The Current Situation of Information Security and Prevention General Course in Universities and a Teaching Approach Based on Students Structure

Wuyungerile Li, Jiachen Liu(✉), and Bing Jia

Inner Mongolia University, Hohhot, China
31709139@mail.imu.edu.cn

Abstract. This paper takes non-computer majors as the teaching object, analyzes the present situation of information security and prevention in today's society, as well as the existing security problems. And then, we design a set of Information Security and Prevention courses for non-computer major students. Finally, a teaching method based on students structure is introduced.

Keywords: Information security · Teaching methods
Experimental methods

1 Analysis of Information Security Present Situation and Existing Problems

In recent years, with the rapid development of computer network and E-commerce, information security and prevention have been paid more and more attention by relevant departments of the Country. Information security is a universal subject, and the improvement of national information security is related to China's political, economic, military and cultural aspects. The Communist Party of China in the fourth Plenary Session of the 16th CPC Central Committee has included information security and political security, economic security and cultural security into four important components of national security. Combined with the situation of China and the education level of the people, there are several problems in Chinese information security and prevention.

1.1 Weak Awareness of Personal Information Security

Security awareness means that by changing views of organizations or institutions, they are aware of the importance of security and the negative consequences of not ensuring security, as well as establishing training stages and reminding successors. According to the report of Beijing Gu An World Science and Technology Co., Ltd. in late 2012, they carried out the investigation of information security

S. Liu et al. (Eds.): eLEOT 2018, LNICST 243, pp. 353–360, 2018.
https://doi.org/10.1007/978-3-319-93719-9_48

to Chinese employees, and the result show that the their information Security awareness still has a lot of room for improvement. Besides, the main reason for the large number of users data leakage at the beginning of 2012 is also because of the low consciousness of the personal information. According to Wang [8] survey that 83.7% of the people fully fill out their own registration data, compared with 78.2% in 2010. Therefore, in order to realize the information security of the whole nation, we must surround the security subject of people, care about the safety of peoples behavior, and to achieve people-oriented is critical. To realize the people-oriented information security management, the first step is to improve the peoples awareness of information security prevention.

1.2 Low Prevention Ability of Personal Information Security

The popularization of computer network, the application of electronic files, mobile terminals, mobile payment, all kinds of social media and the rapid development of logistics business are the main channels to disclose personal information. In recent years, the big data applications became hot-spots and provided more effective analytical data in some aspects and meanwhile brought great hidden danger to people's information security. Accordingly, in the community we live in, workplace, schools generally have no courses about the information security training or advertisements. Especially in China, many middle-aged and aged people as well as people from countryside, although always on the network and utilize many applications on mobile terminals; they are not enough understand and mastered the risks of them. Hence they are easy to be fishing, be attacked by Trojans and hackers. For these, many people have been stolen information or deceived but also have no awareness of this. Therefore, on the basis of raising peoples awareness of prevention, it is the most important to further improve the ability of people to guard against personal information.

1.3 The Surrounding Environment Is Heavily Trapped

People meet personal information disclosure or receiving telecommunications fraud, always because of social engineering means, mainly have the followings: 1. Attackers use or imitate trusted institutions or target stakeholders, such as banks, governments, to send forged e-mails or messages, to defraud or to grow Trojans. 2. Bait and cross-station phishing attacks: Make use of the latest movies, hot information or ultra-low discounts, which people pay high attentions, combined with the security vulnerabilities of application systems caused by crossing the sites to process phishing attacks. 3. Technical support Services: Attackers impersonate Technical Service Companys staff, and requires people to log in to an address or provide technical support through remote access. 4. The insiders of business platforms, logistics companies, hospitals, company human resources, leak or even trafficking users information. These bits of information, once they are integrated by big data technologies, expose a person completely.

1.4 Relevant Laws and Regulations Are Not Perfect

The quality and progress of legislation cannot meet the actual development needs of the information society. Firstly, legal norms are relatively weak and lagging behind; besides, it lacks of specific laws on privacy protection or personal information protection. Secondly, some legal concepts are not clear. To make a kind of behavior as crime, it must be the serious social harmfulness of the behavior, and the serious social harmfulness is the precondition and foundation of the crime. Thirdly, the legal punishment is not enough. Fourthly, the legislative process is slow. "The Cyber Security Act" was implemented on June 1, 2017 and General Secretary of China Jinping Xi proposed that without network security there will be no national security, cyberspace is the fifth territory after land, sea, air and outer space.

1.5 Lack of General Education

In recent years, China and even around the world often occur the events of personal information leakage, spam or phone messages, and even telecommunications fraud events. Colleges and universities are the main institutions for the training of masters, conveying a large number of graduates to the society every year. Since 2001, more than 20 colleges and universities have set up information security undergraduate courses, and more than 10 universities have established information security PhD-awarding branches. However, the proportion of professional students still is small. For other unprofessional students, especially students majoring in liberal arts, there are no courses on information security and prevention that are applicable to them in society or on campus. The unified computer Basic course and programming course in the whole school cannot effectively improve the students information security consciousness, and also cannot provide the safety precaution ability. Therefore, colleges and universities should pay more attention to and improve the information security and precaution consciousness of the unprofessional students while training professional talents, and teach some safety precaution techniques.

According to Lu and Xu [9] empirical analysis on information security education in eight universities in Shanghai, the probability that students of non-information security and computer majors can access information security education is almost zero. Related courses are similar to the "Computer Culture Foundation" and "The basic of computer applications", such as operating system introduction and office software as the core of the teaching content. Even though there are some classes that include computer security and virus-related content, effect is generally not good because college freshman havent had time to get a thorough understanding of computer networks. In teaching materials, for information security or professional textbooks for computer professional students are quite many, but the popularization of technical textbooks and cultural textbooks are very few. This leads to the difficulty of understanding and mastering information security knowledge for people who are not professionally related.

2 Existing Solutions for Improving Personal Information Security Prevention Ability

2.1 Get Knowledge via Self-study

With the rapid development of computer network, people can learn the relevant knowledge on the network, for example, through watching and listening to the teaching video and audio, reading electronic literatures, have discussion or communication on the Internet forum to obtain the required technical knowledge. According to report, China has more than 500 million netizens; and the main group of the network learners is the city white-collars and university students. But for learners who are not computer, information or network professionals, it is difficult to master information security prevention ability via network learning. As a result, the number of people who are able to get information from the Internet to guard against the invasion is very small.

2.2 Students Can Get Relative Knowledge from the General Courses in School

Universities offer information security courses to teach students some information security prevention basic knowledges. However, most of the teaching is mainly based on the popularization of theoretical knowledge, ignoring the actual operation part. For students who are not computer majors, learn theoretical knowledge without any operation skills, difficult to master and easy to forget. In addition, the existing teaching materials are more professional and not very suitable for students who are not computer majors. Therefore, it is need to a better design in teaching method and textbooks as well as experimental teaching.

2.3 Companies and Government Departments Give Their Employees Information Security Training

Some enterprises and institutions or IT companies train their staffs of information security related knowledge. However, more of the content is related to their company and the organization, not suitable for outside and network use, and the number of people involved is less. In addition, there are some information security training institutions in the community, often at the expense of high tuition fees to provide learners with a certain degree of security measures and techniques.

3 The Contents Analysis of Information Security and Prevention Courses

3.1 The Requirements of Information Security and Preventive Courses for Teachers

This paper aims at the research and exploration of the teaching methods of information security and prevention course for non-computer related major students.

Information security is a new subject which is related to the whole nation, and there is no good teaching material for popularization at present. Therefore, the requirements for teachers in this course are as follows:

(1) Teacher allocation requirements: Firstly, the teacher has a good professional knowledge and has a certain degree of ability on information security precautions, detection and remediation. Secondly, the teacher fully understand the basic situation of students who select courses, such as the computer course that they had studied, mastery of the courses, the student proportion of science and liberal arts.

(2) Textbook needs to be well designed: At present, there is no suitable textbook about information security and prevention for the non-professional students. Therefore, after analyzing the present situation of the students, the teacher will edit a course of information security and prevention which is suitable for the students in the current period. Generally, the design of the course is flexible and varies according to the basic knowledge and professional circumstances of students that select the course for each year. For example, when liberal arts students more on the class, then the teaching content should be easier to understand and easy to operate experiments. When the science and engineering students takes a great proportion, teacher should design the lecture content to deepen some and teach more complex operation.

(3) It is the curriculum construction needs: The information security and prevention is a university general education course so that the types of student majors who select the course are various. According to experience, each year due to different major types of students, the degree of acceptance of this course and student personal ability is not the same. Therefore, in the teaching, teacher should adjust their content according to the students understanding, accumulated better teaching experience and methods, ultimately to enable students to get the higher level of information security and prevention knowledge.

3.2 Theoretical Knowledge of Information Security and Prevention Course

- Social engineering and awareness of information security prevention
- Operating system security
- Cryptography basics and digital authentication
- Computer viruses and malware
- Intrusion detection technology
- Firewall Technology
- VPN Technology
- Wireless network security
- E-commerce security.

3.3 Experiment Content of Information Security and Prevention Course

- Security settings of Windows operating system
- Web security
- Phishing attacks
- Social engineering and Cryptography Dictionary
- Intrusion detection
- Firewall settings
- Vulnerability scan and vulnerability scanner.

4 An Elective Course Teaching Method Based on Students Structure

4.1 Adjust the Teaching Content of the Course According to the Proportion of Liberal Arts and Science Students

As a university general course, Information security and prevention generally does not limit the majors of students who select the course. Because of the different curriculum arrangement of students majoring in Art and science, the basic knowledge they can learn is different. Therefore, a unified standard of teaching will be difficult or too simple for liberal arts or science. In addition, currently, professional textbooks are many, popularity textbooks are less. In view of these situations, we will combine students different professional types, arrange the reasonable course content, not confine to a certain teaching material or some widely applied specialized course, widely refer to the teaching experience and teaching content of common general courses in universities, as well as consult the information security education content of enterprises, government departments and the popular prevention techniques on the networks. We teach students to take the essence, step-by-step, from the introduction of the basic knowledge to have a better sense of prevention, eventually obtain daily preventive ability.

4.2 Adjust the Teaching Content According to the Ratio of High and Low Grade Students

Except the students major type, the levels of students grades are not required in this course. On the class, there are always some freshmen, as well as junior and senior students. This makes the basic knowledge of students and the social experiences they mastered are different. Freshman, just came out from high school, did not have an independent life, are full of curiosity to a lot of things, want to try, and lack of personal information protection awareness, always cannot identify and prevent the true and false. The junior and senior students live independently for two or three years, with a certain sense of self-protection and prevention awareness, in the face of problems have in certain ability to deal with or to know consulting with their parents and friends. Therefore, the teaching content of the information security course should be adjusted with the degree proportion of the students. That is, the content of the teaching to meet the accepting ability of the majority of students to, so that more students learn basic knowledge and grasp certain ability of information security prevention.

5 Evaluation of Teaching Effect

5.1 Student Evaluations

In the course of teaching, the students combine the information security events they have seen in daily life, take the questions to the class, or teacher organize class discussion, improve students learning interest and mastery of the knowledge. In addition, group analysis courses are arranged to enable students to analyze and explain principles, steps, and precautions of safety events in daily life, so as to strengthen students awareness of prevention and interest in obtaining relevant knowledge.

5.2 Teacher Evaluation

Teachers combine the teaching content of each class in teaching, give examples to explain relevant knowledge points, combine theory with practice, introduce and analyze latest information security cases, improve students sensitivity to information security and prevent consciousness. In addition, through experimental teaching, students can combine the theoretical knowledge and experimental teaching together to improve students ability of prevention.

6 Conclusion

Based on the research of colleges and universities, this paper analyzes the popularization and existing problems of information security teaching in colleges, and draws up a teaching content of information security and prevention which can be regarded as the curriculum of general education in colleges and universities, and gives an instructional method and its evaluation method according to the type of students of the course.

Acknowledgement. This work is supported by the project of “Elective course construction of general education in Inner Mongolia University, the course of Information Security and Prevention.”

References

1. http://finance.qq.com/a/20130307/006189.htm
2. Li, Y., Yi, Z., Wei, Z.: Analysis on the present situation and countermeasures of information security education in colleges. China Med. Educ. Technol. (03), 300–303 (2016)

3. Yue, Z.: Exploration and practice of network information security education for college students. Comput. Knowl. Technol. **24**, 5735–5736 (2014)
4. Feng, L.: Analysis and formation of college students' information security literacy. Comput. Educ. **21**, 77–80 (2010)
5. Miao, X.: Teaching exploration and research on information security courses for non-information security majors. China Educ. Inf. **05**, 67–68 (2012)
6. Yu, G., Yu, J.: Research on information security teaching of computer specialty. Sci. Technol. Inf. (16), 18–20 (2009)
7. Hong-guang, X., Zuo-wen, T., Ya-hui, Z.: On education of college students' information security awareness. Theory Practice Contemp. Educ. **04**, 29–31 (2009)
8. Wang, Y.: Management observation (26), 141–142 (2012)
9. https://doc.docsou.com/b367bc530186deb06d1f79d39.html