Development of software for teaching students safety work in e-mail

Denys Volodymyrovych Stolbov
Computer Science Department, G. S. Skovoroda Kharkiv National Pedagogical University, 2, Blucher Street, Kharkiv, 61168, Ukraine
denystolbov@gmail.com

Abstract. This paper highlights the main aspects in development of e-mail simulator. The paper shows features of teaching students e-mail security and describes steps of development the simulator. The result of the paper includes an example of working the simulator.

The research focus: to describe design and implementation features of the software for teaching students safety work in e-mail.

Goals: 1) to reveal the need for teaching students safety work in e-mail; 2) determine the technical requirements of software for teaching students safety work in e-mail; 3) describe the software logical model and justify the choice of design tools; 4) implement the development software model.

Object: the learning process of secondary school students.

Subject: development of software for teaching students safety in e-mail.

The research methods: study of specifics of teaching students safety work in e-mail, designing e-learning tools.

The results: design and implemented of software for teaching students safety work in e-mail.

The conclusion: reviewed the features of teaching students safety in e-mail, described main stages of the software design teaching students’ safety in e-mail.

Keywords: e-mail; threats; safety online.

Столбов Д. В. Розробка програмного засобу для навчання учнів безпечної роботи з електронною поштою

Анотація. Стаття присвячена розробці програмного засобу навчання учнів безпечної роботи з електронною поштою, розглянути особливості навчання учнів безпечної роботи з електронною поштою, описани етапи проектування програмного засобу для навчання учнів безпечної роботи з електронною поштою та наведено приклад роботи з таким засобом.

Meta: описати особливості проектування та реалізації програмного засобу навчання учнів безпечної роботи з електронною поштою.

Задачі: 1) розкрити необхідність навчання школярів безпечній роботі з електронною поштою; 2) визначити технічні вимоги до програмного засобу, який розробляється для навчання учнів безпечній роботі з електронною поштою; 3) описати логічну модель та обґрунтовувати вибір
засобів для розробки програмного засобу; 4) реалізувати розроблену модель програмного засобу.

Об’єкт: навчальний процес учнів у загальноосвітній школі.
Предмет: розробка програмного засобу для навчання учнів безпечної роботи з електронною поштой.
Методи дослідження: вивчення праць щодо особливостей навчання учнів безпечної роботи в Інтернеті, проектування електронних засобів навчання.
Результати: спроектовано та реалізовано програмний засіб для навчання учнів безпечної роботи з електронною поштою.
Висновки: проаналізовано особливості навчання учнів безпечної роботи з електронною поштою, описані основні етапи проектування програмного засобу навчання учнів безпечної роботи з електронною поштою.

Ключові слова: загрози; електронна пошта; Інтернет-безпека.
Місце роботи: кафедра інформатики, Харківський національний педагогічний університет імені Г. С. Сковороди, вул. Блюхера, 2, м. Харків, 61168, Україна.
E-mail: denystolbov@gmail.com.

1. Introduction
Today, e-mail is one of the most popular services on the Internet among students. If earlier e-mail was used by students only as a tool of exchange messaging, now it has evolved into a full-fledged virtual space for all kinds of activity: education, work, communication and leisure time.

Apart from the obvious advantages, e-mail, as well as other online services has disadvantages. There are threats that could harm e-mail users. The most vulnerability among the e-mail users are students. The rapid development of the Internet and the associated appearance of new hazards to users are the reason that teaching students of e-mail security has become an important part of the learning safety online.

2. Features of teaching e-mail security
Analysis of the nature of the Internet activity of students and features of the Internet space, in particular e-mail services, has allowed us to identify main reasons that motivate to teach students of e-mail security:

1) the possibility of collision students with unethical, destructive and unwanted information online through e-mail letters;

2) insufficient protection of personal data of the student’s own e-mail account from stolen (Identity Theft);

3) e-mail can be used by criminals to cyberbullying, harassment and fraud of students;
4) vulnerability of students to e-mail threats due to their age and psychological characteristics of growing up.

The reasons allowed us to define the concept and scope of the students e-mail security. Safety of students in the e-mail we define as their state of protection from potential e-mail hazards. E-mail hazards for the students are the probability of causing them harm, harm to their physical health and psychological condition. The e-mail threat is a fact that the expressed intention of harming to student on the e-mail and the situation when the danger will be possible. A lot of e-mail threats which students can meet transformed from their real life. For instance, there can be fraud, bullying, harassment etc. On the e-mail online or offline students can meet with other threats—such that no reflection in real life—spam, viruses, spyware, identity theft and more.

The results of domestic and foreign research show even 10-12 years students have significant experience working with e-mail [1]. In particular, they are able to create, send and view receiving emails. On the one side, teaching such students the basics of e-mail in the computer science lessons is a lagging process, on the other side, it is important to disclosure basics of safe behavior when they are working with e-mail.

There is important to teach students how to correctly create a mailbox and which personal data can be used, how to distinguish between malicious email from a total of letters and how to properly handle them, how to protect own mailbox from spam, hacking and theft of personal data from it.

The students e-mail security is considered by us as the creation of external and internal conditions of their security. External conditions aim to create a safe e-mail environment for students. These conditions include: technical measures to protect mailboxes from unwanted materials, policy measures to regulated Internet activity of users, international co-operation by intergovernmental organizations. Internal conditions should encourage students to develop their own mechanism of protection against e-mail threats. These conditions have to help students to form own skills to prevent, recognize and successfully overcome the e-mail threats. Such skills can be formed in practice using educational software. One of the types of such software is a training simulator. This simulator has some advantages over the basic learning materials that make it irreplaceable in teaching.

3. Design of e-mail simulator

The e-mail simulator has main advantages: a student can “interact” with e-mail threats in a simulation quite safely without damage to self; the simulator removes the element of danger from the situation; the simulator can be paused, whereas real life cannot. The core of simulator consists of training situations. The training situations tend to meet the following criteria [2]:

1. The situations simulate an activity that is “real”. They simulate the
activity so well that there is little difference between the simulated environment and the real one.

2. The training situations should involve students to become participants, not mere listeners or observers. Students learn better from their own experiences than having others’ experiences related to them.

3. They are tailored to the student. When simulations are designed specifically for their audience, they can take developmental requirements into consideration.

4. They are motivators for learning. Student involvement in the activity is so deep that interest in learning more about the activity or its subject matter develops.

During the design process of e-mail simulator have to consider the age-specific and psycho-pedagogical features of students. These features include characteristics of their imagination, emotional state, memory, thinking and changes in their own behavior. Students want to communicate with peers, find new information about the world and can do risky activity. Those students behavior reflected in their Internet activity.

According to the above criteria of simulator training situations, the students’ features of Internet activity, we defined set of requirements for the e-mail simulator design. The set of requirement includes:

– the simulator has to be similar to the real e-mail. This will allow students to completely immerse in a simulated training environment;

– the simulator should “stimulate” the students to take prudent and unwanted in a given training situation modeled operation of e-mail services and display the consequences of this decision;

– the simulator should be include on elements of game and interactivity, assessment of user actions and possibility of multiple repetition of actions;

Based on the above requirements, for a design methodology of the e-mail simulator we selected Rapid Application Development methodology (RAD). We chose RAD methodology for its advantages: RAD methodology provides the ability to rapidly change design of the software; RAD allows revising of software construction; the lack of extensive pre-planning allows writing software faster, and makes it easier to change requirements for the software; The RAD structure includes four stages of software development: stage of forming requirements, construction stage, design stage and cutover stage.

As a logical model of the e-mail simulator we use MARS (Model-Associations-Representation-Scenario)-model. MARS-model determines a theoretical basic to logical structure of educational simulators [3]. MARS consists on: the Model describes the system behavior that depends on user activities; the Representation that responsible for the user interface; the Associations link the model and the representation; the Scenario is a set of
training situations.

4. Features of work with the simulator

Consider the features of a simulator using specific examples. When a user starts working with the e-mail simulator he/she can see the main page of the simulator (Fig. 1). In the page the user can sign in.

![Fig. 1. The main page of the e-mail simulator](image1)

If a login process is unsuccessful (see Fig. 2), the user can try to sign in again through special options. The options can help the user remember own password.

If the user doesn’t have an account in the e-mail simulator, he/she can create the account through special registration form. The form you can see on Fig. 3.

![Fig. 2. An incorrect user login](image2)

In order to get the account, the user has to fill all fields of the form. When the user chooses a password to own account, the e-mail simulator advises him/her how create a reliable strong password (Fig. 3). Similarly, the simulator coordinate user actions when the user enters own name, the birth date, mobile phone number.

On the Fig. 4 you can see the set of letters page of the e-mail simulator. If you move mouse cursor to one of interface elements, you can see a tooltip that explains the function element. The set include different messages. Some of them are safe and some letters are danger.

Several letters are harmless to students. For instance, there is a letter from ‘kafedra informatiki’ that announces about the open day at the university (Fig. 5). The letter only informs the user of the impending open day. If a user
receives such the letter to own real mailbox, it does not harm him/her.

![Fig. 3. The registration form of new e-mail account](image)

However there are letters with e-mail threats. One kind of the malicious letters is e-mail from well-known companies. On Fig. 6 you can see example of such letters.

![Fig. 4. The set of letters page of the e-mail simulator](image)

There is message from Microsoft. If you reply to such letter in reality, you can be a victim of identity theft. It will be because if you link http:\\www.microsoft.com you could be a fake Microsoft page with special registration form. You must fill the form if you want new version of Windows 10.0. But in the e-mail simulator when you try to link, you can see a warning message that notifies you about danger (Fig. 7). If you ignore the warning
message you can see other message that informs you about result of your activity (Fig. 8).

Fig. 5. Example of a harmless letter

Fig. 6. Example of a threatening letter

Fig. 7. A warning message

Other example of the malicious letters is “African letter” (Fig. 9). The African letter is mean to lose users money through their e-mail account or mobile phone. In reality when the user received such letter, fraudster asks him/her to send some money so that he/she was able to get an inheritance. Usually “African letter” ends with link that give user additional information about how and who send money.
Fig. 8. A message about incorrect user activity

In simulator when the user tries to link of “African letter”, the e-mail simulator shows him/her warning message. The message encourage the user to rethink own decision again (Fig. 10).

Fig. 9. Example of “African letter”

If the user ignored the warning message, the e-mail simulator display on a screen message about incorrect user decision in such situation (Fig. 11). The use of such elements command and information about the possible danger of
making the simulator more acceptable in the learning process compared to using real web space. Such a dialogue simulator helps the user last again reflect on their action and may change it in the right direction.

Fig. 11. A result of incorrect user behavior with the e-mail threat

5. Conclusion

This paper examines development of e-mail simulator. The use of simulators allows teachers to supplement overcome the difficulties of presenting educational material only in theory, in which individual objects, facts and phenomena are difficult to explain. Owing to modern software development tools become possible the creation of educational tools with high level of similarity to real work space in particular the Internet. The e-mail simulator enables students in practice the e-mail threats without harming themselves and help them to form skills to successfully avoid and overcome the threats. During the email-simulator development we have to take into account age-specific and psycho-pedagogical characteristics of students and features of the environment which is modeled via simulation.

References


Received: 3 March 2014; in revised form: 31 March 2014 / Accepted: 10 April 2014