

A STUDY OF TWO-FACTOR AUTHENTICATION AGAINST ON-LINE IDENTITY THEFT

Seungjae Shin, Mississippi State University, 1000 HWY 19N Meridian MS 39307,
sshin@meridian.msstate.edu, (601)484-0160

Jerry Cunningham, Mississippi State University Meridian, jac105@msstate.edu

Jungwoo Ryoo, Penn State Altoona, jryoo@psu.edu

Jack E. Tucci, Mississippi State University Meridian, jtucci@meridian.msstate.edu

ABSTRACT

Multi-factor Authentication is one of the tools used by financial institutions to combat Identity Theft and ensures that consumers' on-line transactions are transferred securely through the public Internet. This article describes available authentication technologies, a matrix of selected financial websites showing their implementation of different combinations of authentication methods, and provides an interpretation of survey results to better understand the perceptions/expectations given by on-line customers in contrast to industry best practices.

Key Words: Multi-factor Authentication, Phishing, On-line ID-Theft

INTRODUCTION

According to the 2007 Consumer Bill Payment Trends Survey conducted by Harris Interactive and the Marketing Workshop, consumers in Internet-connected households are paying more bills on-line than by paper check and 74% of U.S. on-line households pay at least one bill on-line. According to the 2006 Identity Theft Survey Report sponsored by Federal Trade Commission [6], the estimated number of U.S. adult ID-theft victims in was 8.3 million. Growth in on-line transactions is explosive, and as a result, the opportunity for on-line theft has increased proportionately. According to the identity theft report from the U.S. Federal Trade Commission [5], identity theft is the number one complaint reported to FTC (36% in 2006) and among the identity theft categories, credit card fraud is number one and bank fraud is number three.

One of the popular ID-theft methods used by thieves to steal a person's electronic identity and gain access to their funds and credit on the Internet is phishing. Thieves using the phishing techniques to deceive users in order to collect information about the user's identity such as user name and password, social security number, account number, birth date, mother's maiden name, and other private information. Using the stolen personal information, the phishers (id-thieves) withdraw or transfer money from the victim's account for their own use. According to the Anti-Phishing Working Group (APWG) [1], the United States is second highest (22.93%) of the top 10 phishing site countries. The number one target industry for the phishing scams in the U.S. is the financial industry (94.4%). Today, various methods are used for money transfer between financial institutes, countries, and individuals. Electronic transfer via ACH (Automated Clearing House) is a frequently used method. It is used for money transfer from one bank to another bank

with a different account owner. One of the popular electronic transfers via ACH is a bill-payment. On-line transaction companies like PayPal is but one example of an on-line bill payment processor.

When attempting to steal users' identities, on-line criminals develop fake web sites and send Internet users a spoofed e-mail. According to Emigh [2], the estimated loss to the U.S. banking and credit card industry from on-line phishing was \$1.2 billion in 2003. As phisher's improve their approach and techniques, anti-phishing countermeasures are also developed to meet these threats. However, most if not all are reactionary measures. Nevertheless, there are many safeguards against on-line identity theft, but most are infrequently implemented across the various sectors of the financial industry. Some effective safeguards face consumer resistance. The reasons for resistance include difficulty of use, complexity, forgotten/difficult/specialized passwords, or inability to guarantee relative financial safety. In 2006, the Federal Financial Institutions Examination Council (FFIEC) recommended that all financial institutions in the U.S. make two-factor authentication mandatory by 2006 year-end. It was not done.

In this paper, a physical review of anti-ID-theft methods in the U.S. financial industry was performed to verify the implementation of safeguards in the major U.S. financial sectors such as banking (regional, nationwide, and on-line), credit card companies, on-line stock brokers, and on-line payment processing companies. In the summary, a user survey was administered and analyzed to match user perceptions and preferences for each anti-ID-theft method with what the financial industry currently offers.

AUTHENTICATION METHOD FOR ACCESS

According to the recommendation of FFIEC [3] to the U.S. financial institutions about Internet identity theft, there are three factors for authenticating a real user: (1) Something the user knows (password, PIN), (2) something the user has (ATM card, token), and (3) something the user is (fingerprint). Experts recommend using at least two of the above factors to establish a user's identification. Using multiple solutions from the same category is not a multi-factor authentication [4]. A good example of two-factor authentication is an ATM card. An ATM card user needs a physical ATM card and its corresponding password. The following is a list of authentication methods used / suggested in the on-line industry against ID-theft.

Category I: Something you know

Shared secrets are the most popular and inexpensive way to authenticate a user. These shared secrets are information elements that are known or shared by both on-line customers and financial institutions [3]. Information elements include passwords, PINs, security questions and answers to verify customer's identity, and customer-preferred images and phrases.

Category II: Something you have

A security token is a small device to authenticate the owner of that token. There are many token types. One of the popular tokens is a USB token, which can be plugged into a computer's USB port. Smart cards are credit cards with a microprocessor saving sensitive information of an owner. Both USB tokens and Smart cards need passwords to use them. A third type of token is a

password generating token. This token generates a one-time password every 60 seconds. However, this type of token needs time-synchronization before it can be used. The above three types of token are hardware tokens. The other type of token is a software token, which is stored in laptop, PDA, or cellular phone. The function of a software-token is similar to that of a hardware-token. However, only the device with the software token can identify a user with a token password. CAT (Cellular Authentication Token) is a software token used in mobile banking. CAT generates a new one-time password on the cellular phone every 60 seconds. Anybody who steals a CAT cellular phone cannot use it without CAT password.

Category III: Something the user is

Biometric identification relies on unique physical characteristics of each human being such as fingerprint, facial structure, voiceprint, iris/retina recognition, hand geometry, etc. Among them, fingerprint recognition is the most mature (technology), accurate, and economic method. One of the disadvantages of the biometric method is that a scanning device is needed on every computer. This is one of the reasons that the biometric authentication is less popular compared to the other authentication methods (something you know or something you have).

IMPLEMENTATION OF ANTI ID-THEFT METHOD IN THE U.S. FINANCIAL INDUSTRY

Based on the methods discussed in the section 2, the authors, acting as customers themselves, tested nine web sites of U.S. financial institutes: two nationwide banks, two local banks, one on-line bank, two credit card companies, one on-line stock broker and one on-line payment processing company. The following table shows assessment results for authentication methods.

[Table 1] Assessment for Authentication Methods

Anti ID-Theft Methods		Nationwide Bank1	Nationwide Bank2	Local Bank	Local Credit Union	On-line Bank	Credit Card1	Credit Card2	On-line Stock Broker	On-line Payment Processing
Password	Minimum Length	7	8	6	6	NA	6	7	7	8
	Special Character	Y	Y	Y	Y	NA	N	N	N	Y
	Case Sensitive	Y	Y	Y	Y	NA	N	N	Y	Y
	Expiration	N	Y	Y	Y	NA	N	N	N	N
	Notification	Y	N	Y	N	Y	N	Y	Y	Y
	OTP	N	N	N	N	N	N	Y	N	N
Security Q & A	Q&A Set	Y	Y	Y	Y	Y	N	Y	N	N
	Registered Computer	N	N	Y	Y	N	N	N	N	N
	Other Computers	N	Y	Y	Y	Y	N	Y	N	N
Customer Phrase and		N	Y	N	N	Y	N	N	N	N

Image									
Visual Encryption	N	N	N	Y	N	N	N	N	N
PIN with Character Set	NA	NA	NA	NA	Y	NA	NA	NA	NA
Token	N	N	N	N	N	N	N	N	Y
Biometric	N	N	N	N	N	N	N	N	N
Secure E-mail System	Y	Y	Y	N	N	Y	Y	Y	N
Enabling Cookies	Y	Y	Y	Y	Y	Y	Y	N	Y
Previous Login Record	N	N	Y	N	Y	N	Y	Y	Y

- Y: implemented, N: Not Implemented, NA: Not Available
- At the time of Feb. 2008

USER PERCEPTION AND PREFERENCE

The following questions were developed, based on the user's perception and preference feedback about anti-ID-theft methods experienced during the testing of the different financial sites. Other questions were added to clarify respondent relationships to using the financial institutions' offerings on-line. We also added some demographic questions such as age, gender, and the level of experience in on-line banking.

Q1: Do you have experience with On-line Banking? (Y or N)

Out of 204 respondents, 151 answered yes to this question. Therefore, for the rest of the questions we only used the 151 respondents that had experience with on-line banking.

Q2: How many times on average per month do you use an on-line banking service including on-line bill payment?

None	1 or 2	5 or less	10 or less	Over 10
21.9%	7.9%	23.8%	31.1%	15.2%

Q3: Have you ever had your identity stolen?

Yes	No
82.8%	17.2%

Q4: Have you ever participated in Mobile Banking using your cell phone or PDA?

Yes	No
79.5%	20.5%

Q5: Have you ever been locked out of your on-line account due to providing incorrect passwords multiple times?

Yes	No
41.4%	58.9%

Q6: In your opinion, which category of financial institution gives you the strongest on-line security safeguard?

Banks	Credit Card Co.	On-line Stock Brokers	On-line Payment Processing Co.
72.2%	14.6%	0.7%	12.6%

Q7: The use of a longer password makes it more difficult to break the password. In your opinion, what is the minimum length of a strong password that makes you feel comfortable?

At least 4	At least 6	At least 8	At least 10
1.3%	41.1%	48.3%	9.3%

Q8: Use of special characters, alphanumeric characters, and using both upper and lower case letters in your password makes it stronger. For example, "tri6#Vial" is a good example of a strong password, but the strong password is not easy to remember.

Are you willing to create and use such a strong password to improve your security?

Yes	No
21.2%	78.8%

Q9: How often are you willing to change your password for the purpose of on-line banking security?

Never	Once a Month	Every three months	Every six months	Once a year
18.5%	30.5%	8.6%	19.9%	22.5%

Q10: Do you want to be prompted by security questions, (i.e. what is your mother's maiden name?) every time you log on to any computer? (Y or N)

Yes	No
57%	43%

Q11: From the following security options, which method would best satisfy your expected ease-of-use requirement from the financial institution's Website and give you a feeling of security about your on-line experience.

Login + Password	Login+Password+Pin	Login+Passsword +Biometric	Login+Passsword+Token Device
33.8%	32.5%	27.2%	6.6%

Q12: If your bank asks you to pay mandatory fees for the use of biometric or token devices, how much are you willing to pay for this service?

\$1 per month	< \$5 per month	\$5 to \$10 per month	>\$10 per month
62.9%	29.1%	6%	2%

It is evident from the survey above that the respondents are mostly willing to sacrifice some convenience in order to feel more secure with their online banking experience. The willingness of over 80 percent of the respondents to change their password with the largest group, 30 percent, willing to change their password once a month shows that security is at the top of customers' goals in participating in online banking. This is further demonstrated by the willingness of the respondents to use a variety of security options such as PIN numbers, biometric devices or token devices in conjunction with their login and password. The financial institutions are mandated to institute such security measures and the public seems to be willing to accept the measures in a reasonable amount of application. Given the increasing popularity of online banking within the

dangerous online environment, a sensible compromise between security measures and customer convenience must be tailored in such a way as to err on the side of security and expect a tolerable amount of inconvenience.

CONCLUSION

In conclusion, the authors have described a number of different potential authentication methods used by various financial institutions. When used in combination, as shown by the matrix provided in Table 1, the institutions can satisfy the mandatory regulations laid out by the FFIEC by providing multi-factor authentication schemes on their websites. The means of providing secure transactions has to be balanced with the inherent demands of customers for convenience. The empirical evidence provided by the survey shows a broad acceptance by end-users for the financial institutions' efforts to provide both a secure and convenient web experience. Given the multitude of current news articles emphasizing identity- theft and phishing attempts, the majority of our survey respondents trust their current institution with the security of their personal information. Furthermore, the survey revealed that there is a willingness to accommodate a reasonable amount of sacrifice of convenience to be able to bank on-line. Therefore the mandated regulations placed on the financial institutions of providing multi-factor authentication techniques on their websites have not deterred the public in general from using the sites. It is our observation that the overwhelming desire by the customers to be able to take advantage of the on-line banking experience trumps the deterrence that a combination of complicated authentication methods may induce.

REFERENCE

- [1] Anti-Phishing Working Group (2007), Phishing Activity Trends, Report for the Month of November, 2007, http://www.antiphishing.org/reports/apwg_report_nov_2007.pdf
- [2] Emigh, A., (2005), On-line Identity Theft: Phishing Technology, Chokepoints and Countermeasure, <http://www.antiphishing.org/Phishing-dhs-report.pdf>
- [3] FFIEC (2006a), Authentication in an Internet Banking Environment, http://www.ffiec.gov/pdf/authentication_guidance.pdf
- [4] FFIEC (2006b), Frequently Asked Questions on FFIEC Guidance on Authentication in an Internet Banking Environment, http://www.ncua.gov/letters/2006/CU/06-CU-13_encl.pdf
- [5] FTC (2006), Identity Theft Victim Complaint Data, http://www.ftc.gov/bcp/edu/microsites/idtheft/downloads/clearinghouse_2006.pdf
- [6] Synovate (2006), Federal Trade Commission – Identity Theft Survey Report, <http://www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf>