**The success of e‐commerce solutions depends on trust. To what extent are viruses and hacking reducing the trust that consumers have in e‐commerce solutions and limiting the potential gains from this?**

Submitted By:

Milan Humagain

10011027

Submitted To:

Ray Scott

**Abstract and Executive Summary:**

This report is mainly about the success of e-commerce and how people react on the services that is being provided by the e-commerce technology timely and in case of threat of hacking and viruses what are the measures that can be put forward to protect ourselves from being the victim of cybercrime. This study was to build a faith on people about e-commerce as it has already been the part of our daily lives and is the easiest way to buy and sell goods. Hackers are trying their best to pull e-commerce back hacking different credit card numbers, computer systems and so on but securities are the one which prevent us from these things and teach us how to co-operate with e-commerce. We know to what extent viruses can pass bad things and harm the customers and impersonate them but use of safe checkout, setting of strong passwords can be helpful to be safe and bright.

The report was requested by Ray Scott and I Milan humagain reflect the security measure, trust and familiarisation along whit the threat of hacking on e-commerce and finally came to know is, hacking not only effect the customers, companies and huge organizations but also effect policy makers and perceive hackers themselves.

**TABLE OF CONTENTS**

**ABSTRACT AND EXECUTIVE SUMMARY**

1. **INTRODUCTION TO E-COMMERCE**
2. **LITERATURE REVIEW**
   1. Trust and Familiarisation
   2. Hacking and viruses
   3. Hacking and its impact on people
   4. Comparison
3. **DISCUSSION** 
   1. Findings
   2. Countermeasures
4. **CONCLUSION**
5. **RECOMMENDATION**
6. **REFERENCES**
7. **Introduction to e-Commerce:**

Simply, e-Commerce is defined as the commercial transactions conducted electronically with the help of internet. Nowadays, most of the people use e-Commerce for buying and selling of goods and services or to transmitting funds or data over an electronic network with the help of internet.

It really changes the lives of many people and sifted the commerce sector from brick and mortar business to the online platform. While the internet has become an effective tool for productivity, it has also become a breeding ground for crime and malicious behaviour. Viruses causes the loss in business or negative impact on people. For some the main goal for committing cybercrime is to profit financially. E-Commerce website utilize internal networks that may interface with the worldwide web. Viruses can destroy all the internal information and a whole working system. If they hacked the system, then they can pass bad things and codes to customers and impersonate them.

Malicious software is used to gather sensitive data, gain unauthorized access to website and even hijack computers. It harms our website as well as website visitors. With the help of Malware attackers can steal confidential data including Credit Card info and SSNs, make unnecessary purchase, create spam and play with the user’s login information.

Google blacklists about ten thousand websites each day. When a website is blacklisted, Google will temporarily remove it from its index. Even Google does its best for the blacklisted websites we shouldn’t rely on its notification and should practice our best to keep our websites secure on our own.

The goal of this paper is to determine whether the people are having trust on themselves towards electronic payment devices or they are worried and got expectation on having more secure payment systems. Hacking, trust and e-commerce are the part of our study. People’s trust on internet is because of companies selling their goods through the world wide web interface. Only the concern of people is on privacy policy. If the proper privacy policy is maintained, there is no doubt about the familiarisation and trust on e-commerce. In every good side there exist some bad one but the good always win. Hacking can also be understood by analysing it through technological and sociological perspectives. Many companies are applying many types of securities to protect themselves from malicious software.

1. **Literature review:**

*2.1 Trust and Familiarisation*

According David Gefen(2000), E-commerce is the one which is growing rapidly and the number of people buying from internet was increased rapidly in these years. People’s trust in internet is because of companies that sell their goods through the World Wide Web interface. In fact, the Better Business Bureau claims that the main reason people don’t buy in online is their concern regarding the lack of privacy policy and security, reliability of companies and online payment security. Trust should be the major issues in e-commerce. While people download web software then too the security comes first. Trust is the main factor in E-commerce as it creates a framework and understanding of the environment and the trusted party within which the expectation of trust can be expected. According to the Author of this report, he suggested that the effect of trust was important on stronger decisions either its purchasing books or something else even through the well-known and popular shopping site like Amazon.com.

* 1. *Hacking and viruses*

“**Are Ethical Hackers the Best Solution for Combating the Growing World of Cyber-Crime?”** written by Devin Marsh, describes about the regular problem facing by various government agencies because of Cybercrimes. Especially, the person who theft the data like credit card numbers and the global system of computer are known as hackers or black-hat hackers.

Black hat hackers are the person responsible for the crime or attacks on big corporations. Many companies prevent themselves by rotating their passwords timely and many use firewalls to prevent malware penetrating the system. As per the article; Computer, smart phones and many new innovations make people more innovative and rely on them for each activity.

* 1. *Hacking and its impact on people*

According to Michael Lee and his team (2009), it lost over fifty million dollars when hackers downloaded more than 50,000 credit card numbers and Citibank lost ten million dollars when its computer network was compromised by a crime group in Russia.

Firstly, they collected the data that are not securely put on the internet and used it for illegal purpose. Secondly, determine the public confidence in safety and in conducting financial online transactions. It effects consumers, policy makers and perceive hackers because hackers are typically characterised as “super-criminals” with extraordinary power and malicious intent. Still many consumers will be afraid in buying and selling goods and services over the internet even with adequate safeguards. The economic threat posed by hackers an only be understood by analysing the term hacking from both technological(code-based) and sociological(norms-based) perspectives.

* 1. *Comparison*

By comparing these three articles as a part of my report I came to know that, the trust on people while buying and selling goods and security on e-commerce are like two sides of a coin as it reflects the future of e-commerce in coming days. The only thing people don’t buy goods through online is because concerns regarding, privacy policy and security, reliability of company and online payment security. We need security in e-commerce because the persons stealing the data like the credit card numbers and the computer system are increasing. To prevent the fraud from e-commerce we can use various methods of prevention such as password rotation, firewall prevention and so on.

People rely on e-commerce for their everyday operation so people use online banking for regular transactions. While people use online banking, it will be easy for the hackers to be rich in a minute as Citibank already lost its ten million dollars when its computer network was compromised. Lastly, it was found the system was hacked by the crime group of Russia.

Hackers aren’t trying the safe network for illegal purpose but they determine the weak and advantageous one and tried them looking at the financial online transactions. As I had already discussed that the trust is everything in e-commerce, still people are afraid of buy and sell goods even knowing that internet have full safeguards. So, hacking is also the part of e-commerce but the strong security can prevent us from various fraud activities.

1. **Discussion:**

*3.1 Findings*

E-Commerce in the present days is being more important to various organizations and they have had a use of it in their daily operations. It is commonly used in electronic activities, communications and interactions. E-Commerce itself is related with crime known as cybercrime. Because of various crimes over the electrical activities the users of victimized company are losing confidence. Such things might also reduce the market value of several victimized organizations

Everything we do in our daily life have risk. E-Commerce is a business that holds various transactions and doing transactions includes various risk such as Stolen Credit card number, buying and selling goods and the paid never arises, stolen security number, etcetera. It needs to have no physical contact. E-commerce these days aren’t like the previous one. When is system is digitalised it creates exceptional challenges for online information and digital information. Wen trust is lost the probability of loss is very high. Open sharing of information with public might create a problem and the international bodies will facilitate us for successful detection and prevention of our information.

Literatures in various academic disciplines try to investigate the behaviour of those who engage in cybercrimes. Mostly, the person who is responsible for cybercrime is hacker or some other computer expert. Cybercrime includes cyber terrorism, electronic theft, espionage, internet credit card fraud and phishing. Mostly from this crime the companies like Amazon, e-Bay and yahoo are affected.

*3.2 Countermeasures*

There are various ways of hacking but it can be counter with several countermeasures. Firstly, choose a secure e-commerce as the information on it are available only on internal network and are completely out of public servers. Use of secure connection for online checkout is very important as it identify and encrypt the data in transit. It protects companies and customers from getting the important information stolen. Also make sure about your PCI compliant and SSL security can prevent fraudulent purchase by comparing the address entered online to the address they have on file with their credit card company. The best way to be safe is to put strong passwords and set alerts for some suspicious activity which can include verification on address, phone number and name. Use of tracking system and the regular site monitoring are also the important steps to keep ourselves safe from fraudulent activities. No systems can be made perfectly and the attacks in e-commerce can also be countered by making security a top priority in designing, implementing and operating network systems. Useful tools and methods include formal method, testing and vulnerable activities and good software engineering practices. If people have trust on e-commerce then there is nothing to do with familiarisation as all the sites tried its best to protect everyone from the hackers.

1. **Conclusion**

Finally; trust, familiarity, viruses, hacking, protective measures and e-commerce are co-related with each other. By the lack of trust on people no familiarity can be maintained. So, to maintain a trust on the people every day reliable security measures are being launched and symbolize better safeguards. While we use better protection operating e-commerce no hackers can steal our information regarding the credit card numbers, unwanted shopping and sensitive data on the network. The bitter truth we everyone should keep in our mind is, we should not play and take the protective measures too easy and light as it is only the factor that can prevent us from being the part of online crime.

Viruses are mainly used to gather sensitive data, gain unauthorised access to the internet and even hijack computers. We shouldn’t rely on anyone about the security and should try our best to be secure. Open sharing of information should be avoiding as it shares our information directly to the public which make hackers a good platform for illegal operations.

Mostly, big organizations should be aware of hacking and security as most of the time hackers target the big companies. Not only consumers, hacking and viruses had already put a huge challenge on policy makers as they have got the extraordinary power to use malicious software. So, as far as possible use the various countermeasures and possibly use strong password and monitor the things on the site regularly.

1. **Recommendation:**

Every part of world is still not the same, some started using e-commerce just before a few years ago and some started it before a long ago. E- commerce is the best way of buying and selling goods so it should be transformed among the people along with its security measures and should made everyone familiar with it. As we had discussed, trust is the part of e-commerce we should try to build a trust on people by creating the various protective websites besides losing the confidence.

# References

Damon. (2017, june 05). *my computer works*. Retrieved october 11, 2017, from mycomputerworks.com: https://mycomputerworks.com/impact-computer-viruses-electronic-commerce/

Doe, G. (n.d.). *It still works*. Retrieved from itstillworks.com: https://itstillworks.com/external-internal-threats-ecommerce-website-8387883.html

Fianyi, I. (2014). *grin*. Retrieved from www.grin.com: http://www.grin.com/en/e-book/300815/investigating-e-commerce-security-cyber-crime-detection-and-prevention

Marsh, D. (2017). *jewlscholar*. Retrieved from http://jewlscholar.mtsu: http://jewlscholar.mtsu.edu/bitstream/handle/mtsu/5256/MARSH%20(Devin)%20Final%20Thesis.pdf?sequence=1

Michael Lee, S. P. (1999, March). *Barkley Law*. Retrieved from scholarship.law.berkeley.edu: http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1250&context=b

Papagalos, L. (2016, June 6). *SiteLock*. Retrieved from blog.sitelock.com: https://blog.sitelock.com/2016/06/what-is-malware/

Schiff, J. L. (2013, June 19). *CIO*. Retrieved from cio.com: https://www.cio.com/article/2384809/e-commerce/15-ways-to-protect-your-ecommerce-site-from-hacking-and-fraud.html