# A Study of Social Engineering Based Attacks in Kathmandu University to Propose a Conceptual Framework

Gajendra Sharma[1*] and Roshan Manjushree Adhikari[2]

[1]Associate Professor, Department of Computer Science and Engineering, School of Engineering, Kathmandu University, Dhulikhel, Kavre, Nepal. Email: gajendra.sharma@ku.edu.np
[2]Student, Department of Computer Science and Engineering, School of Engineering, Kathmandu University, Dhulikhel, Kavre, Nepal.
*Corresponding Author

**Abstract: Social engineering is a major issue affecting organizational security throughout the world. Educating the employees of every organization about social engineering attacks and the negative effects it brings to their organization is a very important step to be taken by every organization but is overlooked most of the times. The objective of this research is to evaluate the current awareness level of staffs of Kathmandu University towards very common social engineering attacks and propose a conceptual framework for prevention of these attacks. A questionnaire was created and a survey was conducted accordingly within teaching and non-teaching staffs of Kathmandu University. Based on the 51 responses achieved, the paper proposes a conceptual framework for the university to adapt to their information system for a more secure environment.**

**Keywords: Awareness, Passwords, Phishing, Social engineering, Vishing, Vulnerability.**

## I. Introduction

Social Engineering is the art of exploiting the weakest link of information security systems: the people who are using them [7]. It involves taking advantage of psychological aspects of human mind like trust, sympathy, empathy, curiosity, greed, desire, ego, fear, urgency, ignorance, negligence or lack of knowledge. A skilled social engineer can leverage these aspects of people in an organization to breach the security of organization by manipulating staffs of organization into divulging confidential information. Would the users of the organization depending on expensive security mechanisms for information security bother to think that they could be unknowingly posing as a biggest threat to security of their own organization?

The issue of social engineering based attacks to my knowledge has not been studied in Kathmandu University before. The objective of this research paper is to present and demonstrate present situation of how aware the staffs of Kathmandu University actually are about security of their information. The study started with a survey that was distributed within 397 employees of the university among which 51 responded. All the responses were from people of the university, working on a computer on a regular basis. The survey questionnaire contained ten experimental situations based on social engineering attacks to find how people would respond to given situation. Analysis of the collected data motivated me to propose a framework to effectively deal with social engineering based attacks.

## II. Literature Review

Hackers prefer social engineering because it's much easier to hack a human than a business [11]. Social engineering is an emerging threat to organizations. Balabit survey results from black hat USA and EU shows social engineering to lead the top ten list of most popular hacking methods [12]. Internet Security Threat Report 2016 reports data breaches, government surveillance, and good-old fashioned scams came together to further encroach on personal privacy, whether it is personal photos, login credential or medical histories. Phishing e-mail scams, social media scams have been continuously increasing each year and many organizations still suffer lot of information loss from these attacks [8] as shown in Table I.

Table I: Phishing Ratio in E-mail by Industry

| Industry Detail | Phish E-Mail Ratio |
|---|---|
| Retail Trade | 1 in 690 |
| Public Administration | 1 in 1,198 |
| Agriculture, Forestry & Fishing | 1 in 1,229 |
| Nonclassifable Establishments | 1 in 1,708 |
| Services | 1 in 1,717 |
| Manufacturing | 1 in 1,999 |
| Finance, Insurance & Real Estate | 1 in 2,200 |
| Mining | 1 in 2,225 |
| Wholesale Trade | 1 in 2,226 |
| Construction | 1 in 2,349 |
| Transportation & Public Utilities | 1 in 2,948 |

Source: Adapted from "Internet Security Threat Report, 2016"

In 2015, Office documents were the most popular attachment type, with executable files becoming less popular for e-mail attachment scams. Overall 13 percent of attachment types were executable, including .exe, .com, .pif, .bat and others [8] as shown in Table II.

Table II: Malicious File attachments in Email

| Rank | File Extension | Blocked in Emails |
|---|---|---|
| 1 | .doc | 55.8% |
| 2 | .xls | 15.0% |
| 3 | .zip | 8.7% |
| 4 | .htm | 7.9% |
| 5 | .docm | 2.4% |
| 6 | .js | 2.2% |
| 7 | .mso | 1.9% |
| 8 | .html | 1.6% |
| 9 | .exe | 0.9% |
| 10 | .png | 0.8% |

Source: Adapted from "Internet Security Threat Report, 2016"

Over the past several years, it certainly looks like the "bad guys" are now shifting to social engineering based attacks rather than technical attacks. Social engineering, when performed confidently and effectively can easily compromise security of big and secure information systems easily. Social engineering does not require some high technical hacking skills. "A high-tech attacker could spend hours, days, or weeks poking at the external box in an attempt to bypass AES-128 encryption and IPSEC to gain access to the private network behind it. Even then, he or she would struggle to bypass the security of the internal machines, to gain access to the 'rocket' box. On the other hand, a no-tech hacker can bypass the security of the entire network in moments, just by peeling a document off his face and hanging on to it [10]."

(Kumar & Kumar, 2016) [9] conducted an online survey among 114 users to know about the awareness of social engineering attacks. They found that, most of the individuals were unknown about social engineering attacks and even a computer literate could be the victim of social engineering. They also found that every user can be cheated by knowing their weak points and needs such as job requirements etc. This behavior however changed after a proposed framework by the writers. The users became more aware and concerned about how they could be manipulated by different social engineering attacks.

(Chitrey, Singh, & Singh, 2012) [3] did a survey done among employees of IT service providing firm and students of top IT colleges in India and proposed a conceptual model by studying social engineering based attacks in India. Phishing, e-mail attachments and social network scams were the most faced attacks by the users. The main motivation behind these attacks was found to gain access to proprietary information followed by financial gain, competitive advantage and revenge. They also found that new employees were in the greatest risk for falling for social engineering based attacks in an organization. The different safeguards to prevent these attacks were found out to be awareness and training program followed by security policy, technical controls and physical security.

We have been unable to find research studies focused on the social engineering in context of Nepal. The study reported herein mainly investigates how the staffs of Kathmandu University would respond in certain scenarios where social engineering attack would occur on them which will help the university figure out how much less or more vulnerable the staffs of the university are to these attacks and what measures could possibly be applied to overcome the negative consequences caused by these attacks.

## III. Social Engineering Based Attacks

### *A. Human Based Methods*

i. *Dumpster Diving*: Dumpster diving simply involves the practice of diving into dumpster in the quest of some valuable information. Usually, an employee does not care about the information he/she has on a piece of paper like his salary slip of previous month. Whereas, this information is much valuable to an social engineer because he can get the employee's bank account number, salary and other proprietary information.

ii. *Shoulder Surfing:* Shoulder surfing is a classic social engineering attack where attacker peers over victim's shoulder to see what he/she is up to in his computer. For example - when entering sensitive data like password or PIN number via a keyboard, attacker can just observe the pattern of password or may record keystrokes from a video recorder device.

iii. *Tailgating:* Tailgating in simple terms means following an authorized person into a building - basically riding on their coattails [10]. It is still commonly used and a very effective method for gaining access to floor or buildings in an effective way. It exploits human weakness of helpfulness or empathy.

iv. *Password Sharing:* Sharing password may look like a light issue but is really a very serious security related issue. Employees share their login credentials with each other on a daily basis, most often because they need to give colleagues access to their machine to delegate work or because they are out of their office [2]. Suppose an employee A given more security clearance shares his password with employee B with less clearance. One can imagine what employee B can do in this scenario to data of high confidentiality levels using employee A's password [6].

v. *Writing Passwords on Post-Its:* Passwords are generally hard to remember. The practice of employees writing passwords or personal ID's on sticky notes and sticking on work monitors or on bottom of keyboards is seen

commonly. While employees may have difficulty remembering each of their passwords, especially when one person may have hundreds of accounts on different sites these days, writing passwords or any other critical information to see to other's eyes is never really a good idea. This behavior is vulnerable to social engineering because a social engineer can just walk to their work desk and view passwords easily.

### *B. Technical Methods*

i. *Phishing:* The common goal of any phishing scam are to steal victim's credentials (password or credit card number) by luring them to go to some web links or attachments. These are the most common forms of social engineering attacks and are generally carried out via e-mails or any messaging services. For example: e-mails are shown to be sent by bank of the user which may request the victim to go to a web link to change their password before their account expires. The victim may instantly go to the link, enter his bank password before he/she realizes that the link was fake and their password has been compromised. The emails are so convincing that unfortunately many people fall for this scam.

ii. *Vishing:* Vishing (or Voice Phishing) is another famous attack where telephone (voice communication system) is used as main method for attack. The main motive of the attack is to gain personal, private or financial information of the victim. Attacker impersonates as some authorized personnel that may have right to access these information and are also difficult to trace back.

iii. *E-mail Attachments:* In these attacks, usually an e-mail comes to a victim from known or unknown sources. Out of curiosity, victim downloads the attachment and usually the program hidden in e-mail attachments can spread viruses, causes damage to the system, steal login credentials stored in the computer or even fry the entire system.

iii. *Leaving Devices for Open Access:* Staffs of any organization nowadays use computers or laptops as their working platform. But what they don't realize is their simple negligence of leaving their computer unlocked while going to bathroom or going for a cup of coffee could affect security of their organization. A social engineer now can take advantage of this negligence and once he/she is gone, the social engineer now has open access to the documents, files and network of the organization.

iv. *Keeping Same Passwords for All Services*: Using the same password for all of your accounts is like having one key that unlocks every door in your life [14]. Nowadays, an average internet user has accounts on many websites including social networking sites, e-banking services, online shopping sites, messaging services and many other web services. According to a study in 2015, an average UK consumer has no less than 118 online accounts [1]. Having different passwords for all these services and remembering them is obviously a difficult job. But we also cannot neglect the fact that having same password for multiple accounts makes a user more vulnerable to social engineering attacks. If a user has the same password for an E-banking service and says another less secure website and if a hacker somehow compromised the less secure website, he now has access to the user's E-banking service.

## IV. Research Methodology

### *A. Online Survey*

This research was conducted by questionnaire and performed within staffs of Kathmandu University, Dhulikhel, Kavre. A total of 397 questionnaires were sent to all teaching and non-teaching staffs of the university, among which 51 responded. The ten questionnaires used experimental scenarios where people were asked what they would do under certain scenarios based on social engineering attacks. The case under which an employee would be a suitable subject for the survey was quite simple - the employee should be working on a computer on his work place on a regular basis on university hours. No personal information was collected- the survey was voluntary and anonymous.

## V. Results

### *A. Keeping Same Passwords for All Services*

The subjects were asked if they had same passwords for all the web accounts they currently use (Table III).

Table III: Questionnaire Results Regarding Keeping Same Passwords for All Services

| Sample Size | Staffs Who Have Separate Passwords for All Services | Staffs Who Have the Same Password for All Services |
|---|---|---|
| 51 | 39 | 12 |

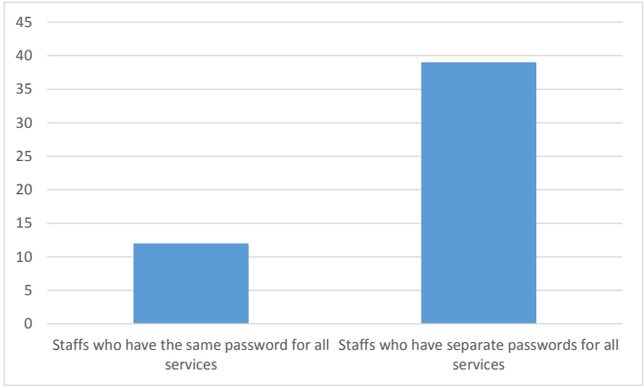


Fig. 1: Questionnaire Results Regarding Keeping Same Passwords for All Services

### *B. Writing Credentials on Post-It*

The subjects were asked if they had the habit of writing login credentials in post-its or a notepad file in their computer (Table IV).

TABLE IV: QUESTIONNAIRE RESULTS REGARDING WRITING CREDENTIALS ON POST-IT

| Sample Size | Staffs Who Only Remember their Passwords | Staffs Who Write their Passwords in a Secret Place | Staffs Who Write Credentials on Post-Its |
|---|---|---|---|
| 51 | 30 | 15 | 6 |

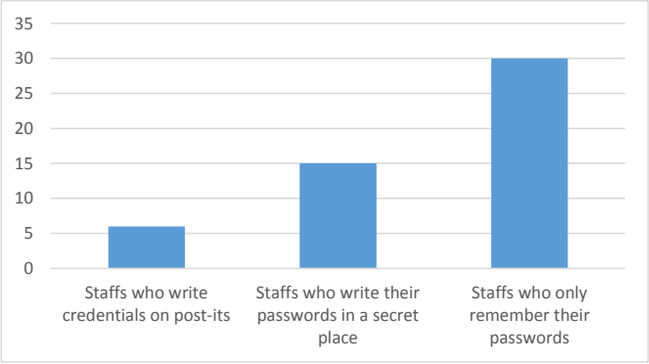


Fig. 2: Questionnaire Results Regarding Writing Credentials on Post-It

### *C. Shoulder Surfing*

The subjects were asked how careful they are while entering PIN number in KU canteen system (Table V).

TABLE V: QUESTIONNAIRE RESULTS REGARDING SHOULDER SURFING

| Sample Size | Staffs Who are Careful When Typing PIN | Staffs Who Are Not So Careful When Typing PIN |
|---|---|---|
| 51 | 26 | 25 |

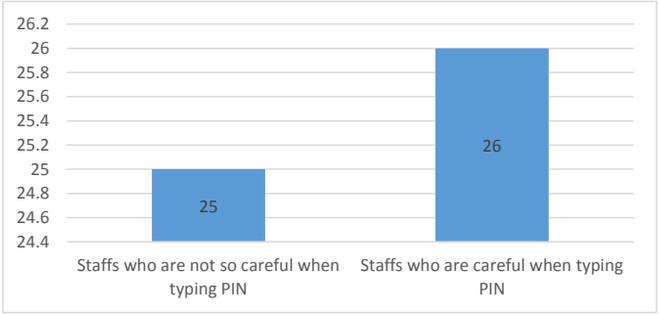


Fig. 3: Questionnaire Results Regarding Shoulder Surfing

### *D. E-mail Attachments*

The subjects were asked about how careful they are while downloading and opening e-mail attachments (Table VI).

TABLE VI: QUESTIONNAIRE RESULTS REGARDING E-MAIL ATTACHMENTS

| Sample Size | Staffs Who Open E-Mail Attachments As Long As They Know Person or Company | Staffs Who Open E-Mail Attachments from Only Expected Source | Staffs Who Think There is Nothing with Just Downloading and Opening Attachments |
|---|---|---|---|
| 51 | 34 | 15 | 2 |

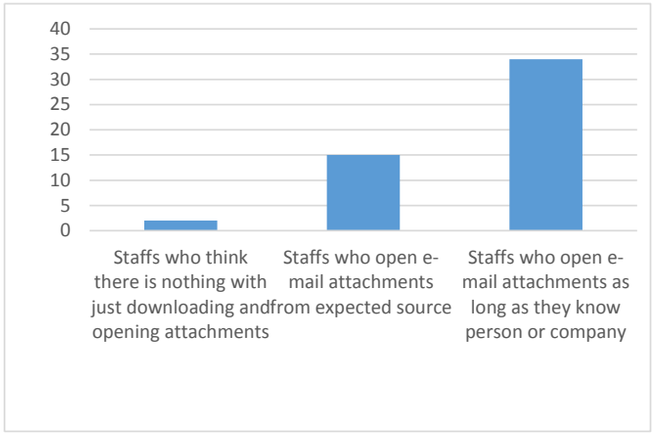


Fig. 4: Questionnaire Results Regarding E-mail Attachments

### *E. Leaving Devices for Open Access*

The subjects were asked what would they do to their computer while going outside for some moment (Table VII).

TABLE VII: QUESTIONNAIRE RESULTS REGARDING LEAVING DEVICES FOR OPEN ACCESS

| Sample Size | Staffs Who Lock their PC Before Going Outside | Staffs Who Shutdown their PC Before Going Outside | Staffs Who Leave their PC as It Is Before Going Out | Staffs Who Close All the Programs Before Going Out |
|---|---|---|---|---|
| 51 | 32 | 7 | 7 | 5 |

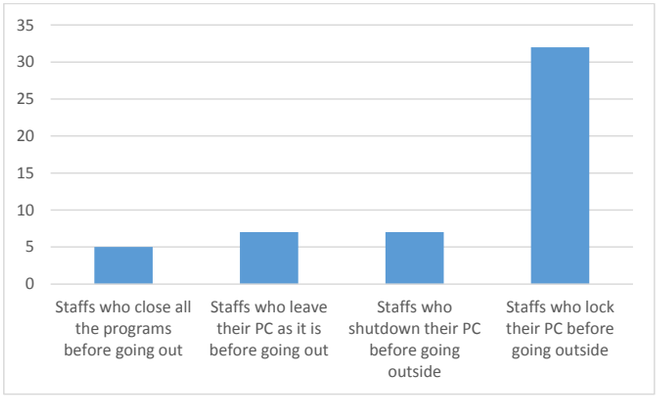


Fig. 5: Questionnaire Results Regarding Leaving Devices for Open Access

### *F. Dumpster Diving*

The subjects were asked how they are handling those papers that contain critical information which they no longer need (Table VIII).

TABLE VIII: QUESTIONNAIRE RESULTS REGARDING DUMPSTER DIVING

| Sample Size | Staffs Who Just Throw their Papers on Trash | Staffs Who Completely Shred or Burn their Papers |
|---|---|---|
| 51 | 29 | 22 |

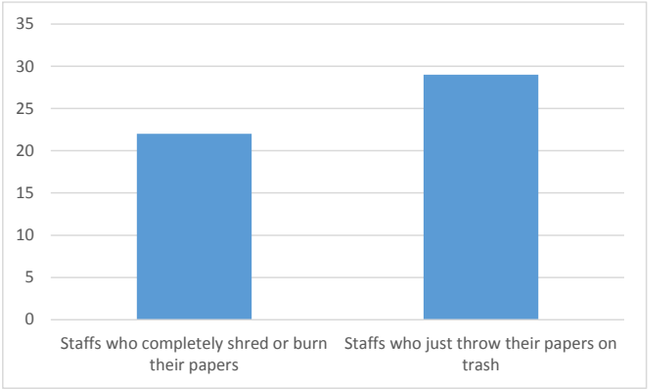


Fig. 6: Questionnaire Results Regarding Dumpster Diving

### *G. Tailgating*

The subjects were asked how would they respond when an unknown person tries to follow them inside their floor or building (Table IX).

TABLE IX: QUESTIONNAIRE RESULTS REGARDING TAILGATING

| Sample Size | Staffs Who Won't Let an Unknown Person Inside their Floor | Staffs Who Will Let an Unknown Person Inside their Floor |
|---|---|---|
| 51 | 31 | 20 |

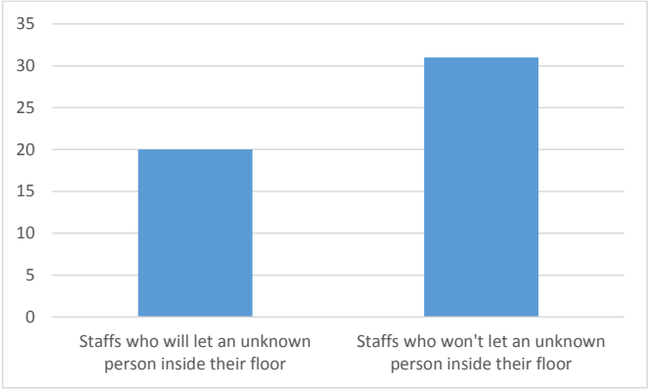


Fig. 7: Questionnaire Results Regarding Tailgating

### *H. Password Sharing*

The subjects were asked what would they do when an close office friend of them asks them for their password (Table X).

TABLE X: QUESTIONNAIRE RESULTS REGARDING PASSWORD SHARING

| Sample size | Staffs Who Will Share their Password to a Close Friend and Change Them Immediately | Staffs Who Won't Share their Password to a Close Friend | Staffs Who Would Share their Password To a Close Friend And Make Them Promise Not to Share It |
|---|---|---|---|
| 51 | 33 | 14 | 4 |

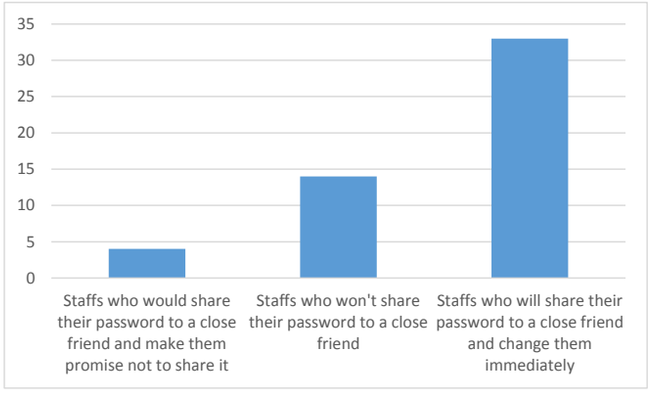


Fig. 8: Questionnaire Results Regarding Password Sharing

### *I. Vishing*

The subjects were asked how they would respond to a given call from an unknown source when the caller asks them for their private information (Table XI).

TABLE XI: QUESTIONNAIRE RESULTS REGARDING VISHING

| Sample Size | Staffs Who Would Not Give Any Information to an Unknown Phone Call | Staffs Who Would First Confirm the Identity of Caller and Give Them their Private Information | Staff Who Would Give their Private Information to an Unknown Caller |
|---|---|---|---|
| 51 | 26 | 24 | 1 |

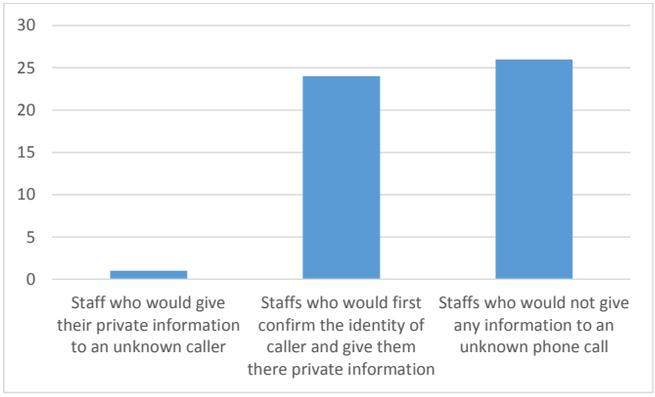


Fig. 9: Questionnaire Results Regarding Vishing

### *J. Phishing*

The subjects were given a sample phishing mail and asked what they would do when such mail comes to their work mail (Table XII).

TABLE XII: QUESTIONNAIRE RESULTS REGARDING PHISHING

| Sample Size | Staffs Who Would Go To the Link From an Unknown Email but Won't Enter Any Credentials | Staffs Who Will Never Click Any Link from Unknown E-Mail | Staffs Who Will Click the Link and Provide their Credentials from An Unknown Mail |
|---|---|---|---|
| 51 | 27 | 21 | 3 |

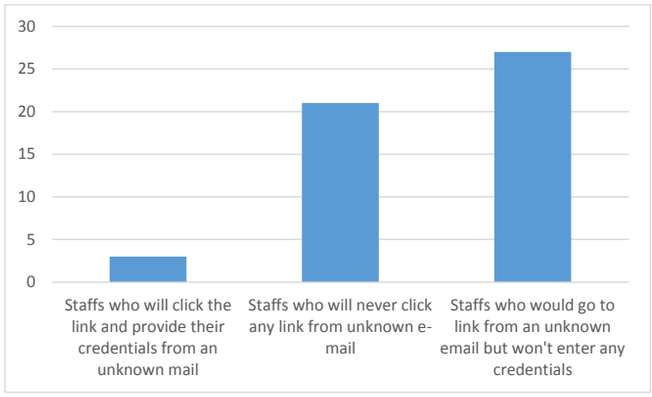


Fig. 10: Questionnaire Results Regarding Phishing

## VI. DISCUSSION/INTERPRETATION OF RESULTS

The observed data from my survey from a sample size of 51 staffs from Kathmandu University shows a certain vulnerability level of the subjects towards both types of social engineering attacks. Between the human based approach and technical approach discussed in Section 3, it was observed that the subjects were more vulnerable to the human based attacks than technical attacks. Between these two classifications of social engineering attacks, it was observed that 46% of subjects were more vulnerable to human based social engineering attacks whereas only 12% of subjects were seen vulnerable to technical based social engineering attacks. On total, it was observed that 29% of subjects were vulnerable towards social engineering attacks (both human based and technical based) on average.

TABLE XIII: COMPARISON OF SUBJECTS VULNERABLE TOWARDS HUMAN BASED VS. COMPUTER BASED ATTACKS

| Vulnerable to Technical-Based Social Engineering Attacks | Vulnerable to Human-Based Social Engineering Attacks |
|---|---|
| 12% | 46% |

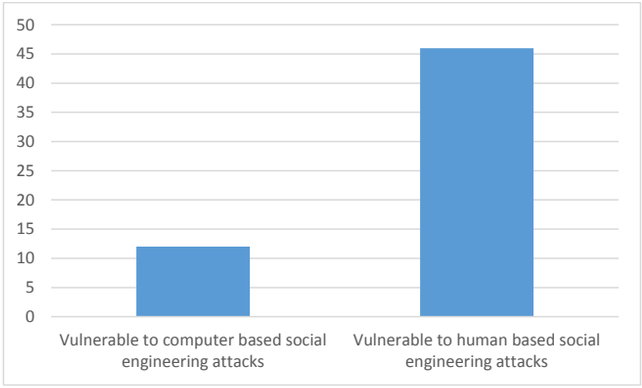


Fig. 11: Comparison of Subjects Vulnerable Towards Human Based Vs. Computer Based Attacks

The main reason behind subjects less vulnerable to technical based attacks rather than human based attacks could be user awareness nowadays. Today's users are well aware of phishing e-mails, fake pop-ups, chain letters and hoaxes and a vulnerable website compared to a user ten years ago. On the other hand, human based social engineering attacks work better because they attack on human's psychological aspects. Especially in country like Nepal, people might have generally a higher level of trust to other people. This could be the main factor why the data on human based social engineering attacks was found a lot higher than technical attacks.

## VII. Proposed Framework

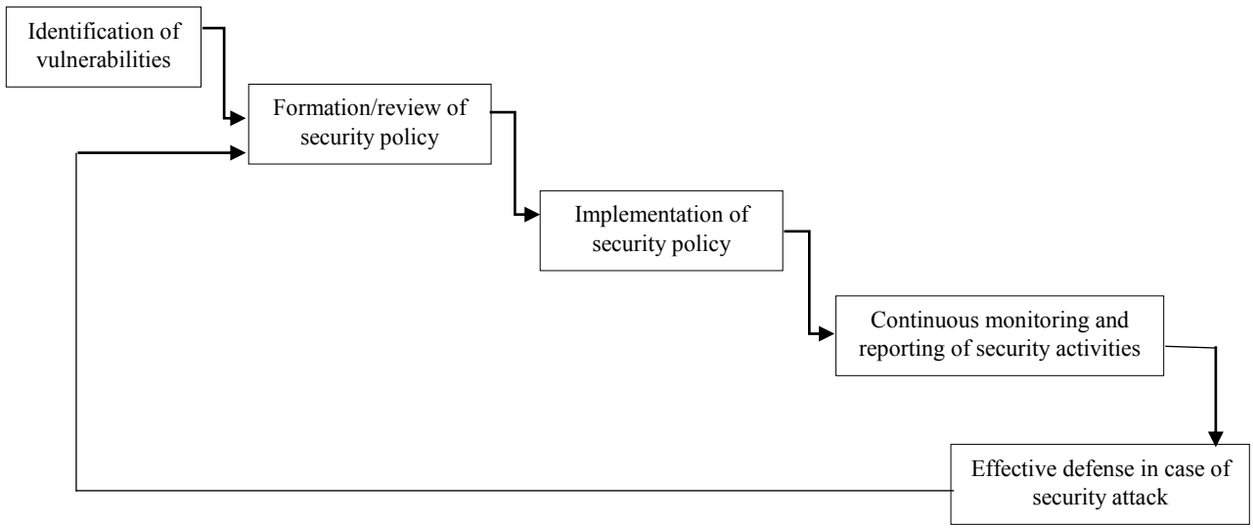


Fig. 12: Proposed Framework

### *A. Identification of Vulnerabilities*

Vulnerability is a weakness in a system or its protections that could be exercised, creating a breach in the security protection of the system [4]. Kathmandu University first must try to identify about the current security state of the university. University should try to perform further study of its employees to actually understand how vulnerable they really are in terms of social engineering attacks. Threat model is considered to one of the three pillars of any secure system. Threat model simply refers to what the adversary or bad guy can do to breach the security of the system. In this case, the bad guy refers to a social engineer.

For identifying the vulnerabilities, further surveys and experiments could be done among the staffs of the university. Experimental surveys may include testing the staffs with a phishing or a vishing attack and observing their behavior against these attacks. University must be able to understand how effective the current security policy of the university against social engineering attacks really is, and what necessary reviews are needed in the policy to make it more secure. For example : if the university found out via a experimental survey that about 30% of its employees were vulnerable to a vishing attack, security policy should be updated and employee awareness must be done.

## VIII. Formation/Review of Security Policy

Information security policies form the cornerstone of an organization's information security program. Without formal information security policies and standards, an organization cannot effectively secure its critical information assets [13]. A well-documented and accessible security policy and associated standards and guidelines form the foundation of a good security strategy [5]. The security policy should be clear, to-the-point, easily understandable and fully cover its scope and content in each area it applies. Given are some important security policies covering some proposed solutions against social engineering attacks discussed in this paper.

- *System Usage Policy:* Monitoring the usage of systems so that only authorized personnel may access the system. For example: only ISMS employees should have the permission to enter the server room.
- *Personnel Security:* Could be performed by going thorough background check for any new employee when joining the university.
- *Password Policy:* Password selection and usage guidelines for generating more secure passwords. For example : all the passwords for KU e-mail system should be at least 8 characters long and contain at least one uppercase, one special character, one numeric value.

- *Protection from Viruses:* To secure the system via use of antivirus, firewall or other authorization system.
- *Physical Security:* Secure the floor or building which contains sensitive information by some validation procedures like ID card verification or fingerprint scanning system.
- *Proper Disposal of Unwanted Stuffs:* Employee must first completely shred all information before throwing them to trash or recycle bin.
- *Implementation of Security Policy:* There is no point in just forming a security policy if it would not be implemented effectively to an organization. The first usual step while implementing the security policy is to identify organizational issues that impact information security policy. Various classes of policy users needed to identified, policies should be organized into meaningful categories, all the personnel in the organization should be trained effectively to follow the security policy, enforce the information security policies and standards and finally review and modify policy as appropriate [12].

### *A. Continuous Monitoring and Reporting of Security Activities*

Monitoring should be done to continuously track changes to the information system that could affect the university's security controls and current security policy. Via monitoring, university could reassess effectiveness of its security policy when the time changes. It also helps minimizes risk to changes a lot of things in the future by patching security holes on small steps. Monitoring may involve maintaining ongoing awareness of information security, vulnerabilities, threats, observing the change in data patterns that could affect the information security of the university.

### *B. Effective Defense in Case of Attack*

After all, no system is 100% secure. So, one should always be ready to face security threat to its security policy. After all the measures applied in the security policy, if an social engineering attack occurs, immediate and effective step should be taken for defense. The strategy could differ person by person or also on the type of attack. After the necessary steps have been taken, the security policy must be reviewed to find what caused the attack and what measures should be added to the security policy so that no such attacks will happen in the future.

## IX. Conclusions And Future Work

The goal of every organization after all is to provide quality service and contribute the society in certain field to make it a better place. People working in an organization are the soul of the organization. People who work in an organization combined have the responsibility of what the organization is going to deliver to the society and how will it fulfill its goals. So, employees of an organization are solely responsible for security of information and data of that organization. For a organization to comprehensively protect its information, it must pay careful attention towards both technical and non-technical forms of security. Even after all the necessary security mechanisms and policies, one cannot deny the fact that their organization could be vulnerable to any forms of attacks.

The study of potential targets of Kathmandu University employees suggests that they have vulnerabilities to both forms of social engineering attacks. The results suggest that certain measures should be applied to eliminate the risk of these attacks discussed in this paper.

Given the small sample size of my study, the findings could be interpreted as a base to be investigated further. Studies could be conducted that involve more employees and more organizations to thoroughly investigate the findings. The employees could also be categorized according to their literacy level, qualifications, IT background, security clearance level and other factors. Experimental surveys could also be performed in an organization for more accurate results from the employees. Furthermore, more social engineering attacks should be taken into account while performing future studies to evaluate the variety of attacks and reaction of people to these attacks.

## References

[1] D. Allan, "We all have too many online accounts - and can't remember the passwords," July 23, 2015. Available http://www.itproportal.com/2015/07/23/we-all-have-too-many-online-accounts-%20and-cant-remember-the-passwords./

[2] F. Amigorena, "Password sharing: How to stamp out a dangerous habit," June 30, 2014. Available http://www.techradar.com/news/world-of-tech/management/password-sharing-how-to-stamp-out-a-dangerous-habit-1255348

[3] A. Chitrey, D. Singh, and V. Singh, "A comprehensive study of social engineering based attacks in India to develop a conceptual model," *International Journal of Information & Network Security,* pp. 45-53, 2012. Available https://core.ac.uk/download/pdf/9428698.pdf

[4] O. Fink, "Vulnerability identification," September 21, 2008. Available Hacking the Universe: http://www.hackingtheuniverse.com/infosec/nist-computer-security/risk-%20assessment/vulnerability-identification

[5] R. Gulati, "The threat of social engineering and your defense against it," 2003. Available https://www.sans.org/reading-room/whitepapers/engineering/threat-social-engineering-defense-1232

[6] "How Password Sharing Destroys Companies," July 21, 2013. Available Perfect Cloud: https://blog.perfectcloud.io/how-password-sharing-destroys-companies/

[7] M. Huber, S. Kowalski, M. Nohlberg, and S. Tjoa, "Towards automating social engineering using social networking sites," *Computational Science and Engineering*, pp. 117-124. 2009. Available // www.sba-research.org/wp-content/uploads/publications/2009%20-%20Huber%20-%20Towards%20Automating%20Social%20Engineering%20Using%20Social%20Networking%20Sites.pdf

[8] "Internet security threat report," 2016. Available https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf

[9] A. Kumar, and N. Kumar, "Social engineering: attack, prevention and framework," 2016. *International Journal for Research in Applied Science & Engineering Technology*. Available http://www.ijraset.com/fileserve.php?FID=4026

[10] J. Long, "No tech hacking: A guide to social engineering, dumpster diving and shoulder surfing," Burlington: Syngress Publishing, 2008.

[11] C. Peterson, "23 Social engineering attacks you need to shut down," March 16, 2016. Available SmartFile: https://www.smartfile.com/blog/social-engineering-attacks/

[12] Social engineering leads the top 10 list of most popular hacking methods-Balabit survey results from black hat USA and EU shows". Available Balabit: https://www.balabit.com/news/press/social-engineering-leads-the-top-10-list-of-most-popular-hacking-methods-balabit-survey-results-from-black-hat-usa

[13] S. Stahl, and K. A. Pease, "Seven Requirements for successfully implementing information security policies and standards: A guide for executives. Los Angeles: Citadel Information Group," 2011. Available https://citadel-information.com/wp-content/uploads/2010/12/seven-requirements-for-successfully-implementing-information-security-policies-1108.pdf

[14] Why You Should Use Different Passwords. Available Privacy and Information Security https://security.illinois.edu/content/why-you-should-use-different-passwords