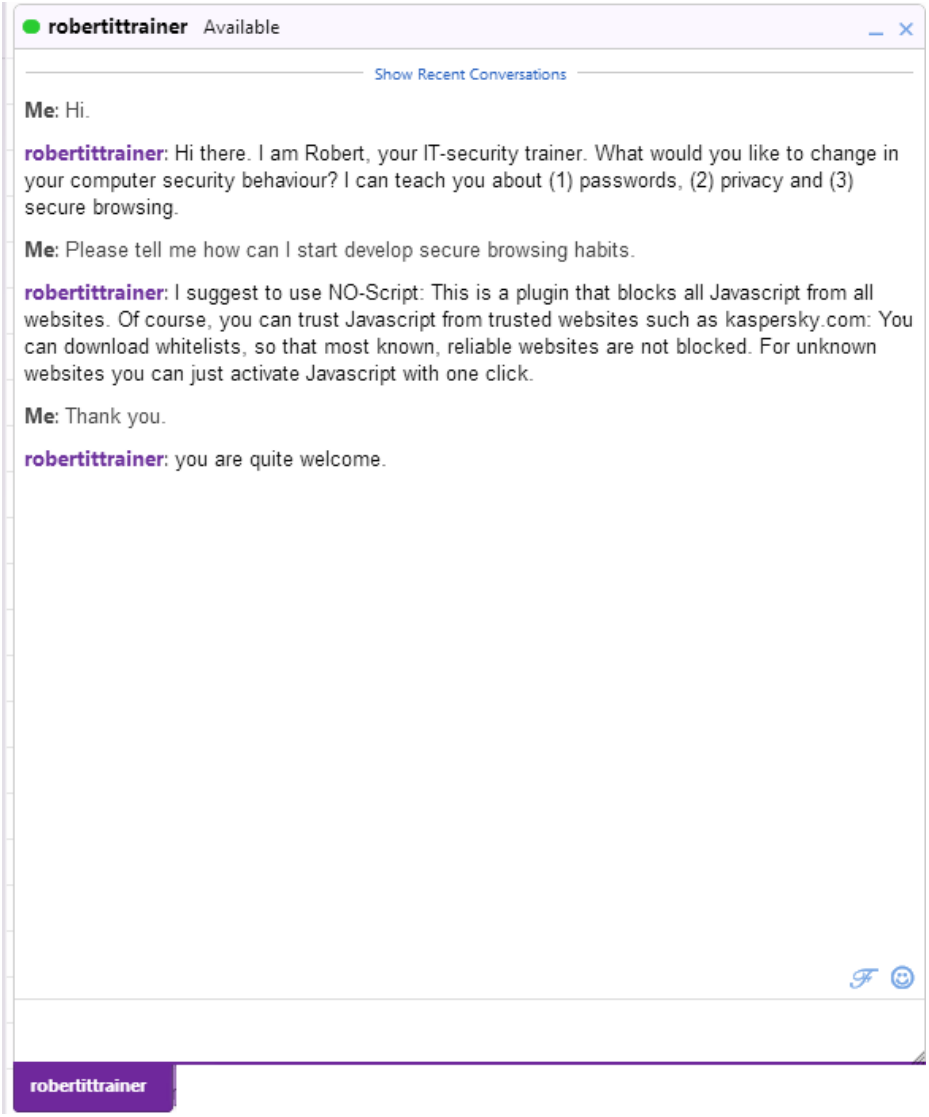

Fig. 4. Chatbot talking about secure surfing habits.

References

1. Miller, W., Rollnick, S.: Motivational Interviewing: Preparing People for Change. Applications of Motivational Interviewing Series. Guilford Press (2002)
2. Grolleman, J., van Dijk, E., Nijholt, A., van Emst, A.: Break the habit! designing an e-therapy intervention using a virtual coach in aid of smoking cessation. In IJsselsteijn, W., de Kort, Y., Midden, C., Eggen, B., van den Hoven, E., eds.: Proceedings Persuasive 2006. First International Conference on Persuasive Technology for Human Well-being. Volume 3962 of Lecture Notes in Computer Science., Berlin Heidelberg, Springer Verlag (May 2006) 133–141
3. Kowalski, S., Pavlovska, K., Goldstein, M.: Two case studies in using chatbots for security training. In Dodge, RonaldC., J., Futcher, L., eds.: Information Assurance and Security Education and Training. Volume 406 of IFIP Advances in Information and Communication Technology. Springer Berlin Heidelberg (2013) 265–272
4. Buhrmester, M., Kwang, T., Gosling, S.D.: Amazon's mechanical turk a new source of inexpensive, yet high-quality, data? Perspectives on Psychological Science **6**(1) (2011) 3–5

Чат-бот для обучения ИТ-безопасности: применение мотивационного интервью для повышения осведомлённости

Иван Гуленко

Мюнхенский технический университет, Мюнхен, Германия
ivrosh@ymail.com

Аннотация При помощи Mechanical Turk проведено предварительное исследование с целью определить какие поведенческие проблемы информационной безопасности наиболее важны для пользователей Интернета. Вопросы были построены в форме мотивационного интервью, позволяющего обучать людей различным формам изменяющегося поведения. На основе этого был разработан чат-бот с использованием Artificial Intelligence Markup Language (AIML). Чат-бот обучен общаться на три темы: пароли, конфиденциальность информации, безопасной просмотр Сети. По материалам предварительного исследования, в котором приняли участие 25 человек, именно эти три темы являются наиболее востребованы пользователями. При помощи чат-бота проведены три обучающих сеанса.

Ключевые слова: обучение ИТ-безопасности, чат-боты, Artificial Intelligence Markup Language, обработка естественного языка.