

CYBERCRIME AND SECURITY IN NEPAL: THE NEED FOR TWO-FACTOR AUTHENTICATION IN SOCIAL MEDIA

Chuda Bahadur Roka (Nepal)

ABSTRACT

History of using computers is not long enough in Nepal. It was started in around 1995, but it got easier for us to access to using computers after 2000. We had no easy access to telephone and internet even before 2006 due to the Maoist Insurgency. In 2006, the users of Internet were 1.1% of the total population of Nepal, which reached around 17.2% at the end of 2016. With this rapid increment of internet users, risk of misuse such as cybercrime has increased through the use of internet. This paper thus will describe in detail about the cybercrime and security and authenticity related issues.

KEYWORDS: Cybercrime, cyber security, cyber mechanism, social media, two-factor authentication

INTRODUCTION

The problem of cybercrime and security is one of the most debated issues globally. The world is going to be narrower through the use of cyber space. Everything is tied up with cyber. Today, cyber space is such a virtual space, where any work is possible with it. Every important task is done in cyber. It is going to become a storage space where the contents of non-important personal chat to most important documents of developed countries can be stored without any hassle. For instance, wikileaks.com can be taken for such a task. What does it do? How it is possible and what are its side effects are the best example to understand cyber security and authenticity.

CYBER

The word “Cyber” does not have its own distinct meaning. Simply defined, it refers to a virtual world that is related with computer, network and internet. When we hear or speak the word ‘cyber,’ we visualize the place from where we use internet. In the dictionary.com it is described, “Cyber is prefix that means ‘computer’ or ‘computer network,’ as in cyberspace, the electronic medium in which online communication takes place.” *The Cambridge Dictionary* describe to it as “in using, or relating to computers, especially the internet.” In the similar way, *Oxford Dictionary* defines it as “relating to or characteristic of the culture of computers, information technology, and virtual reality.”

So, cyber is a place where people are connected to internet and do online activities. In the modern time, cyber not only specifies to a single place or room, but also most of the people use personal computer, tablet and mobile phone for these

internet and online activities. In these scenarios we can take cyber as an activity that is related with internet. In the past, it was just a room, but now its uses are coming out from room to every people's hand.

CYBER SECURITY

Cyber security refers to the protection policy that is related with computers and internet activities. It is designed to protect computer hardware, software, data, information and other things which are produced from or to the computing devices. For instance, whatis.techtarget.com is developed to keep computer related devices and software safe as "it is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access. In a computing context, the term 'security' implies cyber security" (<http://whatis.techtarget.com/definition/cybersecurity>). Similarly, [governance.co.uk](http://www.itgovernance.co.uk) defines this technique as "Cyber security – defined as the protection of systems, networks and data in cyberspace – is a critical issue for all businesses. Cyber security will only become more important as more devices, 'the internet of things', become connected to the internet" (www.itgovernance.co.uk/what-is-cybersecurity). On the website of University of Maryland University College, it is defined as "Cyber security, also referred to as information technology security, focuses on protecting computers, networks, programs and data from unintended or unauthorized access, change or destruction" (www.umuc.edu/academic-programs/cyber-security/about.cfm).

So, it is widely accepted that cyber security is associated with protecting computers from damages of hardware, crack to software, spoofing to others work on computers. In the similar way, it is associated with the protection of computers related devices from piracy to software or other digital products. It is also associated with the issues such as from sending viruses, posting unrealistic news, photographs, videos or articles, hacking of others username and password and any other activities that hindrance computers related devices and services.

SECURITY MECHANISM

There is a famous quote, "Where is security, there occurred the problem of insecurity." For the cyber security, there are many tools and mechanism. Choosing a tool of security depends on the type of security issue, which is important for the type of document and the level of the user's knowledge. For instance, to remove the virus of computer we use antivirus to protect our document. We use a password for user authentication to keep our resources safe. To transfer data from one place to another place, we use digital signature, etc. In most of the cases we use username and password for security proposes. The antivirus and digital signature depends on the company rather than the users, but the password is fully depended on the users. However, a password is easy to break, but if mixed alphanumeric and symbols, it is almost impossible. Latest technique of security is face or eye detection, finger prints, etc. are also in practice, which provides middle level security.

CYBER SECURITY ISSUE IN WORLD

Cyber security is one of the major challenges facing the world today. Due to the cyber activities, the world is going to be centralized in a single chip. This sentence

“Every minute, we are seeing about half a million attack attempts that are happening in cyber space” (Harriet Taylor, 28 Dec 2015, www.cnn.com/2015/12/28/biggest-cybersecurity-threats-in-2016.html) is sufficient to understand the cyber security issue in the world. Machine to machine attack is rapidly increasing. It means that by using computer networks, millions of computers can be used to attack a particular issue or device. Later, everything is going to be stored in the cloud system. So, cloud systems could be the main target for the hackers. In the report of United Nations, Department of Economic and Social Affairs wrote, “Cybercrime has now become a business which exceeds a trillion dollars a year in online fraud, identity theft, and lost intellectual property, affecting millions of people around the world, as well as countless businesses and the Governments of every nation” (UN, Department of Economic and Social Affairs, 12 December 2011, <http://www.un.org/en/development/desa/news/ecosoc/cybersecurity-demands-global-approach.html>).

Let's take for instance “Julian Paul Assange” of WikiLeaks and his challenge to the world. In 2010, America and other powerful countries were also afraid with Assange due to his cyber activities. Some people were accepted and agreed with Assange as free of journalism but it was very dangerous activity to the world including America. Most the American activities over the Iraq issue were published by using hacking tools and networking. It shows that no one is safe from cyber attack.

Latest cyber security issue is concentrating toward the business activities like the use of credit cards. Protecting credit cards from such hacking is one of the major problems for developed countries. A news was published in www.chicagotribune.com and other news letter as “In connection with the international credit card fraud case in which more than 1.8 billion yen (about \$17.6 million) was illegally withdrawn from automated teller machines at convenience stores in Tokyo and 16 prefectures across the country, police have found that there was an unauthorized access of a computer system of the Standard Bank in South Africa that caused a malfunction of the system shortly before the cash was withdrawn, according to sources close to the investigation” (Dave Oswald, Dec-19, 2016, www.chicagotribune.com/sns-wp-japan-hack-ae2c1b22-3d4f-11e6-a66f-aa6c1883b6b1-20160628-story.html). This shows that there are lots of fraud cases over the credit cards.

Another major cyber security issue is related with the use of social media. Facebook and Twitter are commonly used and popular among the people around the world. Most of the people are using social media to connecting and sharing own personal interests and views with among friends, relatives and well wishers. In this case, hackers can steal others' username and password, misusing others' resources. This problem is specially happening with developing countries and uneducated peoples who have little knowledge about the cyber security such as choosing secure username and password technique, etc.

USERS' FACT OF SOCIAL MEDIA

Popularity and users of social media sites is increasing dramatically. “The power of social networking is such that, the number of worldwide users is expected to reach some 2.95 billion by 2020, around a third of Earth's entire population. An estimated 650 million of these users are expected to be from China alone and approximately a third of a million from India. The region with the highest penetration rate of social networks is North America, where around 60 percent of the population has at least

one social account. As of 2016, 78 percent of the United States population had a social networking profile” (May 12th, 2016, <https://www.statista.com/topics/1164/social-networks/>).

| Overview | Values |
|---|--------|
| Number of social network users worldwide | 2.34bn |
| Facebook’s number of active users worldwide | 1.59bn |
| Percentage of global online population using Facebook | 38.6% |
| Number of monthly active Twitter users | 313m |

Source: www.statista.com

According to www.internetworldstats.com, in Nepal, around 6.4 million people use Facebook as of 30 June, 2016 whereas the total population of Nepal is 27.8 million in 2013. It means that around 20 percent people use Facebook and other social media sites. It also shows that with the increase of users, its misuse is also increasing day by dy. As reported by Nepal police, 90 per cent cybercrimes are found to have taken place through Facebook.

TRENDS OF CYBERCRIME IN NEPAL AND SECURITY ISSUE OF SOCIAL MEDIA

In Nepal, most of the cybercrimes are related with social media. Most of the cybercrime cases are happen due to lack of poor authentication like easy password. Nepal has low literacy rate. Other important things are most of the social media users are from the poor academic background. They have no good knowledge about the cybercrime, its effects and how it happens. Most of the users use simple passwords in their account such as their name, their lover/beloved’s name, own mobile number, etc. Most of these passwords are from the English alphabet. Most of the users have no knowledge about the use of symbols in their passwords such as the mix up of symbols like &, \$, %, @, etc. By using the password hacker software the users can easily hack the password of others if they are using only alphabet or alphanumeric. But it is almost impossible to hack such a password that has the mix up of the alphabet, numbers and symbols. For example “nEp&l” is thousands time more secure than the password “nepal”.

So due to the use of poor authentication, another users can easily hack or guess the password and misuse others resources. In most of the cybercrime cases, it happens when the users have simple passwords. The criminals are using others’ accounts by hacking or using fake accounts. In the case of Nepal, mostly the users are careless about their accounts.

In other cases, some criminals have no results of their own work also. They are doing unethical things, but they are not aware of what they do whether it is ethical or not. In most of the cases after arresting by police or complaining by the victims, they realize that what they have done is unethical.

Some facts of cyber crimes in Nepal were published in February 21, 2016 by The Himalayan Times, which shows how cybercrimes are increasing in Nepal.

- According to Crime Investigation Bureau (CIB) Nepal, in the year 2070 BS, a total of 19 cases of social media cybercrimes were reported. With the trending use of social media, the number of cases has increased to 35 in 2072 BS. It has been seen that the number of female victims has risen. Using naked pictures in social media

is one of serious problems. For instance, using Facebook to take revenge has been the most serious cases.

- With greater access to the internet and other technologies, the misuse of social networking sites, especially Facebook, has not only posed a threat for the younger generation but also has become a tool for criminals.
- On July 8, the Metropolitan Police Crime Division in Kathmandu arrested Rahul Balmiki (23) of Nepalgunj, who had hacked Facebook accounts of more than 40 women and posted obscene images and sent lewd messages to blackmail the victims. He was arrested from his home district and was brought to Kathmandu for further investigation.
- On January 13, the Metropolitan Police Crime Division in Kathmandu apprehended two persons for allegedly using fake social media accounts with female names to befriend, lure and blackmail businesspersons in Kathmandu.
- Bikram Gyawali, 23, of Dailekh, and Kevin KC, 22, from Dhapasi, Kathmandu were held by the Metropolitan Police Crime Division from the premises of Bhatbhateni Supermarket in Maharajgunj. They had managed to cheat Roshan Gupta of India, currently operating a fancy store at Mahabouddha, of Rs 55,000. The duo opened a fake Facebook account under the name of 'Subashna Gautam' with a girl's picture as a honey-trap and sent a friend request to Gupta. After Gupta fell in love with the girl, Gyawali and KC approached Gupta masquerading as the girl's brothers and demanded Rs 55,000 from him. They also threatened to file a case against him if he did not pay the amount demanded.
- According to the Metropolitan Police Crime Division in Kathmandu, which handles cases of cyber crime, bringing the guilty to book is next to impossible for the police unless a victim categorically identifies the suspect.
- A data maintained by the Metropolitan Police Crime Division in Kathmandu said police have handled as many as 58 cases of cyber in the fiscal year 2012-13 followed by 90 in 2013-14 and 309 in 2015-16. It has also dealt with 333 cases so far this fiscal year. Crimes related to social networking sites accounted for the largest number of cyber crime cases.
- Any person involved in cybercrime is liable to Rs 100,000 in fine or five years in jail or both under Article 47 of the Electronic Transaction Act, 2008.

CONCLUSION

Cybercrime is rising day by day. It is one of the most dangerous social offenses in the world. If cyber users are careful, it can be reduced radically. Most of the cybercrime happens due to poor authenticity. So, users must have a good knowledge of strong password technique. It is more dangerous in developing countries than in developed countries due to the knowledge level of the users. The cases of cybercrime in developing and developed countries are different. Developed countries are facing cyber security issues such as data stolen, but in the developing and under-developed countries the cyber security issues related to personal issues such as misusing social media accounts. In this way, most of the cases are related with poor authenticity, so both users and service providers should be careful of using authentication.

The Nepal government recently announced the concept of digital signature, but it is not practically implemented till now. Even if the government implemented this digital signature, our resources are not secure if we have not good knowledge about

the authenticity security system. The level of security in the case of password such as poor to strong is a dictionary word. We need to combine lower and upper case letters, alphanumeric characters and alphanumeric characters with special symbols while using authentication. Strong authenticity also depends on the length of characters.

REFERENCES

- Cambridge dictionary*. (2016). Retrieved July 14, 2016, from www.dictionary.com: <http://dictionary.cambridge.org/dictionary/english/cyber>
- Cyber Security, cyber crime, cyber threats*. (n.d.). Retrieved 2016, from www.itgovernance.co.uk: <http://www.itgovernance.co.uk/what-is-cybersecurity.aspx>
- Cybersecurity*. (2016, November). Retrieved March 2017, from www.whatis.techtarget.com: <http://www.whatis.techtarget.com/definition/cybersecurity>
- Cybersecurity: A global issue demanding a global approach*. (2011, December 12). Retrieved September 30, 2017, from www.un.org: <http://www.un.org/en/development/desa/news/ecosoc/cybersecurity-demands-global-approach.html>
- Definition of cyber in English*. (n.d.). Retrieved July 14, 2016, from www.oxforddictionaries.com: <http://www.oxforddictionaries.com/definition/english/cyber>
- Facts on social networks*. (n.d.). Retrieved November 30, 2016, from www.statista.com: <https://www.statista.com/topics/1164/social-networks/>
- Hight, E. (n.d.). *About cyber security*. Retrieved July 2016, from www.umuc.edu: <http://www.umuc.edu/cybersecurity/about/cybersecurity-basics.cfm>
- Mankey, D. (2015, December 28). *Biggest cybersecurity threats in 2016*. Retrieved September 30, 2016, from www.cnn.com: <http://www.cnn.com/2015/12/28/biggest-cybersecurity-threats-in-2016.html>
- Meaning of "cyber-" in the English Dictionary*. (n.d.). Retrieved July 2016, from dictionary.cambridge.org: <http://dictionary.cambridge.org/dictionary/english/cyber>
- Nepal internet users*. (2017, March 25). Retrieved April 4, 2017, from <http://www.internetlivestats.com>: <http://www.internetlivestats.com/internet-users/nepal/>
- News/Yomiuri, T. J. (2016, June 28). *Cross border ATM frauds*. Retrieved September 30, 2016, from <http://www.chicagotribune.com>: <http://www.chicagotribune.com/sns-wp-japan-hack-ae2c1b22-3d4f-11e6-a66f-aa6c1883b6b1-20160628-story.html>
- Himalayan News Service. (2016, February 21). *Cyber crime incidents on rise*. Retrieved April 3, 2017, from www.thehimalayantimes.com: <https://thehimalayantimes.com/kathmandu/cyber-crime-incidents-rise/>

ABOUT THE AUTHOR

Chuda Bahadur Roka received his Bachelor's Degree in Computer Application from Pokhara University and Master's Degree in Information Technology from Sikkim Manipal University. Recently he is working as a computer operator for Kaski District Court, Pokhara. He also lectures on Computer Science at New Model Academy, Pokhara. Previously, he has worked for Child Welfare Scheme Nepal, a non-profit organization that is working for orphanage in Nepal. Email: ccroka@gmail.com