TEACHING INTERNET SAFETY AT UNIVERSITIES USING "HIKARI & TSUBASA'S INFORMATION SECURITY GAME"

Hitoshi Okada
National Institute of Informatics, 2-1-2 Hitotsubashi, Chiyoda 101-8430 Tokyo, Japan

Hideaki Sone
Information Synergy Center, Tohoku University, Aoba, Aramaki, Aoba-Ku, 980-8578, Sendai, Miyagi, Japan

Masaru Ogawa
Kobe Gakuin University, Arise, Ikawadani, Nishi-ku, 651-2180, Kobe, Japan

Keywords: Information security, Security policy, e-Learning, Interactive education material.

Abstract: Nowadays it is becoming more and more important to inform everyone about the potential dangers of this means of communication. Especially it is most important for universities to teach the risk of internet society. This material is designed to develop these abilities through interactive engagement by presenting the information in a dialogue form. We have created a text with CD and a three-choice quiz to bring freshness to the educational materials.

1 INTRODUCTION

Information security management is a huge challenge for higher education institutions, even more so than for other large institutions or companies. Professors and students cannot be prohibited from bringing their own private computers to campus, and universities generally have a lot of traffic in people who are not students or instructors. Knowledge and skill levels are likewise varied, and some students end up accessing and downloading attractive but dangerous software. Universities are also easy practice targets for external attack if they house insufficiently protected PCs and servers.

Information security policies have been put in place at universities and other higher education institutions. Training for professors and students is underway, but materials that discuss the legal and technical aspects of information security tend to be a hard sell for most students. Educational video "dramas" have had some success as a learning tool for professors. Professors, however, are from the TV generation. Students today grew up on the internet and video games. We need to teach about internet risk and safety with materials that appeal to the thinking patterns of the interactive generation—games. Today, I would like to introduce "Hikari & Tsubasa's Information Security Game," a textbook and CD published in March 2008 by our Working Group for Information Security Policy Promotion for National Universities and Institutions.

2 PURPOSE OF THE MATERIAL

This textbook and accompanying CD were created specifically for students. Anyone who uses the internet at home, at school, or on their mobile phone, is vulnerable to many different risks. "Information security" is about protecting people and their computers from this danger. But so many people move in and out of universities, use all kinds of different computers and systems, and learn so many ways of using them from their friends, that campus usage policies are not enough to protect everyone. In fact, we often hear about schools that have victims of the internet. In this textbook, we try to avoid

Okada H., Sone H. and Ogawa M. (2010).
TEACHING INTERNET SAFETY AT UNIVERSITIES USING "HIKARI & TSUBASA'S INFORMATION SECURITY GAME".
In *Proceedings of the 2nd International Conference on Computer Supported Education*, pages 431-433
DOI: 10.5220/0002787504310433

complicated legal and technical topics and focus just on the problem and solution. Please take a look, and if you have access to a computer, test your knowledge of information security using the interactive multiple choice quizzes we put together on the CD. We hope the materials help you learn to ask yourself the right questions and practice "good behaviors" as members of internet society.

(From the Foreword)

2.1 Target Audiences

The textbook and CD were distributed for free to national, prefectural, and municipal universities and technical colleges. A number of universities are using the materials as part of information security training for their students. Some schools have uploaded the CD contents to their campus servers or authentication servers so that students have access from on and off campus. In addition, we continue to introduce the materials to university instructors at information security seminars around the country.

2.2 Emphasis on Interactive Learning

It is difficult to teach students about information security. We need to cater to the needs of kids who were raised on the internet and video games. Working with the cooperation of members of the NII Information Security Measures Policy Team, we have developed an interactive game to teach the latest knowledge about internet risk and safety in an entertaining way.
Following are the sample of the scenarios from the materials. The dialogue is intended to appeal to freshmen students.

2.2.1 Beware of Phishing!

Scenario 2: Beware of Phishing!
Keita and Tsubasa are talking at the bus stop. Let's listen in.
It sounds like Tsubasa got an email from a credit card company asking him to re-register his card number and expiration date as a safety precaution. The instructions say to click on a link that will take him to the registration page. Tsubasa thinks something smells fishy, but at the same time he wants to make sure his credit card isn't cancelled. He asks Keita about it.

2.2.2 Question

What should Tsubasa do?
A: Try entering his card information.
B: Call the phone number listed in the email.
C: Ignore the email.
The right answer is:
C: Ignore the email.

Why is it C?
Banks and credit card companies will never send you an email asking for your card information or telling you to enter it online. You can be sure it's a scam. If you enter your information on a fake website, it will probably be sent to fraudsters. That's called phishing. You shouldn't reply to the email either. Whoever sent it got your email address from some kind of mass list, and if you reply or click on link, it is likely that you will be put on yet another one as a person who is likely to be tricked. The best policy is to ignore these kinds of emails.

How dangerous is A?
If you send your card information to fraudsters, they can use it to make purchases that you could be held responsible for. Some of them even arrange for the credit card company's real website to pop up after you enter your data. They try very hard to keep you from realizing that you've been scammed.

Isn't B okay too?
The phone number is probably fake, but if it does connect to the fraudsters, you've be giving them your phone number. In the case of fake bills, you might be threatened or harassed. If you have questions, you should call the customer service number listed on the back of your credit card.

2.2.3 Lecture Part

What should Tsubasa have done?
Always ignore phishing and fake bills. If you respond, you'll make yourself prone to more attacks. Emails can be faked, so don't carelessly click on whatever links you see in them. Another good security measure is to set up your email so that it doesn't show HTML.
Thanks to the popularity of online services, a lot of internet auction and shopping merchants, banks, credit card companies, and payment agent companies are falling prey to phishing fraud schemes. When you access their websites, manually enter the URL and bookmark it on your computer for future use instead of following links from the email you receive. It is also risky to access the links using search engines since the search results can be fraudulently manipulated. Even portal sites are prone to cross-site scripting and can be dangerous.

Figure 1: Question and Lecture.

Things to keep in mind about phishing are following.
Ignore emails about your card number because they are scams.
If you are worried, call the customer service number listed on the back of your card or on official documents instead of any numbers listed in the email.

2.2.4 Words and Columns

What does "phishing" mean?
Phishing is pronounced the same way as "fishing" and comes from the idea of fishing for victims using email and other sophisticated bait. Recently "spear phishing" has been targeted at small groups of people.
What if you want to make absolutely sure that the email isn't legitimate?
First, remember that important notices like that would not be delivered to you by email. They are sent by postal mail so that there is record. If you do get an email, it would be in conjunction with postal mail. If you're not sure about the authenticity of the notice, you should contact the number listed on your agreement or registration papers, not the number listed in the notice.
What if a shopping site doesn't have a key symbol?
Do not trust the site. Even if you don't have any monetary trouble, the company may not be very careful with your personal information.
What is my 3-digit security code?
A credit card has a 3-digit security code on the back. If someone gets a hold of this code, it serves as the proof of cardholder.

3 CONCLUSIONS

This concludes my introduction of "Hikari & Tsubasa's Information Security Game." Instructors who have used the materials in class reported that they effectively motivated students to learn. The textbook is arranged in the same order as the CD content and provides more detailed explanations for the scenario problems and answers along with summary points and additional factoids at the end of each chapter.

The combination of textbook and interactive FLASH media is ideal for appealing to the interests of young students while at the same time accurately conveying the latest technological information available. It is also makes it possible for students to learn about information security effectively and accurately on their own, something that was difficult for the average student to do in the past. Our next task is to provide translated versions for the many foreign students studying at schools in Japan.

REFERENCES

Okada, H. ed,: Hikari and Tsubasa's Tutorial for "*Putting Our Heads Together" about In-formation Security* (In Japanese), National Institute of Informatics, Japan (2008)