

Evaluating the Perceptions of People towards Online Security

N.K.Jayakumar and A.D.Phippen

Network Research Group, University of Plymouth, United Kingdom
e-mail: info@network-research-group.org

Abstract

People started using online services in day to day life from the period; when they came to know about the use and ease of the technology. Services like online banking, online product purchase or sale, instant messaging, electronic mail, online voting, medical, paying tax, etc are mostly commonly used by the people. The growth of the online commerce is the reason for the significant increase in the use of online services and also increase in the variety of fraudulent web activities. Almost all the users are the victim for the internet threats, in some way. So the project aims in evaluating the perceptions of individual users about the online security and its issues. The perception of online issues differs from each and every individual like 'Normal User, Internet Users and Security Professional' because the normal user just operates/uses the system without having much knowledge about the causes and threats that are caused due to online services whereas the internet users are known to some available threats like virus, spyware, malware, etc but the security professionals are known to all kinds of threats that are available and its causes. Security professionals always keep themselves updated with the change in security issues and its threats because it's their part of the profession, they are known to latest virus, worms, malware, spyware, intrusion option, cookies, firewall, trojan horses and other security related options provided on the client/user systems etc. In this project, a survey is taken as a part of research from the people to reveal their views towards online security; which will increase the awareness about the threats that are caused due to the online transaction and services. The final survey result concluded that the users/people are known to some threats but not all, and there are some hindrances for the user from utilizing the full security, which have been discussed in the final part.

Keywords

Online security issues, Security threats, Grouped survey discussion

1. Background

In today's world almost everything is done with the help of online services 'Buying/Selling/Ordering/Contracting/Renting of products, Bank transaction, E-mail, Messaging, Online Vote, Tax payments etc', the use of these kind of services was increased recently due to the rapid growth of the internet during the past decade. Almost all the users of the system find that the use of technology was an ease but they are not fully aware about the causes and threats behind it. Own instance: - The People instead of going to shops to purchase the needed products; they started to use online to order things to their door steps. The online transaction made mans life easier in processing the information they need; and to do things faster and in an easier way, but it started to cause threats which is mostly unknown to the users because of the awareness towards the causes. Threats caused to the users / people in

the sense; during the online transaction to purchase a product from an online store, the user enters the personal information like credit card number, security code, card holder name, etc., which has been transmitted over the internet for placing the order but the user is not sure whether the given details might be hacked by someone for their personal use or whether it reaches the exact destination for placing the desired product order. The users of online services are facing most of the problems which are not known to them directly but the effects of the problem are caused indirectly by any means of source like 'Phishing attacks, Scam, Unsolicited adverts, Identity/Privacy theft, Virus, Spam' etc.

2. Importance of Security to prevent the online threats

Online services are used by the people in day to day life, which runs fully on the internet where the whole world can access the information stored on it and thus making it an insecure environment for someone who wants to be secure (Joris Evers, 2006). As the service started to grow day by day, the new threats have evolved creating a fear among the users, making them to be more concerned about 'what the particular threat is going to do...?' (Michael Bruck, 2006) and it appears to be like 'Internet/Online' has lots of threats when compared to other technologies that have been developed to ease the living of human being (Andy Sullivan, 2006) the main threats which affects the user system the most are 'Worms, Break-ins, Hackers, Crackers, Hi-jackers, Phrackers, Spoofing, Password sniffing, Denial of service' etc. There are still lots of users using the online service who are very vulnerable to attacks mainly due to the awareness of the nature of the attacks and they still believe that a good password is the only need to be concerned about and they are not worried about the behind threats.

3. Project Survey Procedure

The project work was started with the aim in finding the user's level of awareness in every security aspect and issues 'what they think, why they think like that, what are their fears in threats...' Etc. So after finding the awareness level of the user/people; it would be easy to eradicate the problems just by knowing the right steps to be taken 'whether the problem exist within the user due to unawareness or the problem exist within the developed software/application' (Robert Vamosi, 2006). For this finding, the project works by taking a survey from the user/people which enquires them in all aspects of security issues about the known and unknown threats. The survey is not only taken from students who are doing their degree but also from workman, professionals, normal person who does not know about the security issues, this kind of survey is taken to reach in-depth level of people awareness.

4. Discussion from grouped survey graph

The Figure 1 says that, users fully agree that they are known to 'Existence of viruses, Causes of viruses, Concerned about damage caused by viruses and Regular scanning of computer for virus' but their level of agree to 'Regular updating to virus definitions' is low when compared to other issues, it is because users/people normally forget that virus definitions is most needed part of the antivirus software, so

in total nearly 87% of users are agreeing that they are known to issues of virus threats and 13% of users are not known to the issues of virus threats.

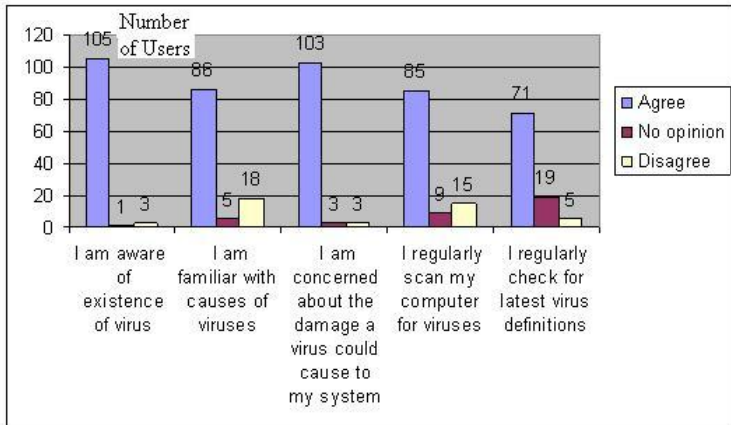


Figure 1: Grouped survey graph for virus threats

The Figure 2 says that, users fully agree that they are ‘Aware of spam attacks, Receiving unsolicited advert in email, Use filters to block spam, and Receiving spam daily’ but their level of agree to ‘Reporting spam to provider’ is very low when compared to other issues, it is because user/people do not want to waste time in doing it, so in total nearly 79.5% of users are agreeing that they are known to issues of spam threats and 20.5% of users are not known to the issues of spam threats.

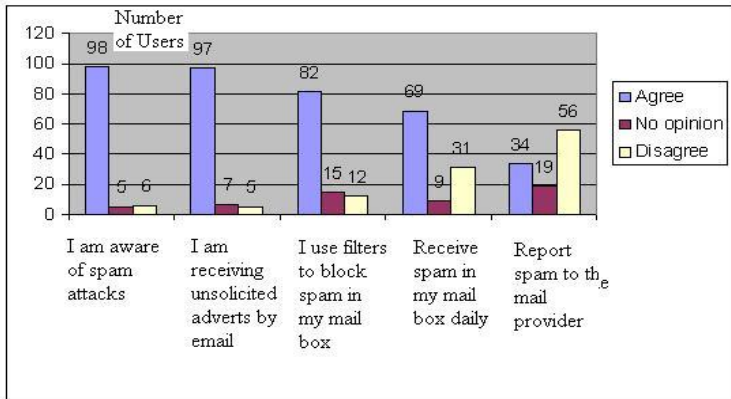


Figure 2: Grouped survey graph for spam threats

The Figure 3 says that, users fully agree that they ‘Always open email from family and friends, Always open email from known companies, Always open email from unknown senders, My responsibility to protect my system from threats and Scan all mails using mail scanner’, so in total nearly 79.5% of users are agreeing that they are known to issues of Email threats and 20.5% of users are not known to the issues of Email threats.

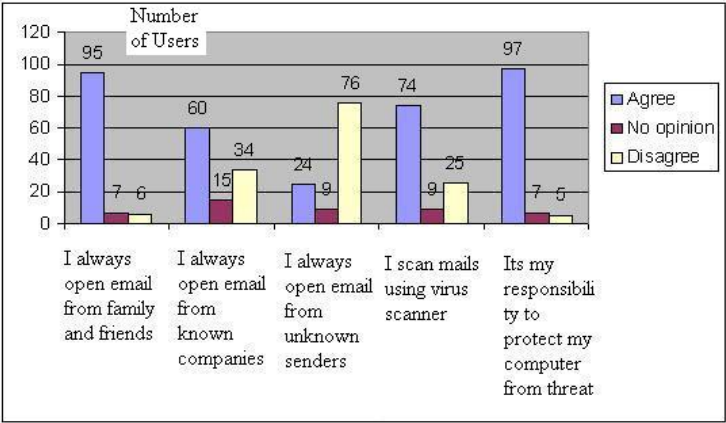


Figure 3: Grouped survey graph for email threats

The Figure 4 says that, users fully agree that they ‘Disclose bank/card details during online transaction, Always use online banking, Feel risk at online fraud, Have required knowledge to protect the computer’ and their level of disagree to ‘Disclose bank/card details via email’ is very low when compared to other issues, it is because user/people is fully aware of not to disclose anything in email messages, so in total nearly 52.5% of users are agreeing that they are known to issues of online threats, also using the online transaction in a safer way and 47.5% of users are not known to the issues of online threats, disclosing the bank/card details online will increase the chances of threat.

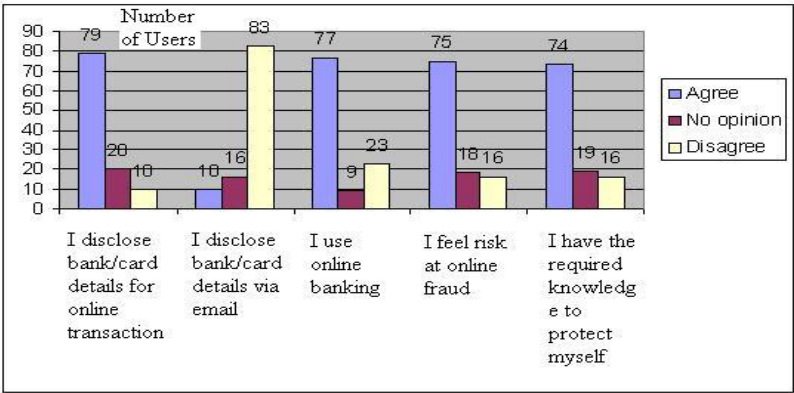


Figure 4: Grouped survey graph for online transaction threats

The Figure 5 says that, users agree that they are ‘Happy to fill tax return online, Happy to vote online, Happy to give medical details online, Worried about amount of data held about them in online’, it is because user/people are fully aware of what they are doing in online life, so in total nearly 50.5% of users are agreeing that they are known to issues of online life threats and 49.5% of users are not known to the issues of online life threats.

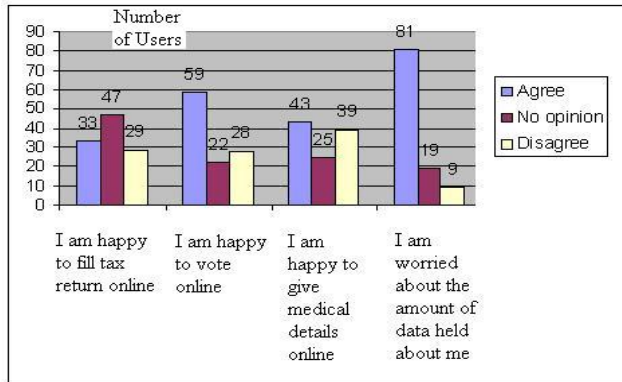


Figure 5: Grouped survey graph for online life threats

5. Limitations

The project research has analysed that there is no limitation in online service and security issues until or unless, the users of the system are getting aware of the upcoming/new online issues and attacks. If the user stays behind without updating their knowledge about the available threats; they might be one of the victims who will be attacked by the online threats, which will led them not to use the online services due to the fear. So its better all the users make themselves updated to latest threats, which will help them to get protected from the attacks and will be able to use the online service without any further interrupts.

6. Future work

Almost all the security companies like ‘HP, Symantec, McAfee, eTrust, BT, Lavasoft...’etc are trying to implement a perfect secure system for the users to use in the future without any threat/attack in online services, for this purpose ‘HP’ has started taking survey to understand a depth knowledge of user ‘In what areas of online service, the users faces the main problem..’, (Peter Szor, 2006) their survey resulted in users awareness as a main conclusion, so the HP company has decided to give a clear view about the software they use or terms and condition they sign or company software licence. Likewise all the security software’s features are to made short and clear, so that the user themselves can make a proper configuration and can prevent their system from threat attacks.

7. Conclusion

The project is concluded with the awareness level of the user related with online security and its issues, from the discussion of grouped graph it is clearly understood that the user is known to the ‘Threats caused due to Viruses, Spam, and Email’ because they are able to see and understand that they have been attacked by someone or something, but they are not known to the ‘Threats caused due to Online transaction and Online life’ because these threats cannot be identified by the user until they are known later that they have been attacked. We know a saying

‘Prevention is better than cure’ likewise it is better that the user being aware to all the existing/new threats, so that they can prevent themselves from being attack instead of noticing later that they have been attacked due to online threats. Not all the people will be able to browse the internet and come to know about the latest threats available because they might be very busy at work or did not find any time to search for new threats. So it is better that the security companies like ‘HP, Symantec, McAfee and others’ start to release threat notes monthly or quarterly year that should be easily readable and understandable even by a normal person, all the companies should take consideration from Normal user – Expert user in case of security issues and threats, so that it will easy for all level of users to be aware of online attacks.

8. References

Bruck, M. (2006), “Security threats from within people”,
<http://www.entrepreneur.com/technology/managingtechnology/article503414.htm>, (Accessed 26 June 2006)

Evers, J. (2006), “The security risk in web”,
http://news.com.com/The+security+risk+in+Web+2.0/2100-1002_3-60992128.html,
(Accessed 24 June 2006)

Sullivan, A. (2006), “Internet technologies emerge as new online threat”,
<http://www.forbes.com/markets/newswire/2006/06/26/rtr1335591.html>, (Accessed 26 June 2006)

Szor, P. (2006), “Security system extends relationship with HP”, <http://phx.corporate-ir.net/phoenix.zhtml?c=933082&p=irol-newsArticle&ID=309055&highlight=>, (Accessed 29 June 2006)

Vamosi, R. (2006) , “AOL Active Security Monitor”,
http://reviews.cnet.com/AOL_Active_Security_Monitor/4505-3667_7-319294263.html,
(Accessed 28 June 2006)