PHISHING – THE THREAT OF INTERNET BANKING

Lívia Krejčířová, Jiří Dvořák

Abstract: *The attractiveness of Internet banking, the dynamics and the integration with e-business is still growing. The current use of electronic banking is defined by cyberspace and abused in the form of cyber terrorism as well. Therefore it is in the interest of all banks to focus on minimizing the real attacks. This article analyzes and compares the current possibilities against so-called phishing and identifies the area of the safe use of Internet banking in terms of the current potential threats in this area.*

Keywords: *Phishing, Internet banking, Spam, Internet banking protection.*

JEL Classification: *G200.*

Introduction

Banks are recording an increase in the use of e-banking. There are banks that operate only online. However, protection against the abuse of sensitive data transmitted through e-banking is more difficult. Every day we can hear information about stolen company's databases or data abuse by means of spam mail. In February 2012 the latest phishing attack against the Czech savings bank was detected. [17] In December 2011 Raiffeisenbank had to block around 3,000 credit cards due to leakage of sensitive data. [19] Raiffeisenbank reported the latest phishing attack in January 2011. Major attacks were also recorded by Citibank, Facebook and various types of e-mail sites.

Literature review

What phishing is and what types of phishing and types of attacks we distinguish was dealt with by Anthony Elledge. [2]

How to recognize phishing e-mails, links or phone calls is also addressed by Microsoft on its official website. [20]

The security of web browsers is addressed by Aditya Sood and Richard Enbody. This study reflects the current state of security in online banking with respect to declarative security. [21]

Andrew Garcia evaluates in his article the web browsers on the basis of different security software. He provides information on the credibility of websites to end users and whether the web pages are connected to any Internet fraud or phishing. [11]

Stuart J. Johnston examines the security vulnerabilities of the web browsers Mozilla Firefox and Safari. [13] Roger A. Grimes adds Microsoft Internet Explorer 8, Opera 9.63, Safari 3.2.1 Apple, Mozilla Firefox 3.12 and Google Chrome 1.0. [12]

Web pages dedicated to e-crime and also phishing include APWG [5] (www.ecrimeresearch.org) and www.antiphishing.org .

1 The current state of the presence of phishing

By spam unsolicited bulk messages of virtually the same content are meant. It is the abuse of electronic communication, especially e-mail. It is mostly used as advertising, although through the brief history of electronic communication spam has been used for other reasons too. There are many different media, which are abused by spammers. They include among others the already mentioned e-mail, instant messaging (e. g. ICQ), Usenet and text messages. One type of spam is phishing. [22]

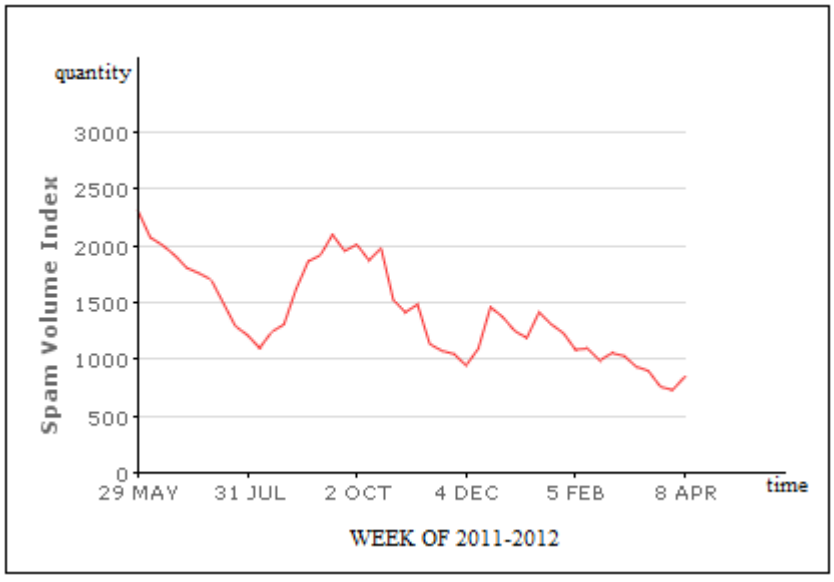
Phishing is such a spam that indicating fraudulent e-mail attacks on the Internet user with the aim to divulge personal information. [7].

Phishing (from fishing, literally to fish for passwords) is an activity in which the scammer tries to lure various passwords from users , e. g. a bank account password. Mostly it takes form of a web site that is created in such a way that it looks like an exact copy of an existing trusted site. The scammer may also offer some benefits if the user logs in through their website. The name and the password entered into the phishing site are sent to the fraudster who can abuse them. Phishing can be also in the form of e-mails that notify the user about account change or update and thus luring passwords. [16]

It might seem that phishing is a financial spam, but it is not the case. The main goal of phishing is to lure any sensitive data from users and their subsequent abuse, while financial spam is primarily about advertisement e-mails.

Figure 1 shows the development of spam volume index (SVI). It is an index which tracks relative changes in the volume of spam sent by representative sample of honeypot domains monitored by M86 Security Labs. It focuses on the occurrence of different types of spam in e-mails around the world. The amount of e-mails which are analyzed is in tens of thousands. As we can see from the chart, this index is decreasing. At the beginning of August 2011 and December 2011 there was a large SVI decrease, but afterwards it followed by a sharp increase in September and late December 2011. Currently, SVI has a decreasing tendency. [23]

Fig. 1: Spam volume index



Source: [23]

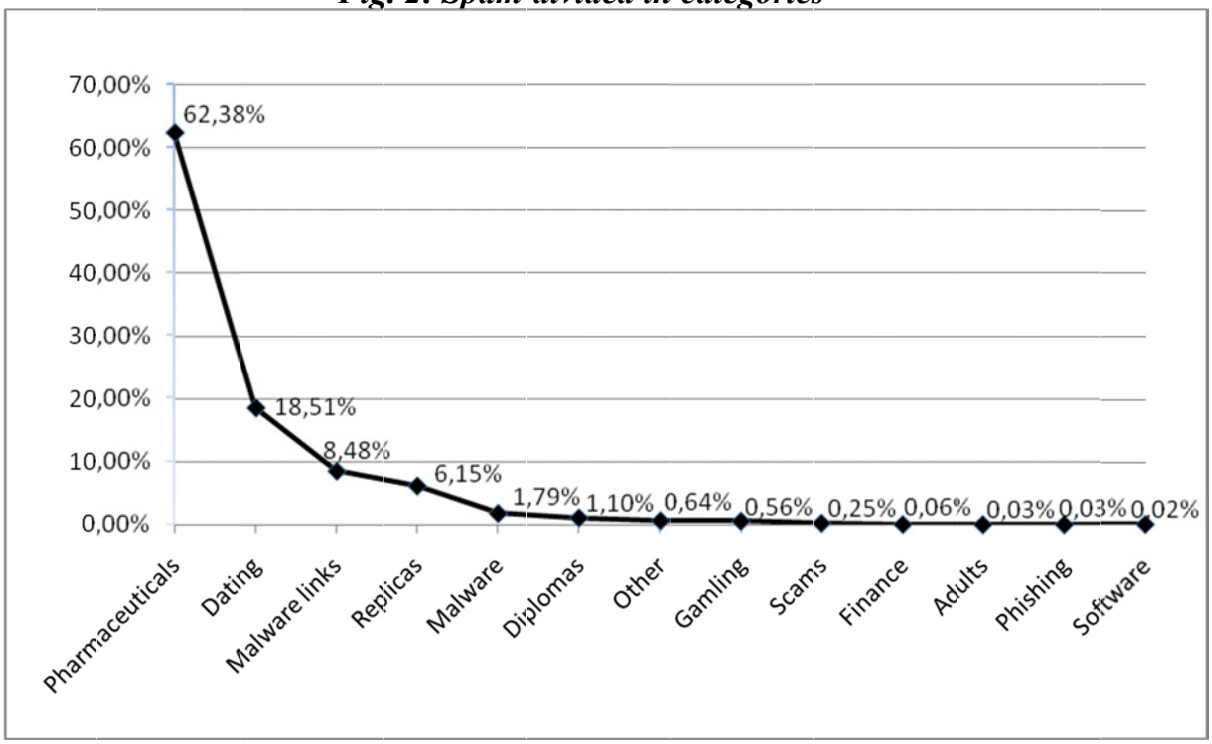
Figure 2 depicts the percentage of spam based on categories listed in Table 1. These values are updated to 16/04/2012. In the long term spam with texts related to pharmaceuticals is at the top. This type of spam includes a variety of promotional e-mails about all kinds of drugs, pills and herbal medicines. The spam often promises better skin, weight loss, sexual enhancement, etc. examples include Viagra and means for weight loss. On the other hand the lowest rank belongs to financial spam which takes form of e-mails offering for instance mortgages and loans refinancing. [23]

Tab. 1: Spam divided in categories

Category	Percentage
Pharmaceuticals	62,38%
Dating	18,51%
Malware links	8,48%
Replicas	6,15%
Malware	1,79%
Diplomas	1,10%
Other	0,64%
Gambling	0,56%
Scams	0,25%
Finance	0,06%
Adults	0,03%
Phishing	0,03%
Software	0,02%

Source: [23]

Fig. 2: Spam divided in categories

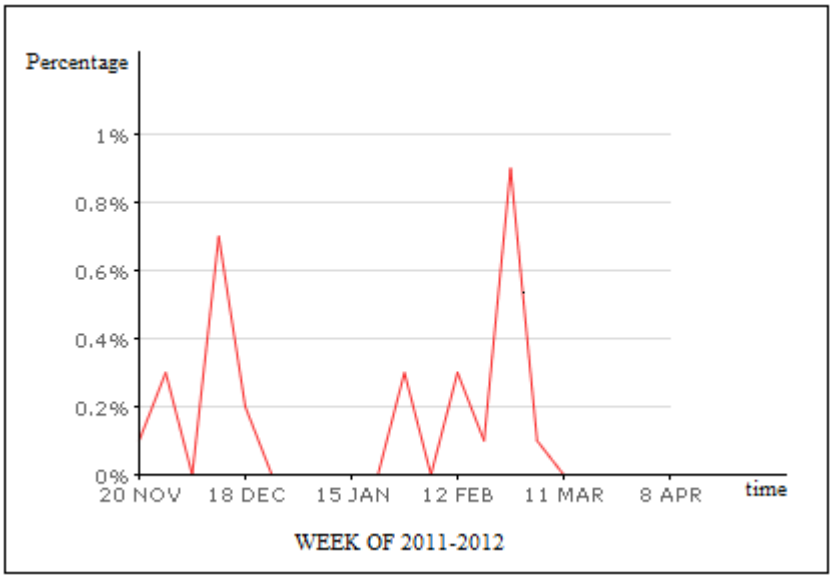


Source: [23]

Figure 3 shows the development of phishing e-mail as a percentage of all unsolicited e-mails over time. By 16/4/2012 phishing achieved the maximum value for the last six months.

There is an interesting development in December during Christmas when phishing was approximately 0.7% of total spam. After Christmas there was a sharp decline. [23]

Fig. 3: Percentage of phishing e-mail over time



Source: [23]

At present we are recording a worldwide decreasing trend of spam presence. But hackers' attacks are becoming more sophisticated and the data security and protection should not be underestimated.

2 The effectiveness of basic level protection against phishing

2.1 Antivirus program

The first and absolutely the most crucial protection, which is inevitable when using the Internet today, is a good antivirus program. It is the first step to protect our PC and also our information.

Statistical summary in Table 2 shows how many times a particular antivirus program was tested, how many times it failed and, how many times it successfully detected all present viruses. The right-hand column presents thesuccess percentage of the tested program. This test was carried out within the project Antivirus Center by the company Amenit s. r. o. and the results were published on 08/11/2011. [24].

Tab. 2: Comparison of antivirus programs

Antivirus program	Number of tests	Failed	Successful	Win percentage
Microsoft ForeFront	14	0	14	100,00%
ESET (NOD32)	71	3	68	95,80%
Symantec Norton	63	7	56	88,90%
Avira	37	5	32	86,50%
Sophos	74	16	58	78,40%
TrustPort	19	4	15	78,90%
Microsoft Security	4	1	3	75,00%
Kaspersky	84	20	64	76,20%
BitDefender	37	10	27	73,00%
F-Secure Anti-Virus	45	12	33	73,30%
CA eTrust	73	24	49	67,10%
Norman	70	22	48	68,60%
McAfee	72	24	48	66,70%
Avast!	64	23	41	64,10%
AVG	60	22	38	63,30%

Source: [24]

2.2 Antispyware program

Antispyware is a program that can detect and remove spyware (spy software). Spyware a type of software which collects users' personal information without first telling them what it does, and it does not allow users to decide whether they wish it or not. The main reason why users should be concerned about spyware is their privacy. These programs record every move they make on the Internet. It can be lists of web sites that were visited or sensitive information such as usernames and passwords.

Antispyware combats spyware that can:

- Download and install additional malware without the user's knowledge (e.g. backdoors, Trojan horses, viruses and " password robbers"),
- change the browser's behavior (e.g. cause it to run slower, refer to sites other than requested change the starting page upon opening the Internet browser, change items in one's Favorites, annoy with advertising, etc.),
- initiate modem connections via expensive phone lines ("yellow lines"). This activity is carried out by a special program which is generally called dialer. [3]

Testing the anti-spyware products showed that the best product recognized 100% active spyware but removed only 70% of it. The only solution is the combination of multiple anti-spyware tools. Only in this way the user has some certainty that their computer will be adequately secured. It is better for the user to invest in prevention and make use of various security packages.[4]

2.3 Web browser

The secondary protection consists in using the latest versions of Internet browsers. On 14.07.2011 site http://extrawindows.cnews.cz published an article by Petr Fiala on

password security. One part of this article comprises the evaluation of web browsers and password administration systems.

Password administrators of the browsers were evaluated on the following criteria:

- **Versatility of use**: if is the solution applicated only for web pages or also for other applications. Application can be divided into applications with graphical user interface (such as FTP clients, remote desktop login and Subversion depository) and console applications in which the credentials cannot be transferred by copying (e. g. Oracle SQLPlus or the network management server via Putty),
- **Compatibility with operating systems or web browsers** (in the case of applications installed as accessories),
- **Security**: protection against keyloggers, protection against clipboard logging, code strength that protects stored passwords,
- **Sharing of passwords among multiple users**: the possibility for more users to work with one set of passwords,
- **The educational effect**: if the application teaches its users how to choose a strong password, and encourages them to change it regularly,
- **Portability** between computers, the use on portable devices,
- **Ease of use and speed**: how many mouse clicks or keyboard shortcuts it takes to log in; the complexity of inserting the password into the database and if the settings are clear [9].

Evaluation included the four most commonly used web browsers: MS Internet Explorer 8, Mozilla Firefox 3.6, Opera 11 and Chrome 9. The evaluation results are shown in the Table 3. [10]

Tab. 3: Web browsers evaluation results

	MS Internet Explorer 8	**Mozilla Firefox 3.6**	**Opera 11**	**Google Chrome 9**
Application universality	only web (credentials are stored only when entered into web page forms and dialog boxes of the HTTP and FTP authentication)			
Operating System Compatibility	only Windows Vista/7	Windows, Linux, Mac operating system		
Security of stored passwords	linked to/interconnected with the user account	Master Password	Master Password	linked to/interconnected with the user account
Portability passwords	no	yes (official Add-ons), synchronized with other Firefox installations	no	no
Attempt to decipher	program is free, password displayed immediately	program is free, deciphering time depends on the strength of the Master Password	program is paid, deciphering time depends on the strength of the Master Password	program is free, password displayed immediately
Keylogger test	When automatically supplied, nothing is overheard	Master Password can be overheard, automatically supplied passwords not	Master Password can be overheard, automatically supplied passwords not	When automatically supplied , nothing is overheard
Clipboard monitor test	password is masked and cannot be copied	password is masked and cannot be copied	the data being supplied are displayed for a short moment at the time of logging-in (cannot be copied)	password is masked and cannot be copied
User friendliness, speed	3/5	5/5	4/5	5/5

Source: [10]

3 Security features of Internet banking

In the Czech Republic, there is no such an Internet banking product that would be completely secure. Banking institutions give their client the choice what risk he or she is willing to accept, and the methods to choose from. There is not too much concern on the clients' part about technical equipment ensuring the above standard safety, probably due to charges. There are several levels of protection.

Username (number) + password

This method is the easiest but the least safe, and neither a long enough password is of help. If a malicious code able to monitor keystrokes (keylogger) attacks the computer, it can easily acquire both entries and send them to a fraudster. If it is not necessary to authorize the subsequent payment, this poses a major risk. Some banks increase security by offering the user to enter the password by the means of a graphical keyboard that is controlled by the mouse. However, Trojan horse can track it too.

SMS key authentication

For confirmation of each single transaction the bank sends a unique code in the form of a text message to an in advance registered mobile phone number. The advantage is that if there is a hacker attack, without a client mobile phone, he cannot make any transaction. The SMS authorization code is entered by the user only at the first active operation within a single login. There is some risk that the SMS code can be intercepted.

Electronic signature

In order to log in and sign their transactions the client needs an electronic signature – a personal client certificate stored in a file or on a smart card. This method places higher requirements on the safe storage and the use of the certificate. The basic rule is not to save the certificate to a disk. It should always be recorded on an external media (floppy, CD, USB drive). Enhanced security is provided by client certificate being stored on a smart card. In this case it is necessary to have a smart card reader.

Electronic calculator

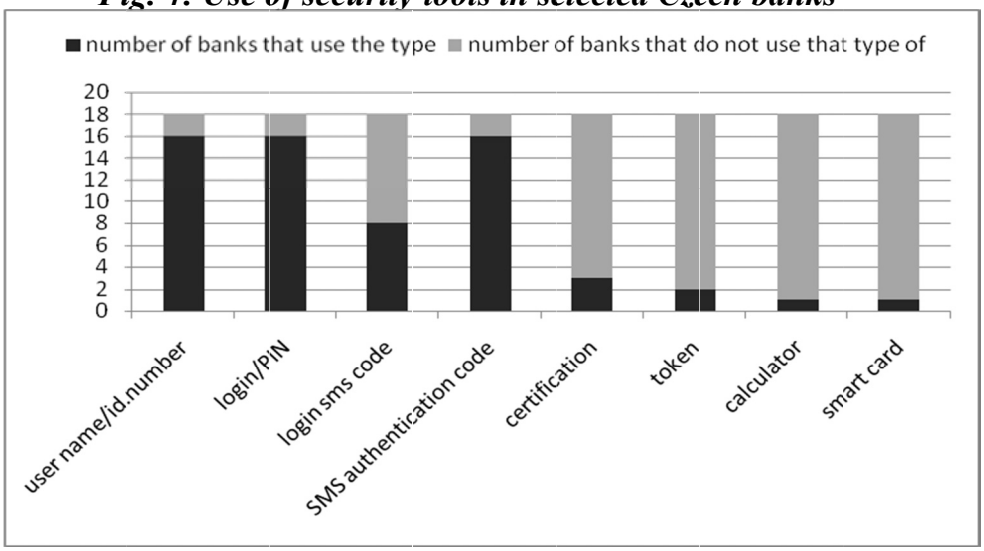
Electronic calculators belong to safe systems that always generate different access code to confirm the transaction. Clients do not have to install anything on the computer but they have to buy an equipment, e.g. in the form of a small calculator. The calculator is portable and is protected by a four-digit password. After entering the password and pressing the relevant button, a six-digit code is generated. The client uses the generated code to access the Internet banking. For each active transaction a new number must be generated. [15]

It is important not to provide these security data to anyone. In this way possible abuse of the sensitive data can be avoided. These data should not be saved in places to where untrustworthy persons have access. Also, all sensitive data should not be stored in one place together.

Comparison of Internet banking security in the Czech Republic

Figure 4 shows the results of the comparison of Internet banking security in selected Czech banks. I conducted the survey by telephone. In total I contacted 18 Czech banks in the week of 2 - 12 June 2012). As shown in table 4, the most common security feature that banks provide is a combination of user name and identification number, password / PIN and SMS authentication code.

Fig. 4: Use of security tools in selected Czech banks



Source: Author

Tab. 4: Comparison of internet banking security in selected Czech banks

Name of bank	User name/id. number	Login /PIN	Login SMS code	SMS authentication code	Certification	Token	Calcu-lator	Smart card
Air Bank	yes	yes	no	yes	no	no	no	no
AXA Bank Europe	yes	yes	no	yes	no	no	no	no
Citibank	yes	yes	no	yes	no	no	no	no
Česká spořitelna	yes	yes	yes	yes	no	no	no	no
Československá obchodní banka	yes	yes	yes	yes	no	no	no	no
Equa bank	yes	yes	yes	yes	no	no	no	no
Fio banka	yes	yes	no	yes	yes	no	no	no
GE Money Bank	yes	yes	yes	yes	no	no	no	no
ING Bank N. V.	yes	yes	no	no	no	no	no	no
Komerční banka	no	yes	no	yes	yes	no	no	yes
LBBW Bank CZ	no	yes	yes	yes	no	no	yes	no
mBank	yes	yes	no	yes	no	no	no	no
Oberbank AG	yes	yes	no	yes	no	no	no	no
Poštovní spořitelna	yes	yes	yes	yes	no	no	no	no
Raiffeisenbank	yes	no	yes	yes	no	no	no	no
UniCredit Bank	yes	no	yes	yes	no	yes	no	no
Volksbank CZ	yes	yes	no	no	yes	yes	no	no
Zuno	yes	yes	no	yes	no	no	no	no

Source: Author

Biometric identifiers

Less common tools to protect electronic banking are biometric identifiers.

Biometric identifiers are commonly used as a part of multifactorial verification system in combination with a password (something one knows) or token (something one has). [6]

Types of biometric methods and identifiers:

- Fingerprint recognition,
- face recognition,
- voice recognition,
- keys recognition,
- handwriting recognition,
- finger and hand geometry,
- DNA recognition,
- retina scan,
- and iris scan. [6]

The most commonly used biometric techniques are handwriting recognition, fingerprint recognition and face recognition [18].

Biometric identifiers can be divided into two groups:

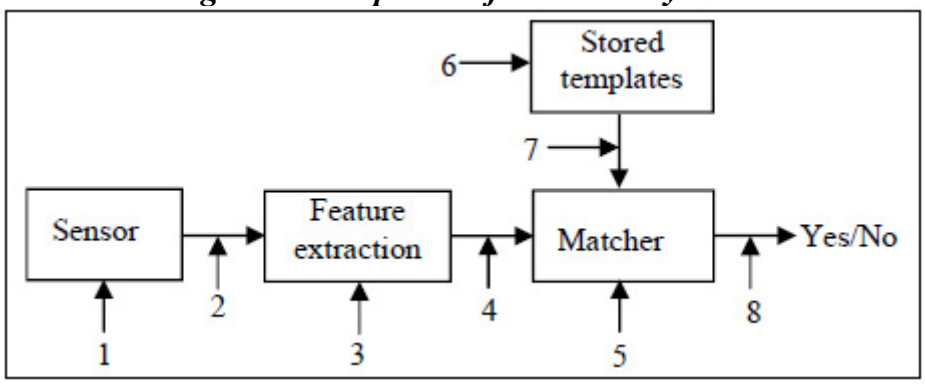
- Psychological (fingerprints recognition, face recognition, finger and hand geometry, retina scan, iris scan, DNA recognition),
- behavioral (voice recognition, keys recognition, handwriting recognition). [8]

Figure 5 presents a biometric system and possible attack points. A short description of these attacks follows. The individual attacks are numbered from 1 to 8 (see Fig. 5):

1. Presenting a fake biometric sample to the sensor: A fake biometric sample such as a fake finger, image of a signature, or a face mask is presented to the sensor in order to get into the system.
2. Replay of stored digital biometric signals: A stored signal is replayed into the system ignoring the sensor. For instance, replay of an old copy of a fingerprint image or a recorded audio signal.
3. Denial of feature extraction: A feature set is formed by the imposter using a Trojan horse attack.
4. Spoofing the biometric feature: Features extracted from input signal are replaced by a fake set of features.
5. Attacking matching module: Attacks on matching module result in replacement of matching scores by fake ones.
6. Spoofing templates in database: Database of saved templates can be local or distant. The attacker tries to fake one or more biometric templates in the database. As a result, either a fake identity is authorized or a rightful user faces a denial of service.

7. Attacking the channel between the template database and matching module: Stored templates are transmitted through a communication channel to the matching module. Data in the channel can be changed by attacker.
8. Attacking the final decision process: If the final decision can be inserted or blocked by the hacker then the authentication system function will be overridden. [1]

Fig. 5: Attack points of biometric system



Source [1]

Structure, architecture, production or implementation of a system may introduce a vulnerability to the biometric system. In some cases a secondary system may be integrated to the biometric system which possibly makes the biometric system vulnerable. There are five points of vulnerabilities:

- Operating systems,
- database management systems (and application software),
- biometric application software,
- software for sensor,
- hardware and drivers. [1]

Table 5 shows the comparison of the characteristics of the biometric identifiers and the potential problems associated with them, where "Low" represents the lowest and "Very high" the highest level. [25]

Tab. 5: Comparison of biometric identifiers

Characteristic	Finger-print	Hand geometry	Retina	Iris	Face	Signature	Voice
Ease of use	High	High	Low	Medium	Medium	High	High
Reasons for errors	Dryness, dirt, age	Hand injury, age	Glasses	Poor lighting	Lighting, age, glasses, hair	Changing signatures	Noise, cold weather
Accuracy	High	High	Very High	Very high	High	High	High
User acceptance	Medium	Medium	Medium	Medium	Medium	Medium	High
Required security level	High	Medium	High	Very high	Medium	Medium	Medium
Long term stability	High	Medium	High	High	Medium	Medium	Medium

Source: [25]

Conclusion

Banks place increasingly greater emphasis on secure Internet banking. They recommend a variety of procedures to minimize attacks on personal data of customers. However, their offer of security tools is limited and the client cannot choose the way that suits him or her best.

The least we can do to protect our data is:

- Not to provide the security data to anyone,
- not to save the data in places where untrustworthy persons have access,
- not to store all sensitive data in one place,
- to update the computer's antivirus program regularly,
- and to update the web browser.

In order to prevent abuse of data by fraudulent e-mail, it is advisable:

- Not to respond to e-mails in which confirmation of our account information is requested,
- not to use personal information in e-mails. Providing information via website is only advisable on condition that the web browser has a security lock,
- to always examine the places where security data are used,
- in case of suspicion of possible abuse, to contact the authorities immediately.

New methods and procedures are still being developed. Today biometrics can already be encountered when applying for national and travel documents such as identity cards and passports. The bank industry has also begun to use it. Electronic signatures are in use but not always for client identification. The future trends in biometrics for banking are varied. Banking abroad has recently built in face or fingerprint recognition tools into their ATMs so as to combat skimming. Since a biometric feature is not a sufficient protection, other

security tools complement it, e.g. a card or PIN. ATM is such a specific device that in the future it may also make use of other biometric tools. These methods could also be employed as a solution to phishing. For instance, when users log in to their e-mail account or to other secure web pages (e.g. Internet banking), user identification may be requested by means of biometric tools. To enable that users may need to have a special hardware and software installed on their computer or they may need external devices connected to it.

So far we have not been able to assess the possibility of banks using biometric identifiers. At present it is associated with high costs for both the service provider and the customer.

References

[1] ABDULLAYEVA, Fargana, Yadigar IMAMVERDIYEV, Vugar MUSAYEV a James WAYMAN. ANALYSIS OF SECURITY VULNERABILITIES IN BIOMETRIC SYSTEMS. In: *Danish Biometrics* [online]. september 2008 [cit. 2012-07-20]. Dostupné z WWW: <http://danishbiometrics.files.wordpress.com/2009/08/1-13.pdf>

[2] ALLEDGE, Anthony. Phishing: An Analysis of a Growing Problem. In: *SANS*: *SANS Institute InfoSec Reading Room* [online]. May 2004, January 2007 [cit. 2012-04-16]. Dostupné z WWW: <http://www.sans.org/reading_room/whitepapers/threats/phishing-analysis-growing-problem_1417>

[3] AntiSpyware. In: *ANTIVIROVÉ CENTRUM* [online]. 2012 [cit. 2012-04-22]. Dostupné z WWW: <http://www.antivirovecentrum.cz/antispyware.aspx>

[4] Antispyware v testu tvrdosti. In: *CHIPonline.cz* [online]. 2006 [cit. 2012-04-22]. Dostupné z WWW: <http://earchiv.chip.cz/cs/earchiv/rubriky/temata/antispyware-v-testu-tvrdosti.html>

[5] *APWG*: *eCrime Researchers* [online]. 2006 [cit. 2012-03-15]. Dostupné z WWW: <http://www.ecrimeresearch.org/>

[6] Authentication in an Internet Banking Environment. *Federal Financial Institutions Examination Council* [online]. 2010 [cit. 2012-04-05]. Dostupné z WWW: <http://www.ffiec.gov/pdf/authentication_guidance.pdf>

[7] Co je to phishing. In: *Hoax* [online]. 2010 [cit. 2012-02-15]. Dostupné z WWW: <http://www.hoax.cz/phishing/co-je-to-phishing>

[8] FATIMA, Amtul. E-Banking Security Issues – Is There A Solution in Biometrics?. *Journal of Internet Banking and Commerce* [online]. 2011, vol. 16, no. 2 [cit. 2012-04-03]. ISSN 12045357. Dostupné z WWW: <http://web.ebscohost.com/ehost/detail?vid=14&hid=12&sid=69402eb9-8df2-4315-910f1aa2471046b4%40sessionmgr12&bdata=Jmxhbmc9Y3Mmc2l0ZT1laG9zdC1saXZl#db=bth&AN=67359751>

[9] FIALA, Lukáš. Jak zabezpečit svá hesla, díl 1/3. In: *EXTRA Windows.cz* [online]. 2011, 14. 7. 2011 [cit. 2012-02-10]. Dostupné z WWW: <http://extrawindows.cnews.cz/jak-zabezpecit-sva-hesla-dil-13>

[10] FIALA, Lukáš. Jak zabezpečit svá hesla, díl 2/3: webové prohlížeče. In: *EXTRA Windows.cz* [online]. 2011, 24. 7. 2011 [cit. 2012-02-10]. Dostupné z WWW: <http://extrawindows.cnews.cz/jak-zabezpecit-sva-hesla-dil-23>

[11] GARCIA, Andrew. In search of the best Web security solutions. *EWeek* [online]. 2008, Vol. 25, Issue 23, 8/4/2008 [cit. 2012-04-06]. ISSN 15306283. Dostupné z WWW: <http://web.ebscohost.com/ehost/detail?vid=10&hid=126&sid=41809330-1a52-423d-b478-3696ef70bf2d%40sessionmgr104&bdata=Jmxhbmc9Y3Mmc2l0ZT1laG9zdC1saXZl#db=a9h&AN=34165686>

[12] GRIMES, Roger A. Malý průvodce zabezpečením prohlížečů. In: *SecurityWorld* [online]. 2009, 26.10.2009 [cit. 2012-04-06]. Dostupné z WWW: <http://securityworld.cz/securityworld/maly-pruvodce-zabezpecenim-prohlizecu-2002>

[13] JOHNSTON, Stuart J. Hackers Focus Efforts on Firefox, Safari. *PC World* [online]. 2008, Vol. 26, Issue 6, Jun2008 [cit. 2012-04-06]. ISSN 07378939. Dostupné z WWW: <http://web.ebscohost.com/ehost/detail?vid=10&hid=126&sid=41809330-1a52-423d-b478-3696ef70bf2d%40sessionmgr104&bdata=Jmxhbmc9Y3Mmc2l0ZT1laG9zdC1saXZl#db=a9h&AN=32013652>

[14] MANIVANNAN a PADMA. Comparative and Analysis of Biometric Systems. *International Journal on Computer Science & Engineering* [online]. 2011, vl. 3, Issue 5 [cit. 2012-04-05]. ISSN 09753397. Dostupné z WWW: <http://web.ebscohost.com/ehost/pdfviewer/pdfviewer?sid=31564bdb-940d-4ea8-9467-9fcaa2e777a9%40sessionmgr111&vid=5&hid=126>

[15] NYKODÝMOVÁ, Helena. Jak je to s bezpečností internetového bankovnictví?. In: *LUPA.cz* [online]. 2006, 19. 9. 2006 [cit. 2012-02-10]. Dostupné z WWW: <http://www.lupa.cz/clanky/jak-je-to-s-bezpecnosti-internetoveho-bankovnictvi/>

[16] Phishing. In: *Wikipedia*: *the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001-, 18.3.2012 [cit. 2012-04-16]. Dostupné z WWW: <http://sk.wikipedia.org/wiki/Phishing>

[17] Phishing - tiskové zprávy a aktuality. In: *Česká spořitelna* [online]. 2012, 21.2.2012 [cit. 2012-04-16]. Dostupné z WWW: <http://www.csas.cz/banka/content/inet/internet/cs/news_ie_1496.xml?archivePage=phishing&navid=nav00156_phishing_aktuality>

[18] Putting an End to Account-Hijacking Identity Theft: The Use of Technology to Mitigate Account-Hijacking Identity Theft. In: *FDIC* [online]. 2004, 2004-10-12 [cit. 2012-02-15]. Dostupné z WWW: <https://cdr.ffiec.gov/Public/HelpFileContainers/WelcomeAdditionalInfo.aspx>

[19] Raiffeisenbank zablokovala klientům kreditní karty. In: *ČT24* [online]. 3.12.2011 [cit. 2012-04-16]. Dostupné z WWW: <http://www.ceskatelevize.cz/ct24/ekonomika/155616-raiffeisenbank-zablokovala-klientum-kreditni-karty/>

[20] Safety & Security Center: Computer Security, Digital Privacy, and Online Safety. MICROSOFT. *Microsoft* [online]. 2012 [cit. 2012-04-16]. Dostupné z WWW: <http://www.microsoft.com/security/online-privacy/phishing-symptoms.aspx>

[21] SOOD, Aditya a Richard ENBODY. The state of HTTP declarative security in online banking websites. *Computer Fraud & Security* [online]. 2011, Vol. 2011, Issue 7, 26.7.2011 [cit. 2012-04-06]. ISSN 13613723. DOI: 10.1016/S1361-3723(11)70073-2. Dostupné z WWW: <http://web.ebscohost.com/ehost/detail?vid=9&hid=126&sid=41809330-1a52-423d-b478-3696ef70bf2d%40sessionmgr104&bdata=Jmxhbmc9Y3Mmc2l0ZT1laG9zdC1saXZl#db=a9h&AN=63569087>

[22] Spam. In: *Wikipedia*: *the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001, 11.4.2012 [cit. 2012-04-16]. Dostupné z WWW: <http://sk.wikipedia.org/wiki/Spam#E-mailov.C3.BD_spam>

[23] Spam Statistics. In: *M86 security labs* [online]. 2012, 3.11.2012 [cit. 2012-04-16]. Dostupné z WWW: <http://www.m86security.com/labs/spam_statistics.asp>

[24] Srovnání antivirových programů, srovnání antivirů. In: *Antivirové centrum* [online]. 2012, 8.3.2012 [cit. 2012-03-01]. Dostupné z WWW: <http://www.antivirovecentrum.cz/aktuality/srovnani-antiviru.aspx>

[25] WHELAN, Steve. Biometrics Technology. In: *Rural Finance Learning Center*: *Technology and outreach Details* [online]. 2003 [cit. 2012-04-05]. Dostupné z WWW: <http://www.ruralfinance.org/fileadmin/templates/rflc/documents/1126265263594_Biometrics_technology.pdf>

Contact

Ing. Mgr. Lívia Krejčířová
Brno University of Technology
Faculty of Business and Management, Department of Informatics
Kolejní 2906/4, 612 00 Brno
E-mail: krejcirova@fbm.vutbr.cz

prof. Ing. Jiří Dvořák, DrSc.
University of Pardubice
Faculty of Economics and Administration, Institute of System Engineering and Informatics
Studentská 95, Pardubice, 532 10, Czech Republic
E-mail: Jiri.Dvorak@upce.cz

Received: 29. 04. 2012
Reviewed: 16. 06. 2012
Approved for publication: 14. 03. 2013