

*Master Thesis in
Computer Science*
Thesis No: MCS-2007:18
September 2007



Exploring Phishing Attacks and Countermeasures

Anders Persson

Department of
Interaction and System Design
School of Engineering
Blekinge Institute of Technology
Box 520
SE – 372 25 Ronneby
Sweden

This thesis is submitted to the Department of Interaction and System Design, School of Engineering at Blekinge Institute of Technology in partial fulfillment of the requirements for the degree of Master of Science in Computer Science. The thesis is equivalent to 20 weeks of full time studies.

Contact Information:

Author:

Anders Persson

Email: one_of_all_81@hotmail.com

University Advisors:

Martin Boldt

Email: martin.boldt@bth.se

Department of
Interaction and System Design
Blekinge Institute of Technology
Box 520
SE – 372 25 Ronneby
Sweden

Web: www.bth.se/tek
Voice: +46 (0) 457 38 50 00
Fax: +46 (0) 457 102 45

Abstract

Online banking and e-commerce applications have good protection against attacks directed direct towards their computer systems. This, the attacker has considered and instead use “social engineering” attacks, such as phishing to gain access to the information inside [1] [15] [20]. Phishing is a growing problem that many different companies are trying to develop a working protection against. The number of new phishing-sites per month increased by 1363 % between January 2005 and October 2006, from 2560 to 37 444 attacks [3] [2]. Today there are several different antiphishing applications as well as implemented methods to prevent attacks, but are they giving enough protection? In this paper we plan to investigate the concept of phishing to better understand the threat it provides. We will analyse 252 different phishing attacks and examine a number of existing antiphishing applications to see if there are possibilities to improve the different protection methods to improve the accuracy of such tools.

Keywords: Phishing, Information Security, Identity Theft, Social Engineering

Acknowledgement

We would like to express our gratitude to our supervisor Martin Boldt, PhD Student in Information Security from the Blekinge Institute of Technology whose help, stimulating suggestions and encouragement helped us at the time of the investigation and writing of this thesis. We would also want to thank Millermiles.co.uk for the use of their archive of phishing attacks that we used in our investigation.

Contents

- 1 Introduction 1
 - Related work 2
- 2 Background 3
 - Phishing 2.0, oncoming versions 4
- 3 Research 5
 - First research question 5
 - Second research question 5
 - Third research question 5
- 4 Result 6
 - First research question 6
 - The e-mail 6
 - Targeted companies 10
 - Targeted information 11
 - The website 12
 - Second research question 14
 - Third research question 15
- 5 Discussion 17
 - First research question 17
 - Second research question 18
 - Third research question 18
- 6 Conclusions 20
- 7 Further research 21
- References 22

1 Introduction

There are different theories of where the “ph” in phishing (pronounced same as fishing) comes from, G. Ollmann believes that it originally comes from the early hacker naming terminology such as “Phreaks” who often were involved in “phreaking” i.e. hacking telephone systems [15]. D. Watson and his colleagues on the other hand states that the “ph” stand for “password harvesting fishing” [20].

Phishing is today a common method for hackers and other malicious people to collect different kinds of sensitive information. Phishing is a kind of “social engineering” attack, where the attacker extract sensitive information by tricking the user, instead of extracting it directly from the computer system [1] [15] [20]. The collected information is often personal information or authentication credentials used to login to different sites, however it can also be sensitive financial data [15] [20]. The collected authentication credentials can thereafter be used by hackers or other malicious people to impersonate the victim to pursue a crime in near anonymity. The collected information, called “phish”, can either be used directly by the people who collected it or be traded as a form of electronic currency, for example against a piece of hacking software or warez, (pirated copyrighted content such as applications or games) [15].

Phishing started as e-mails written to convince the target to reply with the information asked for. This is still the most common type to initiate phishing attacks, but today phishers use several different ways to collect the information they require. Copied websites, Trojans, key-loggers and screen captures are just a number of different methods they use today [8] [15]. By initiating phishing attacks by e-mail the attacker can reach a vast number of specified victims using limited resources. 2004 APWG (Anti Phishing Working Group) concluded that as much as 5 % of the phishing e-mails sent out were to succeed, therefore the more e-mail sent out the more successful attacks [15]. That’s why most phishing attacks initiates with an e-mail sent out in the same quantity as regular Spam. The phishers often turns to specific individuals and can buy lists with authentic e-mail addresses fitting their credentials by the same sources as Spammers do [15] [20]. E-mails are today easy to configure to look like they come from a certain company and by spoofing attacked links (implement the link to view the correct URL but sending the victim to a fraudulent) they can even send the victims to false websites without their knowledge [15] [20]. Therefore the users never should reply to such e-mails or follow a URL (Uniform Resource Locator) in the e-mail, but should instead type in the address themselves or follow a bookmark. Many phishing attacks rely on spoofed e-mails to fool the victim to a fraudulent website where the attacker collects the information the victim inserts [7] [15] [20]. Fraudulent sites and suspicious e-mails can be difficult to recognize but there are a number of things that can be revealing e.g. the design of the email and the URL on the website. Later on I will further explain and discuss both suspicious e-mails and websites and most of all what the public should be aware of. If there is a suspicion of a phishing attack the user should contact the company that appeared to send the e-mail. It is however important to do so through the company’s actual e-mail or by phone and not by responding to the suspicious e-mail that was sent out. Or report the scam to one of the different antiphishing organisations e.g. millermiles.co.uk.

Several companies has realised the threat that phishing really brings out and has designed different methods as well as systems to counteract the attacks. None of these “antiphishing” products provide a total protection, and probably none ever will. To quote Bruce Schneier - *“There’s no such thing as absolute security.”* [17]. The best defence against any phishing attack is for the users’ to be alert and to know what to look after [15]. The biggest problem is that the users are too careless to observe even the most obvious signs of a phishing attack [7]. Some users responding to the threats of phishing attacks installs antiphishing programs and then feel more or less completely secure. But there is no 100 % protection against phishing attacks, although one of the main assignments of an antiphishing system is to make the users feel safe. The result of users feeling too safe is that they tend to act careless and might then more easily fall for possible attacks that have escaped the antiphishing application [17].

One thing the users should be aware of is that no company, in their right senses, would ever send out an email asking for the user to send or re-enter sensitive information such as authentication credentials, credit card numbers or personal information. They would rather contact the users by other means due to security issues.

Related work

There are already a few studies regarding phishing. Dhamija, Tygar and Hearst made in April 2006 an extensive study of how 22 participants observed different signs of phishing-sites and which visual signs that was noticed [7]. The participants were asked to study 20 different websites to see if they could see if it were fraudulent or authentic. The result of this study showed that age, sex and computer habits didn't make much difference. They even noticed that pop-up warnings of invalid signature of the sites and visual signs of SSL (Secure Sockets Layer), padlocks etc. were very inefficient and were overlooked by 23 % of the participants. The participants failed to guess if the site were fraudulent or authentic on average 40 % of the viewed sites.

In February 2007 Schneier published a draft of a paper regarding the psychology behind security and the human aspects of being and feeling secure [17]. Declaring that all security issues are about "trade-off"; meaning that all security is connected to a cost. Home security products come with an increased cost of being forced to carry a set of keys at all time, the cost of security against phishing can include the need of install an antiphishing program and to be more alert while surfing the web. He also discussed how the cost of being secure can alter based on the amount of threat that the users perceive. Previous victims of a phishing attack are more likely to pay a certain amount of money to be able to feel more secure against similar threats than persons who never encountered a phishing attack before.

"The Phishing Guide" by Ollmann from 2004 gives a detailed understanding of the different techniques often included in phishing attacks [15]. The phenomena that started as simple e-mails persuading the receiver to reply with the information the attacker required has evolved into more advanced ways to deceive the victim. Links in e-mail and false advertisements sends the victim to more and more advanced fraudulent websites designed to persuade the victim to type in the information the attacker wants, for example to login to the fraudulent site mimicking the company's original. Furthermore, even advanced techniques such as Trojans, key-loggers and screen grabs are becoming more frequently used [15]. Ollmann also presents different ways to check if websites are fraudulent or not. Except inspecting whether the visited site really is secure through SSL (Secure Sockets Layer) [7], the user also should check that the certificate added to the website really is from the company it says and that it is signed by a trusted-third-party. Adding more attention to the URL can also often reveal fraudulent sites. There are a number of ways for the attackers to manipulate the URL to look like the original, and if the users are aware of this they can more easily check the authentication of the visited site.

Watson, Holz and Mueller describe in their *white paper* "Know your enemy: Phishing" different real world phishing attacks collected in German and United Kingdom honeynets [20]. Honeynets are open computer networks designed to collect information about different attacks out in the real world, for further forensic analysis. They noticed that phishing attacks using vulnerable web servers to be hosts for pre-designed phishing-sites are the far most common compared to using self compiled servers. A compromised server is often host for several different phishing-sites. These sites are often only active a few hours or days after downloaded to the server. Watson and his colleagues were able to describe a couple of real phishing attacks in detail. They noticed that phishing attacks often worked under a network of compromised servers which made it possible for the attacker to redirect traffic from one server that been discovered and closed down to another. In those cases the phishers use one central server to redirect traffic to several different servers holding the actual phishing-sites. Even if the central server is discovered and closed down the phisher just implement another compromised server to be the new central for redirecting the traffic to the servers still online. This is a clear sign that most phishers is not just people playing around but are instead organised groups working together. For the phishers to transfer the stolen money abroad to their own pockets they often need to use people in the same country as the scam is performed, if they send the money directly out of the country the banks will register it and the risk of detection increase.

In the next chapter we will look into the details of different kinds of phishing techniques to learn how to detect them.

2 Background

In 1996 the term “Phishing” started to popup in different hacker newsletters. It appeared that AOL (America Online) had changed their ways to create new accounts that hindered hackers to create new bogus accounts using false credit card numbers [15]. To get hold of other user’s authentication credentials, phishing e-mails were used. These e-mails were designed to fool the victim by claiming there been a security breach in the system and the users passwords needed to be re-entered to the system by responding the e-mail [20]. Several of the earlier phishing attacks were not that hard to discover because the bad spelling and pore language, they often asked the victim to reply the wanted information directly through the e-mail which made victims suspicious. To make the victim answer before they had the time to reflect over the language and spelling in the e-mail the phishers often made the e-mail sound urgent and threaten with deletion of the victims account on the site if not answered directly [9]. Today phishers, besides being more careful with their language and spelling, use more advanced ways to trick the victims. Often they use fraudulent websites that are designed to look like the companies original by copying the design and content [15] [20]. These sites can easily be hosted by compromised home PC’s or web servers and can use similar or disguised URL to look even more authentic [15] [20].

As more users’ gets familiar with phishing attacks the attacks themselves develop to look even more authentic. By making the e-mails look more like the ones the company sends out by both design and language and by masking the link pointing to the fraudulent website in HTML-code with the original site’s URL, the attackers makes it harder for the victim to detect fraud [15]. Today it is easy to copy the content and design of a company’s website, but it is harder to copy the URL. By disguising the URL or making it look more like the original by different methods it can be hard for an untrained eye to notice anything different. By using different obfuscation techniques the phishers make the URL look more alike the company’s original [15]. An easy example is to use “http://www.my.bank.com” or “http://www.my-bank.uk” instead of the original “https://www.mybank.org”, another trick is to use capital “I” or the number “1” instead of lower-case “l”, “r” and “n” instead of “m” and so on [7][20]. The site can even use JavaScript and CSS (Cascading Style Sheets) to hide the real URL with a picture presenting the original URL [9]. Most companies have their eyes on URL’s that are similar to theirs to quickly shut them down when used by phishers. Phishing site’s URL can also become an item at antiphishing organisations database over known phishing-sites (“black-lists”), later be used by different antiphishing systems and applications hindering users to be sent to the fraudulent site [9]. Websites requiring authentication credentials need some kind of encryption for the HTTP-traffic, to avoid passwords and other sensitive information being sniffed. SSL (Secure Sockets Layer) is a well established encryption to HTTP-traffic (HTTPS); this technique is used on most secure sites. To show the traffic is secured by SSL (HTTPS) the browsers inform the users by using icons (padlocks), background colour to the URL and so on. The padlock icon has been used on secure sites for a long time and the sight of a closed padlock often gives the users a more secure feel of the website [17]. To make the victim feel secure on their fraudulent site phishers often insert padlock-icons on the webpage or hides their insecure URL (HTTP) with the original secured URL (HTTPS) [7] [9]. If the phisher have implemented a website using SSL connection they are not able go get a valid certificate to verify the sites authentication. Websites using SSL connections are supposed to have a valid certificate belonging to the actual site, signed by a third party to validate the authentication of the site. If the websites certificate is invalid the browser popup a warning informing the user that the website’s SSL-certificate is invalid and that the site may not be authentic. A large part of the certificates today are invalid, some might be too old or self signed. The result is the users getting too used to the warnings and often clicks OK before realising what the warning is for. The security the certificates are supposed to provide the users, are therefore very inefficient and the HCI (Human Computer Interaction) needs to be overlooked.

If the users don’t pay any attention to the URL, SSL indicators and the authentication of the certificates they can easily be sent to a false site without noticing it [15]. The reason most victims falls for phishing attacks is because they don’t pay enough attention to the obvious signs or don’t see the difference between authentic or fraudulent SSL [7]. But even users with high computer knowledge have trouble to recognise a good phishing attack, even if they know exactly what to look for, it can be difficult to be certain if it is fraudulent or authentic [7].

Phishing 2.0, oncoming versions

“Pharming” uses DNS-poisoning to send the victims to the fraudulent website even if they type in the correct URL, the DNS translate the correct URL to the fraudulent IP-address [11]. Instead of using e-mails and spoofed links to lure victims to the fraudulent website pharmer either reconfigure the victims web browsers DNS-configuration or hijacks the DNS server [11] [19] [20]. “Local-pharming” is when the attacker reconfigures the victims DNS-configuration in their web browser; this is often done through some kind of spyware or even Trojans, virus- or worm attachments [12]. “Full scale pharming” is when the attacker hijacks the company’s or ISP’s (Internet Service Provider) DNS server; this makes all the users on their network victims whenever they try to enter the specific website. To hijack and reconfigure a DNS-server is very complex and takes a lot of knowledge and effort. That’s probably why pharming still is quite uncommon. Still, pharming is both harder to discover and to protect you against compared to phishing. The only good way to discover these attacks is for the user to notice that they are sent to a fraudulent URL or by checking the certificate of the site and make sure it belongs to the right company and that it is signed by a non related third party [9] [11] [19]. To hinder DNS-poisoning we need to make the traffic between the DNS servers secure. There are already a protocol called DNSSEC that encrypts the traffic between the DNS servers, but this protocol is so complex that it is hard to implement it in the real world [11].

“Vishing” is a new kind of attack similar to phishing in the way it tricks the victim to give away sensitive information. Vishing is a social engineering attack based on the bank-services through the telephone system. Vishers use a *war dialler* configured to dial all numbers in a given area. The person answering is informed that his/her credit card is fraudulent used and are encouraged to dial a given number. If the victim dials the number, they are instructed to enter their credit card number, three digit CVV security code and other identification credentials. After a complete call the visher has all the information needed to use the victim’s credit card [10].

In the oncoming chapter we will do a number of examinations to understand which techniques today’s phishing attacks use and how well the most used antiphishing applications can discover them.

3 Research

By investigating a number of phishing attacks we will give a statistic view of which phishing techniques that are most commonly used. By examine a number of existing antiphishing applications and systems we can get a better understanding of how these systems are designed. And by comparing these results with the results regarding phishing techniques we might find ways to improve them.

First research question

Research question: How have the phishing techniques and the use of the different techniques evolved since the beginning of phishing?

Method: We collected information from 252 different phishing attacks and build a statistic view of them based on different credentials such as; convincing techniques, targeted information, visible signs and so on. By collecting statistic information from 6 randomly selected attacks in every month from January year 2004 to June year 2007 we can give a correct view of what kind of different techniques phishers use to convince and trick the victims. We can even see how the different techniques developed and which are the most commonly used today.

The collected information comes from *Millermiles.co.uk* who collects information of every attack reported to them. Each attack we compared with different credentials based on targeted information, visible signs in e-mail, semantic/syntactic convincing techniques, the use of known vulnerability's, the websites design, URL format and security implementations. The name of the targeted company and the country hosting the fraudulent website were also included. Each piece of information was inserted in a Microsoft Excel file, were each column represented one attack and techniques/signs were represented in individual rows. For each attack, every visible sign and used technique were marked in the table with a "1". After investigated all attacks we were able to create graphs and calculate the number of times the different signs and techniques were used totally and for each halfyear.

Second research question

Research Question: Which techniques are most used in today's antiphishing applications and are they able to discover all attacks regardless used phishing technique?

Method: By examining a number of the most used antiphishing applications today and the methods they use, we can discover possible flaws and hopefully come with improving solutions. We selected 4 of the most used antiphishing applications (chosen after number of downloads on Download.com [4]) and checked on the developers website after technical information. By that information we could compare the different methods used to thwart phishing attacks. We also studied previous investigations regarding the functionality of today's antiphishing applications.

Third research question

Research Question: How can the antiphishing applications be improved to more efficient discover new phishing attacks?

Method: We compared the result from our previous research to see if all phishing techniques we encountered can be thwarted by today's antiphishing applications. Antiphishing applications use different techniques to discover phishing attacks, we compared the signs the antiphishing applications were design to discover with the signs and techniques we encountered in phishing attacks in our previous investigation.

4 Result

First research question

After analysing the collected information of 252 different attacks (during the time of January 2004 to June 2007) allowed us to get an extended view of how the attacks evolved. Information regarding phishing websites weren't always available because *Millermiles.co.uk* weren't able to investigate the site before it went offline. 121 (50%) of the 242 bogus websites we were to investigated were taken offline before they got reported. Therefore the statistics regarding targeted information and the design of the website aren't entirely complete.

The e-mail

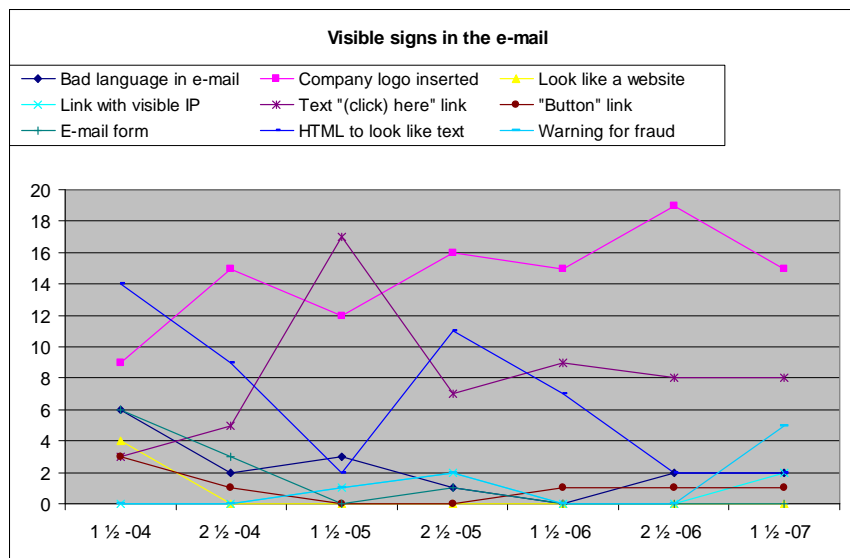


Fig. 1: Signs of fraudulent e-mail, based on 36 attacks per halfyear.

In most attacks we investigated we could find some sign that it wasn't an authentic e-mail. The signs could be everything from the design of the e-mail to the language used. The most common visible sign was by far when the phisher had attached an image of the company's logo in the e-mail to make it look more authentic, see figure 1. This is a simple way to copy the appearance of the company's e-mail without entirely copy their design. Not all companies have an exclusive design of their e-mail, but those with a logotype simply attached can easily be copied and can therefore be considered more suspicious. The most obvious sign we encountered was e-mails with bad spelling and language. If it were authentic the author of the e-mail wouldn't be long at that company.

Explanation of figure 1:

- "Bad language in e-mail" was more usual in early phishing scams but has decreased thereafter and is quite uncommon today.
- "Link with visible IP" can seem like a clear sign of a fraudulent link, but it is still used in a number of attacks. The phishers using this technique aren't just too lazy to spoof the link but rely on knowledge that most users don't know what the URL stands for or what IP numbers are. At the same time the link isn't spoofed and don't create warnings in e-mail clients and/or spam filters.
- "E-mail form" was a common technique in 2004 to collect the requested information without relying on a fraudulent website. Over time the users became more aware of the existence of fraudulent e-mails and were informed that the companies would never request that kind of information through e-mail.
- "Company logo inserted" is a very common technique to make the email seem more authentic. Most companies' use more advanced design in their e-mails for making it harder to copy the design. An e-mail with only a logotype attached to the body of the e-mail is too easy to copy and therefore can be considered as a cause to be more suspicious.

- “Text (click) here link” is another technique to avoid spoofing the link which can create warnings on different e-mail clients and spam filters. Instead of viewing an URL in the link the phisher choose to implement the link with simple text.
- “HTML to look like text” was a common technique until the beginning of 2007. By making the e-mail look like a simple text mail, spoofed link seem less probable.
- “Look like a website” were a technique used in 2004 but weren’t used there after. By making the e-mail look more advanced by designing it after the company’s website, the phisher hopes to convince the victim of its authenticity.
- “Button link” is another technique for sending the victim to the bogus website without spoofing the link. By using a button (same as in a webpage) the phisher avoids spoofing the link and in the same time makes it look more advanced to seem more authentic.
- “Warning for fraud” were only used a few times under 2005 but increased rapidly in 2007. By warning for fraud in the e-mail, phishers hopes to make the victim less suspicious.

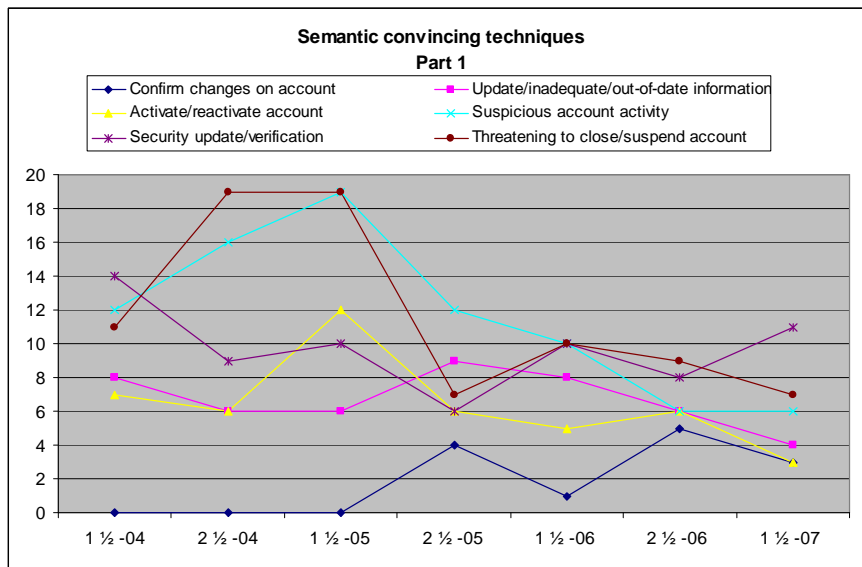


Fig. 2: The development of “semantic convincing techniques” in phishing e-mail, based on 36 attacks per halfyear. First graph showing techniques regarding the users account.

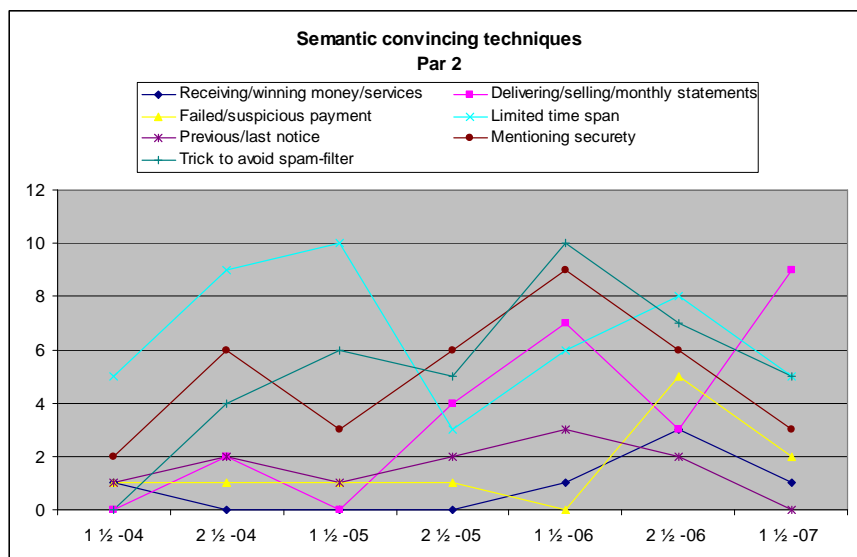


Fig. 3: The development of “semantic convincing techniques” in phishing e-mail, based on 36 attacks per halfyear. Second graph showing the remaining techniques.

“Semantic Convincing Techniques” represents the different ways the phishers tries to convince the victim to follow the instructions without paying to much attention to the possible flaws in the e-mail. Most

semantic techniques are in some way designed to convince the victim that there is some problem with their account, which needs urgent attention e.g. suspicious account activity or new security updates. The most common semantic techniques were; “threatening to close/suspend account”, “suspicious account activity” and “security update/verification”, see figure 2. To clarify we divided the semantic techniques in two different graphs, see figure 2 and 3. In these figures it is showed that the spread of use between the different techniques has decreased the last year and a half. This shows that the phishers use all techniques equally much and has not specialised on any specific one. “Delivering/selling/monthly statements” has in contrary to most other techniques increased the last halfyear. This because the attacks against e-bay has changed technique from claiming suspicious account activity and security update/verification to more often trick the users by bogus sales, to cause less suspicion.

Explanation figure 2:

- “*Confirm changes on account*” were used first in the second half of 2005. Here the phisher claims that there have been changes on the victim’s account that might have been made by intruders. To check their information is correct, the victims are tricked to logon to the fraudulent site.
- “*Activate/reactivate account*” is a technique were the phisher claims that the account already has been deactivated or the access has been limited, often used in relation with “suspicious account activity”. To reactivate the account the victim needs to follow the link to the fraudulent site and insert the information required.
- “*Security update/verification*” was in the beginning of our investigation the most popular technique but has decreased over time to be replaced with “threatening to close/suspend account” and “suspicious account activity”. Under the first half of 2007 this once again increased to become the most used technique. By claiming the information on the company’s system needs to be updated or verified to be more secure, the victim’s are tricked to insert the information required.
- “*Update/inadequate/out-of-date information*” has been frequently used in our investigation; it increased some under 2005 and 2006 but decreased again in 2007. By claiming the information on the company’s system is inadequate and needs to be updated to function the victim’s is tricked to insert the information required.
- “*Suspicious account activity*” is one of the most used techniques found and it was used in over 50% of the attacks in the fist half of 2005, but has then decreased. By claiming there has been suspicious activity on the victims account, the victim is tricked to enter the fraudulent site and insert the information required.
- “*Threatening to close/suspend account*” is also a popular technique and is often used in relation with “suspicious account activity” and “security update/verification”. This is a technique to stress the victim to follow the link to the fraudulent site.

Explanation figure 3:

- “*Receiving/winning money/services*” is a technique to entice the victim with money or other prices to trick the victim to insert the required information to receive their price.. Were used a few times in the beginning of 2004 but became more frequently used first in 2006.
- “*Failed/suspicious payment*”, by tricking the victim that there is a suspicious payment connected to their account, the phishers hopes the victim will follow the link to check they haven’t lost any money and that their information on the account is correct. The technique increased in the second part of 2006 but decreased again in 2007.
- “*Previous/last notice*” by convincing the victim that there have been previous messages and that this is their last notice before their account is suspended, the phisher stress the victim to answer before thinking it through. Has been used frequently until the end of 2006.
- “*Trick to avoid spam-filter*” there are different techniques for the phishers to avoid spam-filters. Often the whole e-mail consists of an image to avoid the spam-filter to check the containing text. Another trick is to imbed the link in an invisible image covering the e-mail and in this way avoid the link to be checked. If the e-mail is marked as spam the victims will not read them and the scam has failed. Was used first in the second half 2004 and were well used until the end of 2006.
- “*Delivering/selling/monthly statements*” is a technique often connected to online shopping (e.g. E-bay and PayPal) were a false sale tricks the victim to visit the bogus website. This technique has been well used since the second half of 2005 and is one of the leading techniques today.

- “*Limited time span*” by limiting the time span the phisher hopes that the victim will respond directly without paying attention to the possible signs of an phishing attack. Has been well used under the first and second half of the investigation but decreased in the second half of 2005 and in 2007.
- “*Mentioning security*” is a trick to give a false sense of security and thereby seem more authentic. Has been well used under the whole investigation but decreased during the last year.

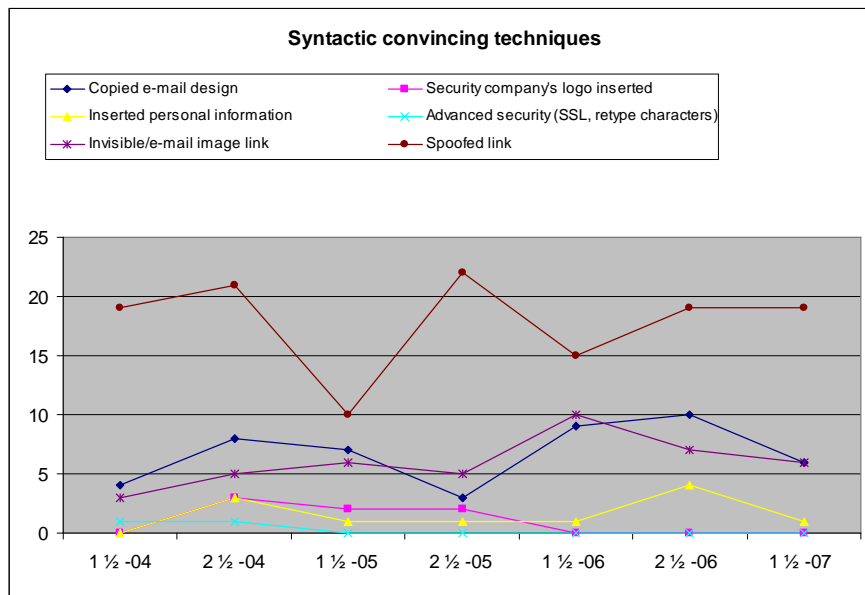


Fig. 4: The development of “syntactic convincing techniques” in phishing e-mail, based on 36 attacks per halfyear.

“Syntactic Convincing Techniques” represents different techniques used by the phishers use to make there scam look more authentic. The most common technique is to spoof the link to the phishing site in the e-mail. In early phishing attacks this was often done by designing the e-mail in HTML-code to look like regular text mail and in this way make the link less suspicious. Today the phishers often disguise the real link with the original URL, “spoofing”. This can though create warnings in spam filters and e-mail clients. Some phishers tries to circumvent spam filters by constructing the whole email as an image since it is rendered impossible to analyse the text. Another technique is to cover the whole e-mail with an invisible image containing a link to the bogus website. This way the spam filter can’t check if the link is authentic or not. Even if these techniques seem like efficient ways to avoid spam filters, they are not used that often yet, see figure 4.

Explanation of figure 4:

- “*Copied e-mail design*” is when the phisher has tried to copy the original company’s e-mail design, and not only attached a company logo. Phishers hopes that if the e-mail looks authentic enough, the victims will be fooled. It’s a relatively frequently used technique.
- “*Inserted personal information*” e.g. name, part of credit card number etc., is to convince the victim that the e-mail is sent personally to him/her and is authentic. Is not often but frequently used.
- “*Invisible/e-mail image link*” is a technique to avoid spam-filters. By either attaching an image containing the e-mail or an invisible image covering the e-mail containing the link to the bogus website. If the e-mail is marked as a spam, the victims will not read it and the scam has failed.
- “*Security Company’s logo inserted*” is to give a more secure feeling over the e-mail. By inserting a logotype of an internet security company known from the Internet, the phishers hopes to give the e-mail a more secure and authentic look. Was often used between the second half of 2004 and the first half of 2006.
- “*Advanced security (SSL, retype characters)*” are used in a few of the attacks under the first year of our investigation and is a technique mimicking advanced security features often used on websites, to give the e-mail a secure and authentic look.
- “*Spoofed link*” has always been the far most used technique to give the e-mail an authentic look. Spoofing means to make it look like the original e.g. viewing the original URL in the link, but

implementing the fraudulent websites URL. This technique is well used but many e-mail clients and spam filters create warnings for spoofed links.

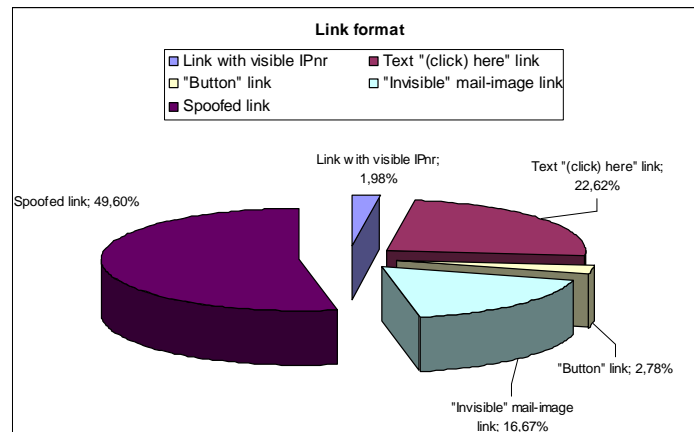


Fig. 5: The distribution of the format on the link in the e-mail.

In 50% of the investigated attacks the e-mails contained a spoofed link directing to the bogus website, see figure 5. Links viewing text e.g. “click here”, represented 23% and were the second most used. But there were occasions where the phisher didn’t bother to disguise the URL, some times even the IP-number were shown. For any computer aware person a visible IP-number in the URL seems very suspicious for a big company, but for less initiated in computers it might seem less suspicious and even assuring.

Every phishing e-mail we investigated had spoofed the sending e-mail address. This is possible because it’s easy to manipulate the SMTP (Simple Mail Transfer Protocol) and disguise the actual sender to make it look like the e-mail comes from the real company. In the same time it’s harder tracking the sender.

Targeted companies

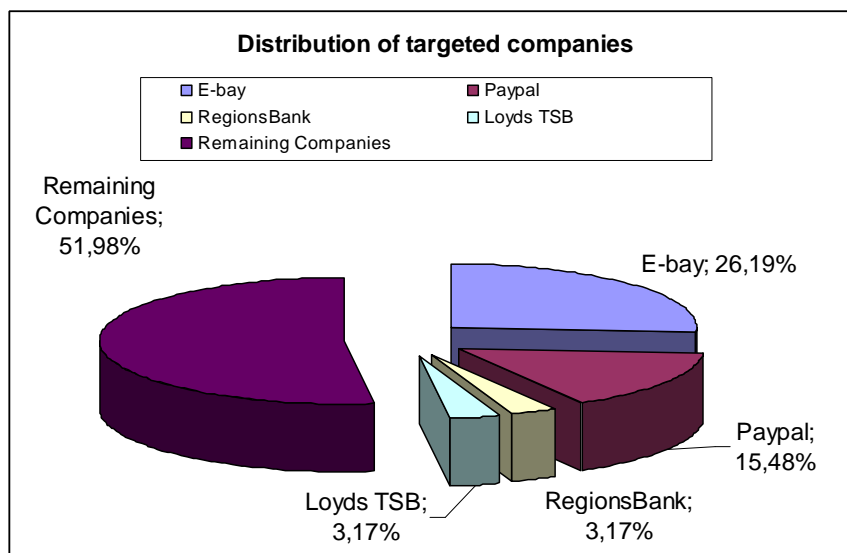


Fig. 6: The distribution of targeted companies.

41,7% of the attacks we investigated were aimed at E-bay and PayPal, see figure 6. Possibly because the inadequate security and the possibilities involved in having access to another users account, such as embezzlement and phish in the form of personal and credit card information. Most of the attacks towards E-bay have used very similar design of their bogus websites; a copy of the original E-bay logon site. The syntactic technique in the e-mail has on the other hand developed under the time of our investigation. In the beginning they looked just like any phishing e-mail, often carrying a warning of some suspicious activity on the victims account. But under the last year they have become harder to spot, now the e-mails are more

efficiently disguised by copying E-bays own e-mail design. Even the semantic techniques has changed, now the e-mails more often claims to regard buying or selling fictive objects and therefore draws less suspicion. The technique “failed/suspicious payments” increased prominent in 2007, see figure 3.

Most of the targeted companies are connected with some kind of e-commerce, e.g. Internet banks, credit card or online shopping companies. Of 74 attacked companies, 56 (75,7%) were only attacked once or twice and it was a few companies that dominated the attacks, e.g. E-bay with 66 attacks (26,2% of all attacks), PayPal with 15,5% and Regions Bank and Loyds TSB both represented 3,2% of the attacks, see table 1.

| Top Four attacked companies. | | |
|------------------------------|----|--------|
| E-bay | 66 | 26,19% |
| PayPal | 39 | 15,48% |
| Regions Bank | 8 | 3,17% |
| Loyds TSB | 8 | 3,17% |

Table 1: Most attacked companies.

Targeted information

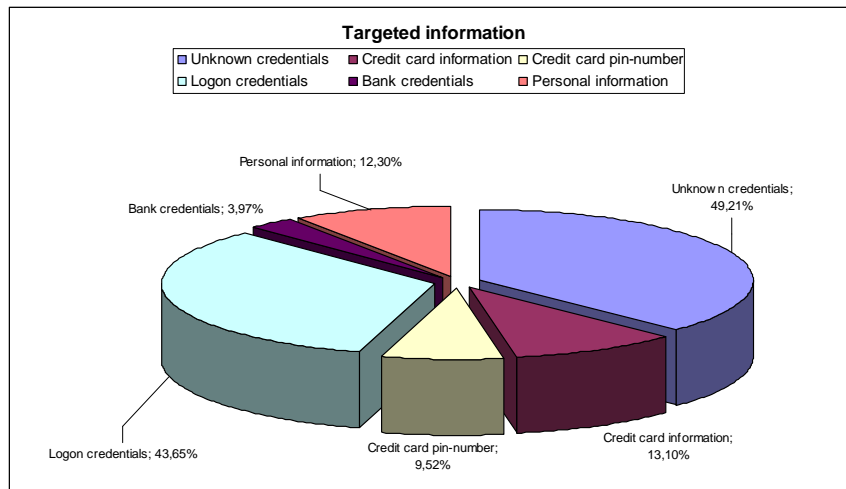


Fig. 7: The distribution of the targeted information.

All phishing attacks have a specific target (*phish*); often sensitive information e.g. bank- and/or credit card credentials. But in most cases it is simpler than that, 43,7% of the attacks we investigated were targeting “Logon credentials, see figure 7. Probable because remaining information can later be collected on the victims account.

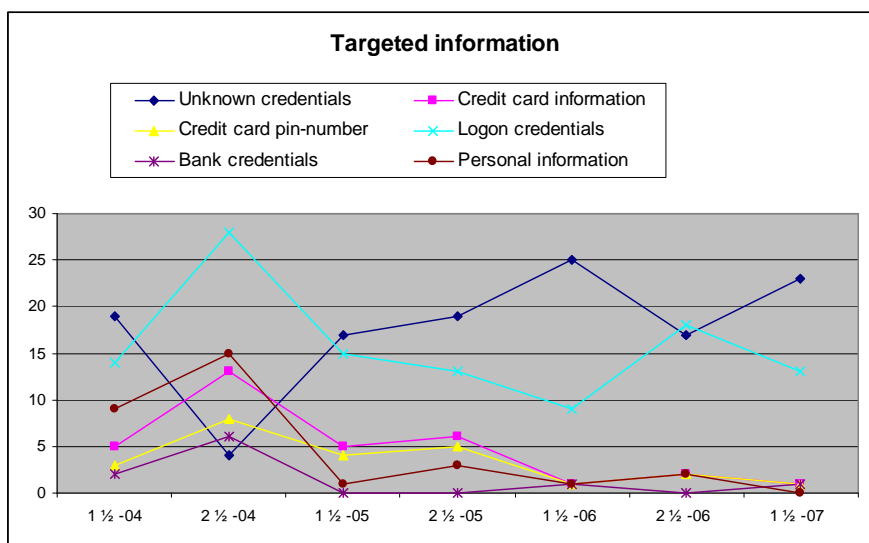


Fig. 8: The Targeted Information in the attack, based on 36 attacks per halfyear.

After logon credentials the most targeted information were credit card numbers and associated pin-codes, see figure 8. Personal information, such as social security number, home address, mothers' maiden name etc., were frequently requested under year 2004 but descended there after. Bank credentials, such as bank account numbers etc. are seldom requested and it was more frequently in the beginning of phishing than today. "Unknown credentials" represent the times when the site were down before the attack been reported. It has become significant more frequent that the site is offline when the attack is reported, this can depend on both that the sites only are online a restricted time and that there are significant more attacks reported today compared to the beginning of the investigation and claims more time to be handled.

The website

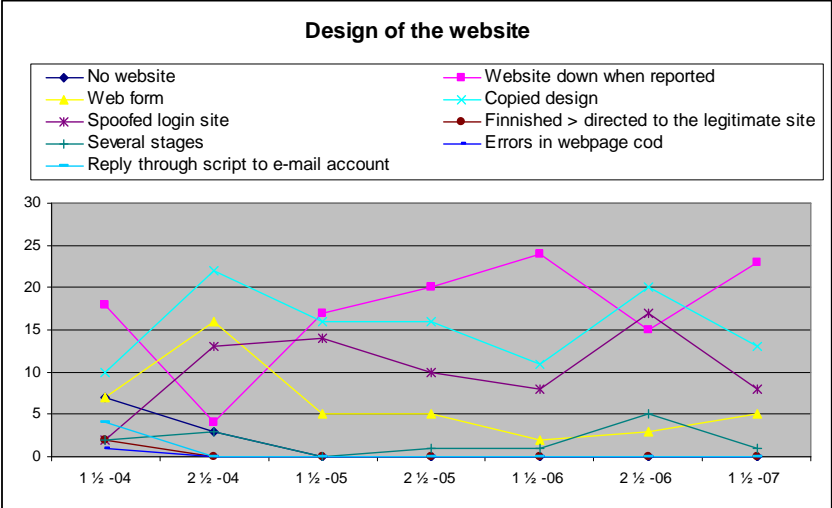


Fig 9: The different credentials regarding the bogus website, based on 36 attacks per halfyear.

The design of the fraudulent website makes big difference when the user is to decide if the site is authentic or not. There are several different ways for the phisher to create an authentic "look". Figure 9 includes the different characteristics used in the fraudulent websites we investigated. The goal of most phishing-sites is to be as authentic looking as possible, to achieve this phishers use different techniques to copy the original design. 108 (89,3%) of the 121 investigated websites were copying the design of the original site. 72 sites (59,5%) were spoofed logon sites. 43 sites (35,5%) used web forms to be able to collect several pieces of information. Some sites consists of a number of stages e.g. after entered with the logon credentials the victim is sent to other stages to enter new information. Some sites send the victim back to the original site after entered the requested information. In that way the victim might never realise what happened but just suspect that they entered the wrong credentials. One site we encountered in the beginning of the investigation had errors in their HTTP-code which were displayed in the web browser. In the beginning of the investigation we encountered several sites that send the information back to the phisher by e-mail; this was not visible to the user.

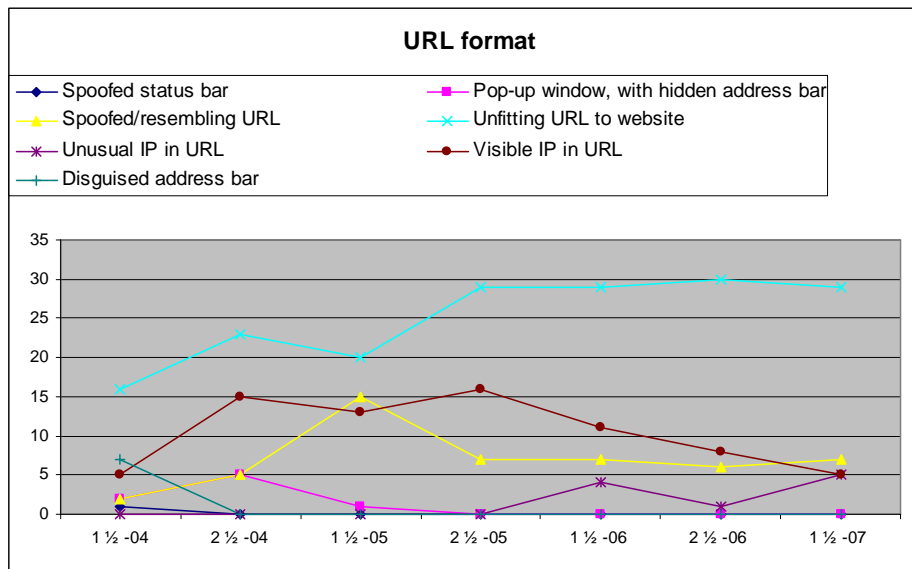


Fig. 10: The different URL formats, based on 36 attacks per halfyear.

The most efficient way to authenticate a website is to check the URL, but not all users know what the URL stands for and have difficulties determine if it's authentic or not. To make it harder for users to determine the authenticity of the website phishers use different techniques to disguise the URL e.g. spoofing the URL (using a domain address resembling to the original company address), disguise the address bar with an image or use a pop up window without an address bar placed over the original site. However, most of the time phishers don't bother to hide or disguise the URL but instead goes after knowledge that most users don't pay any attention to the URL, see figure 10. But even if the URL is disguised the victim always has the possibility to control the authentication of the site by checking the sites *properties* and the *certificate* to the SSL connection. Not all users know how to do this but the possibilities are there.

Explanation of figure 10:

- “*Spoofed status bar*” were used once in 2004 and were possible thanks to a flaw in Microsoft Internet Explorer, after the flaw were fixed the technique couldn't be used. By spoofing the status bar the phishers were able to show the false URL in the status bar (placed in the bottom of the web browser), besides disguise the address bar.
- “*Spoofed/resembling URL*” were seldom used under 2004 but became more usual after that. By using a domain name resembling the original it can be difficult for the victim to authenticate the site.
- “*Unusual IP in URL*”, by using different ways to view the IP-number it makes it even harder for the victim to understand what the URL means. By confusing the victim, the phisher hopes that the URL seems advanced and therefore authentic. The technique isn't that usual, and has increased since 2006.
- “*Disguised address bar*” is when the phisher hides the address bar with an image of the original URL. In the beginning the technique was often connected to the use of Windows Explorers original settings, if the user had other settings applied, the image might not be suitable to the web browser and became visible.
- “*Pop-up window, with hidden address bar*” were used a number of times between 2004 and 2005 but has not be implemented since. Probably as a result of most users don't allow pop-up windows in their web browsers anymore e.g. to avoid annoying advertisements. By using a pop-up window without address bar the phishers could load the original site in the main window and placing the pop-up window on top. This way the victims were tricked to believe that the pop-up window was connected to the window in the background containing the original site.
- “*Unfitting URL to website*” is when the phishers haven't made anything to change or disguise the URL but are simply showing the true URL of their site's location, this includes the URL's with visible IP-numbers. Most phishing sites view the sites real URL, even if it isn't remotely similar to the original, if the victims notice this they can easily lay down the site as fraudulent.
- “*Visible IP in URL*”, sites with visible IP-number can be compromised personal computers that aren't connected to a domain. The number of sites with visible IP-number increased rapidly under the second half of 2004 and topped with 16 (44,4%) of 36 attacks in the second half of 2005. Thereafter the use

has descended and under the first half of 2007 the IP-number was only visible in 5 (13,9%) of 36 attacks. Since most users don't know what IP-numbers is or it's role in the URL many users takes it as a more advanced URL than those built on real domains.

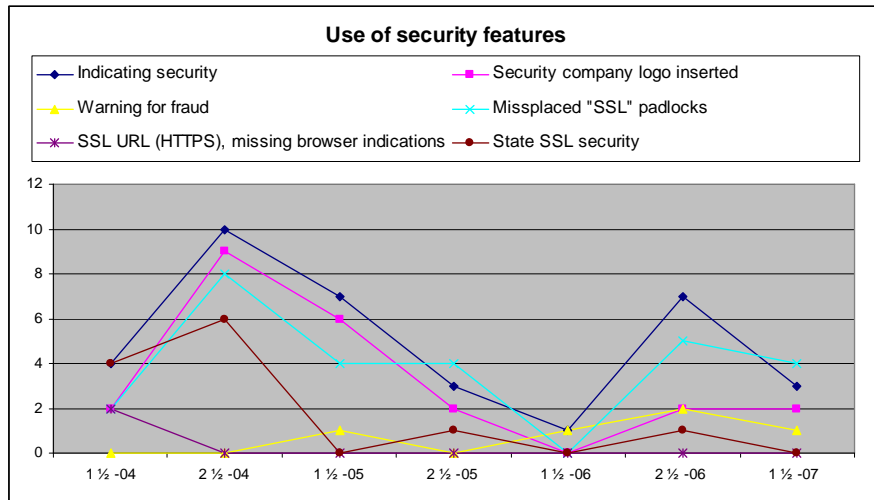


Fig. 11: The claimed use of security features in the bogus websites, based on 36 attacks per halfyear.

The next step in the design of an authentic looking phishing site is to mimic the original website's security features as a way to convince the victims of its authenticity and to give a feeling of security. Sometimes phishers only mention the claimed security behind the website in an attempt to improve the feeling of security. In 2004 phishers often claimed to use SSL (HTTPS) connection to their bogus website and sometimes placed "SSL padlocks" inside the website to further convince the victim. Even though simple claiming to use SSL security decreased, the use of misplaced "SSL-padlocks" continued to be regularly used, see figure 11. The use of known security company's logos increased steadily during the second half of 2004 and was frequently used thereafter. By warning the victims of fraud in phishing e-mails the phishers hopes to trick the user not to suspect the received e-mail. This technique is still quite unusual but has increased the last year. Under the first half of 2006 the use of any security features were almost non-existent, but have thereafter recovered.

The compromised servers hosting the bogus websites we investigated were located in 42 countries all over the world. USA hosted 69 (37,1%) of the 190 attacks we investigated where we could locate the origin of the website, see table 2. The rest of the sites were spread over remaining 41 countries. Except USA, only Korea, with 14 (7,5%) hosted over 10 sites.

| Top five countries | | |
|--------------------|----|--------|
| USA | 69 | 37,10% |
| Korea | 14 | 7,53% |
| China | 9 | 4,84% |
| Germany | 9 | 4,84% |
| France | 7 | 3,76% |

Table 2: The top five countries hosting most bogus websites in our investigation

Our Microsoft Excel file containing the collected information can be found at: <http://www.student.bth.se/~anpf03/masterthesis.html>.

Second research question

We set out to investigate four of the most used (most downloaded) antiphishing applications according to Download.com, [4]. Thereafter we studied previous investigations testing different antiphishing applications.

All antiphishing applications create warnings to inform the user when an e-mail or website appears to be fraudulent. Most antiphishing applications is an extension or improvement of an existing web browser or e-mail client, even applications that's a part of a bigger internet security package implements existing web browsers and e-mail clients.

Microsoft's new version of Internet Explorer (IE) has been marketed as one of the most efficient antiphishing applications [13]. As many other antiphishing applications it use "black-lists" to check if the URL points to a known phishing site. A "black-list" is a dynamic list of known phishing-sites that updates frequently with newly reported attacks. But IE use several different methods to more thorough control the sites authenticity. First step is to compare the URL to a local "white-list" containing URL's of known authentic sites; secondly it checks the content of the site after known phishing characteristics (which, they didn't reveal). Third and last step is to send the URL to Microsoft's online service to be compared to a frequently updated "black-list" containing reported phishing-sites. To handle URL's with unusual characters, IE has implemented Internationalized Domain Name (IDN). This way phishers can no longer use foreign or special characters to spoof the URL. Except implementing the new antiphishing supplement Microsoft also changed the visual aid informing when websites use SSL-connection. Instead of the little SSL-padlock in the bottom of the browser there is now instead a clear display indicating with both icons and vivid colours the occurrence of SSL-connection and the authenticity of the SSL-certificate. These indicators are placed beside the address bar to be clear in sight of the user. To make it easier for the users to check the certificate of the visited website is easily available in the new security display.

One of Microsoft Internet Explorer's competitors Mozilla Firefox claims that their antiphishing application is more efficient than IE's [14]. They can choose between two different "black-list" sources to compare the URL, either a local "black-list" placed on the user's computer or by an online service collaborating with Google.com. They even made their own test to prove their statement, but that source can't be considered objective. They on the other hand have under some time used colours and clear indications in the address bar to indicate SSL-connections and the authenticity of the SSL-certificate.

Both Mozilla's and Microsoft's e-mail clients, Thunderbird and Outlook, scan the e-mails after attached links and check that the visible URL on the link is the same as the website it is pointing to. When suspicious, the link is blocked and the user is informed.

Symantec Norton 360 is Symantec's security package that is containing a number of security applications, including antiphishing [18]. Symantec don't mention on their website what methods their antiphishing application use, but it's made to facilitate for law enforcement agencies to shut down fraudulent websites by collecting necessary information.

WinProxy 6.1 is an internet security package that includes among others antiphishing and spam filter [21]. Their antiphishing product consists of a URL-filter collaborating with a database containing a list of "inappropriate websites". The same URL-filter can be manually setup to block pornographic sites and/or other inappropriate sites.

L. Cranor, S. Egelman, J. Hong and Y. Zhang made an extended study regarding the functionality of a number of antiphishing toolbars [6]. Antiphishing toolbars inform the users of the authenticity of the site they are to visit. This is often done as a toolbar extension of the existent web browser to improve the signs of authenticity, e.g. by colours and icons inform the user of SSL-certificates authenticity, real domain name etc. The tests carried out were based on a list containing URL's to both authentic and fraudulent websites that the different toolbars were to mark as authentic or not. Only half of the tested toolbars were able to identify the majority of tested fraudulent sites. Of ten tested toolbars only three were able to identify over 75% of the tested phishing sites; four of them didn't even identify 50%. One on the other hand incorrectly identified 38% of the authentic sites as fraudulent. Most of the antiphishing toolbars showed warnings in form of coloured address bars, icons and pop-up dialogs when the site was visited. Internet Explorer 7 was found to show a local webpage warning before loading suspicious sites.

Third research question

Most of today's antiphishing applications use "black-lists" to discover phishing attacks, this is an efficient technique to stop ongoing attacks. But, it's not efficient regarding new unreported attacks, because their URL's aren't yet added to the "blacklist". To handle new attacks the application must check after characteristics that is connected to phishing attacks.

To have a relative complete protection against phishing it's not enough to have an antiphishing application installed. Instead the protection needs to be implemented on several levels. First of all the user needs a good e-mail client including a spam-filter that can handle both spoofed links and links implemented in images. The user should also benefit from an antiphishing application using both "black-", and "white-list" to check the URL. To discover phishing attacks not yet reported the antiphishing application should also check the targeted site after known phishing characteristics. In addition the web browser should use Internationalized Domain Name (IDN) to handle unusual characters in spoofed URL's. For all applications to follow the development of phishing they need to be dynamic. But most important of all, antiphishing applications can't be allowed to give false positives or to wrongfully classify authentic sites as fraudulent. Other ways the credibility of the application is rapidly decreasing.

Regardless of what protection the users use, it's still the users' responsibility to respond to the warnings and to not feel too comfortable and secure. It's always a question of time before phishers finds ways to overcome the existent protection. The security applications must consider all possible angles an attack can use, while the phishers only need one working way to escape the security applications.

5 Discussion

First research question

In most phishing attacks there are signs that reveal the fraudulent e-mail, i.e. various tricks the phishers use to either make the victims follow the link before suspecting fraud, or to make the scam so hard to discover that the victims take the e-mail as authentic. Almost all phishing e-mails spoof the sender address as a way to copy the appearance of an authentic e-mail. In the beginning of phishing, many e-mails were created in HTML-code, but appeared to be simple text. This way the phishers could easily spoof links without making them seem suspicious. Today, several e-mail clients and some spam filters check attached links so the visible URL on the link agrees with the URL implemented in the link. To avoid warnings from these the phishers use different ways to trick both the user and the spam filters without spoofing the link. The best way is to use spoofed URL to the fraudulent website, this way both the viewed URL on the bogus site and the link looks authentic. There are several techniques to create similar domain-names, e.g. using capital “I” instead of lower-case “l”, “r” and “n” instead of “m” and so on. But there are simpler ways to trick the victim. The most used is by far “text-links, links with simple text visible, e.g. “Click-here”. But some attacks have the real URL showing, and several of them even contain the IP-number to the compromised server holding the website. In these cases the phisher probably relies on the fact that most victims are less initiated in computers and don’t know what the IP-number stands for. For these the IP-number might even seem more advanced than a regular URL and might even experience it as assuring.

As we mention in the result section, the most common visible sign of a fraudulent e-mail is when the company logo is simply attached to the e-mail. Not everyone might agree that this can be considered a sign of a fraudulent e-mail due to not all companies have exclusive e-mail design. In the beginning of phishing this was true, but today at least most companies have more advanced design just to make it harder for malicious people to copy. Except copying the original design, phishers use other techniques to convince the victim of the e-mails authenticity. As more and more phishing e-mails contain warnings for fraudulent e-mails and websites, the phishers hope that the victim will discard the possible threat from that very e-mail just because the warning.

The different semantic techniques used are often aimed at the victim’s fear of losing money/services and in the same time plays with the fact that other people already has lost money on online fraud. The more attention online fraud gets on the news, the more afraid the users are to become victims themselves. Several attacks claim that the victims account already has been closed or suspended as a result of suspicious activity, this convince the victim that they already are victims and becomes urgent to control what they have lost. And in doing so, they become a new victim of the phishing scam. The similar thing applies on new security updates. Many phishing attacks claims that the company needs to update their data to be able to upgrade the online security. This many are thankful for and eagerly follows the attached link to update their data, when they actually gives the phishers the information they required. Phishers plays with other feelings than the fear of losing something. Stress, is another good way to trick users to not pay attention to more or less obvious visible flaws. By presenting the victim with a limited time-span or convincing them that there have been previous messages that they have missed, phishers hopes to make them more eager to follow the attached link. By giving the victim a feeling of security they are more easily convinced that the e-mail is authentic. Except stressing the victims to respond, many attacks tried to give the victims a feeling of security, to make them mellower and more secure in themselves. By achieving this phishers hoped the victims being less suspicious when entering the bogus website. There are a number of techniques trying to create a secure feeling, e.g. by mentioning security in the e-mail or by attaching logotypes of internet security companies. A few attacks even faked advanced security features often used on websites such as SSL and retyping text viewed in an image. By making the e-mail seem well protected by a number of security features the phisher hoped to convince the victim that it was secure to reply information directly through the e-mail.

Because phishing descend from spam it also has the same problems. It is not easy to implement e-mails that seem personal while sending it out to thousands. Only 11 of the 252 attacks we investigated contained some kind of personal information, e.g. a part of the credit card number, e-mail address. Spam filters are another problem for the phishers, but we encountered a number of ways to avoid them. First, by embedding

the whole e-mail in an image with the link implemented makes it impossible for the spam filter read the text. Secondly, by attaching an invisible image containing the link that covers the whole e-mail. By separating the visible URL (the typed URL in the e-mail) and the URL to the links destination (the one implemented in the image) the phisher makes it impossible for e-mail clients and spam-filters to check that the visible URL is consistent with the one implemented.

In the beginning of phishing it was common that phishing attacks targeted credit card- and bank credentials. Over time phishers realised that it's more rewarding to phish for logon credentials to sites containing that information, e.g. internet banks or other e-commerce. Our investigation showed that 41,7% of the attacks were aimed at E-bay and PayPal and 43,7% of the targeted information was logon credentials.

Even if there are efficient ways to mimic the different security features used in the original sites, there are very few attacks that implement them. Of the 252 attacks we investigated, none implemented SSL connection despite known techniques to use self signed certificates. However there were though several attacks that claimed to use SSL both by mentioning it in text and by inserting false SSL-padlocks on the site. Even the different techniques that are available to trick spam filter were used significantly less than expected.

The purpose of SSL-padlocks is to indicate that the connection between the user and the web server is encrypted by SSL. However, many users today has come to believe that the padlock more or less indicate overall security for the site. Even authentic sites use this icon to indicate security by attaching it to the body of the website. This has undermined the authority the icon used to represent. Since users nowadays are used to see the icon in the body of the website, instead of in the status bar at the bottom of the browser were the real SSL-padlock used to be located, it becomes easier for the phishers to falsely indicate security.

Second research question

We can determine after investigating the different antiphishing applications that the most used method is a dynamic "black-list", either local or online that consist the URL of known phishing-sites. Some applications use a number of techniques to determine if the site is authentic or fraudulent. Microsoft Internet Explorer use both a local "white-list" containing known authentic sites, an online "black-list" that are frequently updated with new reports of phishing attacks and search uncategorized websites after known phishing characteristics. Even most used e-mail clients have functions to thwart phishing attacks. If the e-mail includes links where the visible URL doesn't match the targeted websites URL it's considered a fraud and are blocked.

Antiphishing applications using nothing other than "black-lists" are depending on previous reported attack and are inadequate to hinder new attacks. Even the best antiphishing application can't stop all possible phishing attacks. If a new attack is created with previous unknown characteristics it's possible that all antiphishing methods fail. However, thanks to the dynamic function the antiphishing application "learns" the new characteristics and techniques after one attack has attracted attention and been reported. Regardless of which antiphishing programs used it's up to the users to act upon the given warnings. If the application incorrectly claims authentic sites as fraudulent the trust for the application decreases, and if this is repeated too often the users starts to ignore the given warnings rendering the application useless.

Too avoid dynamic antiphishing applications the phishers might make their attacks more targeted and specialised by sending it only to a smaller group instead of distributing it to as many e-mail addresses as possible. That way the phishing site is less possible to be registered on a "black-list" before the attack is over and the site is taken offline.

Third research question

There are many difficulties with creating an efficient protection against phishing, because phishing touch upon many different security issues. Phishing e-mails use a number of different appearances and use a number of techniques to avoid existent spam-filters and to manipulate attached links. Fraudulent websites

can be both well designed to mimic the original site and at the same time use a number of techniques to disguise or spoof the URL and mimicking security features.

Most web browsers indicate when the site is encrypted with SSL and checks that the certificate is authentic. But it's not uncommon that even authentic SSL-certificates create warnings, often the SSL-certificates isn't renewed in time. Several e-commerce websites only use SSL-encryption on a part of the site which results in absents of those indications, it's therefore harder for the users to control that the site really is secure and to check the certificate. If the security applications create too many false warnings the users soon starts to ignore them. Even earlier web browsers warned the users when they were entering an insecure website, but after some time that warning only became annoying and most users ignored and simply clicked "OK" before learning what the warning was for. It's therefore important that the new security applications take this into consideration and instead of just flashing warnings at the user, inform them what the warning is for and what the user needs to consider before entering the website or e-mail. Another problem that might occur is that all these controls claim both time and network recourses which many users dislike.

The war against phishing can't be fought by only antiphishing applications. Legitimate companies need to improve their security toward their users. We believe that some responsibility lies on the companies that are being attacked. It should not be the user's responsibility to assure that the e-mails they receive is authentic. Security can no longer be confined to the company's computer system; it needs to include the users too. Therefore it's important that the authenticity is controlled both between the company and their users, and costumers and the company. The company needs to prove that e-mails sent from them are authentic, the same way users prove their identity when accessing the company system.

PGP (Pretty Good Privacy) is a well established privacy/authentication technique created by Philip Zimmermann in 1991, which enables both encryption and signing of e-mails [16]. Each user of PGP has both a private and a public key, with the private key the user can encrypt and sign the e-mails they send out. The receiver of a signed e-mail needs the public key of that sender to control the signature. If companies would use a similar technique to sign their e-mails this would make it impossible for malicious people to spoof their e-mails as long as only the company has access to the private key. This would make it possible for users to securely authenticate any sender of an e-mail by clicking a button.

In the paper titled "A Forensic Framework for Tracing Phishers" by D. Birk, S. Gajek, F. Gröbert and A-R. Sadeghi a possible way for banks to trace phishers after taking contact with the bank accounts they'd phished is described [5]. By reporting "phoneytokens" (credentials to a specially created account used for just this purpose) to known phishing sites, the company can trace the phisher when they try to connect or withdraw money from the fake account. With this technique the banks can expose the phishers without any advanced technological technique or any financial risks.

6 Conclusions

Our goal with this thesis was to better understand how phishing has developed over the last four years, how antiphishing applications have responded to that development and to give a better understanding in how phishing might develop in the future.

By thoroughly investigate 252 previous attacks we've created a data set containing information regarding what different techniques have been used and how the usage of the different techniques has changed over time. The fact that basically the same phishing techniques are used today as in the beginning of phishing is an indication that there hasn't been much efficient protection. Even though there are efficient techniques to mimic security features such as self-signed certificates, it wasn't used in a single one of our 252 investigated attacks. Probably because the phishers know that most users don't know how to check the security and often assumes that sites requesting sensitive information are secure. This further indicates that most users don't consider online security a problem, sites requiring sensitive information always claims to be secure without the users really understand how and therefore just takes it for granted. When users don't now how, but just that they are secure it's not easy for them to see the difference between authentic security and mimicked security features.

The biggest part of today's antiphishing applications is to more clearly inform the users of the security of the site they are visiting. Antiphishing applications most often use "black-list" containing the URL of known phishing-sites to compare the requested URL. But new antiphishing applications e.g. Microsoft Internet Explorer, use both "black-" and "white-lists" (containing known authentic URL's) and checks remaining sites after known phishing characteristics. This can be considered an efficient way to even discover unknown phishing sites and by the fact that all features are dynamic the protection can follow phishing's development. To yet another time quote Bruce Schneier - "*There's no such thing as absolute security.*" [17], the users must still pay attention to the information given by the different security features. If ignoring them, there is no protection.

We believe that the responsibility to protect the users against phishing also lies with the companies attacked, not only by the users themselves. It's the companies' responsibility to control that the communication between them and their costumers include the authenticity necessary. Most companies have impressing security concerning their computer system, but there is no way for the users to check that the information they receive through e-mail is indeed from the company. By including some kind of signature from the company (e.g. PGP) the users would be able to trust the authenticity of the e-mail. Resulting in that the number of companies vulnerable to phishing attacks would decrease significantly; making phishing scams a very unprofitable business.

7 Further research

As more and more advanced antiphishing applications being shaped, the development of phishing techniques might speed up. To address these new threats more research is needed.

Below follows a list of possible future investigations:

- By continuing our investigation over phishing techniques and their development over time, future research can see if the new antiphishing applications change the development of phishing attacks.
- The usability of new antiphishing applications should be tested to see if they facilitates for the users to check the authenticity of the sites. It's also important that the users understand what the different warnings stands for and how they should react to them.
- The technique to sign the company's e-mails should also be investigated to see if it is feasible and if it indeed stops phishers from spoofing e-mails.
- Banks should test the technique to trace the phishers by inserting "phoneytokens" to known phishing attacks.

References

- [1] R. Anderson, "Security Engineering", John Wiley & Sons, Inc. New York USA, 2001
- [2] APWG (Anti-Phishing Working Group), "Phishing Activity Trends Report, January 2006", January 2006
- [3] APWG (Anti-Phishing Working Group), "Phishing Activity Trends Report for the Month of February, 2007", February 2007
- [4] Download.com "Search results matching: antiphishing" webpage:
http://www.download.com/sort/3120-20_4-0-1-4.html?qt=antiphishing&ca=20, last checked: 2007-08-12
- [5] D. Birk, S. Gajek, F. Gröbert and A-R. Sadeghi, "A Forensic Framework for Tracing Phishers", IFIP Summer School on The Future of Identity in the Information Society, Karlstad, Sweden 2007
- [6] L. Cranor, S. Egelman, J. Hong and Y. Zhang, "Phishing phish: An Evaluation of Anti-Phishing Toolbars", CMU-CyLab-06-128, Pittsburgh, November 2006.
- [7] R. Dhamija, J. D. Tygar, M. Hearst, "Why Phishing Works", in the Proceedings of the Conference on Human Factors in Computing Systems (CHI2006), 2006.
- [8] M. Jakobsson, A. Tsow, A. Shah, E. Blevis, Y-K. Lim, "What Instills Trust? A Qualitative Study of Phishing." Extended abstract, USEC '07, 2007
- [9] M. Jakobsson, "The Human Factor in Phishing", Privacy & Security of Consumer Information '07, 2007
- [10] R. Jaques, "Cyber-criminals switch to VoIP 'vishing'" webpage:
<http://www.vnunet.com/vnunet/news/2160004/cyber-criminals-talk-voip?page=2>, last checked: 2007-05-17
- [11] M. Leon, "The looming threat of Pharming", Infoworld.com, May 2005
- [12] M. Leon, "The Poor man's Pharm", Infoworld.com, May 2005
- [13] Microsoft, "Technology Overview: Microsoft® Windows® Internet Explorer 7", October 2006
- [14] Mozilla, "Stay Secure on the Web", webpage: <http://www.mozilla.com/en-US/firefox/features.html#secure>, last checked 2007-08-21
- [15] G. Ollmann "The Phishing Guide", September 2004
- [16] B. Schneier, "Secrets & Lies", Wiley Publishing, Inc. Indiana USA, 2000
- [17] B. Schneier, "The Psychology of Security" (draft) webpage:
<http://www.schneier.com/essay-155.pdf>, last checked 2007-08-15
- [18] Symantec, "Comprehensive, automated protection", webpage:
<http://www.symantec.com/norton/products/overview.jsp?pcid=os&pvid=n3601>, last checked 2007-08-21
- [19] Symantec. "Pharming – Vad är det och hur skyddar du dig mot det?", webpage:
http://www.symantec.com/region/se/clubsymantec/2006_1_11.html, last checked 2007-05-13

[20] D. Watson, T. Holz, S. Mueller “Know your Enemy: Phishing”, The Honeynet Project & Research Alliance, May 2005

[21] WinProxy, ” WinProxy 6.1 “, webpage: <http://www.winproxy.com/products/winproxy.asp>, last checked 2007-08-21