Evaluation of Phishing Scenarios in Nepal and Its Preparedness to Handle Them

Conference Paper · October 2014

CITATIONS
0

READS
462

2 authors:

Rajendra Bahadur Thapa
Gandaki College of Engineering and Science
6 PUBLICATIONS **13** CITATIONS
SEE PROFILE

Sunil Chaudhary
56 PUBLICATIONS **336** CITATIONS
SEE PROFILE

Evaluation of Phishing Scenarios in Nepal and its Preparedness to Handle Them

Rajendra Bahadur Thapa[1], Sunil Chaudhary[2]

[1] IOE, Central Campus, Pulchowk, Nepal

[2] University of Tampere, Finland

Corresponding Email: rajendrathapa@gmail.com

Abstract: A gradual increase in Internet and mobile phone users in Nepal has encouraged banking sectors to offer online and mobile banking to their customers as well as contributed in the emergence of various e-commerce websites. People are using internet and mobile phone to perform different monetarily sensitive activities like paying their bills, transferring funds, and online shopping. These whole things have attracted many phishers, which is escalating. Therefore, in our study we have evaluated the phishing scenarios in Nepal to determine how prepared are the Internet and mobile users and the authorities (both private and government) responsible to handle cybercrime in Nepal. Last but not least, we have suggested anti-phishing mechanisms which can be appropriate for Nepal as well as other developing countries in protecting their citizens from falling for phishing.

Keywords: Internet, mobile phone, e-commerce, phishing, anti-phishing, Nepal

1. Introduction

Information and Communication Technologies (ICT) including Internet users are rapidly increasing in developing world. In the year 2013, half of the households connected to Internet were in developing world, and likewise mobile-cellular penetration reached to 89% in the developing world [International Telecommunication Union, 2013]. Internet and mobile open doors to numerous opportunities for enterprises and individuals; however, at the same time they are misused by criminals to conduct their illegitimate activities. More importantly, most of the cybercrimes are financial-driven acts [United Nations Office on Drugs and Crime, 2013], and one of such cybercrime is phishing.

Cybercrimes including phishing are rapidly rooting in developing world, and Nepal is no exception. Ironically, most of the past studies which had been performed are to determine the situations of phishing and Internet users' online behavior often targeting developed world. Undoubtedly, all the studies on phishing are important irrespective to where they are conducted, but we cannot negate the possibility that such studies conducted keeping in mind the users from developed world may not fit and provide a clear picture of developing world. Primarily, there are two reasons: literacy, essentially computer literacy rate in developing world is far below in comparison to developed world; and business culture in developing world is significantly different to its counterparts in developed world; in developing world most of the business still works on trust and phishing is harmful for trust. Moreover, there are no proper researches in cybercrimes like phishing in Nepal. Therefore, we strongly believe it is very important to study the phishing scenarios and Internet users' online behavior in Nepal and other developing countries to realize the actual situations and ascertains suitable anti-phishing measures for them.

In this study, we have analyzed the phishing scenarios in Nepal using meta-analysis method. In order to perform that, we have studied the trends in Internet and mobile-phones usages in Nepalese society. Furthermore, we have studied the current state and future prospect for online business and transaction in Nepal. Then, we have examined the current situation of cybercrime and phishing attacks, and measures implemented to deal with them in Nepal utilizing meta-analysis method as well as an analysis of the cybercrime data received from Nepal Police Information Technology (IT) Division. We have provided a special attention to recognize the awareness in the Internet users in Nepal about phishing by conducting a quiz in which participants have to differentiate between legitimate and phishing websites. Then, we examined the anti-phishing mechanisms employed by the banks and e-commerce business, appropriateness of existing laws for phishing cases, and preparedness of the police department responsible to curbs cybercrime and phishing in Nepal. Last but not least, we have suggested anti-phishing solutions which can be more appropriate for the Internet users in Nepal and other developing countries to protect them from falling for phishing attacks.

The paper proceeds as follows: section 2 discusses about different mechanisms used to conduct phishing and various categories of anti-phishing solutions that are available. Section 3 includes current trends in the use of ICT media, and various activities for which they are implemented or will be implemented. Section 4

presents the current situations of cybercrime and phishing in Nepal. Section 5 explains about the awareness and knowledge related to phishing in the Internet and mobile users. Section 6 describes the anti-phishing measures that are in practice or implemented by individuals and organizations to protect themselves and their valuable customers respectively from phishing attacks in Nepal. In section 7, we suggest anti-phishing mechanisms which can be more suitable for Nepal and the reasons behind them. Section 8 is the conclusions.

2. Phishing and Anti-Phishing

2.1 Phishing

Phishing is a fraudulent activity carried out using an electronic communication to acquire personal information for malicious purposes. This information can include bank or financial institution authentication credentials, social security numbers, credit card details, and online shopping account information with which phishers usually defraud their victims. Phishers employ a number of techniques, such as social engineering scheme and technical subterfuge [Anti-Phishing Working Group, 2014] in order to allure potential victims and make them divulge their account details and other susceptible information.

Phishing is a leading cause of identity theft online and causes billions of dollars of damage worldwide every year. In the year 2013, there were nearly 450,000 phishing attacks and record estimated losses of over USD $ 5.9 billon [RSA EMC^2, 2014]. In fact, phishing makes adverse impact on the economy through direct as well as indirect losses experienced by businesses and their customers [Chaudhary S., 2012].

The direct loss is the financial damage incurred of the amount that phishers withdraw from their victims' accounts. Likewise, the indirect losses are due to adverse impact on customers' confidence towards online commerce and services, the diminished reputation of victimized organizations, and the resources spent to combat phishing attacks. Moreover, the convenience of e-commerce seems to be embraced by both cybercriminals and users on an equal basis. Financial services are the most targeted industries by phishing attacks occupying around 67% followed by online retail service with 11.48% [Anti-Phishing Working Group, 2014].

In general, phishers use emails masquerading as being from a legitimate and trustworthy source, such as a bank, or an auction site, or an online commerce site [Anti-Phishing Working Group, 2014] and redirect victims to an authentic looking counterfeit website to deceive the recipients into disclosing sensitive information. But sometimes phishers can ask the recipients to send their sensitive information in reply email [Yle, 2014]. Many other mediums, such as snail mail, phone call, and instant messenger are also used to reach the potential victims and lure them to disclose their confidential information.

Phishers can plant crimeware, for examples, keystrokes logger and mouse click interceptors in the Personal Computers (PCs) of potential victims to steal their credentials directly [Milletary, J., 2006]. Even advanced mechanisms such as pharming, cross-site scripting attack, cross-site request forgery, domain name typos, and man-in-middle attacks are also implemented to carry out phishing.

From the last one decade, a dramatic increase in the mobile/smart phone usages, even to perform monetarily sensitive activities like banking transactions and online shopping has attracted phishers towards mobile phone users [Ruggiero, P. and Foote, J., 2011]. By the end of 2012, there were already 4,000 mobile phishing Uniform Resource Locators (URLs). Of the total combined URLs used in phishing attacks against the top targeted entities, 7% were mobile URLs. [Trend Micro, 2013] In the future, varying social engineering schemes will target mobile phone users by voice (vishing), SMS (smishing), app-based phishing (rouge apps), as well as classic email spam that users will receive and open on their mobile devices [RSA EMC^2, 2014]. Cybercriminals launch mobile phishing attacks because they can take advantage of certain limitations of the mobile platform. A mobile device's small screen size, for example, inhibits the mobile browser's ability to fully display any anti-phishing security elements a website has. This leaves users no way to verify if the website they're logging in to is legitimate or not. [Trend Micro, 2013]

2.2 Anti-Phishing

There are several promising solutions provided by security experts and researchers against phishing. These systems build an awareness of potential phishing attempts, and develop and promote suitable technology solutions that help to protect Internet users against phishing. They implement prevention, detection, and response measures. These techniques have to deal with both technical and non-technical factors. Therefore, in the first level, phishing prevention techniques can be classified into technical methods and non-technical methods. The technical methods can be further categorized into list based methods and heuristics methods [Dunlop et al., 2010].

Technical methods deal with technical vulnerabilities in Information systems; tools for phishing detection, prevention, and response; designing game, online tutorial, quiz for Internet awareness etc. Some of the examples are: Anti-virus integrated with phishing prevention; in-built system in web browsers; software tools, such as FraudEliminator, Netcraft toolbar, eBay toolbar, EarthLink toolbar, Geo Trust Trustwatcher toolbar, SpoofGuard, CallingID toolbar, Cloudmark Anti-Fraud Toolbar Google Safe Browsing, SpoofStick, TrustBar , Anti-Phishi, DOMAntiphish, PwdHash etc.

Likewise, non-technical methods deal with the factors which are related to studying Internet users' behavior, social engineering principles and techniques used by phishers, legality of using any techniques, training Internet users about phishing, information and guidelines for safe browsing, and cyber laws to punish phishing culprit.

3. Current Trends in the Use of Internet and Mobile Phone

In the year 2013, mobile cellular penetration in Nepal was 71.46% and Internet penetration rate was 26.10%. Interestingly, around 93.6% of the Internet users use Internet in their mobile phone. [Nepal Telecommunications Authority, 2013]

Banking and business sectors are gradually changing and turning more generous in adopting new ICT technologies in order to offer better quality service to their customers. There are thirty commercial banks in Nepal which have been categorized as 'Class A bank' by the Nepal Rastra Bank (The central bank of Nepal). Besides, there are hundreds of banks in categories 'Class B' 'Class C' and 'Class D'. We found that majority of the 'Class A' commercial banks offer online banking service to their customers. Most of the banks even offer mobile banking and SMS (Short Messaging Service) banking. Everyday a large number of individuals and businesses (which is gradually increasing) are using such services to transfer funds and pay their bills. More importantly, e-banking and mobile banking users will significantly increase in the future. A study conducted by [Singhal, D., and Padhmanabhan, V., 2008] on bank's customer perception towards Internet banking revealed that a large number of customers (in their study 81% of the respondents) feel Internet banking a very convenient and flexible way of banking.

Many local e-commerce websites- muncha.com, thamel.com, harilo.com, bhatbhatenionline.com, yeskantipur.com, nepbay.com, and rojeko.com to name but a few have emerged in the last one decade. Moreover, in the financial budget for the fiscal year 2071-2072, the Government of Nepal liberalized foreign currency exchange for its citizens who require to shop from e-commerce websites like amazon, ebay, and other [The Government of Nepal Ministry of Finance, 2014].

Even the governance is moving towards e-governance. The administrative activities concerned to general public, for examples, passport application, and taxation system are gradually moving online. The financial budget for the fiscal year 2071-2072 declared to build a suitable infrastructure for the introduction of e-payment system in tax as well as facilitates to view tax related information online [The Government of Nepal Ministry of Finance, 2014].

4. Cybercrime and Phishing Scenarios

The changing scenarios in the use of ICT in Nepal have attracted many cybercriminals [Munankarmi, P., 2012; Shrestha, P.M., 2013]. Some of the cybercrimes reported to the Nepal Police IT Division in the year 2067 and 2068 are shown in the figure 1. The numbers of reported phishing cases were only three in the year 2067 and 2068, however, these numbers are gradually increasing. Moreover, there is always possibility that some people may not be aware about phishing and the victimized banks may be hesitant to report to police due to fear that such incidents can adversely impact their reputation and their customers trust towards the banks. Besides, in the near future the probability of a dramatic escalation in phishing attacks is very high, since Internet users, particularly online banking and shopping users are increasing which will make phishing more lucrative for the phishers.

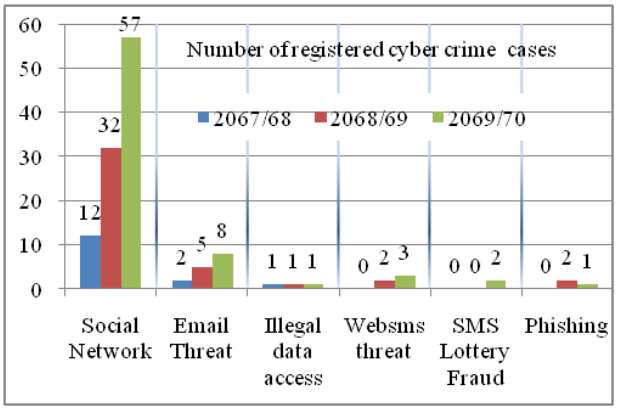

Figure 1: Cyber crime statistics in Nepal from the years 2067/68 (Source : Nepal Police IT Division, Hanumandhoka)

4.1 Phishing in Nepal

In the recent years, several banks in Nepal have suffered from phishing attacks. Some of the cases which came in the media spotlight in 2012 and 2013 are included next. Ironically, it has been found that not all the incidents of phishing attacks are reported [Shrestha, P.M., 2013] so there may be several other cases of phishing attacks and losses incurred due to them which did not lodged any police complaints.

4.1.1 Case 1: Nabil Bank

Naresh Lamgade, a resident of Anarmani Villege Development Committee (VDC) of Jhapa District Nepal, allegedly hacked into the accounts of the Nabil Bank's customers by creating a fake website of the bank. He sent email messages to the Nabil Bank's e-banking customers asking them to change their security codes and provided a link to perform so. When the customers clicked the provided link, it directed them to a fake e-banking website of the Nabil Bank. Several of the customers fell prey to his trick and unsuspectingly revealed their online banking credentials to him. Using the details obtained from the phishing attacks, he was successful to withdraw money from the victims' accounts. According to the investigating officer, Lamgade admitted that he illegally withdrew Rs 32,000 from the victims' accounts, whereas the bank claimed that he withdrew Rs 50,000.

4.1.2 Case 2: Nepal Investment Bank

The customers of Nepal Investment Bank Limited (NIBL) received emails stating that their e-banking accounts has been disabled and asked to visit the provided link to enable it. The link directs them to a fake website where the victims were asked to provide their online banking credentials. After the customers enter their online banking credentials, the website inform them their account has been successfully enabled. But in fact it was just an attempt to dupe and illegally collect e-banking credential from the bank's customers and misuse it to withdraw money from victims' accounts. As a result, Rs 1.2 million was stolen from victims' accounts.

The Central Investigation Bureau (CIB) of the Nepal Police was investigating the incident. The police said that the IP address of the email was from outside the country. The issue received less priority as the bank did not lodge a formal complaint on the issue, said a CIB official.

4.1.3 Case 3: Bank of Asia

E-banking customers of the Bank of Asia (BoA) received an email asking them to change the security code of their account. One of the customers, who himself is a bank employee (employee of NMB Bank), informed the BoA about the email. Immediately after that, the BoA, lodged a complaint at the cyber crime cell of Metropolitan Police Range, Hanuman Dhoka. The bank did not reveal whether any of its customers lost money or not.

5. Internet Users and their Knowledge on Phishing

We conducted a quiz to find out the awareness and knowledge about phishing in Internet and mobile user. In order to conduct our quiz, we designed a web application that holds 20 websites' snapshots. The selected websites were mixture of phishing as well as legitimate websites listed randomly. The websites were from different ranges of organization, such as banks; email services, government organization's websites, social networking sites, and popular brands and payment gateways. We sent the quiz link to various people who are in our contact and asked them to take the quiz. The quiz taker has to provide a pseudo name and then has to identify the displayed snapshot whether it is of a legitimate or a phishing website.

Sixty eight participants took the quiz. All the participants were with engineering background and most of them were computer engineering graduates. All the participants use Internet and mobile phone on daily basis. More importantly, most of them use online banking and online shopping portals.

The results we obtained from the experiment are included in the table 1.

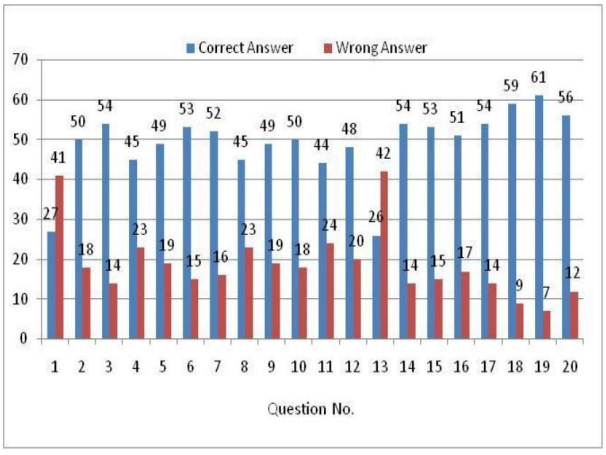

Figure 2: Results from the experiment

Surprisingly, three of the participants were able to identify all the websites correctly. The mean value of correctly identified websites is 14.05. But there were four participants who were able to identify less than 10 websites correctly. However, it is difficult to tell that the participants did not make blind guess. Since the

participant has to reply in terms of 'yes' or 'no', so it was quite easy to make a random guess with probability that 50% of the time it will be correct guess.

6. Anti-Phishing Measures in Practice

We examined the login page of e-banking services, login page of e-commerce websites, legal provisions, and preparedness of police department responsible to handle cybercrime in Nepal.

6.1 e-Banking Services

We checked the login page of e-banking service for all the 'A Class' banks in Nepal. We found that all the banks use 128 bits encryption and Transport Secure Layer (TSL) 1.0., with exception the "Standard Chartered Bank Nepal Limited" which uses 256 bits encryption and TSL 1.2. Furthermore, we found that most of banks do not put any visible information about phishing in order to bring awareness in their users. More importantly, most of the banks employ username-password pair for authentication. Few banks implement multiple passwords but all the passwords are entered in the login page, which we believe is a very poor idea from phishing perspective. "Nepal Investment Bank Limited" is the only bank that implements multi-level password. Furthermore, most of banks do not have any kind of visible information about phishing included in their WebPages. Some of the banks allow their customers to register for online banking, request for password reset, and add new online users who can access his/her account. Table 1 shows details.

Surprisingly, most of the banks include online virtual keyboard in their e-banking service to type credentials. In online virtual keyboard characters' position shuffles after each character type.

Table 1: Login page information of the e-banking service of the various banks of Nepal

Bank	Safe Banking Information	Login Mechanism
Nepal SBI Bank Limited	Three level information on phishing before e-banking login (even on the login page)	User ID-Password
Nepal Bank Limited	Static information in 'help' section	Username-Password
Rastriya Banijya Bank	No visible information	Customer code-Password
Nabil Bank Limited	Ask user to copy paste the e-banking link	Card number-Password
Nepal Investment Bank Limited	Safe login information on the login page	User ID-Password (Multi level password)
Standard Chartered Bank Nepal Limited	Safe login information on the login page	Login ID-Password
Himalayan Bank Limited	No visible information	User ID-One time password-PIN
Nepal Bangladesh Bank Limited	No visible information	Customer code-Password
Everest Bank Limited	Dynamic information on login page	User ID-Password
Bank of Kathmandu Limited	No visible information	Login ID-Password
Nepal Credit and Commerce Bank Limited	No visible information	Customer code-Password
NIC Asia Bank Limited	No visible information	User ID-Password
Machhapuchchhre Bank Limited	No visible information	Username-Password
Kumari Bank Limited	No visible information	Username-Password
Laxmi Bank Limited	Safe login information on the login page	User ID-Password
Siddhartha Bank Limited	No visible information	User ID-Password
Global IME Bank Limited	Safe login information on the login page	Username-Password
Citizens Bank International Limited	No visible information	Used ID-First Password-Sub code
Prime Commercial Bank Limited	No visible information	Customer code-Sub code-Password
Sunrise Bank Limited	No visible information	User name-Password
Grand Bank Nepal Limited	No visible information	Username-Password
NMB Bank Limited	No visible information	Customer code-Password
Prabhu Bank Limited	No visible information	Username-Password
Janata Bank Nepal Limited	No visible information	User ID-Password
Mega Bank Nepal Limited	No visible information	User ID-Password
Civil Bank Limited	No visible information	Username-Password
Century Bank Limited	No visible information	Customer code-Password
Sanima Bank Limited	Safe login information on the login page	Customer code-Password

6.2 e-Commerce Services

We verified the login page of the top e-commerce websites (Muncha.com, Thamel.com, Harilo.com, Bhatbhatenionline.com, YesKantipur.com, NepBay, Rojeko.com, FoodMandu, MetroTarkari, and Karobarmart). Ironically, none of them use encryption to transmit data, with exception

"Bhatbhatenionline.com" which uses 256 bits encryption.

6.3 Acts and Laws in Nepal for Cybercrime and Phishing and their Enforcement in Practice

Electronic Transaction Act (ETA) is the major cyber law of Nepal [Nepal Law Commission, 2008] and provides for the legal recognition of electronic records and digital signatures and their security. The act consists of three significant aspects: legal recognition of electronic records and communications; regulation of certifying authorities; and cyber contraventions [South Asia Partnership-International & Ballanet Asia, 2007]. Its goal is to discourage cyber crimes in the country. Furthermore, it makes specific provisions of penalty for damages made by cybercrimes. It also empowers police and provides provisions for a special cyber court for cybercrime related prosecutions. In a nutshell, the act applies for all cybercrimes conducted from inside or outside Nepal.

The major problem is enforcement of the laws. The laws are not effectively implemented. General civilians and even authorities are not fully aware about cybercrimes and cyber laws existing in the country. Low literacy rate of the country which is 57.4% (definition of literacy: age 15 and over can read and write) [Central Intelligence Agency, 2014] may also be a reason making it difficult to bring awareness about phishing, specifically, in mobile phone users. Furthermore, computer literacy is worse than general literacy.

Another factor can be failure to update the laws. Related authorities do not revise the laws periodically to reflect the changing trends in cyber world and nature of cybercrimes.

Corruption is another factor which hinders the proper implementation of the cyber laws in the country. Alike all other sectors, ICT sector is also maligned by corrupt officials. Many organizations do not meet the minimum requirements specified by the laws, which are crucial for protecting users' information and property in the cyber world. Officials responsible for monitoring such misdeeds turn blind eyes after being bribed.

People perception and attitude towards laws also play a pivotal role in obstructing proper enforcement of laws. There is a general misconception in Nepalese community that "laws or rules are made to be broken". Laws cannot do anything of its own, unless people are aware and determined to bring those laws in practice.

Lack of infrastructures and skilled personnel for handling cybercrimes is also responsible factor, which impedes an effective implementation of the laws. Cybercrime falls under "Computer Directorate" of Nepal Police [Nepal Police, 2014] and it does not have enough resources and infrastructures, essentially, when crime is committed from outside the country [Shrestha, P.M., 2013]. Scarcity of skilled personnel to handle cybercrime is not faced by the government sector alone, but also by the private sector as well.

7. Suggested Anti-Phishing Solutions Suitable for Nepal

A wide diversity of anti-phishing mechanisms exist and are in practice among Internet and mobile users. But something that matter is, do we succeed to achieve a satisfactory result; reality shows otherwise. The reason behind this failure is that we miss to gauge the relevancy of a given anti-phishing mechanism with respect to the context in which it will be used. We have listed out some anti-phishing mechanisms on priority basis which are necessary to curb phishing attacks in context of Nepal.

Public Awareness on Phishing. In information security human is the weakest links. But human can be made a strong point by educating them and bringing awareness in them. Since phishing is a form of identity theft that differs substantially from other physical based identity theft techniques, it is the responsibility of government and private sector towards public to update them about latest phishing techniques and method to recognize them. Banks and other organizations can train their employee. Likewise, to educate their customers, they may include dynamic or static information in their webpage or brochure, but it is essential to verify those information is usable and understandable.

Legislative Framework. A strong legislative framework is also fundamental to combat identity theft, and specific mechanisms that can end such phishing. More importantly, an effective and comprehensive response to identify theft requires the investigation and prosecution of appropriate cases involving phishing schemes. Phishing attacks do not have any boundary and can origin from any part of globe. Therefore, international coordination is highly important to tackle them.

Well Resourced Authorized Body with Skilled Personnel. Technical-human resource in the law enforcing agencies has to be developed to embark upon accelerating computer crimes in Nepal. Moreover, they should have adequate resource to carry out their duties.

Encourage Education and Research on Phishing. It is equally important to produce skilled personnel. Encouraging students and researchers towards cybercrimes and phishing by allocating resources for them to carry research and also promoting job markets for them can help. There are few institutions which have included cybercrimes in the university education. But a large part of working group has never been to university. Therefore, including fundamental information and prevention mechanisms about cybercrime at the secondary and higher secondary level can helpful in great ways.

Use of Security (anti-phishing) Software. Various types of anti-phishing software are available. They are available in a variety of forms: integrated with popular anti-virus systems, e.g., anti-phishing tool in Norton antivirus software, as an embedded feature of renowned web browsers, e.g., Google Safe Browsing toolbar [Google Safe Browsing, 2012] used in Mozilla Firefox browser, and as separate tools and add-ons that can be used in server and client machines, e.g., eBay toolbar [eBay Toolbar's Account Guard, 2012]. They employ different techniques, such as blacklist, e.g., Netcraft Anti-phishing toolbar [Netcraft, 2012] , whitelist, e.g., SmartScreen Filter [MSDN IEBlog], content based detection, e.g., CANTINA [Zhang et al., 2007], analysis of source web page source code or URL, e.g., CANTINA+ [Xiang et al., 2011], comparing visual similarity of the whole webpage or layout or logo, e.g., online tool called "SiteWatcher Anti-phishing Tech" [Liu et al. ,2006], analysis of data submitted by users online, e.g., SpoofGuard[Chou et al. ,2004] , and use of a reputable search engine, e.g., CANTINA [Zhang et al., 2007].

Despite all anti-phishing solutions that come inbuilt with web browsers are more appropriate for Nepal. Web browser is the most common method used by Internet users to get access of web contents. There are other methods too, but they are usually tricky and complex, which makes them unsuitable for general Internet users. Furthermore, it is the foremost layer with which Internet user interacts, and tracking user's activity at this level is potentially more effective. Its strategic positions make it suitable to warn Internet users directly and effectively [Sheng et al., 2009]. Even a study by Egelman et al. [2008] found that phishing warning in Mozilla Firefox 2 was very effective, and was able to stop all participants in their study from entering sensitive information into fraudulent websites. In addition, web browser market is dominated by selected number of browsers, i.e., Google Chrome, Internet Explorer, Mozilla Firefox, Safari, and Opera. All together, it is easy to handle phishing at the browser level.

Last but not least, using anti-phishing solution that comes inbuilt with web browser solves the problem of buying and extra software. In a country, where a large number of people use pirated software, asking them to buy and install software is definitely tedious task.

8. Conclusions

Phishing is a serious threat in global scenario. Every year it causes billions of dollars damage worldwide. Even in Nepal, some cases of phishing have been reported to the police. Even though the economic loss in Nepal is not as huge as many developed countries, it is still noteworthy in the scenario of Nepal. More importantly, Internet users in Nepal are continuously and rapidly growing and to keep pace with them, Banks and financial institutions in Nepal are embracing online/mobile media to offer their services. Likewise, Nepal government is also striving towards e-governance. These all indicate that in the coming year, phishing cases in Nepal will dramatically escalate.

In order to thwart such phishing attacks, first people have to be aware about phishing. Equally important are the laws and an effective enforcement of those laws. It also demands well equipped authorized body with skilled personnel who can successfully apply preventive, detective and responsive measures in order to protect civilians from falling for phishing.

In technical measure, browser's inbuilt anti-phishing system is more appropriate. Since, most of the Internet users use browser to perform online activities, the inbuilt anti-phishing system will prevent them from a necessity of installing a separate anti-phishing tool.

References

International Telecommunication Union (2013). The World in 2013: ICT Facts and Figures. Retrieved on 16th September 2014 from: http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2013-e.pdf

United Nations Office on Drugs and Crime (2013). Comprehensive Study on Cybercrime. Retrieved on 16th September 2014 from: http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

Anti-Phishing Group (2014). Phishing Activity Trends Report: 1st Quarter 2014. Retrieved on 16th September 2014 from: http://docs.apwg.org/reports/apwg_trends_report_q1_2014.pdf

RSA EMC^2 (2014). 2013 A Year in Review. Retrieved on 18th September 2014 from: http://www.emc.com/collateral/fraud-report/rsa-online-fraud-report-012014.pdf

Chaudhary, S. (2012). Recognition of phishing attacks utilizing anomalies in phishing websites. Retrieved on 18th September 2014 from: http://tampub.uta.fi/bitstream/handle/10024/84169/gradu06373.pdf?sequence=1

Yle (2014). Customs Warns Against Email Scam. Yle News on 7 April 2014. Retrieved on 1st August 2014 from: http://yle.fi/uutiset/customs_warns_against_email_scam/7177240

Milletary, J. (2006). Technical Trends in Phishing Attacks. United States Computer Emergency Readiness Team (US-CERT), 2006. Retrieved on 2nd May 2012 from: http://www.us-cert.gov/reading_room/phishing_trends0511.pdf

Ruggiero, P. and Foote, J. (2011). Cyber Threats to Mobile Phones. US-CERT Report. Retrieved on 18th September 2014 from: https://www.us-cert.gov/sites/default/files/publications/cyber_threats-to_mobile_phones.pdf

Trend-Micro (2013). Mobile Phishing: A Problem on the Horizon. Retrieved on 18th September 2014 from: http://about-threats.trendmicro.com/us/mobilehub/mobilereview/rpt-monthly-mobile-review-201302-mobile-phishing-a-problem-on-the-horizon.pdf

Dunlop et al. (2010).GoldPhish: Using Images for Content-based Phishing Analysis. In: Proc. of Fifth International Conference on Internet Monitoring and Protection, 2010, ICIMP, pp.123-128.

Nepal Telecommunications Authority (2013). Management Information System. Annual report, issue 56, vol. 104, published in August 2013.

Singhal, D., and Padhmanabhan (2008). A Study on Customer Perception Towards Internet Banking: Identifying Major Contributing Factors. The Journal of Nepalese Business Studies, Vol. 5, No.1, pp.101-111.

The Government of Nepal Finance Ministry (2014). Budget Speech of Fiscal Year 2014/2015. Retrieved on 18th September 2014 from: http://www.mof.gov.np/uploads/document/file/Budget%20SpeeSp%20Final%20English_20140727050302.pdf

Munankarmi, P. (2012). Beware of Phishing Email – Targeted to Nepali Internet Banking Users. Retrieved 9th September 2013, from: http://nepallica.com/beware-of-phishing-email-targeted-to-nepali-internet-banking-users/

Shrestha, P. M. (2013). Phishing Incidents Wake-up Nepali Banks to Security Threats. Retrieved 9th September 2013 from: http://www.ekantipur.com/2013/04/16/business/phishing-incidents-wake-up-nepali-banks-to-security-threats/370064.html

Nepal Law Commission (2008). Electronic Transaction Act 2063. Retrieved on 12th September 2014 from: http://www.lawcommission.gov.np/site/sites/default/files/Documents/the-electronic-transaction-act.pdf

South Asia Partnership-International & Ballanet Asia (2007). Passage to Cyber Crime? Published by SAP International and Bellanet Asia, Kathmandu Nepal.

Central Intelligence Agency (2014). The World Fact Book . Retrieved on 12th September 2014 from: https://www.cia.gov/library/publications/the-world-factbook/fields/2103.html

Nepal Police (2014). Computer Directorate. Retrieved on 12th September 2014 from: http://www.nepalpolice.gov.np/computer-directorae.html

Google Safe Browsing (2012). Google Safe Browsing API. Retrieved on 12th July 2012 from: https://developers.google.com/safe-browsing/

eBay Toolbar's Account Guard (2012). Using eBay Toolbar's Account Guard. Retrieved on 12th July 2012 from: http://pages.ebay.com.au/help/account/toolbar-account-guard.html

Netcraft (2012). Why use the Netcraft toolbar? Retrieved on 23rd July 2012: http://toolbar.netcraft.com/

MSDN IEBlog (2012). IE8 Security Part III: SmartScreen Filter. Retrieved on 22nd July 2012 from: http://blogs.msdn.com/b/ie/archive/2008/07/02/ie8-security-part-iii-smartscreenfilter.aspx

Zhang et al. (2007). CANTINA: A Content-Based Approach to Detecting Phishing Web Sites. ACM 978-1-59593-654-7/07/0005.

Xiang et al. (2011). CANTINA+: A Feature-rich Machine Learning Framework for Detecting Phishing Websites. ACM Transactions on Information and System Security (TISSEC) Volume 14 Issue 2, September 2011, Article No. 21.

Liu et al. (2011).Smartening the Crowds: Computational Techniques for Improving

Human Verification to Fight Phishing Scams. In: Proc. Symposium On Usable and Secuirty (SOUPS) 2011, July 20-22, 2011, Pittsburgh, PA, USA.

Sheng et al. (2007) Anti-Phishing Phil: The Design and Evaluation of a Game that Teachers People Not to Fall for Phish. In: Proc. of Symposium on Usable and Security (SOUPS) 2007, July 18-20, 2007, Pittsburgh, PA, USA

Egelman et al. (2008).You've Been Warned: An Empirical Study of the Effectiveness of Web Browser Phishing Warning. In: Proc. of CHI 2008, April5-10, 2008, Florence, Italy. ACM 1-59593-178-3/07/0004.