An Assessment of Security Advisory Websites

J.Thomas and S.M.Furnell

Centre for Information Security and Network Research,
University of Plymouth, Plymouth, United Kingdom
e-mail: info@cscan.org

Abstract

Home users have been an interesting target for the hackers as home computers are always more vulnerable and less protected with the security software's. Home users feel that security is not necessary to be maintained and is not their duty to maintain it. But at the same time home users do online banking and shopping and store valuable information in their systems which are very precious for the hackers, as they can earn money by selling it to third party. The research was carried out to assess the online security websites that the end-users normally access in getting help and also the online banking websites which the home users normally use for their daily purposes. The research found out that many websites did not prove to be useful as they ought to be. The websites were being developed in a way which the end-users normally, most of them who falls in the novice users would find it difficult. At the same time websites like Microsoft provided with a good structure of the contents thereby dividing into subsections for the better use of the end-users such that they could select what they want. But there was also some problems with the websites because there was much content in the websites, which may sometimes trouble users who are visiting the websites for the first time.

Most of the websites just provided links to some other websites for assessing the security, but did not mention anything much about the software and it's functioning. The websites were just pointing to some common threats, thereby not giving any examples of how to deal with the problems apart from just mentioning the names. Many of the websites did not show any information about the last updates they made on the website there by leaving the users in a confused state of mind. Most websites did not mention the latest threats apart from Microsoft which releases patches and updates for all its products. The research also provided some safety tips for the end-users when connected to the internet.

Keywords

Antivirus, Spywares, malwares, online Security websites, online banking, phishing

1 Introduction

The low cost of communication over the internet has made people to use it for maximum purpose, whether it may be sending mail, shopping or banking. The reliability has changed everybody to make use of it. The websites has been one of the main targets for the hackers; the main noticeable thing is that the common websites are being targeted where users spent much of their time when connected to the internet. The websites are being targeted to get the personal information's very easily by sending Phishing mails or some links which might contain some adware or Spyware which might work without the knowledge of the user if the link is clicked.

Most of the websites are interlinked to each other such that it makes easy for the hackers to get the information quickly. According to report published by the

Symantec it states that threats are sky rocketing and in 2007 there was around 711,912 threats as compared to the 125,243 in 2006. So it clearly states that the threats are not going to come down. The reason for this threats increasing is because most of the people are not concerned about the Security. People just open all the e-mails and post everything on the computer with using correct security software's like anti-virus, anti Spyware and e-mail filters being enabled.

2 A Report on Different Attacking Trends

Symantec reports that Microsoft Internet Explorer is the most widely affected web browser because of its dominance all over the world. During the first half of 2006 it states that Microsoft was attacked with 47% against 20% Mozila Firefox, 31% having multiple browsers and just 2% with Netscape navigator. It also found out that home users were the most targeted sector when compared to other sectors with 86% as that of 96% before, though there was reduction it does not mean that there is no threat to the home users. The ISP providers were also attacked with 38% affecting them with the denial of service attack. In the windows exposure which means that there are some loop holes in the operating systems. It was Mozila which had the largest number of vulnerabilities when compared to other web browsers even though it was not that popular as that of Microsoft Internet Explorer.

3 Assessment of online Security Website

3.1 Introduction

When talking about the online security websites some names that come into our mind is the Viruses, Trojan horses, Spyware, Adware and Phishing that make the users always vulnerable. While each one of them had there own functions but in general it could be categorized as some software that is used to track the user's habits of browsing and gain unauthorized information from the user. When people use online websites, they use for many purposes, like banking, shopping, downloading music or movies by paying them online by having some membership in some websites. When using the Internet it is necessary that it should keep it updated with all security software and firewalls being enabled.

3.2 Methodology and Analysis

In the methodology the researcher is going to find out what are the resources available for the End users from the security websites which claim to provide help for the end-users from protecting them from all sorts of attacks. The researcher before choosing the methodology went through the Google search engine in determine the evaluating the websites that provide online security for the End-users. So while going through the search engines different varieties of online security websites came in the search and from there the researcher chose some websites for assessment depending on the founders and sponsors of the website. Since most of the

websites chosen were supported by Governments, Microsoft, Internet Industry Corporation and National cyber security Alliance. The other reason for choosing these websites were because of its popularity like Microsoft which is famous for it's regular updates and patches. Also while going through different web pages the researcher found some of websites being mentioned and recommended for security, so based on all the above factors the researcher found that the selected websites would be having many new updates and it would be more useful than the other websites since they can be trusted about the contents in the websites, since all of them are widely accepted and standard.

In the second case the researcher used most of the popular bank websites which people uses more for their daily banking needs and based upon their outreach in the country. So the researcher chose almost majority of the banks that provide online banking to the customers. So once the websites have been chosen the researcher tried to analyse how to assess the selected websites and after evaluating the websites the researcher came to some points that could be used.

In the analysis the researcher is going to assess some websites based on some factors that provide the some valuable information to the user. They are as follows:

- Based on latest online threats
- Based on methods to troubleshoot the online threats
- Based on providing users with the information to keep updated
- Based on the software's for protecting the system and the information
- Based upon examples given in the website
- Based upon checking the websites that provide online self assessment in their websites than rather other websites.

A. Staysafeonline

So based on the above mentioned factors it was noticed that many of the websites did not provide the users with the required details when they encountered problems. They just mentioned some names of the software but did not explained how to configure it or where to find the resources that was needed to update the system. The website was not arranged in a simple manner, finding the resources was very difficult, everything was complex for the user. The website provided with many online scans but did not mention about the version they are using.

B. Getsafeonline

The website when compared to Staysafeonline was much better because it was arranged in an appropriate manner; everything was arranged in a perfect manner which allows the users to get what they want. So there was no difficulty in accessing the resources. The website had a clear description about all that is being provided and it would be helpful for the novice users for they can understand about everything that is being posted on the website.

C. Microsoft

Microsoft is one of the best websites which provide the users with what they need, the website is always updated with latest threats and the vulnerabilities being displayed on the website whereby making the user to know exactly what is happening in the internet world. The website has been divided into different sections whereby enabling user to select what they want, it has security and update section together such that no user will miss anything, on clicking the respectful link it will take the user on that particular website. It also has a page where it is possible to have the problems solved if they are mailed to them, they also provide online help.

But at the same time there is also one disadvantage that is the webpage consists of much information and it would not be easy for everyone to get the desired information even though everything is there. It would be difficult for the novice users. So it is very necessary to think it in a way that would make every body self sufficient. The websites can do is, they can create a feedback form such that the designers could get a clear understanding of the problems that users face.

4 Assessment of online banking website

Online banking websites are now one of the major websites the hacker's attacks, due to the amount of the information they possess with them. The banks claim to have many security options being developed but the fact is that still there are some loopholes which the hackers find out in claiming the information's they want. One form of success for the hackers is the Phishing where by many users pass their vital information to third parties not knowing that they are giving away which might cause much problem afterwards.

The HSBC bank offers an individual webpage for security, the website offers many of the most common problems being faced by the users, but the information is in sufficient for the end users because they are not given a complete description of the problems and how to rectify it. It is not necessary that all the users of the online banking system be an expert user of computer, because even expert users are being fooled by the cyber criminals. The bank claims to use some extra protection like EV-CERTS which means extended validation SSL certificate, whereas at the webpage they claim that even though they provide with security, it does not mean that it is secure, when users sees it they are confused.

On the other hand Lloyds bank claims that they have some in built features which enable the security of the users like automatic log off if the webpage is idle for sometime or if more numbers of incorrect entries are being made. This is something good when compared to other banks even though some other banks also provide the same features, each bank has own there own way of security.

Banks like Barclays they provide a new mechanism called PIN SENTRY which gives the users a card reader and they have to insert their card onto the reader and it displays and eight digit number which has to be entered while using online, the fact is good but if the user's system is not updated then some software can find out their key strokes, but what the bank claims is that every time the user enters the card it

creates random numbers thereby making hackers unable to track the number, but also there is another problem what if they get hold of the card reader such that they can make duplicate cards. So security is never going to be an complete factor.

5 User awareness and usability of security

People now a days use computer in all their daily activities, it is quite noticing that people use internet more for browsing and sending e-mail, shopping and banking which all stands above the 60%. So it shows people's interests in the internet. But the case is that most people do not use much of the security that is being provided to them and also this is causing much trouble to the end-users. A research survey (Furnell *et al*, 2007) had been conducted for the home users and around 415, responded to the survey and it was very interesting to find out many facts about the security awareness that home users possess. From the survey it found that people had problems in all the above mentioned five points, on the security related terms the respondents mentioned that they knew almost about every terms, the only term that they did not know was the term Phishing. But the factor is that how much of the mentioned terms has been clearly understood by the home users, is it that they had just heard the name or whether they have faced some problems is not known. So it depends upon the user's knowledge in the field of security and if working in the IT field, then it would be good to know that what they say is correct. Home users always depend on their assumptions rather than finding out the fact.

When based on security software awareness, majority of them claim to say that they know about the security softwares but it is also noticing that many do not understand about the security software's in real which could also be an problem why the users get problems. Majority of the users claim that they know well about the web browsers because they normally quite often use that. When taken into consideration about the software's it was those softwares which the people normally use like the office programs, e-mail programs like the outlook and above all the operating systems. One of the great reasons for mentioning this is because users they do not feel that it is the responsibility of them to understand them. Even though people are being given with the available resources that are for the better management of security many people do not offer to make use of that. Around four websites had been selected and this websites are developed to provide security help for the users, the websites are Getsafeonline, itsafe, internetsecurityzone and the BBC website.

From the survey it was found that people heard of the BBC website much more than the other three and also visited the website and found it useful in their quest for solutions to the problem. What was noticed is that people visit websites that are much popular and because of that only they visited the BBC website. So the researcher found that the other websites which was also designed for security reasons being avoided by the home users.

Based on the factors of reporting problems it was not sure which way to go for the end-users, so it was more vulnerable than the previous conditions leaving the system at a higher state of risks , this shows that people do not know how to maintain security and they are not worried about safeguarding it. What the users did was that they tried to solve by themselves and the remaining people went to government

agencies, some to IT professionals and some to their ISP providers. This shows that they are neither interested in security or they find it as their responsibility to report it. The problems that prevented from using the security could be the following reasons:

1. The user thinks that it is not their responsibility
2. The user feels that the security issues are of not great concern for them.
3. It might be because of lack of time that they do not keep an eye on the security of the system.
4. Security softwares would be much expensive
5. The users not knowing how to use the security products.
6. They might not know how to keep secure the computers which is because they do not know about the threats or they do not understand about the threats that they come through.

Given the above points it is much sure that users feel trouble in understanding the problem and getting the correct help they need. So where is the fault that happened because of which the users were not able to keep their systems safe. The problem lies with the designers of the websites whereby confusing them in selecting the desired link and get to the help. In general the websites should have the following four foundations such that to make the users use the resources available to them.

1. Understandable

The security descriptions should be given with much responsibility and they should be intended for all types of user, the helps should be written in simple language which makes it easy for the novices who are not familiar with the technical words.

2. Locatable

The contents on the webpage must be divided into subsections that might make the users easy to find out what they want, because if it is designed in a complex way then it would bring much trouble to the users and they would leave the website without accessing it making it not useful for any body. People nowqdays do not spent much time on spending with security matters searching long time.

3. Visible

Most of security configurations are hidden, one has to go to the security page and configure each setting which many users may find it very difficult. Security options should be known to the user and there should be some alerts if the security has not been configured, then only the users will know which security has been applied and would know the level of protection they have.

4. Convenient

On the other hand the most important thing is to make sure that everything is convenient, in the sense the security options should not be displayed openly such that others could know and make use of the loopholes if the program is being displayed openly. Security packages are costly for some of the users at the same time some

users do not know how to configure because there is not much information given about the configuration of the softwares which will also lead in people discarding the software.

All the websites should be developed in such a way thereby making the users knowing sure where they have to go. The websites should be designed in a simple manner with simple language and perfect arrangement for the users, when developing the websites they should also provide some feedback form for the users to take part, such that the developers would know the user attitudes. According to an Symantec global internet security threat report, it reveals many of the factors that are happening in the computing world. Some of the findings are as follows- it states that United States accounted for 31% of the malicious activity, which is an increase from 30 percent which was in the first half of 2007. The United States was also the top country in terms of origin of attacks. The education sector was accounted at 24% of data breaches which could lead to identity theft. Government sector accounted for the top sector in revealing the identities outside without the user's knowledge. Bank accounts were the most commonly advertised item for sale without the customer's knowledge. The other thing noticed was that there was also theft of computer and information's on other data storage devices, this all shows that the security is at a very bad stage whereas even though the security is not considered as a top priority by the many organisations that should have kept the data safe

6 Conclusions

What the researcher would recommend will be that the safeguarding of the data should be the responsibility of both employer and the employee whatever be the organization. The interesting thing is that even though after providing with much information about the threats the users face problem, and are still ignorant about the security. The people should be made to sign some agreements before using the online services in the bank.

There must be rules for the home users as well and also for the ISP providers, they should make sure that the network is safe and also should create awareness from the children to the old people about the latest threats, educational institutions should must teach the students by showing of the threats and ways in which they can be targeted. Home users should be encouraged to use legitimate softwares such that they get good softwares and updates. There is tremendous work to be done on the basis of security, because the developments in the technology are very fast but safeguarding principles lack. The users of computer should be made to read the rules and regulations before working with the computer.

7 References

Barclays Online banking website (2008) , http://www.barclays.com/. (Accessed 28 August 2008)

Furnell, S. M., Bryant, P. and Phippen, A. D. (2007) "Assessing the security perceptions of internet users", *computers & Security* vol 26(5): Pages 410-417

Furnell, S.M., Jusoh, A. and Katsabas, D. (2006) "The challenges of understanding and using security: A survey of End-Users", *computers & Security* vol. 25(1): Pages 27-35.

Getsafeonline website (2008), http://www.getsafeonline.org/ . (Accessed 29 August 2008) HSBC Online banking website (2008) , http://www.hsbc.co.uk/1/2/ .(Accessed 28 August 2008)

LloydsOnline Banking website (2008), http://www.lloydstsb.com/. (Accessed 28 August 2008

Microsoft website (2008),http://www.microsoft.com/en/us/default.aspx. (Accessed 29 August 2008)

Staysafeonline website (2008), http://www.staysafeonline.org/. (Accessed 28 August 2008)

Symantec (2006), Symantec Internet Security Threat report: Trends for January 2006- June 2006.vol .10 http://www.symantec.com/specprog/threatreport/ent-whitepaper_symantec_internet_security_threat_report_x_09_2006.en-us.pdf (Accessed 27 August 2008)

Symantec (2008), Symantec Global Internet Security Report: Trends for july 2007- December 2007. Vol.13. http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiii_04-2008.en-us.pdf (Accessed 28August 2008)

Symantec (2008), Symantec Report: Attacks increasingly target trusted web sites. http://www.symantec.com/business/resources/articles/article.jsp?aid=20080513_sym_report_attacks_increasingly (Accessed 29 August 2008)