Preventing and Handling Phishing Attacks

Javier Echaiz* Jorge R. Ardenghi

Laboratorio de Investigación en Sistemas Distribuidos (LISiDi)
Departamento de Ciencias e Ingeniería de la Computación
Universidad Nacional del Sur – Bahía Blanca, Argentina
T.E.: +54 291–4595135 Fax: +54 291–4595136
{je,jra}@cs.uns.edu.ar

Abstract

Phishing (also known as carding and spoofing) is the act of attempting to fraudulently acquire sensitive information, such as passwords and credit card details, by masquerading as a trustworthy person or business with a real need for such information in a seemingly official electronic notification or message (most often an email, or an instant message (IM)). It is a form of social engineering attack.

Customers of banks throughout the world have been victims of phishing. This paper covers the technologies and security flaws phishers exploit to conduct their attacks, and provides advice on security measures that can be employed by financial service providers such as Banks in order to prevent and handle phishing attacks. The customers' perspective is also considered.

Keywords: phishing, spoofing, e-banking, computer security.

1 Introduction

The exponential growth in Internet in general and specifically in online financial transactions made possible phishing as a profitable technique for attackers. These days nearly all the banks provide to its customers online banking (also known as e-banking or home banking) facilities so this customers can potentially become a victim of phishing. Taking advantage of stolen banking information hackers can perform dishonest acts, which may include:

- Performing unauthorized transactions utilizing credit or debit card numbers.
- Logging into the home banking application, usually through a web page, using a username and a password. The thief can get access to all the financial information of the real user, as well as carry out transactions on his behalf.
- Commercialize real user's personal data such as IDs, phone numbers, address, birthday, old transactions information, account numbers, etc. to third parties for different illegal activities.
- Denying e-banking service to real users by changing their passwords and sometimes even other personal details.
- Damaging the customer's confidence in his bank.

*Supported by a fellowship of the "Consejo Nacional de Investigaciones Científicas y Técnicas", Argentina.

2 Attack Techniques

Usually phishing attacks combine fake emails and resembling web sites to trick customers in order to make them reveal their personal financial details. Users think they are sent (by clicking on a link "offered" by the fake mail) to an official site. They are hooked by this forged email since it appears to come from the real enterprise but is actually sent by the attackers. This email lures the users into logging into a forged web site where they use their personal (secret) information in the logon process, revealing their details since all the data is logged for the attacker.

In the Figure 1 we illustrate a typical phishing attack. This phishing attempt, disguised as an official email from Charter One Bank, attempts to trick users into giving away their account information by "confirming" it at the phisher's linked website. The 'FROM' address has been modified to make it look like it has been sent from the genuine bank.

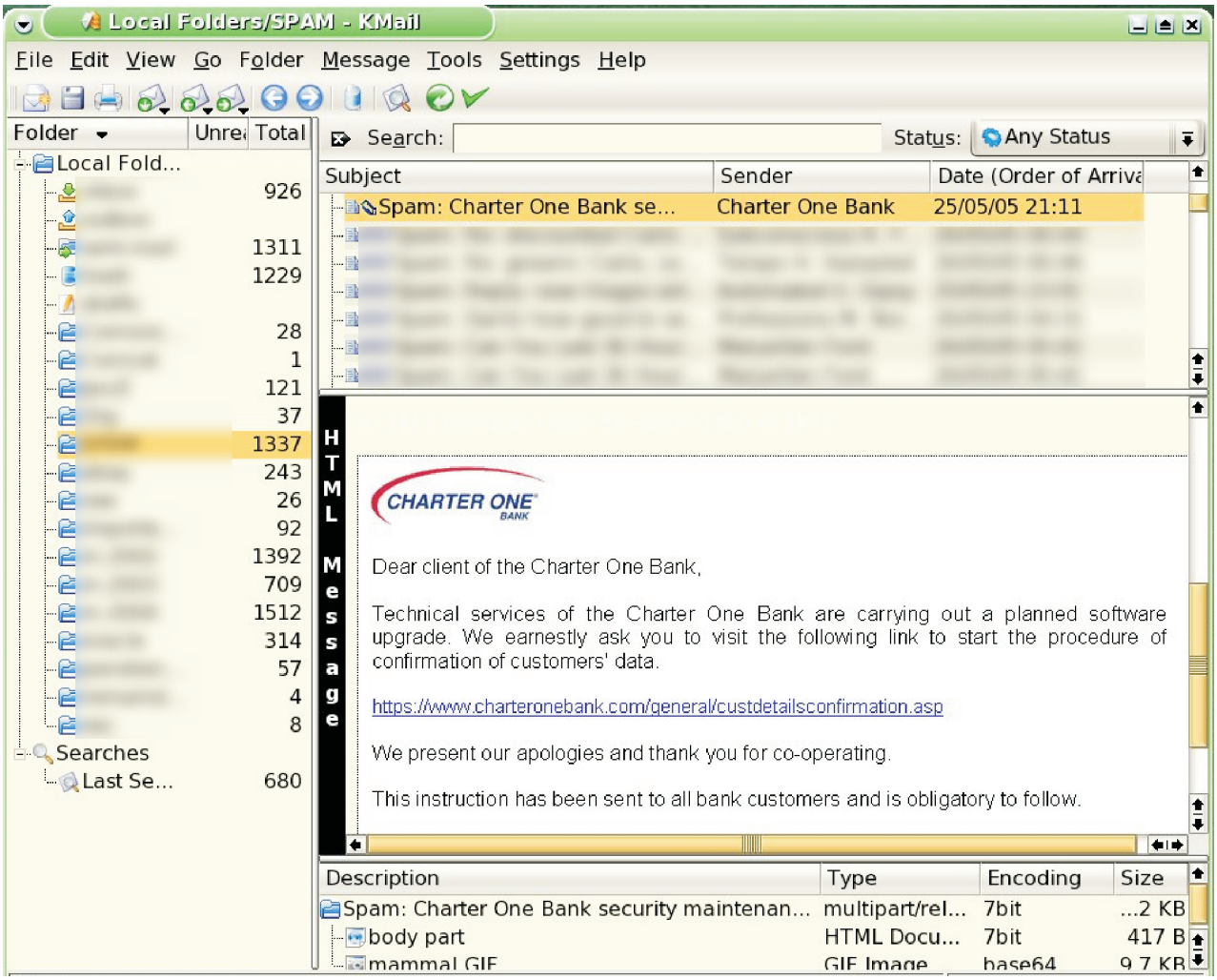

Figure 1: Fake email pretending to come from a Charter One Bank.

The email asks the users to log on to the e-banking web site in to verify customers' data by clicking on an embedded link in the email. When users click on the link (apparently from the real site), they are taken to a copy of the real bank site and are tricked into providing their username and password. In order to make the bogus email look genuine, phishers usually the bank's logo, security guidelines, etc.

In another example (Figure 2), now pretending to be from PayPal, we can see the IP address of the bogus site at the lower left corner when we hover the mouse over the provided link. IP addresses

just mean more problems for the naive user.

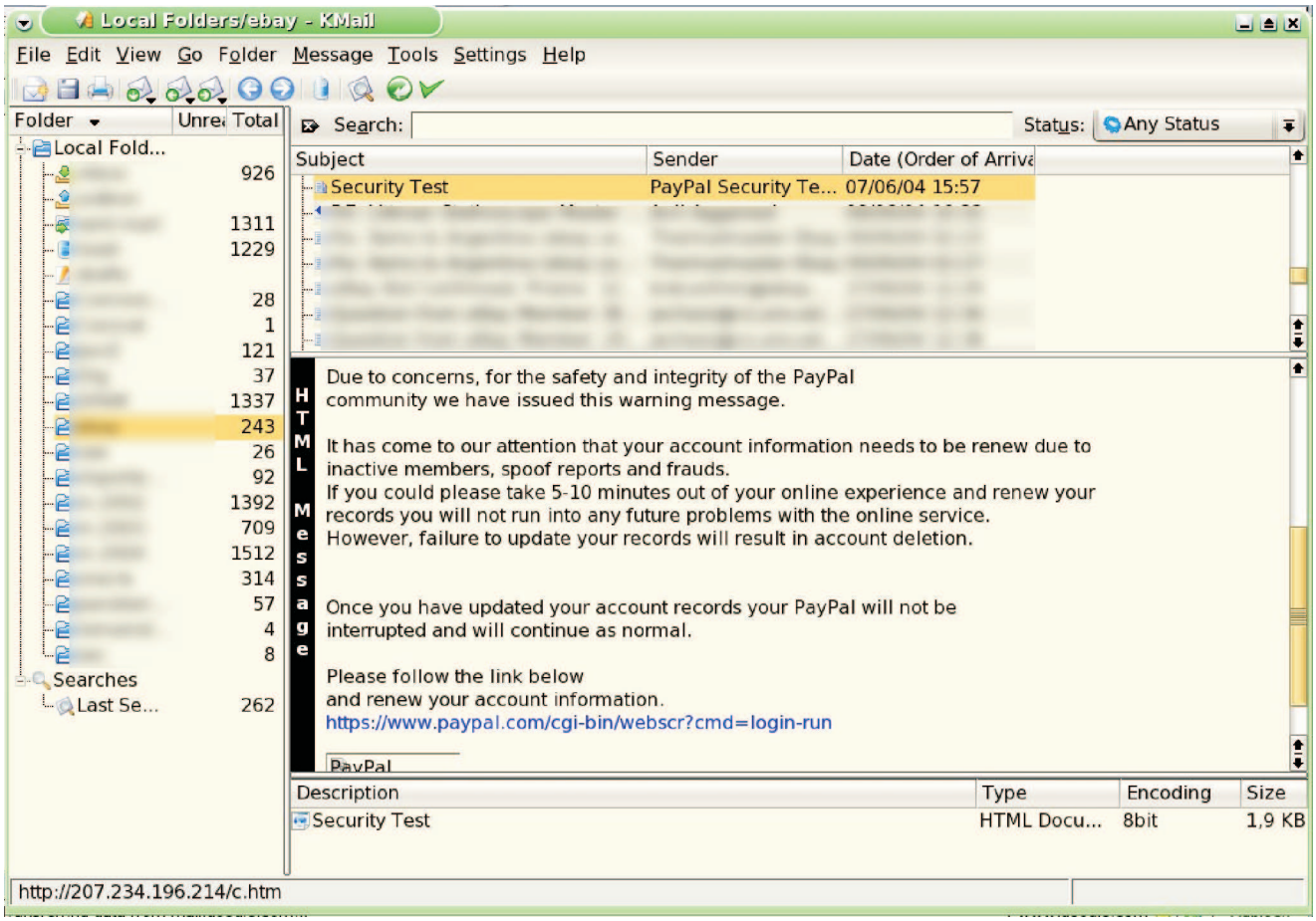

Figure 2: Fake email pretending to come from PayPal.

2.1 Exploited Weaknesses

Let us explore a little deeper into why phishing attack works. User's lack of knowledge about this kind of attack is probably the highest responsible to the success of phishing. Since users can not differentiate between the true and a forged email or web site, they usually provide their personal data.

Another important reason is the handiness to email addresses. Attackers can easily get access to huge data banks of email addresses, therefore they can quickly reach a large number of potential preys. These email data banks are composed by random users or customers of a specific bank. Of course since the former are easier to get some attackers simply send the same fake email to everyone they can, including persons that are not related with the intended financial organization. In this case, even when the target will surely discover the deceive, the attacker is confident he will catch some victims.

Ease of use of technology also contributes to the success of this attack. Current web technologies allow attackers to quickly build and deploy a bogus web site. This technique is trivial if we compare it with the creation of viruses, worms, trojans and the like. The attacker just needs to tempt users to visit this bogus web site, which is effectively accomplished through a fake email (or sometimes through some instant messaging service).

The existing defects in the email related protocols, designed in a computing age when security was not necessary, provide even more help to the phishers. For example, attackers can easily modify the `FROM` address in an email header to make it look from a real source.

The main techniques [Oll04] used within phishing emails are:

- Official looking and sounding emails.
- Copies of legitimate corporate emails with minor URL changes.
- HTML based email used to obfuscate target URL information.
- Standard virus/worm attachments to emails.
- A plethora of anti spam-detection inclusions.
- Crafting of "personalized" or unique email messages.
- Fake postings to popular message boards and mailing lists.
- Use of fake "Mail From:" addresses and open email relays for disguising the source of the email.

Also there are simple HTML web programming methods used to trick users. Consider the HTML statement given below:

```
<a href= http://bogussite.com> https://realsite.com </a>
```

This code[1] inserts a URL link into a web page, and since most email clients can interpret HTML code, this also works in emails[2]. The user views the link as `https://realsite.com` but on clicking the link he/she is taken to `http://bogussite.com`. Besides this, there are other URL obfuscation techniques that can be used to obscure the final destination displayed in the browser. Some of the most used tricks include:

- Lower-case Ls replaced with upper-case Is. This is used to help bypass many standard anti-spam filters, and in most fonts fools the recipient into reading them as Ls.
- Hidden within the HTML email there can be many random words. These words are usually set to white (on the common white background of the email) so they are not directly visible to the recipient. The purpose of these words is to help bypass standard anti-spam filters.
- Within the HTML-based email, the URL link can be obfuscated using an escape-encoded version URL.

The idea is to make the user see the correct web site name displayed in his/her browser, whereas he/she might be going to a completely different bogus web site.

Some recent browser vulnerabilities have introduced more problems for the naive user. For example the Internet Explorer URL spoofing vulnerability[3], which allows the attacker to change the address displayed on the address bar of the browser when displaying a fake web site. For instance, consider the following URL:

```
http://www.realsite.com%01%00@bogussite.com/
```

If this link is followed, the address bar in the browser will only display `http://www.realsite.com`, while on the contrary the user will actually go to a page located on `bogussite.com`. This vulnerability is produced by an incorrect interpretation of URLs that contains special characters, such as %01 and %00. To solve this vulnerability the user needs to apply a patch released by the vendor.

Often, the web is a protective (anonymous) place for these kind of attackers. They can quickly launch a phishing attack and easily cover their traces. Anti-spam software and content filters can not stop phishing emails in an effective way. Moreover, most of the currently online web applications ain't anti-phishing features. All these reasons together are helping to the tremendous growth in phishing attacks.

[1] Href is probably one of the most used attributes of anchor.

[2] Besides it is common the use of web browser as email clients on systems that implement an IMAP or POP based webmail.

[3] `http://security.openwares.org/`

3 How Not to Get Hooked by a Phishing Attack

Since the phishing problem is rather new the defenses are still in their first stages. The best solution is to combine different mechanisms. The following subsections describe techniques that can be used by organizations, specially banks, to avoid these worrying attacks. The customers' side is also considered.

3.1 Security Controls in Web Applications

There are controls able to help mitigate phishing attacks. These controls should be part of any financial related web application. The first line of defense should include an enhanced authentication method in web applications. Username/passowrd based authentication schemes are not enough for important, money related, web sites. Client certificates or hardware tokens should be used.

The three components of authentication are commonly expressed as:

- What you know: a password or PIN
- What you have: a security key or token.
- What you are: a fingerprint, retinal/iris scan, etc.

While the third factor remains exotic for most purposes, a combination of "what you know" and "what you have" is usually adequate for protecting sensitive information.

Hardware Tokens

The "what you have" portion can be implemented in hardware as a physical key or token, or in software as a numeric key stored as a binary file. Software keys are convenient since they can be distributed electronically. However, a better approach to control access to crucial corporate data is to embed the security key in a hardware token.

Generically, this method provides a challenge-response system. The security server generates a numeric code, which is usually displayed on the user's screen as a bar code, a "challenge" the client must answer before gaining access to the secure system. Then the bar code is read and it is generated an appropriate cryptographic response, which appears as a numeric code on an LCD screen, and which the user must type into the computer before gaining access to the application.

Figure 3: Hardware token used as a keychain.

Now anybody having remote access to the organization (using the web site) has to have three things: the user ID, a password and the challenge-response token. The challenge is a random number fed into the hardware token device to generate a new random response. Then we can be 99 percent sure that the person getting into our system is authorized to do so, since the hardware token provides a second and extra level of certainty, avoiding among others the phishing attack. A token can be used from any workstation, including office, laptop or home computers.

On a per-user basis, the remote site is able to know exactly what users are doing, assuring "non repudiation" as an useful side effect. This way, since the token can not be faked, the customer can not deny his/her financial transaction.

Of course the introduction of hardware tokens can induce some resistance. There's a learning curve involved with everything, but the tokens are easy to use. The only problem they present is its size, they are bulkier than, a credit card for example, so it isn't something that people can just stick in their wallets and carry around. But it is something that people can carry attached to a keychain, and the authentication security gets improved, since now the phisher needs the token to be authenticated successfully besides the much more easy to get username and password.

Smart Cards

A smart card, or integrated circuit(s) card (ICC), is defined as any integrated circuitry embedded into a flat, plastic body. Although there are a diverse range of applications, there are two broad categories of ICCs. Memory cards contain only non-volatile memory storage components, and perhaps some specific security logic. Microprocessor cards contain memory and microprocessor components.

The standard perception of a "smart card" is a microprocessor card of credit-card shaped dimensions (or less, e.g. the GSM SIM card) with various tamper-resistant properties (e.g. a secure cryptoprocessor, secure file system, human-readable features) and is capable of providing security services (e.g. confidentiality of information in the memory).

Figure 4: Smart card used for health related payments.

In web applications that support smart cards only a user having the correct card may get access. Since a phisher would not have a legitimate smart card he/she would be denied access to the application even if he succeeded in getting the personal information we already mentioned in Section 1. The problem with smart cards is the additional infrastructure required to implement this solution. The infrastructure overheads originated by smart cards is significantly more important than that caused by hardware tokens devices.

Web Page Personalization

Using hardware token devices or client certificates may require various changes in the existing web application; as such these are more pertinent for any new application that is being developed. Already developed applications can introduce other simple solutions to decrease the hazard of phishing.

One simple capability that can be built is to make it difficult for attackers to impersonate a site. In this sense it is possible to personalize the web application for the users. Web sites can use two pages to authenticate the users. The first one can ask the user to provide only the user name. On receiving a valid username the user is given a personalized page for entering password. The second page can be personalized based on some user provided phrase or a user chosen image, etc. It would be troublesome for a bogus site to provide the second page.

Personalization of web pages can also be accomplished in other ways. Client side persistent cookies can be used to present a personalized login page to the user. When the user logs in for the first time, the application can set a cookie with a simple personal but non-confidential string (e.g. user's first name). Next time the user logs in, the applications can greet the user with this string before he logs in. A phishing site will not be able to read the cookie containing the string, if it is limited to the right

domain. Therefore, the user will not see the greeting string and would discover that the site is not the real one. The success of these methods again basically depends on the carefulness of the end user.

3.2 Implementing Secure Internal Processes

Banks handle sensitive information of their customers, both personal as well as financial details. Besides technical security controls as part of web applications, it is important for such organizations to follow secure processes while managing any customer information. Secure internal processes would help in preventing any leakage of customer information, including email addresses that may be used for phishing. This can include activities such as:

- Limit customer databases access just to authorized users.
- Make all the personnel managing customer data aware of confidentiality requirements and the risks of breach.
- Do not expose email addresses in any massive email.
- Share email addresses only with authorized marketing alliances or other organizations with alike security controls.

Security standards, such as GLBA, [Resb] can be utilized for building in the required security controls. For example the Section 314.4 of Safeguard Rules in GLBA specifies following requirements to be obeyed by financial organizations to protect customer data:

- Limit access to customer information to employees that need to know this information.
- Encrypt sensitive customer information when it is transmitted electronically over networks or stored online.

Brand Monitoring

As an extra control, the financial organizations, should also try to keep track of the use of their brand over the Internet. This would involve looking for activities such as similar domain name registration, use of brand within web pages and email spam. Today some companies like NetCraft, Verisign, Cyota, NameProtect and Envisional supply these services. This information can be used to track down suspicious activities in order to take remedial actions.

3.3 Customer Awareness

Success of a phishing attack mainly depends on the response of the users. Hence there are some security measures that need to be implemented on the user side. Some attacks can be avoided if the users are aware of the threats. Banks should take steps to make their employees and customers aware of basic security practices.

Customer awareness should be managed by banks in order to instruct them on identifying legitimate emails and web sites. Guidelines should be issued to the customers to inform them about the way the bank would communicate to them. This awareness session should be conducted periodically and in a way that is easy for the end user to understand. Guidelines can be provided in the form of documents that are given at the time of customer registration. Guidelines can also be displayed as security instructions on the web site and shown to the user before he/she logs on. Figure 5 shows the real page of the bank of our first example presenting these guidelines to their customers at the lower right corner (Online Fraud Prevention Center). This information often include informing the customers about the kind of emails that will be issued to them and what can be false (hoax) emails. Specifically the users should be warned that:

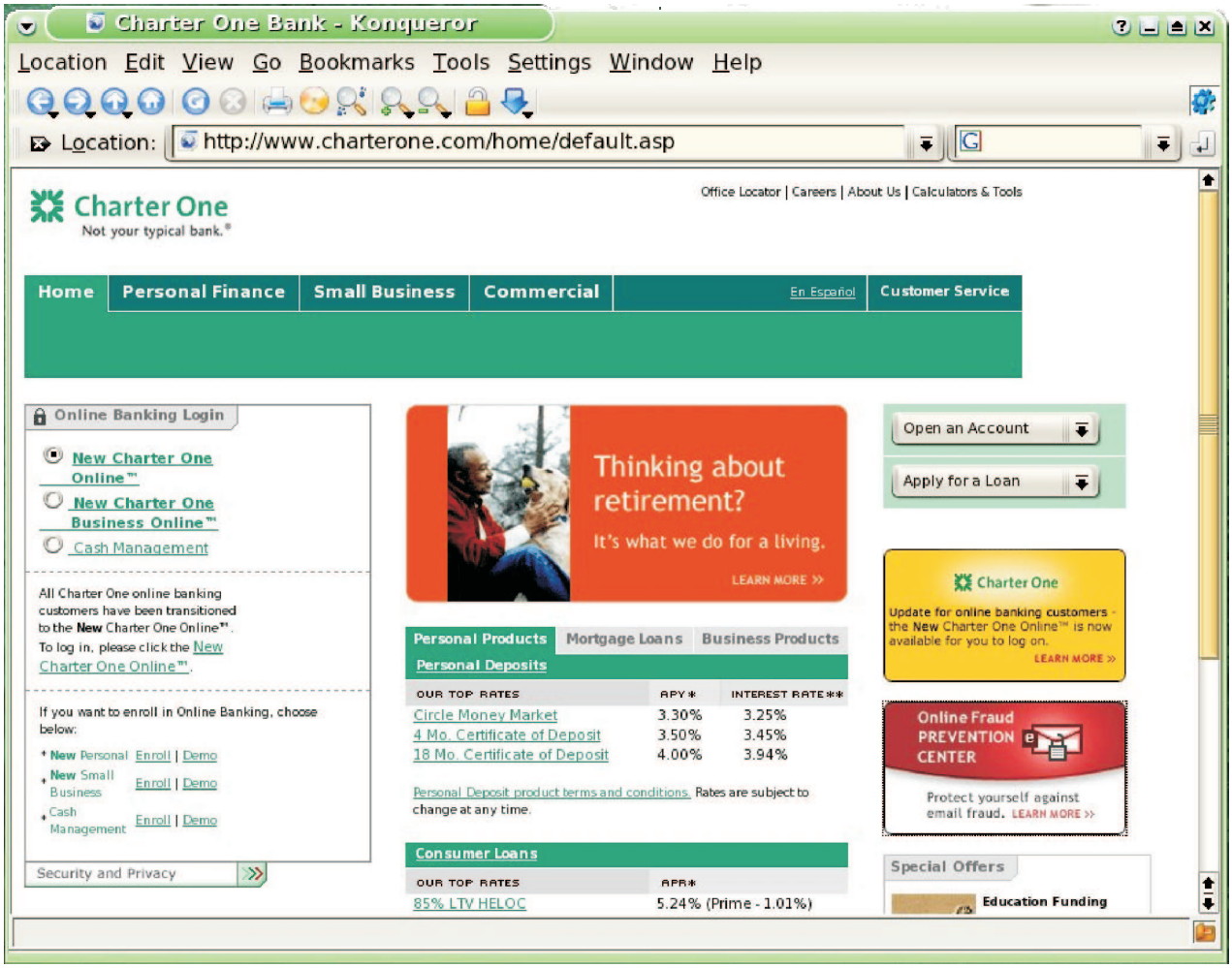

Figure 5: Genuine Charter One website site presenting security guidelines for their customers.

- They would never be asked to provide their username, password, credit card number, full name, bank account number, etc. by email.
- That the emails would not contain any embedded links or asks the users to fill information in forms.
- Email from the bank would never ask the users to download software program from other sites or ask them to go to other sites apart from known banking sites.
- That they should always visit the web site by directly typing in the address in the browser and to look for secure website indications (https connection and lock icon) when submitting username, password, credit card number or other sensitive information via the Web browser.
- Users should be suspicious of any email with urgent requests for personal information.

The customers must also be informed about other security good practices, which can include:

- Keeping the browser up to date with all the security patches applied.
- Having a well configured personal anti-spam and anti-virus software on the computers.
- Using a simple pop-up blocker to help in stopping automatic execution of malicious code.

- Using anti-spyware tools to remove any lurking malware from the computer.

The risk of phishing would be lessened a lot if the users are able to identify fake emails. Use of digital signatures, for instance utilizing PGP [CDFT98] or S/MIME [DHR+98], is a good option to differentiate a fake email from the real one (by using this tools the sender is now authenticated). As far as possible banks should digitally sign all customer communication through emails and inform them on how to identify a valid signature. The public key required to verify the bank's signature can be provided to the user in a CD-ROM with the required instructions.

Client Side Tools

Apart from awareness sessions, users can also be provided with some simple and free browser tools such as SpoofStick, Netcraft Toolbar, ScamBlocker which can help them in identifying the fake websites.

SpoofStick by CoreStreet works on the principal of visual alert and displays the most relevant domain information of the site on the browser as shown in Figure 6. If the users are alert they would see a wrong domain name and would be able to identify a fake site.

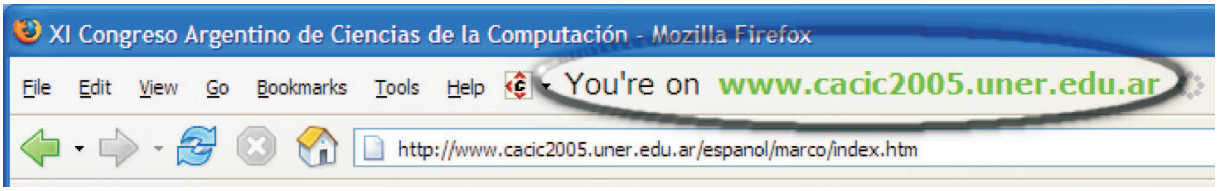

Figure 6: SpoofStick.

ScamBlocker by EarthLink (Figure 7) goes a step ahead and maintains a database of fraudulent web sites and updates it frequently, so users have a proactive solution. Users are alerted if they visit a potentially dangerous web site. These tools are not a complete solution to phishing but can help in detecting spurious web sites.

Figure 7: ScamBlocker.

The Netcraft Toolbar (Figure 8) community is a giant neighbourhood watch scheme, empowering the most alert and most expert members to defend everyone within the community against phishing frauds. Once the first recipients of a phishing email have reported the target URL, it is blocked for community members as they subsequently access the URL. Widely disseminated attacks simply mean that the phishing attack will be reported and blocked sooner. The Toolbar also:

- Traps suspicious URLs containing characters which have no common purpose other than to deceive.

- Enforces display of browser navigational controls (toolbar and address bar) in all windows, to defend against pop up windows which attempt to hide the navigational controls.
- Clearly displays sites' hosting location, including country, helping you to evaluate fraudulent URLs (e.g. the real `citibank.com` or `barclays.co.uk` sites are unlikely to be hosted in the former Soviet Union).

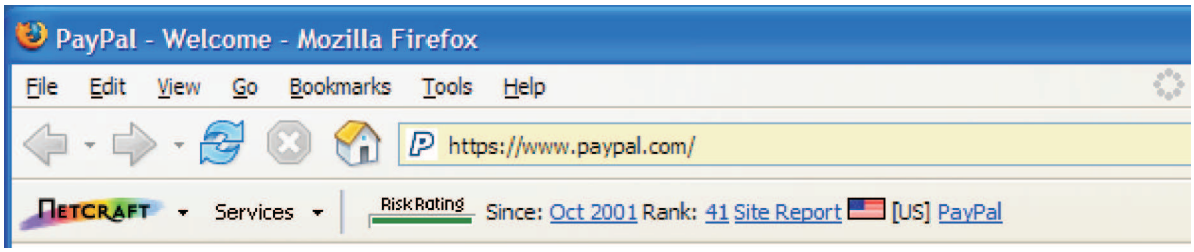

Figure 8: Netcraft Toolbar.

If a phishing website is detected it will be stopped by this tool, as we can see in Figure 9.

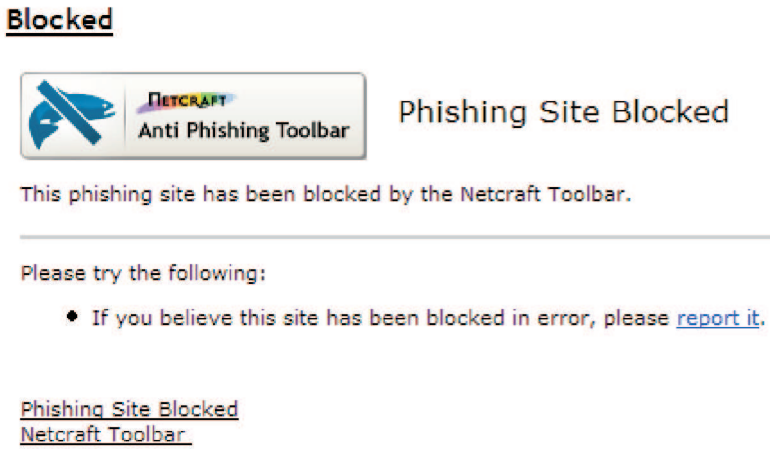

Figure 9: Netcraft Toolbar stopping a phishing website.

3.4 Contingency Actions

No solution is a foolproof solution. Companies should be prepared to reduce the impacts of a successful phishing attack. Various contingency measures should be put in place to quickly recover from a phishing attack. Banks should provide an easy to use fraud reporting mechanism to the customers and make them aware on how to report frauds. This can be through email, web page or phone. Banks should have a way to quickly contact all the customers and inform them of the safety measures that they should take in response to a phishing attack.

Applications should also have a feature to force all the users to securely change their passwords in case of an attack. Once an attack is detected the applications introduce an additional page after the login page that asks for some information unique to the user and unknown to the phishers. This can be anything like birth date, spouse name, social security number, etc. Once a user fills this, another page can come up asking the user to change his password. Thereafter the user logs on to the site as normal user in future. This additional module can be activated as soon as a report of phishing is noticed and this mechanism can stay on the site for a few months so that all users can change their password. This is a non-intrusive way to protect user and make them change their password.

The users should also take immediate remedial measures if they detect that they have received a possible phishing email. This could include activities such as:

- Informing the bank about the email and its details.
- Immediately changing the password used to logon or perform transactions.

3.5 Looking Forward

A few upcoming future technologies can help in curbing the growing phishing menace. Microsoft championed "Sender ID Framework" is one such effort. Another approach is the "Identified Internet Mail" (IIM) proposed by Cisco [Cis]. Both the proposals aim to stop forged emails from reaching the end user.

In most phishing emails the `FROM` address is modified to make it appear from a genuine source. The Sender ID Framework tries to prevent email domain spoofing. It verifies email messages to ensure that it originates from the domain from which it claims to come from. The email sender's server IP address is used to check this. The receiver's inbound mail server forwards a mail message only if it originates from the right domain.

The Cisco Identified Internet Mail is a signature based authentication mechanism to decide the validity of the mail. Using public key cryptography the sending domain signs the email, which is verified by the receiving domain. IIM can be used for signing and verification either at the domain or at user level. A policy can be implemented to decide upon the results of verification. Unsigned email messages or messages with invalid signatures can be categorized as possible phishing attack.

A few consortiums such as FSTC[4] (Financial Services Technology Consortium) and the APWG[5] (Anti-Phishing Working Group) are also working towards a solution. These groups have pooled their resources to come up with a standard framework that can be implemented by financial organizations to counter phishing threats.

In the coming time the efficiency of the anti-spam and content filter software would also improve. The number of spams and fake emails that are detected and stopped by these applications would increase, as they improve their detection signatures.

4 Conclusion

The problem of phishing does not have a single solution as of now. phishing is not just a technical problem and there is no doubt phishers would keep coming up with new methods to trick the users. Financial organizations should take care of running periodic vulnerability analysis in order to identify and stop weaknesses that can lead to a successful phishing attack. The most effective solutions will come from a combination of controls arranged by the organization and user awareness. It is essential a continuous process involving, at the same time, three aspects:

- Technical measures on the server side.
- Conduct and knowledge on the end user side.
- Secure handling of personal and financial information.

Another key to lessen the effect of the phishing problem is to add security solutions that work in combination with client-side and server-side security mechanisms[6]:

[4] http://www.fstc.org/

[5] http://www.antiphishing.org/

[6] Also helping with various other current threats.

- Automatic validation of sending email server addresses.
- Digital signing of email services.
- Monitoring of corporate domains and notification of "similar" registrations.
- Perimeter or gateway protection agents.
- Third-party managed services.

This work shows that more important than enhance communication security is to adopt a security policy that considers "good security practices". Moreover, history proves that improvement in communication security needs to break years of inertia, e.g. IPv6 [HOD98, HOD98], DNSSEC [3rd99], etc.

References

[3rd99] D. Eastlake 3rd. Domain name system security extensions. RFC 2535, Internet Engineering Task Force, March 1999.

[CDFT98] J. Callas, L. Donnerhacke, H. Finney, and R. Thayer. OpenPGP message format. RFC 2440, Internet Engineering Task Force, November 1998.

[Cis] Cisco. Identified internet mail. http://www.identifiedmail.com.

[DHR+98] S. Dusse, P. Hoffman, B. Ramsdell, L. Lundblade, and L. Repka. S/MIME version 2 message specification. RFC 2311, Internet Engineering Task Force, March 1998.

[HD98] R. Hinden and S. E. Deering. IP version 6 addressing architecture. RFC 2373, Internet Engineering Task Force, July 1998.

[HOD98] R. Hinden, M. O'Dell, and S. E. Deering. An IPv6 aggregatable global unicast address format. RFC 2374, Internet Engineering Task Force, July 1998.

[Lam05] Jason Lam. Handling phishing attack. http://isc.sans.org//diary.php?date=2005-01-21, January 2005.

[Lit04] A. Litan. Phishing Victims Likely Will Suffer Identity Theft Fraud. March 2004.

[McA04] McAfee. Anti-Phishing: Best Practices for Institutions and Consumers, March 2004.

[Mic] Microsoft. Sender ID Framework. http://www.microsoft.com/mscorp/safety/technologies/senderid/default.mspx.

[Oll04] Gunter Ollmann. The Phishing Guide. http://www.technicalinfo.net/papers/Phishing.html, September 2004.

[Resa] AntiPhishing Resources. http://www.antiphishing.org/.

[Resb] Financial Privacy: The Gramm-Leach Bliley Act. http://www.ftc.gov/privacy/glbact/.

[Resc] Financial Services Technology Consortium. http://www.fstc.org/.