Don't Be a Target

"This is just like I have got an ATM in my room!" When I used Internet Banking at first, I was impressed by the usefulness of the Online Banking system. Thanks to the Internet, rapid information technology advances have led us to a more convenient world. Now we can manage our own account without going to the bank. Even if you don't have enough time to go to a bank, you will immediately be able to transfer your money by using the Internet. However, in this convenient way to access a bank account, your money might be exposed to serious problems and has the potential to be stolen by someone whom you don't know. To protect our property from crime, and to use the Internet Banking effectively, there are several ways in which we should pay more careful attention.

A few years ago, my sister told me that, on her credit history, she had found some weird withdrawals. According to my sister, one day she was looking at her credit account to check monthly payments by using the Internet. Actually, she hadn't recognized the fact, until that day, that a small amount of money had been taken from her account over a few months (Mori). She wondered what she had paid for, so she soon checked all receipts, which she had kept just in case. However, she couldn't find any receipts for the payments. Moreover, she still had no idea about the purchases, so she called to the bank and asked a bank worker to stop the account. Fortunately, the bank returned the money to her, and the bank worker said to her she might have been cheated on her credit number and password while she was shopping online.

If so, how can we protect money from crime? First, the most basic thing is don't access your bank account from the computers in an Internet cafe or other public places. The computers in public places have a much greater possibility to be a target of the "Key Logger" program (Kim). If the program is set up on a computer, the program will memorize every key operation which you type. Furthermore, the program has an automatic function itself to send the collected information, such as your password or ID number, to the criminal.

Next, you shouldn't keep the same password for a long time. Even if you only accessed the bank account from your own computer, it's not enough to prevent your account being a target. Especially, if you are using the automatic login system, the possibility to be cheated on your password will increase. Hackers have attempted various ways to get people's information; furthermore, hacking is not such a difficult thing to do. Therefore, we have to recognize that our security isn't perfect any time and we should make a new password frequently.

Another way to protect your account is to avoid using your password for just any request. Recently, many people have been damaged by “. phishing." The technique to steal people's account information is simple but intricate. The criminal sends an HTML e-mail which pretends it comes from the bank (Kim). The form looks just like a real web site, so customers put their information in the fake window without deep concern.

In addition to these ways, we shouldn't forget to check our own account history regularly. And then, if you find a strange record, you should immediately call the customer service center of the bank. If you find it sooner, the bank's response will be better, and your lost money will be recovered.

As online banking becomes popular, many problems can potentially result. Sometimes we have an unexpected and serious problem. To make good use of the online systems, we have to take appropriate

steps and have to protect own property from `high-tech" crimes. Sometimes, Internet banking is really useful for us; however, we might lose financial security if we’re not careful.

Works Cited

Mori, Noriko. Personal Interview. 12 Feb 2011.

Kim, Won, et al. "The Dark Side of the Internet: Attacks, Costs and Responses."

Information Systems 36.3 (2011): 675-705. Academic Search Premier. EBSCO. Web. 22 Feb. 2011.