Phishing and Countermeasures in Spanish Online Banking

Ilkka Uusitalo
VTT Technical Research Centre of Finland
Kaitoväylä 1, Oulu, Finland
ilkka.uusitalo@vtt.fi

Josep M. Catot
Caixa Catalunya
C/ Pi 2, 08820 El Prat de Llobregat, Spain
josep-maria.catot@caixacatalunya.es

Ramon Loureiro
Pompeu Fabra University
Plaça Mercè 12, Barcelona, Spain
ramon.loureiro@upf.edu

Abstract

This paper surveys the current situation of phishing attacks in Spain and discuss some of the currently used countermeasures. Based on specialist interviews we estimate the costs of phishing to both individual clients and the banks. The focus of this paper is on authentication and transaction signing methods. We give examples of "two-factor" and "two-factor, two-channel" authentication and transaction signing methods that are more resistant to phishing than the currently used username/password + coordinates card method. We consider the costs usability and security of these more robust methods.

1. Introduction

Phishing is defined as a form of social engineering in which an attacker attempts to fraudulently retrieve legitimate users’ confidential and sensitive credentials by mimicking electronic communications from a trustworthy or public organisation in an automated fashion [10]. The aim of phishing is to steal sensitive information such as online banking passwords and credit card information from internet users. Phishing attacks use a combination of social engineering and technical spoofing techniques that persuade users into giving away sensitive information that the attacker then uses to make financial profit [13].

Phishing has a significant negative influence on companies’ reputation and market value regardless of company size [7]. For online businesses such as online banking, where the customers cannot verify the quality of products or services in advance, establishing and maintaining trust is key [12]. Phishing erodes companies’ trustworthiness and reputation and is therefore a major threat to online business. Lack of trust discourages users from engaging in online transactions [11], so better countermeasures against phishing are essential.

In this paper we study the current situation of phishing attacks against online banking in Spain. We discuss some of the currently used countermeasures and estimate the costs of phishing to both individual customers and the banks. The cost estimations are based on specialist interviews.

The focus of this paper is on authentication and transaction signing methods that are more resistant to phishing than the currently used method. Currently the method that is most widely deployed is based on username + password authentication. A coordinates card is used for transaction signing. The methods we focus on utilise two factor authentication: authentication and transaction signing is based on what the client knows and what the client has. We discuss the usability of the methods and give a limited costs evaluation of implementing and using them.

In the next sections we provide a brief overview of related work and describe the typical online banking authentication scenario. In Section 3 we discuss current trends of phishing attacks in Spain. Section 3.1 gives a rough estimation of monthly costs incurred by phishing in a bank with 1 million customers. After this we discuss countermeasures, focusing on authentication and transaction signing methods. Section 5 discusses usability and gives rough estimations about the costs of implementing and using the more resistant methods. Finally, conclusions are given in Section 6.

2. Related work

Phishing attacks can be categorized into malware, phishing e-mail, bogus Web sites, and indentity theft [6]. Mal-
ware, such as viruses and trojans, represents a technical means of phishing. It is used to steal victims’ confidential information surreptitiously.

Phishing e-mails and bogus Web sites are social engineering means of phishing. Phishing e-mails are sent to a massive amount of receivers. Phishers pretend to be a trustable third party and ask the recipients for confidential information such as online banking credentials. Bogus Web sites are sites that mimic legitimate sites. The victims are invited to log on to the bogus site by giving away confidential information for verification.

After the phishers have obtained victim’s confidential information, such as credentials for online banking, they commit identity theft by impersonating the victim at the actual Web site of the bank they mimic.

In [15] the authors outline five phishing countermeasures for online service providers: education, preparation, avoidance, intervention and treatment. Among these education is most important [6]. The best protection against phishing is to stay informed and maintain a healthy level of suspicion.

In [6] Bose and Leung investigate phishing preparedness of banks in Hong Kong. Web sites of Hong Kong banks are analysed and information related to phishing and countermeasures adopted by the banks gathered. The authors conclude that although the banks attach importance to information related to countermeasures they need to improve the accessibility of such information on their Web sites.

Technical countermeasures fall into the latter four categories of countermeasures. The users can protect their equipment from malware with proper firewalls and by keeping their antivirus software and operating system up-to-date. More advanced technical measures against malware include using a Secure Running Environment (SRE), such as secure kernel or secure middleware. These measures could be applied at both the clients and servers. In the client side, technical measures that are commonly applied include the hardening of web browsers, so that they are less vulnerable to Man-In-The-Middle (MITM), Man-In-The-Browser (MITB), certificate forging, and other such attacks.

An efficient measure against phishing e-mail would be to use origin authentication mechanisms in email systems or DNS, such as DNSSEC [2].

Yue and Wang propose BogusBiter [17], a client-side anti-phishing tool that feeds a relatively large number of bogus credentials into a suspected phishing site making the life of scammers a bit more difficult.

Below we discuss the typical internet banking scenario and phishing attacks against the authentication procedure.

2.1 Online banking scenario

In high level of abstraction we can say that the typical internet banking scenario consists of two phases:

1. An encrypted, integrity protected channel is set up between the user’s end device and the bank. SSL/TLS is the de facto standard used in this phase.
2. The user authenticates to the bank. There are no de facto authentication and non-repudiation standards. Many different methods with varying security are being used, and no single method has become predominant yet.

In Figure 1 above some online banking authentication methods are classified according to their resistance to offline credential-stealing and online channel-breaking attacks. The cost of the methods typically grows the more secure the method. Also, the more secure methods tend to be more complex toward the user.

In online channel-breaking attacks the attacker unnoticeably intercepts the messages between the client and the bank by masquerading as the bank towards the client and client towards the bank. MITM and MITB are examples of such attacks. The bank server is normally authenticated via a public-key certificate. The users sometimes ignore messages about invalid or untrusted certificates, or are fooled to trust fake online-generated certificates from a nested attacker Certificate Authority (CA). As a result, the attacker can hijack the authenticated banking session or silently manipulate transaction data.

Online channel-breaking attacks do not necessarily compromise the user’s credentials but rather the session’s credentials and therefore require the user-initiated session to work properly.

Offline credential-stealing attacks, on the other hand, aim to fraudulently gather user’s credentials. The attack can be carried out either by invading the user’s computer via malware, or by tricking the user into voluntarily revealing her credentials via phishing e-mail or bogus site.

In the next section we take a look at the current situation of phishing in Spain, and give a rough estimation of the monthly costs from phishing to an imaginary online bank.
3. Current situation in Spanish phishing

Figure 2 gives a view on how the amount of phishing attacks has evolved in Spain since March 2005 until the end of 2008. As can be seen, the amount of attacks has remained quite constant. Only just recently has the trend started to point steeply upwards.

![Figure 2. Phishing attacks in Spain](image)

For every 1,000 phishing emails send, around 15 are successful [1]. In a study conducted by Inteco [9], 3 out of 10 internet users in Spain admitted to have been an object of attempted fraud in the Internet, although only 2.1% admit having suffered economic losses. The average economic damage suffered is quite high, 593 Euros.

The Inteco report is based on an online fraud survey of 3,076 Spanish internet users. If we assume there are over 17 million internet users in Spain (October 2008, [5]), then the total number of users who have been subject to online fraud attempts in Spain can be assumed to be over 350,000.

Albeit the average loss due to fraud is almost 600 Euros, in little more than two of three cases the economic damage does not surpass 400 Euros and in 25% it does not reach 50 Euros. Although there are many attempts of fraud and relatively few are successful, those that are successful represent a great damage for the affected users, since besides the possible economic impact they lose time in organising their bank affairs after the attack. The banks face costs for protecting their assets from fraud, mitigation of the damages, and also in the form of reputation loss and loss of clientele. Online fraud can also form a barrier that hinders the entrance of new clients to online services.

This seemingly small amount of fraud might be due to the fact that often fraud remains unnoticed by the user. The attackers prefer stealing small amounts of money from an individual user, but attacking a greater number of users. That behaviour might be due to the Spanish legislation. It regards the quantity of 400 Euros as the limit to consider the fraud a petty theft.

The users’ confidence on using the Internet does not seem to falter because of these attacks. Even after an attempted fraud the Spanish users continue trusting the Internet: 80% do not change their habits of bank use online and a 73.1% continue purchasing online. Even when the attempt of fraud is successful a massive abandonment of services does not take place: 52.4% of the bank users and 31.9% of online shoppers do not alter their behaviour [9].

3.1 Cost estimations

Table 1 presents our estimations of the cost of phishing. The estimations data are based on specialist interviews. The specialists work with these issues in Spanish banks, but they wish to remain anonymous.

We assume a large bank with 1,000,000 users using online banking. According to our interviews, out of the million users approximately 15 become victims of a successful phishing attack each month. In other words, the credentials of 15 users fall to the hands of attackers. We assume that the attackers are able to transfer 2,000 Euros per month from the account of the user, attacking her several times. In addition to these direct losses we have assumed costs in working hours when employees of the bank work preventing, neutralizing or mitigating the attacks. The users also loose time settling their bank affairs after a phishing attack. Other countermeasures against phishing include the costs of informing clients about phishing-attacks. Regarding the transferred money we have estimated a distribution of 50% in responsibilities between the client and the bank.

<table>
<thead>
<tr>
<th>#</th>
<th>Credentials stolen/month</th>
<th>Setting costs (bank)</th>
<th>Setting costs (user)</th>
<th>Phishing prevention</th>
<th>Other countermeasures</th>
<th>Monthly costs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unit cost</td>
<td>2000</td>
<td>40</td>
<td>40</td>
<td>40</td>
<td>6000</td>
<td></td>
</tr>
<tr>
<td>Costs (bank)</td>
<td>15000</td>
<td>1200</td>
<td>1760</td>
<td>6000</td>
<td>23690</td>
<td></td>
</tr>
<tr>
<td>Costs (per user)</td>
<td>1000</td>
<td>400</td>
<td></td>
<td></td>
<td>21000</td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td>30000</td>
<td>1200</td>
<td>6000</td>
<td>1760</td>
<td>6000</td>
<td>44690</td>
</tr>
</tbody>
</table>

Table 1. Monthly costs from successful phishing attacks
With the above assumptions we conclude that currently, each month, the direct costs of phishing in Spain per one million clients are in the order of 50 000 Euros/month. These costs are surprisingly small. However, they do not include such indirect costs as damage to the bank’s reputation, loss of clientele, etc.

Naturally, the possibility of a large scale attack cannot be ruled out. In the worst case scenario the attackers have stored the credentials of a large number of users during a prolonged time and initiate a massive attack. If the attackers manage to transfer small amounts of money from a large number of users the loss could be calculated in the range of millions of Euros.

The above numbers are only a very rough estimation. However, we claim that the order of magnitude is correct. The above cost estimations are compared later with the costs of implementing more robust authentication and transaction signing methods.

4. Countermeasures

The focus of this paper, more secure authentication and transaction signing methods, are discussed in this section.

The following methods present varying levels of security. For this we define three levels of authentication. We lean on the definitions coined at [16]:

Level 1: "What you know".
Description One factor authentication. Based on the fact that the user knows the credentials. Authentication and authorization methods that fall to this class do not protect from identity theft by phishing using social engineering or technical means.

Level 2: "What you know + what you have".
Description Based on something the user possesses and something she knows. Methods in this level protect from identity theft by social engineering means.

Level 3: "What you know + what you have + what you are".
Description Based on something the user is, what the user possesses and what the user knows. This level offers protection from the theft of credentials by phishing, and also is not vulnerable to the physical theft of the electronic token.

In addition to the above, several hardening measures can be used in each level to give some additional protection against attacks. These include the use of antivirus software, firewalls, secure boot, SRE, and so on.

Examples of each protection level can be found below. The first one is the method currently most widely used in Spain. It represents Level 1, as it is based on one factor authentication: what the user knows. The password used for authentication is static, and can be changed by the user.

Method 1. Username/password authentication. Coordinates card for transaction signing (Level 1)
Description Coordinates card contains 50-100 short, alphanumerical passwords. Passwords can be one-time or can be used several times.

Needed equipment None. Coordinates are printed on a card.
Security considerations Vulnerable to phishing and online channel breaking attacks.

In the €-Confidential project [4] we experimented with the following authentication methods. They represent Level 2. They are based on two-factor authentication.

In Method 2 the smartcard can be an electronic Spanish national identity card (DNIe), or an EMV (Europay, Mastercard, VISA) card. The working principals of this method are discussed e.g., in [8].

Method 2. SmartCard reader + Smartcard + X509 certificate + PIN (Level 2)
Description The user possesses an X509 certificate in a smartcard. The user authenticates with a PIN code, and the authentication is based on the X509 certificate stored in the card. Transactions are also signed using the smartcard.

Needed equipment Smartcard reader + Smartcard.
Security considerations Vulnerable to theft of the card + PIN, online channel breaking attacks.

In method 3 the transactions are signed using the user’s mobile phone SIM-card. Secured SMS is used as the channel for transaction signing messages. We experimented with the system provided by Valimo [3]. Method 3 is more resistant than the previous methods to certain channel breaking attacks. Now the attacker would need to break two channels to mount a successful attack: the connection to the bank and the SMS connection. This two-channel scheme is depicted in Figure 3.

Method 3. As Method 2 + Digital transaction signing using the SIM of a mobile phone (Level 2)
Description As above + transactions are signed using a mobile phone based two-factor, two-channel scheme.

Needed equipment Smartcard reader + Smartcard + mobile phone
Security considerations Vulnerable to theft of the smart card + PIN, and mobile phone.

Adding biometrics would give us an example of three factor authentication. In addition to what the user knows and has, the authentication would be based on what he or
she is. Biometrics can be used in both authentication and transaction signing. For additional security against channel breaking attacks also here a two channel signing method, like in Method 3, could be used.

5 Cost and usability of the selected methods

We have chosen to estimate the costs of implementing and using Methods 2 and 3 because they adhere to the current legal requirements in Spain. Figure 4 below gives an overview of the methods. The user authentication is based on the DNIe. For transaction signing there are two options: SIM signing or signing based on EMV cards.

![Figure 4. Chosen authentication and transaction signing methods](image)

We base our assumptions on the amount of bank operations per 1 million clients each month, see Table 2 below. These numbers are again rough estimations.

<table>
<thead>
<tr>
<th>Access to services</th>
<th>3,500,000</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operations</td>
<td>900,000</td>
</tr>
<tr>
<td>Authentications</td>
<td>3,500,000</td>
</tr>
<tr>
<td>Signatures</td>
<td>1,000,000</td>
</tr>
<tr>
<td>Transfers (external)</td>
<td>300,000</td>
</tr>
<tr>
<td>Transfers (internal)</td>
<td>150,000</td>
</tr>
</tbody>
</table>

Table 2. Monthly banking actions

On the basis of the assumptions we give a rough cost estimation for Methods 2 and 3:

<table>
<thead>
<tr>
<th></th>
<th>Unit cost</th>
<th>Costs /user</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNIe readers</td>
<td>15</td>
<td>3</td>
<td>3,000,000</td>
</tr>
<tr>
<td>Opt 1: SIM signing.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Updating mobile phones</td>
<td>30</td>
<td>3</td>
<td>15,000,000</td>
</tr>
<tr>
<td>Transactions (450 000/ month, 2 messages each transaction)</td>
<td>0.10</td>
<td>0.045</td>
<td>45,000</td>
</tr>
<tr>
<td>Opt 2: EMV signing.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EMV reader</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Table 3. Monthly costs from successful phishing attacks

A DNIe reader is a considerable cost to the users. A reader can cost up to 15 Euros. We divided this cost by 5, because the users will use the reader for many services with other companies and with the Spanish authorities.

With respect to SIM transaction signing we see that there are running costs per each transaction. We assumed two messages per transaction, one from the bank to the user, and an answer from the user. The user pays the message originating from his mobile phone. We also assumed that half of the clientele need to update their phones.

As the same reader can be used for both DNIe and EMV there would be no costs for the user attached to the EMV transaction signing.

Calculating costs for the banks proved to be difficult. We will not give any numbers because we do not have enough information, and there are many aspects that influence these costs, such as how easy or difficult the new systems are to integrate to the bank’s existing IT infrastructure.

Acquiring the DNIe system inflicts an initial cost to the bank. The bank joins the already existing DNIe infrastructure, so these cost would probably not be too high. There are no significant running cost attached.

There are costs attached to the purchase or implementation of the SIM transaction signing system. Again, we are not in the position to evaluate these costs. There are also some running costs: each signed transaction cost approximately 0.10 Euros, or around 45,000 Euros per month.

For the EMV card based signing the initial costs are mainly related to two aspects: purchasing or implementing the system and generating the X509 certificates. There are no major monthly running costs.

Anyhow, in both cases the overall cost are higher than what is currently lost in successful phishing attacks each month, and more or less similar to the potential costs of a massive attack. However, we claim that the value of lost reputation to the financial organization certainly compensates the differences in the cost.
5.1 Usability and security considerations

For the user, the methods discussed above are a bit more complex than the currently used methods what comes to usability. In Method 1 the user needs to remember and type in a username + password combination when he or she is authenticating to the bank. For transaction signing the client needs to take care of and carry with him or her the coordinates card. There is no need for additional equipment.

For DNIE authentication (Methods 2 and 3) the user needs to acquire a smartcard reader. When authenticating to the online bank the user inserts the DNIE and types a PIN code. Currently there are no identity federation mechanisms in use for DNIE authentication. The usability of DNIE would be greatly improved with identity federation, as currently one needs to sign up for each DNIE authenticated service separately.

Transaction signing with EMV is equal to DNIE authentication regarding usability. The downside with smartcard-based authentication is the need for the smartcard reader. How would the user authenticate in situations (travelling etc.) when there is no reader available? Transaction signing based on SIM is a bit more complex still, as the client needs to have his or her mobile phone at hand. For both transaction signing methods some kind of a fallback system would be needed.

However, Method 2 and 3 are also far more resistant to phishing than the currently used method. Method 3 is even resistant to some online channel breaking attacks. What is lost in usability is easily won security wise.

6. Conclusions

In this paper we discussed the current situation in phishing attacks in Spain against online banking. Currently the direct costs inflicted by phishing each month are comparably small. However, the costs estimated in this paper do not take into account indirect costs such as damage to banks’ reputation and loss of clientele. Also, the possibility of a large scale attack can not be ruled out. When these are taken into account the costs of implementing authentication and transaction signing methods that are resistant to phishing are well justifiable.

With the above estimations in mind we discussed authentication and transaction signing methods that would be more resistant to phishing. The method currently mostly wide used is based on what the user knows, i.e. username and password. Transactions are signed using a coordinates card. This kind of system is vulnerable to phishing as by means of social engineering it is possible to make some clients submit their credentials to adversaries.

We focused on authentication and transaction signing methods that are based on something more than what the user knows: what he or she has. In the methods we discussed authentication is based on the Spanish national identity card. Transaction signing is based on the EMV card, or on mobile phone SIM signing. These methods are resistant to phishing by social engineering means. Transaction signing with SIM is even resistant to certain channel breaking attacks (such as MITM or MITB); the attacker would need to break in to two separate channels: the SSL/TLS connection and the SMS connection.

With simple updates to the current bank authentication and transaction signing systems online banking would be much more resistant to the most frequent form of online fraud, phishing.

References