Why we fall for Phishing

Jussi-Pekka Erkkilä
Aalto University School of Science
Department of Computer Science and Engineering
juerkkil@cc.hut.fi

ABSTRACT

Phishing attacks, a form of social engineering, have been one of major security issues in the Internet for years. In order to decrease the problems caused by phishing, we need to know why people fall for phishing. This is the question discussed in this paper. As finding it is proposed that main reasons for success of phishing are the lack of knowledge, lack of attention and feeling of being secure among average users. Anti-phishing tools are available to detect phishing content; however, most users do not either use them or do not care about the security warnings. In this paper it is proposed that users are so accustomed to accept security and other warnings that they are not able to distinguish the real threats from routine acceptances. Also, users are not aware of the structure of computer systems and the Internet, which makes them easy target for attackers.

Author Keywords

security, usable security, usability, phishing, social engineering

INTRODUCTION

Phishing attack is a semantic type of computer security attack. Instead of trying to find vulnerabilities in network or software, phishing attacker – or phisher – pretends to be someone else in order to obtain confidential information, such as passwords or credit card numbers [7]. Phishing is a typical social engineering technique. Typical forms of phishing attacks are fraudulent websites, e-mail messages where sender might be spoofed or even phone calls. Phishing has spread all over the Internet, especially in payment and financial services. Recently phishing attacks have been reported also in social media [3]. The total costs of the phishing in 2007 was approximated to be over 3 billion USD [8]. The phishing is clearly a critical problem and much research and software development have been done in order to reduce the problems caused by the phishing.

Despite the work that have been done to detect and prevent phishing, which has caused some positive impact, it is still a major issue. Different technical solutions are available to automatically detect fraudulent websites or email messages and warn the user. Moreover, some of the phishing attempts are seemingly poorly implemented: a person who is aware of the threats and understands the Internet technology can easily detect the fraudulent website in most cases. However, people still tend to fall for phishing, thus the problem is not only the software and technology, but also usability.

This is the problem discussed in this paper. In order to develop web browsers or applications to shield users from phishing, we need to know, which properties and details in fraudulent websites or emails make people to trust those [6]. Also, we need to know which is the major reason for success of phishing: the lack of knowledge among users, successful phishing strategies or something else. The purpose of this paper is to find and provide answers for these questions.

The main findings are listed below.

- The users feel that they are in the control on the Internet. That may lead to false assumption, that security is not necessary.
- The users are so accustomed to security warnings that they do not care them. They might not even notice those.
- The users lack knowledge about computer systems. They may not be aware of basic functionality and structure of the Internet and computer software.

There is no experimental part in this study. All the facts are based on other scientific surveys or valid statistics. The findings of other surveys and statistics are assembled and as the result new findings are being proposed.

The main purpose of this paper is only to find out, why phishing works - not to find out, how to prevent phishing. That question would be wide enough for another survey. However, as some results have been found out, some possible solutions are also proposed, though the solutions are not on the main focus. As most of the reasons for success of phishing are associated to users, it is clear that improving usability of the applications and training the users might mitigate the success of phishing attacks

This paper is divided in five sections. After the introduction the background of phishing is reviewed: different phishing strategies are explained and compared, motivation for phishing is explained and efficiency of phishing is evalu-

CHI 2011, May 7–12, 2011, Vancouver, BC, Canada.

ated. In third section phishing detection and prevention technologies and strategies are explained. In fourth section the user awareness and phishing detection technologies are evaluated to find out, what makes people to fall for phishing. At the end of this section the reasons for success of phishing are summed up and some possible solutions for preventing phishing attacks are mentioned. Finally the whole paper is concluded at the last section. In the conclusion the paper is shortly summed up and main points are listed.

BACKGROUND

Anti-Phishing Working Group defines that phishing is "a criminal mechanism employing both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials" [3]. Phishing is not completely new threat in the Internet. The word "phishing" was invented already in 1990s among hacker communities [15]. According to Anti-Phishing Working Group reports, already in 2004 hundreds of phishing attacks was reported every month. [1]

Since 2004 the amount of reported phishing attacks have increased significantly. Between April and June 2010 more than 30,000 unique phishing websites was detected every month. However, the number of new phishing sites had significantly decreased since record high August 2009, when 56,000 unique phishing websites was detected. [3]

Most of phishing attacks are targeted on payment and financial sector. These combined over 70% of all phishing attacks at second quarter of 2010. Other remarkable sectors of industry where phishing was targeted were classifieds, auctions, retail and service, gaming and social networking. [3]

Phishing emails are usually considered to be spam. This is not wrong classification, although phishing emails significantly differ from the ordinary spam messages. Typical spam message tries to sell a product or service, whereas phishing message tries to convince the user and make her to believe that message is from legitimate organization. Phishing messages differ from the other spam by their form, content and purpose, thus spam filters are not effective on detecting and preventing phishing messages. However, phishing message contains no useful information and can be categorized as spam. [8]

Motivation for phishing

Considering that large majority of phishing attacks are targeted against payment services or financial industry, it is obvious that motivation for phishing in most cases is financial. However, also other motivators for phishing exists, including identity thefts, malware distribution, password harvesting and even industrial espionage. [15]

Since beginning of 2000s as the Internet became popular among ordinary, non-expertise users, it has been very fertile place to fool people. Users are not aware of how fast and easy is it to generate a random web page which claims that every visitor will have money, if they provide their credit card number. These facts have made phishing to a tempting chance to fool people and it have been proved to work at some level.

As phishing attackers mostly appear to be someone else and the identity can be spoofed, chances of getting caught are relatively low. Moreover, phishing activity can be ran from anonymous server and targeted to other countries, which makes the phishing even more safe from attackers point of view.

Phishing is also technically much easier to do than hacking and breaking firewalls. Also, phishing produces almost always immediate profit such as personal data or credit card numbers. In contrast, in order to gain financial benefit, traditional hackers should break very secure bank systems.

Phishing attacks

There is several possible strategies to implement the phishing attack. Phishing attack can be an email message targeted to a limited group, a website targeted to all possible visitors or phone call against a single person.

In most cases phishing websites and emails are targeted for anyone. Usually the motivation for phishing is a financial profit, thus phishers do not care who they fool. The only essential requirement is to get users to give up some confidential information. Hence, the phishing websites are mostly targeted against anyone who is vulnerable to phishing attacks. Phishing attacks are considered to be successful when the attacker is able to manipulate user to trust the website or email and to give up something personal or confidential information.

In some cases the phishing attacks may be specially targeted against a single person or organization. In these attacks the motivation is mostly different - instead of the money, the phisher is probably after something else such as trade secrets or personal damage.

Usually the phishing websites are advertised somehow - for example by spamming emails. In practice, phishing websites may be as simple as copy-pasted HTML content from the legitimate site. Phishing attacks can be implemented in many different ways, which require more or less technical skills. Some of the most common phishing attack strategies are listed below.

Domain based attack

In domain based attack, the DNS server or DNS cache memory of the victim's computer have been compromised. When user accesses to her web bank, the connection is actually redirected to malicious server which steals the username and password. This is so called man-in-the-middle attack. Implementing this requires, however, some technical knowledge. Some solutions are also available to avoid DNS attacks, such as utilizing DNSSec.

Another way to do domain based attack is to register a domain name which resembles a common, known domain name, for example pàypal.com. This makes the detection of phishing difficult for the user. [5, 13, 14]

Spear Phishing
Spear phishing [5, 7] is a method where phishing is focused on a single user or very limited group, such as a work team or the department of organization. Spear phishing could be for example an email message which appears to be sent by team leader who asks team members to update their passwords in the malicious website. Spear phishing messages may seem more personal than generic spam post.

Search engine phishing
One way to fool people is to develop a convincing web site, such as e-commerce, and optimize it so that it will be detected and indexed by search engines. Once the site has many visitors, it is likely that some users will register and give up their personal information. [5]

Content injection
Content injection is a method where a real, legitimate web page or email message is modified so that for example a link is replaced by the malicious one. Users mostly trust the links in legitimate websites, which makes this strategy efficient. [5, 13]

Malware
Another way to find out data and passwords is to develop the software which looks like trustworthy and useful. The software might, however, include some invisible components which collect passwords from the computer and sends them to the malicious server. In this strategy, the trick is to make people download and install the malicious software. [5, 13]

Popup-window attack
A popup-window attack [14] is a type of attack where the phishing link actually redirects the user to correct, legitimate website. However, the link also opens a popup-window which might ask some confidential information. From users' perspective this looks like that the popup-window is opened by the legitimate website, although it is the actual phishing site.

Context aware phishing
Context aware phishing [9] refers the scenario, where the phisher has collected something personal information about the victim, such as information about her browsing history, background or relationships. These details make the phisher look more trustworthy, as the message is much more personal. Also, the victim easily thinks she can trust the phisher because the phisher already knows much about her. The victim does not always realize that all the information might be quite easily available for anyone.

Efficiency of phishing

There is no reliable statistics on the success rates of phishing attacks. The reason for this is that not all phishing attacks are reported and the victims do not always realize that they are getting phished. Moreover, implementing an authentic study is not simple. The participants should be selected randomly and they should not be aware of the study. Basically, real phishing attacks should be made to get authentic results. This is, however, morally questionable way to do research. [10]

Some approximations about the success rates of phishing have been made. The studies are mostly based on a single phishing strategy and limited target group. However, these studies give us some approximative results which are good enough.

According to study of research and analysis company Gartner Inc. [2] about 19% of all participants reported having clicked link in phishing email. About 3% of the participants had also given up personal or financial information. The study was conducted in 2004, thus the numbers might have changed since.

Study performed by Jagatic et. al (2007) [9] shows that up to 70% of users fall for phishing messages which seem to be sent by their friend. The same study also points out that about 15% of users enter their personal credentials in the link provided by an unknown person from the same domain name. The study was targeted for college students and the phishing messages were sent from the university's domain name.

Another survey by Jakobsson et. al (2006) [10] proposes that success rate of a single phishing attack could be around 11% realizing in 24 hours. In the study, content injection attacks were conducted using instant messaging system.

All of these studies are relatively old by now. The users' awareness might have be improved since but also the phishers are more active and quality of phishing attempts may have been improved. Anyway, the assumption that success rate of a single phishing attempt is around 5% is probably not overestimated. Moreover, it seems that the success rate of a single phishing attempt can be significantly improved by utilizing technical subterfuges such as spoofing email address or using content injection attack or social contacts of victim. Regardless of exact value of success rate, the phishers can anyway spam the phishing messages for thousands of users and thus easily get dozens or even hundreds of victims.

DETECTION AND PREVENTION OF PHISHING

If we want to find out, why phishing works, we need to know how phishing attacks can be detected. There is different strategies for detecting a phishing website or email, some of those used by human and some by computer software. In this study the strategies are divided in two parts: human strategies and automatic strategies. The human strategies are those, which users use to decide if they trust the website. The automatic strategies are the strategies used by security software to help users to detect phishing.

Some of the strategies are used both by computer and human. In practice the decision is mostly a mixture of human and automatic strategies: for example the security software may warn user that the website has no valid certificate and then human needs to make decision if the website is trust-

worthy or not.

Human strategies

Human strategies are based on users' knowledge and intuition. Typically the human strategy is to find some security indicators from what they see: the website content and browser [6]. Here the most common indicators used in human strategies are listed, explained and their relevance is evaluated.

Look and feel

For many users, the look and feel of the website is the most important factor when determining legitimacy of the website. The trust decision is made based on what the website looks like: is there images or animations, does the overall look like convincing or is it easy to use.

These are not totally irrelevant points because some phishing sites might include broken images or poor translations. However, many phishing sites are well implemented and in these cases, detection strategy based only on look and feel is useless.

Address or domain name

Many users are aware of domain names and thus understand to check the location of the website or sender's email address. Spoofing the email address or implementing attack against domain name system (DNS) is possible, but this strategy, however, is an improvement compared to strategy based only on look and feel.

Security features

Some users understand also the real security indicators, such as "https" in the address bar, padlock icon on the browser's status bar or even security certificates. These are very relevant indicators and user who checks these always before sending confidential information, is quite safe.

Other strategies

Some users utilize several miscellaneous strategies to define the credibility of website. Users might, for example, do Google search with the page title and look for the same website among search results [6]. Some users even try to input their username and wrong password to the website and make their trust decision if the password is rejected. However, this strategy fails on man-in-the-middle attacks. [14]

Also, the source of the link is very significant factor in trust decision. If the link is sent by a friend in social media or by a student of same university, the user is much more likely going to trust the website [9].

Automatic strategies

In order to mitigate the damage of phishing attacks, much software development have been done. Several anti-phishing tools have been developed, for example browser plugins and anti-virus software, to warn about malicious websites and detect so called Trojan horses or spyware. Many browsers also have some built-in security features to warn about suspicious websites.

In most cases, the anti-phishing tools do not make the trust decision: usually they only warn the user or ask the confirmation if the user is really willing access to the website. Like humans, anti-phishing tools also use different strategies and utilize different heuristics to detect the malicious website, email message or software [7]. These strategies and heuristics are discussed next.

Blacklists

Blacklist is a database, which keeps up-to-date list of all known phishing websites. The idea is that every time a website is loaded, the browser connects the database and asks, if the website is trusted or not. The problem with blacklist is that lifespan of a single phishing website is very short. Moreover, it takes some time before the phishing website is detected and reported. Thus, keeping the database up-to-date requires much resources.

Blacklists may decrease the amount of phishing sites, because once the website is blacklisted, it is mostly removed quite soon. However, using the blacklists causes also redundant network traffic for the end user, as the browser needs to make requests to the blacklist service at times. The end user also needs to trust the maintainer of the blacklist.

Whitelists

Whitelists are the opposite of the blacklists. The idea is same: the web browser asks from the external service if the website is trusted or not. However, instead of the phishing websites, the service has up-to-date database of trusted websites. If the website is found from the database, it must be trustworthy.

The problems in whitelists are partially same as in the blacklists. It is practically impossible to maintain an up-to-date list of all websites in the world. However, the idea in whitelists is not to detect a malicious websites, but verify and certify the legitimate websites. The whitelists could for example include all the web banks and financial services which is not impossible.

Content based heuristics

Another common way to automatically detect a malicious website or email message is content based heuristic. This method is based on assumption that phishing emails or websites have some specific characteristics that can be programmatically detected. For example the anti-phishing tool might look for some common words or sentences that are typically found in phishing websites.

Content based heuristics is definitely not reliable way to detect malicious content, but in some cases it may provide useful information for a novice user. The same method is a commonly used in spam filters.

Security feature verification

The browsers and email servers can also verify the common security features and notice the user if any suspicious found. For example the browsers commonly verify that the TLS/SSL-certificate is signed by trusted authority and is not

expired. Also, some mail servers make so called reverse DNS lookup for the sender's domain name before accepting mail, because they have noticed that the majority of spam is sent from false domain names.

The problem with these methods is that many services and websites may use expired certificates or the certificate is not always signed by valid authority. This does not necessarily make the website malicious, which may cause confusion in users. Moreover, this is how users get accustomed to accept security warnings.

REASONS FOR THE SUCCESS OF PHISHING

Despite all the effort to detect and prevent the phishing attacks, they are still a common problem. There is a few optional reasons for this: either the users do not use anti-phishing tools, users do not care about security warnings, or anti-phishing tools do not detect the malicious websites. In this section we discuss about user awareness and knowledge about phishing, efficiency and usability of anti-phishing tools and efficiency of different phishing detection strategies. The goal is to find out the main reasons for success of phishing

Efficiency of anti-phishing tools

As discussed previously, anti-phishing tools utilize different strategies to detect the phishing and warn the user. However, these tools may never be able to effectively protect the user against all phishing attacks, as tool developers and attackers are in continuous race against each other. Moreover, it may be impossible to develop heuristics which could always detect if the website is trustworthy or not, without any false positives or negatives.

Blacklist based anti-phishing tools have some strengths, but there is always some delay before a new phishing site is added to blacklist. Moreover, blacklist based phishing filter can be bypassed by DNS-poisoning: according to study by Abu-Nimeh et. al (2008), none of the seven different anti-phishing tools detected the DNS-poisoning based phishing attack [4]. The content was copied from the legitimate website but the service was actually running on wrong server.

Even though anti-phishing tools may detect many malicious websites, they are not perfect and user can not trust that installing anti-phishing tool is the solution for the all possible phishing attacks. However, even the more critical problem is that users who are not aware of the threats – such as phishing – are unlikely going to install and use any anti-phishing tools. Even the users who have anti-phishing tools installed, do not always notice the warning or care about them [7].

Wu et. al (2006) pointed out at their study that passive security toolbars are very ineffective in preventing the users from visiting fraudulent websites [14]. The most of their participants totally ignored the toolbar security notifications. The possible drawbacks in the usability and functionality ofthe anti-phishing toolbars are listed below. [14]

- A toolbar is a relatively small compared to large main window which shows the content of the website. Users may not even notice if there is some warning text.
- The toolbar shows security-related information but users are mostly not interested in security as it often only slows down their web browsing.
- Users may not trust the security toolbars, especially if the toolbar has given false information sometimes.

Popup warnings produced significantly better result than passive toolbars warnings. Those did not completely prevent users from accessing to website, but the users were much more careful. Some users, however, ignored also the popup warning. They thought that the warning was wrong or they did not trust it because they did not have seen such a warning before. [14]

Knowledge and awareness of users

Generally, the purpose of anti-phishing tools is not to completely prevent users from accessing to possibly fraudulent websites. The purpose of them is only to give users some external security indicators, if the user is unsure whether the website is trustworthy or not. Many users have not any anti-phishing tools installed at all. The user is anyway the one who makes the final trust decision.

Human users rely on different cues to avoid falling for phishing attacks. These cues might be, as explained earlier, address bar and domain name, content of the website, email address of the sender or real security indicators such as TLS certificates and "https" at the address bar.

Some of the cues can be easily spoofed but some of them are trustworthy. Expert users are mostly aware of how to avoid falling for phishing. In contrast, many novice users are not even aware of such a threat – and even many of those who are, do not have any idea which security indicators are trustworthy and which are not. Hence, the Internet is full of potential victims for phishing attacks.

In study conducted by Dhamija et. al (2006) they point out several factors for success of phishing [6]. One key factor is lack of computer system knowledge among the Internet users. Users may not be aware of how operating system, applications and web works. They may not even know what is difference in web applications and native applications.

Furthermore, many users lack of knowledge of security. They do not understand, what the closed padlock icon means in browser status bar – and even if they do, they can be fooled by placing the icon on the body of website [6]. Users also have difficulties on understanding, which area of the display is part of the website, and which is part of web browser or operating system. Some users are not aware of the syntax of domain names. For example users might think that website in www.paypayl-security-login.com must be part of Paypal service and belong to paypayl.com [6, 14].

Phishers often use visual tricks to mimic legitimate websites [6]. For example very convincing texts or images on the website may fool even an advanced user. Some users

may even have a false understanding that for example logo of the Google can only appear on the websites of Google and its partners.

Another factor is lack of attention. Even if the users are aware of the basic security indicators and have the understanding about the domain name system, they might still be vulnerable for phishing attack. When the users are focused on their tasks, they may not read warning messages or notice other security indicators.

Maybe even more common problem is lack of attention to absence of security indicators. If the user is in hurry or very concentrated, she may not remember to check the existence of the padlock icon or correct domain name. For example, if the web bank login page seems otherwise normal, even the expert user may not check the existence nor validity of TLS certificates.

In study by Dhamija et. al (2006), they also point out that more than half of users make the decisions about trusting the websites based only on the website content and domain name. Participants in the study were randomly selected university staff and students. About 30% of the participants were aware of the padlock icon or the security certificates. As a result of the study, even 80%-90% of participants were not able to distinguish the well made spoofed websites from real websites.

Feeling of security

One more important factor is the feeling of security. The security is not only reality but also feeling. For example, people are not afraid of risks that are familiar, under their control and not discussed very much. On the other hand, people exaggerate risks that are talked about much or affecting them personally [12]. Hence, as long as phishing attacks are not talked about in media, nor affecting the users themselves, users do not consider phishing attacks to be a big risk. Especially as experienced Internet users feel that the computer and websites are under their control and they can close the browser on any second, it is natural that phishing does not feel very critical risk.

Personal security – as security in general – is always a trade-off. In order to obtain security, user needs to give up something. That may be money (buying anti-virus software) or work efficiency (time spent for virus scanning) or something else. [12]

For the most users, security is not a primary goal. Actually for many users security is something necessary but boring or even unwanted. Some users find it irritating to answer security related questions [11]. Users may feel that security features only slow down their primary tasks. Most users who work much on computer are used to accept security or other warnings regularly. Many programs show error messages and warnings frequently despite the fact that users do not understand them and in many cases users do not even read them. This is not good for any stakeholder: all the error and warning messages only slow down the users' tasks and the real security warnings are useless as users only skip them. It is a known fact that the more popup confirmations user needs to do, the less effective those are. [14]

Thus, it is not a surprise that users may not be willing to spend much time or money because of security in the Internet. They may feel that it is not a good trade-off: they need read security messages at times, check the security indicators frequently and care about privacy every time they input their username and password to website. For the users' point of view they may not get anything as response. They could as well stop caring the privacy or security; the risk that somebody would get their password feels to be very low and the risk that something really harmful could happen them even lower.

This is why people may intentionally disable or ignore security warnings. They do not feel them to be so important that they should waste time for reading those. They may think that the risk is overestimated in general and that they can take care of themselves in the Internet.

Findings

As a result it seems that there is no single reason for success of phishing. Several factors affect to behavior of users in the Internet and also usability and functionality of web browsers, websites and computer software in general might make the phishing easier from the phishers' point of view. The main findings are listed and explained below.

- **Lack of knowledge**
  Most users do not have the basic understanding of structure of Internet and computer systems in general. This implies that users also have false assumptions of which factors make website credible and which security indicators are relevant.
- **Lack of attention**
  Even though users might have appropriate knowledge to avoid phishing websites, they often lack the attention when working intensively or browsing websites. They may not notice or read the security warnings or other security indicators. Also, users may not notice the absence of the security indicators, such as padlock icon in the status bar, when there should be one.
- **Inefficient anti-phishing tools**
  The current available anti-phishing tools include problems related both functionality and usability. Tools may not detect malicious websites that are well implemented. Moreover, anti-phishing tools are not efficient even though they might technically work, as users mostly ignore them.
- **Usability of computer systems in general**
  Users are so accustomed to accept security warnings and other error messages that they do not feel that those are important. Hence, this poor usability of software and operating systems make people to ignore also real security warnings.
- **Feeling of security**
  Users feel that web browser is under their control and they

do not need redundant security features to slow down their job. They might think that security risks in the Internet are over-hyped.

According to current knowledge, it seems that lack of knowledge and lack of attention of the users are the major reasons for success of phishing. However, there is not much research results available about feeling of the security and how that affects the users' behavior on the Internet, thus there could be space for further research on this area.

Solution proposals

Considering these facts, some possible solutions should be available to prevent the phishing or at least to mitigate the harm caused by phishing attacks. These may be training the users, developing new usability solutions or developing better anti-phishing tools with also better usability.

Training all the Internet users is not practically possible. Also, even if the users were trained, it is still unclear how efficient that would be – the users could still not care about their security as they might not feel that important. Developing better anti-phishing tools is one option – however, it is likely that developing a perfect anti-phishing tool is not possible in practice.

Hence, the way to go is improving the usability of the web browsers and other relevant software so that users would take the warnings more seriously. In most cases it is not efficient to only warn user that something is wrong and user should not proceed. Users mostly take the risk, because they have some reason to do whatever they are doing. The better solution could be to advice the users how to finish their tasks in a safe way. [14]

As pointed out earlier, one reason for the ignoring of the security warnings is that there is so much warnings and error messages shown for the users. Most of these are also totally useless. For example, some firewall softwares ask confirmation from the user for every single process that is accessing to the network. Average user is not aware of the meaning of all those messages. Users mostly accept all those warnings to get rid of them. Thus, the warnings are useless as they are not read but only accepted.

Also, web browsers always show large warning message if the user is accessing a website, which security certificate has expired. This is not correct approach. The website with an expired or not validated security certificate is technically not any less secure than the website with no certificate at all – like almost all websites. Actually even an expired or invalid security certificate provides a secured connection between the client and the server. However, the legitimacy of the service can not be verified if the certificate is not valid.

Thus, the correct approach would be not to show big warning messages to users, which they should accept. Instead, the website with invalid certificate could be shown same way as the websites without certificate at all. The users should not get a false assumption that the website with invalid certificate is verified to be legitimate. However, users should not either get a false assumption that the website is fraudulent, as an expired certificate does not mean that.

In overall, the computer systems should show less alerts for the users. Most of them are never read and they are mostly slowing down users' primary tasks. In really important cases the user should be warned clearly in a way that standard user understands. Warning which says that website certificate has expired means nothing to most users.

Finally, to avoid confusion the companies should follow some standard practices when building security critical websites [14]. For example, the certificates should be up to date and verified by an authority. It is very common that even large companies have expired certificates on their web services. Also, the companies and organizations should use the one, consistent domain name, so that users could not easily be spoofed with false domain names.

CONCLUSION

In this paper we discussed about why people fall for phishing. At first, background of phishing was explained, such as what motivates phishers, and different phishing strategies were listed. After that the automatic and natural strategies for detecting and preventing phishing were presented. Finally, the reasons for why phishing works were evaluated and some new findings were proposed.

There is several strategies for detecting phishing. Human decisions are often based on look and feel of websites, the correctness of text content or visual appearance. More advanced users are aware of the security indicators, such as encrypted connection and validity of the security certificates. Automatic strategies used by security software are based on lists of known malicious websites or technical properties, such as validity of certificates or correct domain name.

The main reasons for success of phishing are users' lack of knowledge and attention or false assumption about functionality of the Internet and software. Also, the users do not always feel that they need any external security features or warnings. As a solution it is proposed that usability of the software should be improved – and not only the security software but all software. Users should not be disrupted with useless warning messages. Also the companies should keep their security certificates up to date and domain names and services in standard format to avoid the confusion among users.

REFERENCES

1. Anti-phishing working group: Phishing activity trends report, march 2004.
2. Gartner inc.: Gartner study finds significant increase in e-mail phishing attacks.
3. Anti-phishing working group: Phishing activity trends report, 2nd quarter 2010.
4. Abu-Nimeh, S., and Nair, S. Bypassing security toolbars and phishing filters via dns poisoning. In

Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008. IEEE (30 2008-dec. 4 2008), 1 –6.

5. Badra, M., El-Sawda, S., and Hajjeh, I. Phishing attacks and solutions. In *Proceedings of the 3rd international conference on Mobile multimedia communications*, MobiMedia '07, ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering) (ICST, Brussels, Belgium, Belgium, 2007), 42:1–42:6.

6. Dhamija, R., Tygar, J. D., and Hearst, M. Why phishing works. In *Proceedings of the SIGCHI conference on Human Factors in computing systems*, CHI '06, ACM (New York, NY, USA, 2006), 581–590.

7. Downs, J. S., Holbrook, M. B., and Cranor, L. F. Decision strategies and susceptibility to phishing. In *Proceedings of the second symposium on Usable privacy and security*, SOUPS '06, ACM (New York, NY, USA, 2006), 79–90.

8. Irani, D., Webb, S., Giffin, J., and Pu, C. Evolutionary study of phishing. In *eCrime Researchers Summit, 2008* (oct. 2008), 1 –10.

9. Jagatic, T. N., Johnson, N. A., Jakobsson, M., and Menczer, F. Social phishing. *Commun. ACM 50* (October 2007), 94–100.

10. Jakobsson, M., and Ratkiewicz, J. Designing ethical phishing experiments: a study of (rot13) ronl query features. In *Proceedings of the 15th international conference on World Wide Web*, WWW '06, ACM (New York, NY, USA, 2006), 513–522.

11. Oza, N., Karppinen, K., and Savola, R. User experience and security in the cloud – an empirical study in the finnish cloud consortium. In *Cloud Computing Technology and Science (CloudCom), 2010 IEEE Second International Conference on* (2010), 621 –628.

12. Schneier, B. Psychology of security.

13. Watson, D., Holz, T., and Sven, M. Know your enemy: Phishing.

14. Wu, M., Miller, R. C., and Garfinkel, S. L. Do security toolbars actually prevent phishing attacks? In *Proceedings of the SIGCHI conference on Human Factors in computing systems*, CHI '06, ACM (New York, NY, USA, 2006), 601–610.

15. Yu, W., Nargundkar, S., and Tiruthani, N. A phishing vulnerability analysis of web based systems. In *Computers and Communications, 2008. ISCC 2008. IEEE Symposium on* (july 2008), 326 –331.