# A Survey on Security Solutions of Top e-Banking Providers from an European Market


## Abstract

In this work we analyse the security of e-banking services from top e-banking providers on the Romanian market. This location is relevant from at least two reasons: it's a dynamic and diverse market situated at the crossroads between central and eastern Europe and half of the providers come from foreign markets (CitiBank, ING, Raiffeisen, etc.) or are acquired by Western European providers (Societe Generale, Erste Bank, Unicredit). Therefore, most of the solutions employed here are not at all different from their foreign counterparts, we do in fact observe to be no correlation between the security level and the origin of the provider. We show the security mechanisms to be technically sparse: from simple password based authentication to stronger authentication based on one-time password calculators or digital certificates installed in browsers. We do conclude that many of them are insecure against phishing attacks and in fact none of them is completely secure against stronger attacks such as Man-in-the-browser (MitB) attacks. Finally, we conduct a study on user awareness on security threats and preferences for e-banking authentication. This shows a significant percentage of users to be still unaware of attacks but fortunately the vast majority of users prefer security rather than usability in e-banking products.



## Keywords

e-banking, security, social engineering, user perception, usability


## Introduction and motivation

E-banking solutions have expanded in the last decade mostly because they don't require the client to be present at the bank in order to commit a transaction. Thus, the client gains time and potentially spears some money. A survey done by ABA (http://www.aba.com/) in September 2010 shows that 36% of consumers prefer Internet Banking instead of other solutions. Malhotra and Singh (2007) analyze the factors that determine e-banking adoption and emphasize that these services are also a valuable mean for increasing the bank's market share. With the development of on-line banking, fraud related to e-banking transfers started to increase as well, bringing risks associated to the user benefits. Most of this fraud is caused by social engineering attacks, such as phishing or pharming (Zhang et al., 2007).

To increase security, several e-banking providers started to use hand-held devices, such as one-time password computers, in order to authenticate their users. But this is not enough when more complex attacks take place, such as a mixed attack in which the bank server is disabled by a DDoS attack and a phishing attack is mounted on the clients. Practice shows that treating attacks individually does not always cover the vulnerabilities of the systems. Thus, even if a Denial of Services (DoS) attack on the website may appear harmless with respect to client's information, this is not the case when the attack is followed by a phishing email sent to all users. This is because, although the users are educated, such messages become more plausible in the absence of the genuine bank server.

Phishing can be defined as a form of acquiring sensitive information (like user-names, passwords or credit card details) by impersonating an entity that is trusted by the user. From a financial point of view, phishing is an ever increasing phenomenon, even if it is not relatively new (the term was introduced by Garfinkel (1995) 17 years ago), affecting more and more people around the world. According to McCall (2007) 3.6 million of persons in the US suffered from a phishing attack, $ 3.2 billion being lost to these attacks in the U.S and 35.4 million in the U.K (FFA, 2012). Even if phishing targets different industry sectors, the most affected one is the financial sector (42.4% of the phishing attacks target the financial industry (APWG, 2012)). Such attacks are usually deployed by means of e-mail or instant messaging, where the message sent by the adversary contains a link to a fake web site that tries to reproduce the look and feel of the original site. Phishing is a form of social engineering that exploits vulnerabilities present in current web security technologies. Because phishing attacks can be identified by the educated user, another form of social engineering has evolved: pharming. In this case the

adversary redirects the traffic for the original web site to a scam website. This can be achieved by changing the victim's host files or by exploiting the DNS server used by the victim.

To go even further, the most recent attacks involved infected browsers, also known as Man-in-the Browser Attacks (MitB), a kind of attack on which even Public-Key Infrastructure (PKI) based mechanism, such SSL/TLS or related protocols are completely ineffective. But the main cause of this attack is that authentication in e-banking services is only one-way, only the client authenticates to the site and not vice-versa. In the best case, website authentication is left alone to a digital certificate that is signed by a trusted third party. But as practice shows, it is possible sometimes for an adversary to use a valid certificate or, even more common, for the client to accept a certificate that is untrusted. In this context, at least a minimal effort should be done by e-banking providers to give clients stronger hand-held devices that can authenticate the e-banking website and user input as well. But the main cause of such attack is that authentication in e-banking services is one-way, only the client authenticates to the site and not vice-versa. In the best case, website authentication is left alone to a digital certificate that is signed by a trusted third party. But as practice shows, it is possible sometimes for an adversary to use a valid certificate or, even more common, for the client to accept a certificate that is untrusted. In this context, at least a minimal effort should be done by e-banking providers to give clients stronger hand-held devices that can authenticate the e-banking website and user input as well.

Nevertheless, these attacks are relevant from various reasons. On the adversary side they are easy to lunch even at a large scale (in contrast to common physical card theft which are usually isolated events) and increasingly easy to reproduce (since more and more software tools are available on Internet). On the user or legal authorities' side they are hard to trace back (since adversaries act through remote botnets) and hard to be identified by the users, (a card theft is easy to note, but it is harder for user to figure out that his browser based transaction was stolen). These viewpoints are commonly acknowledged, for example by Weigold and Hiltgen (2011), while the later view point was recently advocated by Pavía et al. (2012).

| | Name | Share | Headquarter and miscellaneous info | Founded |
|---|---|---|---|---|
| 1 | BCR | 20.12% | Bucharest, Romania (majority (61%) aquired by Erste Bank in 2006 Vienna, Austria) | 1990 |
| 2 | BRD | 13.57% | Bucharest, Romania (majority (59%) held by Societe Generale Paris, France) | 1923 |
| 3 | Transilvania Bank | 7.27% | Cluj-Napoca, Romania | 1993 |
| 4 | CEC Bank | 6.99% | Bucharest, Romania (Romanian national bank) | 1865 |
| 5 | Raiffeisen Bank | 6.69% | Vienna, Austria | 1927 |
| 6 | UniCredit Tiriac Bank | 6.31% | Bucharest, Romania (part of Unicredit (Rome, Italy), fusioned with HVB bank Munich, Germany) | 1991 |
| 7 | Alpha Bank | 4.67% | Athens, Greece | 1879 |
| 8 | ING | 4.04% | Amsterdam, Netherlands | 1991 |
| 9 | Bancpost Romania | 3.47% | Bucharest, Romania | 1991 |
| 10 | CitiBank | 1.62% | New York, USA | 1812 |
| 11 | Millennium Bank | 0.59% | Athens, Greece | 2000 |
| 12 | ProCredit Bank | 0.32% | Frankfurt, Germany | 1998 |

Table I: Studied Banks: headquarters, history and market-share (as reported on 18.02.2012 by Hostiuc (2012))

In what follows we make an analysis of existing solutions on the Romanian market to find their vulnerabilities. To emphasize on the relevance of our study with respect to foreign markets in Table I we make a brief analysis on the origin of service providers. As it can be easily seen half of the providers come from foreign markets, and more than half of the remaining banks are already acquired by other western European banks. As it results from the analysis that follows, there is no correlation between the security level and the origin of the provider; national e-banking providers do not rely on mechanisms that are necessarily weaker.

The paper is organized as follows. In the second section we make a brief overview of related work on e-banking authentication and we give some details on phishing, pharming, DoS and MitB attacks. In the third section we survey the e-banking solutions provided by: ING, BCR Erste, CitiBank, ProCredit Bank, Raiffaisen, BRD Societe Generalle, Bancpost, Millennium, Transilvania, CEC, Alpha and Unicredit Tiriac Bank. The forth Section holds the conclusions of our paper.

# Existing solutions

We start by investigating solutions related to e-banking authentication. Then we give a brief overview on phishing, pharming, DoS and MitB attack. These attacks are relevant as none of the solutions that we analyse in the forthcoming section is completely resilient to such attacks in the sense that an adversary may compromise at least in part a legitimate session.

## *E-Banking authentication*

In order to assure authentication, solutions are usually divided in two categories (Hiltgen et al., 2006): short-time passwords and certificate based solutions. Short-time passwords are using scratch lists or one time passwords generated by tokens. The use of scratch lists is insecure because often the client stores these lists on his PC making the list vulnerable to anybody that gains access to his PC. To overcome this problem, banks have started to issue tokens that are either time-synchronized with the bank or they use a challenge-response mechanism. Indeed, the large majority of these solutions fall in the context of multi-factor authentication since the user needs a token as well as his card and password in order to obtain the Transaction Authentication Number (TAN). While this is clearly a good engineering option and it significantly increases the security level, it is still not enough to guarantee security. One issue with all these devices is that almost always they rely on security-by-obscurity, which is not a recommended practice. Even if this method is more secure than the previous one, it is still susceptible to active eavesdropping attacks like Man-In-The-Middle (MITM) if the adversary places itself between the client and the bank server. This type of eavesdropping can be avoided if SSL/TLS is used, but the adversary can use social engineering attacks (phishing/pharming) to remove the SSL encryption between the bank and the client. Certificate based solutions require the bank to make use of the PKI to create a second factor of authentication together with user-name/passwords, PIN numbers or security questions. In this case the client receives a certificate that is stored on a smart card or a tamper proof USB stick. But one must avoid a solution that is too difficult for the client to use since, as shown in several research papers, in this case the solution will fail to meet its purpose. Thus making a correct trade-off between the actual security, user's perception on security and the usability of the solution is a difficult task (Gunson et al., 2011; Kim et al., 2010; Murdoch and Anderson, 2010; Weir et al., 2009; Li and Unger, 2012). But the gap between usability and security is still an open issue in e-banking security as clearly noted by Mannan and van Oorschot (2008). More, even well-established solutions such as SSL/TLS are not always correctly used (Herzberg, 2009) and users' perceptions over security are often wrong, especially in the case of novice users (Furnell et al., 2008). Thus relying on users' choice while unavoidable it is not the best option.

An excellent hierarchy of e-banking authentication techniques is presented by Hiltgen et al. (2006). The solutions are divided between the following categories:

- Solutions that are not resistant to malicious software attacks, these solutions are based on: no security (level 0), static passwords (level 1), digital certificates (level 2),
- Solutions that are not resistant to social engineering, these solutions use: one-time passwords (level 3),
- Solutions that are resistant to social engineering, these solutions require: short-time passwords based on timers (level 4), short-time passwords based on challenges (level 5), SSL/TLS authentication with hard token PKI (level 6), and transaction signing on trusted platforms (level 7).

Also, according to Hiltgen et al. (2006), the e-banking solutions that have a security level smaller than 5 are considered to be insecure against off-line credential stealing attacks, only two from the analysed banks have a security level equal to 5. All e-banking applications that have a security level smaller than 6 are considered to be insecure to on-line attacks, none of the analysed banks has a security level greater than 5.

A distinct taxonomy can be built based on the technology behind the authentication tokens. In order to provide a reference architecture for universal strong authentication, the Institute for Open Authentication (OATH - http://www.openauthentication.org/) has proposed open standards for one-time password generators based on counters (HMAC-based One-time Password - HOTP) [28] or on timers (Time-based One-time Password - TOTP) [29]. Unfortunately, the banks in our scrutiny do not specify if their tokens are compliant with these standards and while making

assumptions is possible, it is still without any certainty as long as the cryptographic operations behind the tokens are not known.

Another wide-used standard is the EMV-CAP, here EMV (Europay, MasterCard, Visa) is an authorization mechanism for PoS and ATM transactions while CAP (Chip Authentication Program) is the MasterCard extension for on-line transactions. The only official statement that we could identify is for Raiffeisen Bank which is using a specific VASCO token (http://www.vasco.com) that, according to the producer's site, is built on top of EMV-CAP.

## *Phishing, pharming, DoS and MitB*

The main security objective of e-banking providers is authentication, that's why in most cases e-banking applications don't offer a dedicated anti-phishing solution. But they tend to educate the user (CECBank, 2008) about what information to keep private from any site, for example PIN codes. For phishing alone, there are a few banks that use third party anti-phishing applications like VerificationEngine from Comodo (WindsorFederal, 2011).

Usually software based solutions are employed against phishing, requiring a program or a browser plugin to be installed so that the user is warned when he tries to access a site that is suspicious of being a phishing site. A common taxonomy, also employed by Dunlop et al. (2010), is to divide these solutions in two categories: *list-based* and *heuristic-based*.

The *list-based* solutions use either black-lists (only the sites from the list are blocked) or white-lists (only the sites from the lists are allowed) to block the user from accessing a phishing site. These solutions are very popular among web browsers. Still, this approach relies on the completeness of different sources, like PhishThank (http://www.phishtank.com/), and thus it cannot be always effective because it takes some time for a phishing site to be added on a list. In practice, most of the phishing sites get disabled before they are even added to a list (Moore and Clayton, 2008). Also this type of protection cannot detect targeted attacks.

To improve on this, *heuristic-based* solutions try to find different patterns of phishing in a site. These patterns can be found in the URL of the page, in the HTML or JavaScript code, or in the embedded content. Pan and Ding (2006) propose a solution based on webpage anomalies. These anomalies are found based on an identity of the webpage that it is extracted from its Document Object Model (DOM). A solution based on the information extracted from the HTML code and from the URL of the page is presented by Ludl et al. (2007). A heuristic solution, based only on URL patterns, is proposed by Garera et al. (2007).

Usually, all data used by the heuristics is based on the text that it is contained on the webpage, but most of the phishing sites use images. To overcome this problem Dunlop et al. (2010) propose a similar solution that uses Optical Character Recognition (OCR) to convert the images from the page into text that is further used as heuristic.

Regarding e-banking phishing websites detection, Aburrous et al. (2010) propose a solution based on fuzzy data mining, the solution uses the URL and the domain keys for phishing identification. The solution presented by Latze and Ultes-Nitsche (2007) tries to solve the phishing problem by achieving a stronger authentication through the usage of the TPM (trusted platform module). Even if the adversary obtains personal information from the victim through phishing, it doesn't have the required hardware for a successful authentication.

Most of these solutions are hard to deploy because there is a need of changing the existing infrastructure or they are based on URLs failing, thus, against a pharming attack. To overcome these problems, the Sender Policy Framework (SPF) (Wong, 2004) was proposed, SPF tries to mitigate the phishing problem by using e-mail source authentication, even if it easy to deploy, this standard is not very popular (Görling, 2007).

Regarding *pharming* attacks, Gastellier-Prevost et al. (2011) propose a solution based on a DNS request to a third party DNS server. If the response is not identical to the one offered by the normal DNS, a page analysis is conducted based on the HTML content of the page. This solution is not effective if the adversary can determine the user to connect through a proxy that the adversary controls because in this way the third party DNS request can be redirected to the rogue DNS server.

DoS attacks are commonly reported against various servers, including e-banking servers. A recent report confirms a DDoS attack that forced a Dutch bank to go offline (Bakker, 2011). Because DDoS/DoS attack against bank servers are real threats, these servers must be resilient to DoS attacks. Man-in-the-Browser (MitB) is an advanced form of attacks that are very hard to detect, because the adversary can hijack a genuine user session and the user's machine (Eisen, 2010) making

device identification inefficient against such an attack. MitB attacks are deployed by using trojans. This trojans come in form of browser extension, and a review of existing trojans for Internet Explorer and Firefox is presented by Utakrit (2009).

In order to prevent such attacks user awareness is very important, a model of assuring user awareness is presented by Kritzinger and von Solms (2010). Besides this there are also several tools for MitB attacks mitigation (Gühring, 2006). Also, research has focused on MitB prevention, leading to some interesting solution. Stahlberg (2007) instructs the banks to identify a MitB attack by analyzing users' behavior in the context of e-banking applications. A cost-efficient solution against MitB attacks, called ZTIC, is introduced by Weigold et al. (2008). The solution is based on a USB device with a display; the device is responsible for the authentication and encryption of all the critical information, the PC deals only with IP packets transmission and reception.

# Overview of the security solutions

We now survey the security of the top e-banking providers from the Romanian market. Indeed, the state of affairs that we report here may change over time. We do note however that over a period of more than one year, since our study started, none of the banks changed the methods described here. The only modifications that we could note are the following. One of the banks introduced new authentication tokens (i.e., Transilvania Bank added an authentication token while preserving the previous certificate and phone based technologies) and one of them made a small change to the existing tokens (i.e., initially Raiffeisen Bank provided tokens that worked with a dedicated card, but now these tokens work only with the user's bank card). Clearly, the lack of sudden changes is motivated by: backward compatibility, usability and as users get familiar with a particular system they may lose confidence in the provider if they are forced to switch to another technology too suddenly.

According to BitDefender (2011), of the Romanian Internet users haven't heard of phishing. Possibly, that's why Romania was the second issuer of credit cards that were used to commit Also, 32% of all the electronic fraud in 2010 had originated from Romania (Epayment, 2011), being the number one source country for this kind of fraud.

The authentication mechanism together with the transaction authorization (the process of allowing a bank transfer from the user's account to another account) is summarized in Table II. As general notations we use *U* for the user, *B* for the bank website, *Adv* for the adversary and $Sign_{token}$ for a signature done with the token. We note that $Sign_{token}$ does not refer to a digital signature in the common sense of cryptography, and denotes a tag that is computed with the password calculator. We used the word $Sign_{token}$ as these tags are commonly referred as signatures in the technical documentations of the tokens. Notations from Table II can be summarized as follows:

- user-name or passwords: $user_B/user_U$ which is the user-name as given by the bank or chosen by the user, $password_{token}$ is a 6 digit password obtained from the Vasco digipass (http://www.vasco.com/), protected by a PIN code, while $password_B$ /$password_U$ represents a password given by the bank or chosen by the user;
- personal information: $iban_R^4$ which represents the last 4 digits of the receiver's iban (the bank account number), $amnt_R$ is the amount of money for the receiver, $cnp_U^2$ are two random digits from the user's personal number, $pass1_U^3/pass2_U^3$ are three random characters from the 1st/2nd user defined password;
- process data: $authorize_U$ which represents an user initiated authorization request for a transaction, $nonce_U$ is the nonce created by the bank for the user's authorization request, $Sign_{token}(x)$ is the digital signature on input *x* using the digipass - 8 digits long, *t* represents the time, *cnt* is the counter used by the digipass to generate unique passwords, $authcode_B^{SMS}$ is the user initiated transaction authentication code sent by the bank via SMS, $authcode_B^{PC}$ is the authentication code for the user's transaction sent via PC, $cert_U$ represents the user's client certificate signed by the bank.

## *Mechanisms and Vulnerabilities*

For the security analysis that follows we discuss various attacks: stolen credentials, channel break and content manipulation. These three scenarios are relevant as the first one corresponds to the case in which the user credential are stolen (e.g., by some malware on its computer), the second to the case of a regular phishing site in which the adversary has access to the communication channel (e.g., an insecure certificate) and the third one in which the input of the user can be modified (e.g, a MitB attack). Under these three attacks we analyse whether an adversary can successfully login or even perform an authorization.

1. *BCR Erste Bank:* uses a one-time password calculator based on a time-stamp. An active eavesdropper can monitor the connection between the user and the bank's server during an authentication attempt, from the user and capture the token generated password, but this can be used only for a brief period of time later (for all banks that we analysed the life-time of the password was around 30 seconds). A phishing site that replicates the BCR home page can work for this purpose and an adversary may gain access to the user's financial situation. To authorize a false transaction it is not very feasible since the adversary must either create an account that has the same last 4 characters from the iban as the one that is used as a destination by the user. However a MitB will be successful since the adversary can manipulate the last 4 characters from the destination iban. In both ways the adversary can only successfully authorize the amount of money the user wants to transfer, because this is signed by the user.

2. *BRD Bank - Groupe Societe Generale:* The on-line system of BRD Bank has one of the simplest and most insecure authentication/authorization mechanisms which is based only on a user defined password and user-name chosen by the bank. The password characters must be entered in a virtual keyboard. Both the user-name and the password can be captured easily by a phishing site, and then reused to get inside the on-line account and to authorize transactions. In particular this mechanism is vulnerable to any of the three attacks.

3. *Transilvania Bank:* has three types of authentication. The first type uses a digital certificate installed in the browser, a user-name set by the bank and password chosen by the user. For the authentication process the password is introduced via a virtual keyboard. After the process is completed, the user can view its account status and make transfers. Because the client certificate request can be made on-line, a two stage attack is feasible. First, the adversary acts as a passive eavesdropper to capture the information needed to create such a request, i.e., the PIN of the client. Second, he makes a request using the client's PIN to obtain the client's certificate for himself. Once the adversary has all the credentials and the client certificate he can authenticate to the user's account and authorize transactions in its own interest. Indeed, in a third stage the adversary (acting as the banking server, e.g., via a pharming attack) can send the acquired certificate to the client misleading him to believe that he is the only owner of this certificate. The e-banking solution offered by Transilvania Bank is annoying to many users because of the need to install digital certificates in the browser. Beside this, the application needs to connect to another port than 80, which is used for HTTP, making it unusable for employees of some companies that use firewalls.
   The second method of authentication is by using a code sent by the bank to the client via SMS. The adversary can capture the code sent by the bank using a phishing web site but it has a limited life time (around 30 seconds). To authorize money transfers, in the first and second case, the user only needs to enter his password which can be captured by the adversary through social engineering.
   The third method of authentication is a stronger one, requiring a token generated code, like in the case of BCR. For the authorization the bank requires also a code from the token, if this code is captured by the adversary, it can be used to authorize any transaction regardless of the amount, but the code has only a limited life time (≈ 30 sec.), and can be used only once. While credential stolen is ineffective, a channel break or content manipulation will succeed against this service, thus the solution is not resilient against MitB attacks.

4. *CEC Bank:* Being one of the most emerging banks on the Romanian market, CEC uses a token authentication/authorization mechanism which is similar with the third solution from Transilvania Bank, having the same vulnerabilities.

5. *Raiffeisen Bank:* For the authentication mechanism Raiffeisen uses the same authentication scheme as CEC Bank, but a counter is used instead of a time stamp for the password generation process. This password, if it is captured, can be used at any point in time by the adversary (note that there is no time-stamp associated with this password). For the case of

transaction authorization they use the same method as the one from BCR Bank, exposing the same security risks as from the other bank. We also note that the on-line application of Raiffeisen Bank doesn't use obfuscated JavaScript code and contains a lot of commented code which can contain useful indications for an adversary.

6. *UniCredit Tiriac Bank:* Here the same authentication mechanism as for BCR is used. For the transaction authorization process, the same method as the one from CEC is used thus the same vulnerabilities are inherited.
7. *Alpha Bank:* The e-banking application of Alpha Bank uses a certificate based authentication mechanism which is similar with the one from Transilvania Bank, exposing the same security risks and has also the same usability problems. Regarding transactions Alpha doesn't use any authorization mechanism.
8. *ING Bank:* In the case of ING Bank the authentication mechanism is the same as for BCR, having the same vulnerabilities. For a transaction authorization, the adversary must wait until the user wants to authorize a transfer of his own and then change the value of the nonce with the one needed by him.
9. *Bancpost Bank:* In this case the authentication is done in two steps. First, the user needs to enter a user-name provided by the bank and its chosen password. In the second step, the user can choose what type of authentication he wants. The possible types of authentication are: challenge-response token authentication, token generated code, or code sent by the bank via SMS. In all three cases even if the adversary captures a valid authentication code, it can used only once in a limited time interval. But, this code is required only once during a session, so an adversary can authorize transfers once authenticated.
10. *CitiBank:* has a simple authentication mechanism, based on user chosen password and user-name, and an answer to a random chosen question ($question_U$) from a list of 8 standard questions. All this information can be easily captured using a phishing site. The user's password is used also for transactions authorization, but transactions can be made only to predefined bank accounts. In order to define a bank account ($add_R$) the user must validate it by entering a code sent by the bank via SMS. By using a MitB attack the bank account can be modified by the adversary, but this can be noticed by a careful user.

| Bank | Authentication | Transaction authorization |
|---|---|---|
| BCR Erste Bank | 1. $U\rightarrow B$:$user_B$,$password_{token}(t)$ | 1. $U\rightarrow B$:$authorize_U$<br>2. $B\rightarrow U$:$iban_R^4$,$amnt_R$<br>3. $U\rightarrow B$:$Sign_{token}(iban_R^4,amnt_R,t)$ |
| BRD Bank - GSG | 1. $U\rightarrow B$:$user_B$,$password_U$ | not required |
| Transilvania Bank | 1a. $U\rightarrow B$:$user_B$,$password_U$,$cert_U$ or | 1ab. $U\rightarrow B$:$authorize_U$,$password_U$ or |
| | 1b. $U\rightarrow B$:$user_B$,$password_U$<br>2b. $B\rightarrow U$:$authcode_B^{SMS}$<br>3b. $U\rightarrow B$:$authcode_B^{PC}$ or | |
| | 1c. $U\rightarrow B$:$user_B$,$password_{token}(t)$ | 1c. $U\rightarrow B$:$authorize_U$,$password_{token}(t)$ |
| CEC Bank | 1. $U\rightarrow B$:$user_B$,$password_{token}(t)$ | 1. $U\rightarrow B$:$authorize_U$,$password_{token}(t)$ |
| Raffeisen Bank | 1. $U\rightarrow B$:$user_U$,$password_{token}(cnt)$ | 1. $U\rightarrow B$:$authorize_U$<br>2. $B\rightarrow U$:$iban_R^4$,$amnt_R$<br>3. $U\rightarrow B$:$Sign_{token}(iban_R^4,amnt_R,t)$ |
| UniCredit Tiriac Bank | 1. $U\rightarrow B$:$user_B$,$password_{token}(t)$ | 1. $U\rightarrow B$:$authorize_U$,$password_{token}(t)$ |
| Alpha Bank | 1. $U\rightarrow B$:$user_B$,$password_U$,$cert_U$ | not required |
| ING Bank | 1. $U\rightarrow B$:$user_B$,$password_{token}(t)$ | 1. $U\rightarrow B$:$authorize_U$<br>2. $B\rightarrow U$:$nonce_U$<br>3. $U\rightarrow B$:$Sign_{token}(nonce_U)$ |

| | | |
|---|---|---|
| Bancpost Bank | 1. $U \rightarrow B: user_B, password_U$ | not required |
| | 2a. $B \rightarrow U: nonce_U$<br>3a. $U \rightarrow B: Sign_{token}(nonce_U)$ or | |
| | 2b. $U \rightarrow B: password_{token}(t)$ or | |
| | 2c. $B \rightarrow U: authcode_B^{SMS}$<br>3c. $U \rightarrow B: authcode_B^{PC}$ | |
| CitiBank | 1. $U \rightarrow B: user_U, password_U, question_U$ | 1'. $U \rightarrow B: add_R$<br>2'. $B \rightarrow U: authcode_B^{SMS}$<br>3'. $U \rightarrow B: authcode_B^{PC}$<br>1. $U \rightarrow B: authorize_U, password_U$ |
| Millennium Bank | 1. $U \rightarrow B: user_B, password_U, cnp_U^2$ | 1a. $U \rightarrow B: authorize_U, pass1_U^3 \mid pass2_U^3$ or |
| | | 1b. $U \rightarrow B: authorize_U$<br>2b. $B \rightarrow U: authcode_B^{SMS}$<br>3b. $U \rightarrow B: authcode_B^{PC}$ |
| ProCredit Bank | 1. $U \rightarrow B: user_U, password_U, password_{token}(t)$ | 1. $U \rightarrow B: authorize_U, password_U, password_{token}(t)$ |

Table II: Authentication and transaction authorization for the Romanian banks (providers are in the order of market shares)

11. *Millennium Bank:* The Internet banking application of Millennium Bank uses personal information about the user to authenticate him or to authorize a money transfer. But this information can be captured using a phishing site and used by the adversary afterwards to authenticate and authorize its own transactions. For the SMS based authorization the adversary must act as an active eavesdropper, between the user and the bank, at the moment when the user wants to authorize a transaction. The adversary needs to change the transaction information in its own interest and then use a phishing web site to capture the code from the client.

12. *ProCredit Bank:* This bank uses for authentication, besides user chosen password and user-name, a token generated code. Even if this information is captured by an adversary, the code generated by the token can be used only in a very small time interval, before it expires. For transactions authorization the user's password is required and a new code generated by the token. Content manipulation attacks, such as MitB, will succeed against this solution.

## *A hierarchy of security levels*

Figure 1 presents a hierarchy of the security of authentication and transaction authorization mechanisms of the e-banking applications. The hierarchy used in Figure 1 is based on the security levels defined by Hiltgen et al. (2006) (these criteria are clarified at the end of section 2.1).

Note however that their placement in the taxonomy for authentication and transaction authorization is not always similar. For example, in the case of transaction authorization, ING uses a challenge response mechanism to authenticate transactions. Although this is challenge based and not timer based as in the case of BCR and Raiffeissen this is less secure because the amount of money and iban account are not signed, making it possible for an adversary to change these values. Because of this, we downgraded the security from ING to level 4 and upgraded the security level of BCR and Raiffeisen to level 5.

As a partial conclusion to our survey, we present a chart (Figure 2) with a comparison between the Romanian market share of the banks, as of 2012 (Hostiuc, 2012), and the security level of the e-banking applications against fraudulent money transfer. We need to mention, that the security of e-banking applications has evolved since 2012, and that banks haven't made public the figures regarding the electronic fraud on their systems, reinforcing the idea that they rely on security-by-obscurity.

## *A hierarchy of usability*

First we enumerate some attributes of the devices in Table III. For each of the bank we outline if the authentication device (absent in case of passwords and denoted by "*") offers input or output and rank it for cost and convenience. We consider that mobile phones are more expensive than hard tokens while passwords are the cheapest. Also, passwords offer the highest convenience followed by phones which are frequently carried by users, hard tokens have lower convenience since they are an additional device that has to be taken by the user. Hard token based solutions that use more than one input are even less usable. The certificate based solution is the least usable since all clients in our usability study rejected this solution.

Usability is also important because it enhances the e-banking experience for insecure customers, through the additional features provided by the e-banking application that assure a reliable assistance (Mäenpää, 2006). A hierarchy of usability, which not surprisingly is almost the upside-down security, is suggested in Figure 1.

| | Raiffeisen Bank | ING | Alpha Bank | Millenium Bank | BRD | BCR | UniCredit Tiriac Bank | CEC Bank | Transilvania Bank | Bancpost Romania | ProCredit Romania | CitiBank Romania |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Input | Y | Y | * | N | * | Y | Y | Y | Y | Y | Y | * |
| Output | Y | Y | * | Y | * | Y | Y | Y | Y | Y | Y | * |
| Cost | Medium | Medium | Low | High | Low | Medium | Medium | Medium | Low | Medium | Medium | Low |
| Convenience | Low | Low | Low | Medium | High | Medium | Medium | Medium | Low | Medium | Low | High |

Table III: Attributes of the authentication solutions: input, output, convenience and cost

Besides building a hierarchy of usability, we also made a user study that involved more than 100 individuals. The group was balanced around gender 55% males and 45% females at age between mostly between 18 and 40. The results are presented in Figures 4 and 5.

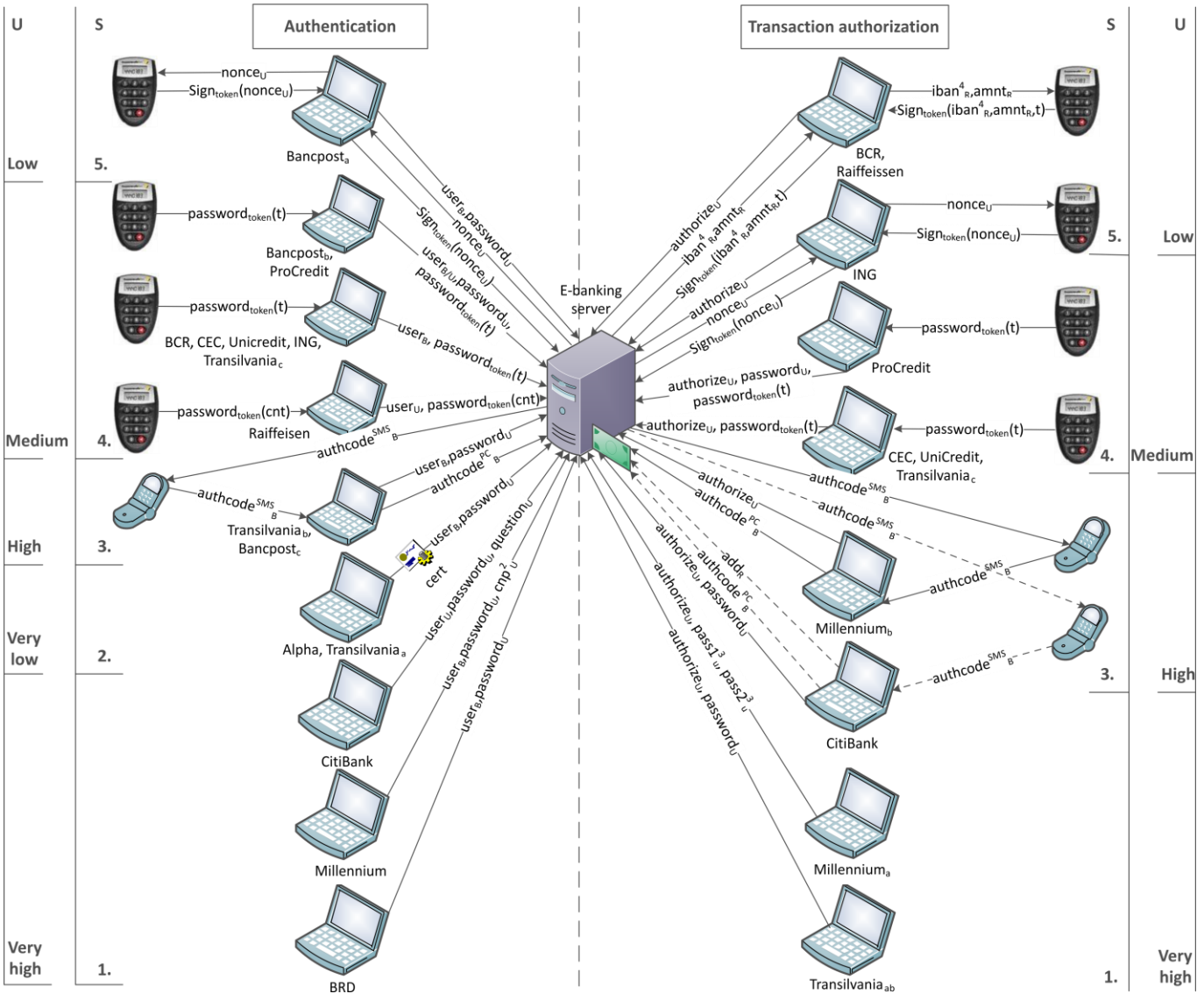



Figure 1: Possible security [S] and usability [U] hierarchy of authentication/authorization mechanism in e-banking

We roughly separated between questions that address attack awareness and security versus usability. The results showed that the large majority of the individuals do not open messages that are marked as spam. Also half of the individuals are aware of what security indicators in a browser are and will not accept certificates that are not signed by trusted providers. We believe these results are fine but they are not the best possible since they clearly show there are lots of individuals that do not know what phishing or signed certificates are. On the brighter side, it seems that the large majority of users are concerned more about security than usability and prefers hard tokens or at least a confirmation over the mobile phone which is more secure than simple passwords. This confirms the fact that ignoring security in e-banking applications is a critical shortcoming (Enos, 2011) since it represents a major concern for most of the customers. It is our opinion that passwords can be secure enough for users that are aware of what a trusted site is and use only clean computers to establish connections. The large majority of users from our study were Windows based and kept antivirus software that was up to date.

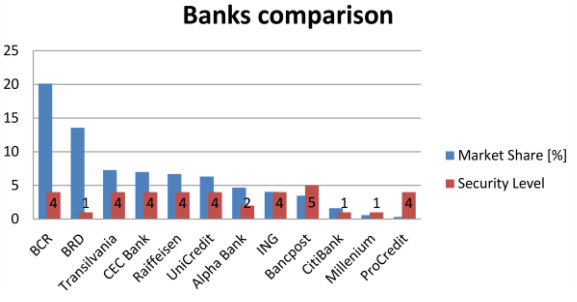



Figure 2: Comparison between the market share and the authentication security level

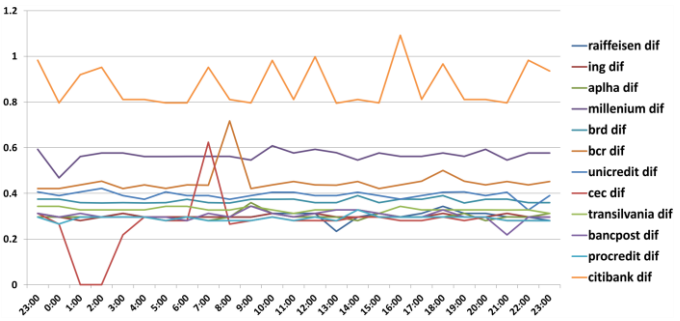



Figure 3: SSL connection response time

Also, we considered the response time of the sites as part of our usability study. The main reason behind this is that individuals usually have accounts from more than one provider and they can be tempted to drop on sites that work inappropriately. As can be seen in Figure 3, the response times are the same with low peaks at lunch time and after work due to an obvious increase in the response traffic. Only CitiBank had a significantly slower response time which is visible to the user but shouldn't be troublesome. The measurements were done by using a script that ran for 24 hours, we did these over several days and the results were similar.

# Discussion and conclusions

We further tried to find a potential correlation between the security level and the financial profit of the provider but we couldn't find any. One assumption would be that banks with higher security levels will have the highest profits, but BRD (controlled by Societe Generale France) has the highest profit for 2011 (472 million lei) at the weakest security level - a simple password of at least 6 digits. Another assumption would be that banks with low security levels will have a decrease in the profit, indeed BRD is declining in the last 3 years, but Transilvania Bank, with a security level of just 2 (a simple certificate in the browser and a password) is increasing. On the other hand, BCR (controlled by ERSTE bank Austria) with one of the highest security levels (password token) has a loss of 327 million lei (indeed, this could be part of bank strategy since its market share increased with more than 1% during the same financial losses). But even if we considered the market share we couldn't find any notable correlation with the security level. In fact, Bancpost which has the highest security level on our study appears to be in continuous decline for the last 3 years both in terms of market share and income. This will not hold for the banks that follow as security level, ING and Raiffeisen, which were in a continuous increase both as market share and income for the last 3 years. Thus, the security level appears to be no predictor for income or market share of a bank. We could not even conclude that banks with an increasing revenue will invest more on their security since BRD, which has the highest income in 2011 didn't change its security (a simple password) for at least 5 years (however, its market share declined from 14% to 13.57% in the last three years). Indeed, security was previously shown to be a critical factor for the success of e-banking (Shah et al., 2007; Susanto et al., 2013). Other works underline trust as a critical success factor in mobile banking, while trust is built upon structural assurances that derive from payment security itself (Zhou, 2011). Our conclusion does not contradict this since the answers from our scrutiny confirms as well that the large majority of users are concerned with security, notably even before usability. However, we believe that the explanation for the increased market share of banks that provide only weak security is a consequence of both poor user awareness on the security level (a conclusion supported by the fact that the majority of users do not have a proper technical education) and of the bank's publicity complement by various incentives that it offers. Indeed, a complete answer to this question may be offered by future research.

The provided analysis of the top e-banking providers from the Romanian market showed that the solutions used by them are technically sparse: from simple passwords chosen by users to more advanced one-time password calculators or digital certificates. These solutions are vulnerable in part or entirely to phishing/pharming attacks which become more dangerous when correlated to DoS/DDoS attacks. To improve resilience against such attacks we recommend a mixed solution in which smart cards are used for mutual authentication between the user and the website. As a general policy, increasing the number of authentication factors, as long as the solution does not become too complex, is convenient. For this purpose, using handy devices, such as smart-cards and mobile phones, to authenticate a website, can prove to be an easy to use and efficient solution. At present time, the employed solutions are not completely secure against modern attacks.

A future work that is of great interest to us would be the study of mobile banking technologies. So far, only some of the providers give special appliances for mobile banking and these rely on the same authentication technology. We do believe

that in this case, due to an increasing number of lost or stolen devices, security will become an even more critical aspect and due to the wide spread adoption of mobile devices; security may have a clearer impact on the market success of the provider.

# References


Aburrous, M., Hossain, M., Dahal, K., and Thabtah, F. (2010). Intelligent phishing detection system for e-banking using fuzzy data mining. *Expert Systems with Applications*, 37(12):7913 – 7921.

APWG (2012). Phishing activity trends report @Antiphishing. Accessed: 01/10/2013.

Bakker, J. (2011). Ddos attack forces dutch bank offline @CSO Online. Accessed: 01/10/2013.

BitDefender (2011). 27% of romanian internet users haven't heard of phishing @bitdefender. Accessed: 01/10/2013.

CECBank (2008). Personal protection for accessing internet banking at cec bank @CEC bank. Accessed: 01/10/2013.

Dunlop, M., Groat, S., and Shelly, D. (2010). Goldphish: Using images for content-based phishing analysis. In *Proceedings of the 2010 Fifth International Conference on Internet Monitoring and Protection*, ICIMP '10, pages 123–128, Washington, DC, USA. IEEE Computer Society.

Eisen, O. (2010). Catching the fraudulent man-in-the-middle and man-in-the-browser. *Network Security*, 2010(4):11 – 12.

Enos, L. (2011). Report: Critical errors in online banking @Ecommerce Times. Accessed: 01/10/2013.

Epayment (2011). Rates of attempted online payment fraud decreased by 50% in 2010 @epayment. Accessed: 01/08/2011.

FFA (2012). Fraud - the facts 2012 @Financial Fraud Auction UK. Accessed: 01/10/2013.

Furnell, S., Tsaganidi, V., and Phippen, A. (2008). Security beliefs and barriers for novice internet users. *Computers & Security*, 27(7–8):235 – 240.

Garera, S., Provos, N., Chew, M., and Rubin, A. D. (2007). A framework for detection and measurement of phishing attacks. In *Proceedings of the 2007 ACM workshop on Recurring malcode*, WORM '07, pages 1–8, New York, NY, USA. ACM.

Garfinkel, S. L. (1995). Aohell @The Boston Globe. Accessed: 01/10/2013.

Gastellier-Prevost, S., Granadillo, G., and Laurent, M. (2011). A dual approach to detect pharming attacks at the client-side. In *New Technologies, Mobility and Security (NTMS), 2011 4th IFIP International Conference on*, pages 1 –5.

Görling, S. (2007). An overview of the sender policy framework (spf) as an anti-phishing mechanism. *Internet Research*.

Gühring, P. (2006). Concepts against man-in-the-browser attacks. Accessed: 01/10/2013.

Gunson, N., Marshall, D., Morton, H., and Jack, M. (2011). User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking. *Computers &; Security*, 30(4):208 – 220.

Herzberg, A. (2009). Why johnny can't surf (safely)? attacks and defenses for web users. *Computers & Security*, 28(1–2):63 – 71.

Hiltgen, A., Kramp, T., and Weigold, T. (2006). Secure internet banking authentication. *IEEE Security and Privacy*, 4(2):21–29.

Hostiuc, C. (2012). Top banks in 2011 @Ziarul Financiar. Accessed: 01/10/2013.

Kim, C., Tao, W., Shin, N., and Kim, K.-S. (2010). An empirical study of customers' perceptions of security and trust in e-payment systems. *Electronic Commerce Research and Applications*, 9(1):84 – 95. Special Issue: Social Networks and Web 2.0.

Kritzinger, E. and von Solms, S. (2010). Cyber security for home users: A new way of protection through awareness enforcement. *Computers & Security*, 29(8):840 – 847.

Latze, C. and Ultes-Nitsche, U. (2007). Stronger authentication in e-commerce: how to protect even naive user against phishing, pharming, and mitm attacks. In *Proceedings of the IASTED International Conference on Communication Systems, Networks, and Applications*, CSNA '07, pages 111–116, Anaheim, CA, USA. ACTA Press.

Li, T. and Unger, T. (2012). Willing to pay for quality personalization? trade-off between quality and privacy. *EJIS*.

Ludl, C., Mcallister, S., Kirda, E., and Kruegel, C. (2007). On the effectiveness of techniques to detect phishing sites. In *Proceedings of the 4th international conference on Detection of Intrusions and Malware, and Vulnerability Assessment*, DIMVA '07, pages 20–39, Berlin, Heidelberg. Springer-Verlag.

Mäenpää, K. (2006). Clustering the consumers on the basis of their perceptions of the internet banking services. *Internet Research*.

Malhotra, P. and Singh, B. (2007). Determinants of internet banking adoption by banks in india. *Internet Research*.

Mannan, M. and van Oorschot, P. C. (2008). Security and usability: the gap in real-world online banking. In *Proceedings of the 2007 Workshop on New Security Paradigms*, NSPW '07, pages 1–14, New York, NY, USA. ACM.

McCall, T. (2007). Gartner survey shows phishing attacks escalated in 2007; more than $3 billion lost to these attacks @Gartner. Accessed: 01/10/2013.

Moore, T. and Clayton, R. (2008). The impact of incentives on notice and take-down. In *In proceedings of the 7th Workshop on Economics of Information Security*, pages 1 – 24.

Murdoch, S. J. and Anderson, R. (2010). Verified by visa and mastercard securecode: or, how not to design authentication. In *Proceedings of the 14th international conference on Financial Cryptography and Data Security*, FC'10, pages 336–342, Berlin, Heidelberg. Springer-Verlag.

Pan, Y. and Ding, X. (2006). Anomaly based web phishing page detection. In *Proceedings of the 22nd Annual Computer Security Applications Conference*, ACSAC '06, pages 381–392, Washington, DC, USA. IEEE Computer Society.

Pavía, J. M., Veres-Ferrer, E. J., and Foix-Escura, G. (2012). Credit card incidents and control systems. *International Journal of Information Management*, pages –.

Shah, M. H., Braganza, A., and Morabito, V. (2007). A survey of critical success factors in e-banking: an organisational perspective. *EJIS*, 16(4):511–524.

Susanto, A., Lee, H., Zo, H., & Ciganek, A. P. (2013). Factors Affecting Internet Banking Success: A Comparative Investigation between Indonesia and South Korea. In *Journal of Global Information Management (JGIM)*, 21(2), 72-95.

Stahlberg, M. (2007). The trojan money spinner. In *Proceedings of virus bulletin conference*, pages 1–7.

Utakrit, N. (2009). A review of browser extensions, a man-in-the-browser phishing techniques targeting bank customers. In *Proceedings of the 7th Australian Information Security Management Conference*, AISM '09, pages 110–119.

Weigold, T. and Hiltgen, A. (2011). Secure confirmation of sensitive transaction data in modern internet banking services. In *Internet Security (WorldCIS), 2011 World Congress on*, pages 125 –132.

Weigold, T., Kramp, T., Hermann, R., Höring, F., Buhler, P., and Baentsch, M. (2008). The zurich trusted information channel — an efficient defence against man-in-the-middle and malicious software attacks. In *Proceedings of the 1st international conference on Trusted Computing and Trust in Information Technologies: Trusted Computing - Challenges and Applications*, Trust '08, pages 75–91, Berlin, Heidelberg. Springer-Verlag.

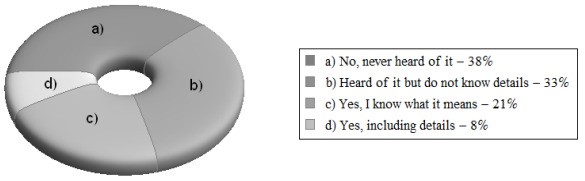
Weir, C. S., Douglas, G., Carruthers, M., and Jack, M. (2009). User perceptions of security, convenience and usability for ebanking authentication tokens. *Computers & Security*, 28(1–2):47 – 62.

WindsorFederal (2011). Online banking security – anti-phishing solution from comodo @Windsor Federal Savings. Accessed: 01/10/2013.

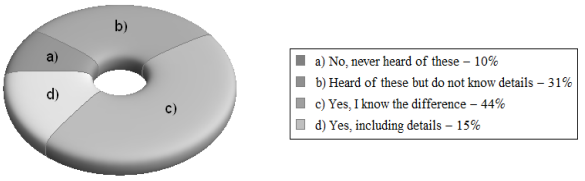
Wong, M. W. (2004). Spf overview @Linuxjournal. Accessed: 01/10/2013.

Zhang, Y., Egelman, S., Cranor, L., and Hong, J. (2007). Phinding phish: Evaluating anti-phishing tools. In *In Proceedings of the 14th Annual Network and Distributed System Security Symposium (NDSS 2007)*, pages 1 – 16.

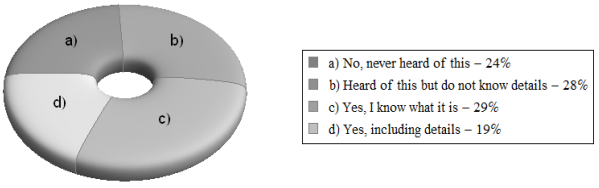
Zhou, T. (2011). An empirical examination of initial trust in mobile banking quality and privacy. *Internet Research*.



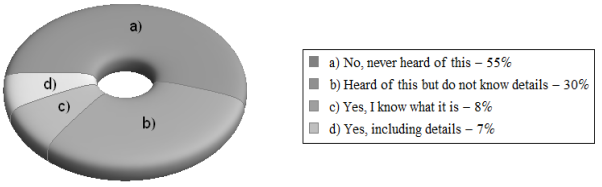

Do you know what SSL/TLS is?



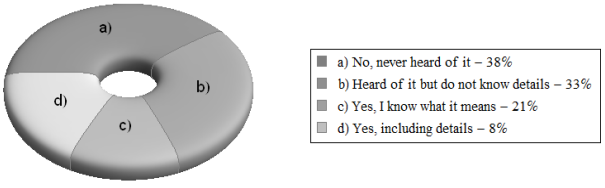

Do you know the difference between HTTP and HTTPS?



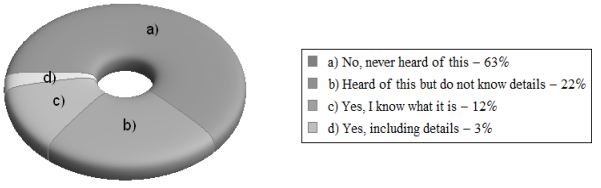

Do you know what a phishing attack is?



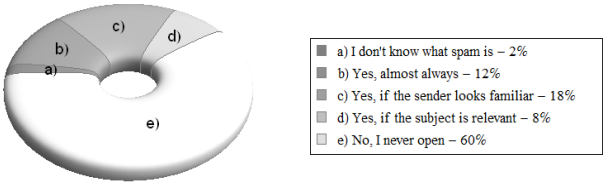

Do you know what a pharming attack is?



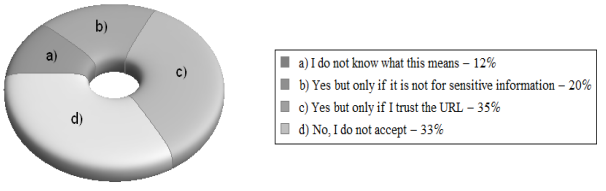

Do you know what a DoS attack is?



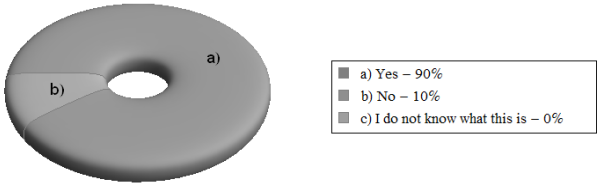

Do you know what a Man-in-the-Browser attack is?



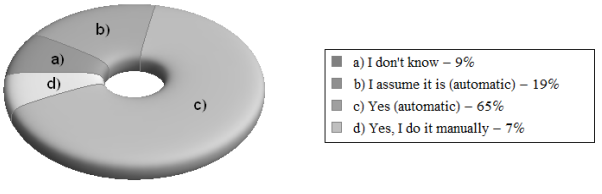

Do you usually open spam messages?




Do you accept certificates that are not signed by a trusted authority?

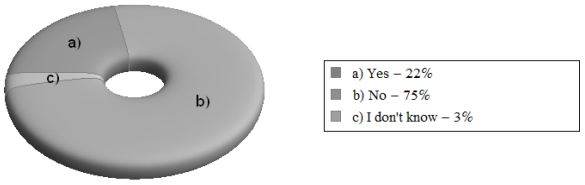



Do you use an antivirus software?

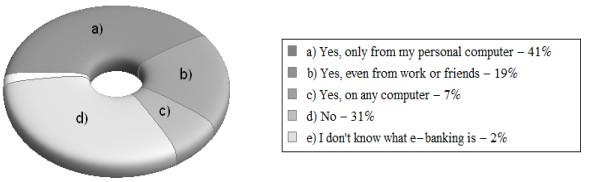



Do you keep your antivirus updated?

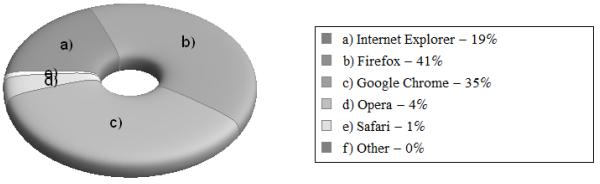
Figure 4: Attack and defense awareness questions



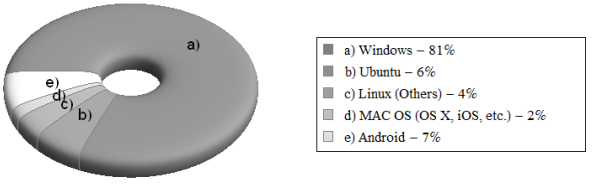

Do you use more than one antivirus software?



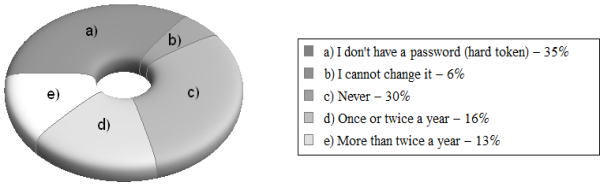

Do you use e-banking services?



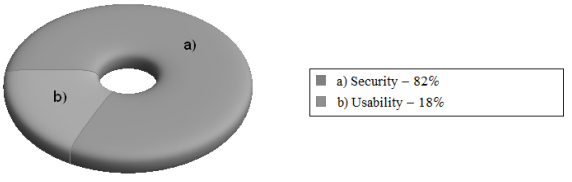

What browser do you use for e-banking?



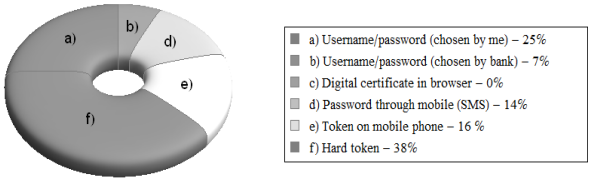

What OS do you use for e-banking?



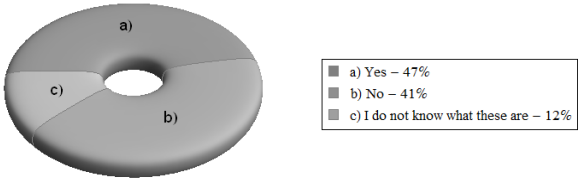

How often do you change your e-banking password?



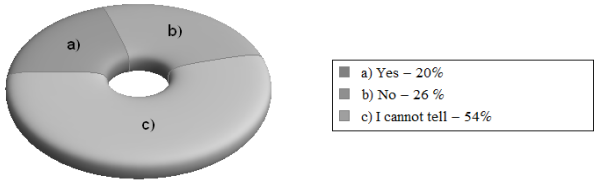

What is more important for you security or usability?



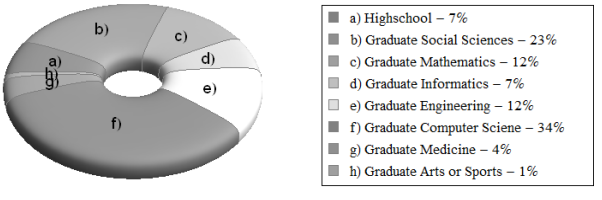

What authentication do you prefer for e-banking?




Do you check security indicators in browser?




I consider that my security policy is correct.




What is your education level?

Figure 5: E-banking security/usability questions and miscellaneous questions