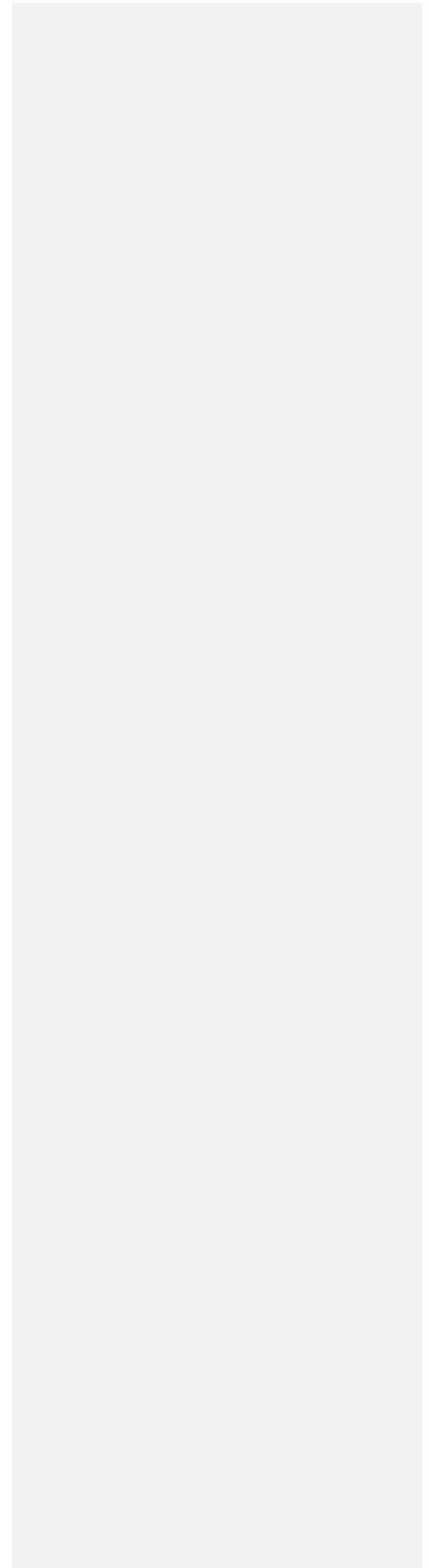


**CYBERSECURITY AWARENESS
ASSESSMENT REPORT
TO ESTABLISH A NATIONAL
CYBERSECURITY AWARENESS
PROGRAMME FOR
NEPAL
OCTOBER 2015**



*This report was prepared by Mr. Raj Kumar under the direction of the
Telecommunication Development Bureau (BDT).*

Acknowledgement

The International Telecommunication Union (ITU) would like to express sincere gratitude to the representatives from Nepal for the support and assistance they provided to the ITU Expert. Our sincere appreciation also goes to individual staff in the organisation in particular, for their advice, support, and comprehension of objectives and challenges of this study. Finally, we would also like to thank the participants from Nepal who have shown great enthusiasm and participated well in every single activity during the workshop.

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU. © ITU 2015

1. Executive Summary

In the second decade of the 21st century we now live in a hyper-connected world, where almost everyone and almost everything – is connected to information and communication technologies, ICTs. Indeed, there are as many subscription of cellular subscriptions worldwide as the population of the world, and there are already over 3 billion people online.

Unfortunately, hyper-connectivity has not come without risks and disadvantages with growing issues of cybersecurity. Cybercrime has already take a huge toll on the global economy: Some of the common examples include online fraud, identity theft, lost intellectual property affecting governments, companies and individuals around the world inflicting damage on the innocent, on the vulnerable, and on our children.

We need to address these issues, because in the world today everything depends on ICTs – and particularly on the networks which underpin them. This includes emergency services; water supplies and power networks; food distribution chains; aircraft and shipping; navigation systems; industrial processes and supply chains; healthcare; public transportation; government services; and even our children’s education.

Recognising the significance and the importance of raising security awareness to further enhance socio and economic development, the Ministry of Information and Communication (MoIC) and Nepal Telecommunications Authority under the technical collaboration of the International Telecommunication Union (ITU) carried out National Cybersecurity Awareness workshop on 2nd September, 2015 in Kathmandu, Nepal. The National Workshop was inaugurated by the Minister of MoIC. There were representation from other relevant ministries and organizations and latest information sharing by ITU, NTA, relevant organizations and industry.

This programme addressed the most pressing and key areas of concerns with today’s Internet users from businesses, organisations to users, and from desktop users to mobile users. Areas such as social media security, mobile security, malware infections, Child Online Protection (COP) and secure communication among the key areas was addressed.

This document is a report of a field mission by an ITU expert to Kathmandu, Nepal to elaborate on the identified gaps and make recommendations to implement a National Cybersecurity Awareness Programme. Before producing this report, the expert has consulted and interviewed key stakeholders and also conducted multiple studies and research to gather as many facts as possible regarding the

Comment [SS1]: Name specific ministries invited

current state of awareness before recommending and implementing a National Cybersecurity Awareness Programme. However, there were times when reasonable assumptions were made due to unavailability of information from the stakeholders.

2. Introduction

Cyberthreats continue to escalate in volume and variation facing all users and virtually connected organisations. As these attacks are known to be sophisticated and highly technical in nature with the availability of tools and techniques, it will continue to have damaging effect on users, systems and infrastructures. Today the Internet has become a critical backbone for information exchange and communication, and it has raised national, economic, societal, legal and regulatory concerns. At the national level, countries need to implement reactive and proactive measures and raise their capabilities in managing these threats in order to remain resilient.

Nepal has been a target of cyberattacks. There has been reported cases of web defacement and advanced persistent threats aimed towards the websites of government and companies. Many of these incidences goes unreported but often identified by the global cybersecurity communities and mentioned in news and blogs. The adoption of proactive and reactive measures are vital in order to identify, manage and mitigate these risks. The cybersecurity awareness programme lies at the heart of all efforts to protect the cyberspace.

One of the key concern is that the internet users may not have the necessary skills or knowledge to identify and manage these online risks. As global reports of threats continue to take the limelight in the global media with increasing frequency and sophistication of cyber threats it is vital for the internet users to be aware and understand the threats in cyberspace. It is understood that online risks cannot be completely eliminated as perpetrator and attackers are usually able to adopt new strategies to attack and increase its complexity to the extent where it is likely to be undetected or unidentifiable. In order to build the confidence and trust in use of ICT, users need to be fully aware in identifying the threats and understanding their weaknesses.

This report describes the outcome of the current awareness study based on the input provided by the stakeholders and the methodology for raising cybersecurity awareness for users, businesses and organisations.

3. Mission Background

Under the supervision of Mr. Sameer Sharma (Senior Advisor for ITU Regional Office for Asia and the Pacific) and the support of the Ministry of Information and Communication and Nepal Telecommunications Authority, Mr. Raj Kumar (ITU Expert), conducted an awareness readiness assessment and workshop exercise for Nepal with the aim of implementing a National Cybersecurity Awareness Programme. The field mission was conducted by the ITU expert over the duration of four days in Kathmandu, Nepal with relevant stakeholders and representatives. The findings and outcomes of this activity form this report for consideration by interested parties.

4. Mission Objectives

The objectives of the mission were to assess the current state, capability, resources and readiness of Nepal to build a sustainable National Cybersecurity Awareness programme based on input from various representatives and stakeholders.

The National Cybersecurity Awareness programme will be the trusted platform for users, businesses and government to understand the current threats and gain tips and best practices to identify, manage and mitigate cyber threats from a user and organisational perspective and at the same time to enhance the cybersecurity sovereign of the country.

The objectives and deliverables of this mission were to:

- a. To raise cybersecurity awareness among key drivers and stakeholders
- b. To study current posture and propose awareness raising framework
- c. To identify key drivers and elaborate on the importance of awareness programme
- d. To disseminate survey questionnaire to identified stakeholder
- e. To develop a project plan and identify resources
- f. To share best practices and experience from other countries
- g. To share success factors and foreseen challenges for implementers
- h. To gain stakeholder support

5. What is a National Cybersecurity Awareness Programme?

A National Cybersecurity Awareness Programme is a formal approach and often, an initiative by the government to raise awareness on current cyber threats and best practices for its citizens, businesses

and related agencies, in order to remain resilient to such attacks. The programme is designed with the target audience in mind, using appropriate communication channels and language to ensure the message is well understood by each target audience. The aim of the awareness programme is to reduce incidents and to raise the confidence in the use of ICT for communications, business transaction and dealing with personal information, by means of maintaining confidentiality, integrity and availability at all times. At national level, if there are many incidents occurring, it would affect eventually economic growth and adoption of ICT as people and investors would not have the trust and confidence in what is seen as critical services, e.g. online banking would not be successful, if there are high reported cases of phishing attacks, scams and web defacements.

6. The Need and Benefits of a National Cybersecurity Awareness Programme?

With the increasing frequency and sophistication of cyber threats, it is increasingly vital for users to be aware and understand the threats in cyberspace. It has been noted that many of today's attacks are facing users, including kids and teenagers at home and staff in the office as they are seen to be the weakest link. The proactive and reactive technical measures are readily available today and they are able to identify and contain latest threats and attack while the human factor remains to be vulnerable. Attacker know this and using this weakness as their most effective form of attack vector as seen in phishing and scam incidents. The society wellbeing and resiliency remains as the government's responsibility as with the physical safety and security. As for the businesses and the government sector who provide vital services for the people, they need to ensure that their information and systems are protected based on international standards, best practices and guidelines.

By informing and motivating people, this structured and targeted programme will create a strong security culture, improve security compliance and cut net costs due to breaches. The awareness programme will address general employees, management, IT people and general public through various streams of awareness measures, resources and campaigns.

7. Assessment Methodology

The readiness assessment was divided into offsite assessment work and an onsite assessment workshop. The offsite assessment involved preliminary work to better understand the current cybersecurity awareness level in Nepal. The offsite work also involved development of questionnaire

which was sent to the relevant stakeholders to prepare the local team and stakeholders for the onsite assessment exercise.

Onsite, the assessment involved awareness sessions to help stakeholders understand what constitutes a National Cybersecurity Awareness Programme. The expert covered areas in Child Online Protection, current threat landscape, applicable laws and current awareness framework.

For data and information collection, the expert provided general consulting, organised meetings and interview sessions attended by relevant government officials including regulatory bodies, law enforcement agencies, ministry of information and communications, telecommunications regulatory bodies. :

The specific activities were:

- a) interviews and discussions with local stakeholders, law enforcement representatives, private sector executives, government representatives and representatives from financial institutions and regulatory bodies;
- b) conducted awareness workshop session, to impart the idea of a National Cybersecurity Awareness Programme and how it can benefit society, businesses and organisations;
- c) discussions with local ICT experts, particularly those performing cybersecurity roles and responsibilities and with regulators and law enforcement officers;
- d) gather information using assessment questionnaire to collect stakeholder opinions and views;
- e) conducted online research to review key websites and publications with information related to ICT and cybersecurity in Nepal

8. National Awareness Framework

The National Awareness is design to provide a strategic direction, concepts, methodology and processes for developing a national cybersecurity awareness programme. The strategy for each target group varies and must be well understood and adopted to ensure the right formulation and effectiveness of the awareness programme. One of the key aspects of a successful awareness programme is to ensure that the target audience receives the message in a manner that is easy to understand and applied. As cybersecurity is often seen as a technical domain but the users are not technical in nature. They are considered to be general users who will understand general terms and concepts relevant to the applications and services they use online.

There has to be “process modelling” for kick starting the scoping, planning, execution and assessment. Each process has to be analysed with time related activities with dependencies identified. The tools and templates must be identified and agreed upon by the project team. Work plans must be drawn up with clear roles and responsibilities of the each of the members. Any obstacles must be understood and method to overcome them. Based on the findings from the assessment exercise in the initial stage, ITU proposes the next stage, that is, the development of cybersecurity awareness programme plan and strategy.

The strategy and plan contained in this document will discuss the following elements:

- Objectives of an awareness and training programme.
- Goals to be accomplished for each aspect of the programme
- Target audiences for each aspect of the programme
- Suggested topics to be addressed for each target group
- Communication channels and strategy
- Project Timelines

- Foreseen challenges in awareness programmes
- Sample Awareness materials

Once the cybersecurity awareness strategy and plan have been agreed by the stakeholder and project lead has been appointed, an implementation or project plan document will be produced with the required input and resources. It is important to decide the factors to be used in determining which initiative to be scheduled first and in what sequence in the project deliverables and the target audience to be addressed initially.

8.1 Stakeholders for National Awareness Programme

National Cybersecurity programme requires appropriate stakeholders commitment in order to be successful. Each stakeholder need to understand their roles and responsibilities in ensuring the awareness messages and campaigns are delivered in the most effective way and the results are gained. Cooperation among key government agencies, private sector, and international organisations will allow for greater sharing of resources and delivery of the programme. There are “no one size fits all” strategy when dealing with people both at home and work, with various background and experience in using ICT. When appointing stakeholders, the project lead must

ensure that they will be able to deliver the target audience and the responsibilities they have bear. There must be cooperation agreement signed, with clearly defined roles and responsibilities with expected deliverable within the given timeline. There must be regular meetings to keep track of the progress and adjustments made, where and when required.

The following are the recommended stakeholders for the national cybersecurity awareness programme:

- Ministry of Information
- Ministry of Finance
- Ministry of Education & Ministry of Higher Education
- Ministry of Health
- National CERT & IT Task Force
- Ministry of Religious Affairs (where applicable)
- Ministry of Justice / Department of Justice
- Police force (Cybercrime Division)/ Law enforcement
- Telecommunications Regulatory Authority
- NGOs/Civil Society
- Industry representatives
- Academia
- Parent/Youth Groups e.g. General Organisation for Youth, Sports and Cultural Activities, Association of Early Intervention for Children with Special Needs.

9. Nepal Awareness Assessment Outcome and Recommendations

This section sets out the key findings, issues, analysis and recommendations for the enhancement of cybersecurity awareness in Nepal. These are based on general research, questionnaire responses and key findings gathered during the onsite assessment and are divided into the following subsections with recommendations:

9.1 Importance of Raising Cybersecurity Awareness

Almost all respondents of the questionnaire and interviews session indicated the importance of raising cybersecurity awareness among all target group due to the increased internet penetration rate and multiple internet connected devices, including smart phones, tables, desktop computers and notebook. Smartphones and tablet computers have become cheaper, thus the increased

ownership of such devices by children and teenagers, parents and adults, senior citizens at home and workplace or schools. Most respondents were IT literate and some were concerned that having access to the internet and especially social media, has raised inter-personal issues and privacy breaches. There were cases of cyberstalking and harassment mentioned but the victim didn't know what to do except reporting to the police.

9.1.1 Recommendations

Cybersecurity awareness in Nepal generally remains low based on the findings. As many citizens have access to internet through their mobile phones and computers, a basic internet safety tips and best practices should be inculcated based on their behaviour and application they use. Nepal having a total population of 26,494,504¹ with 43.67% Internet penetration rate.², which is quite high and these are good indication that there are great interest among people to interact, transact and gather information online. We predict that these numbers will continue to grow as the internet connected devices becomes more affordable. It is clearly evident and important to develop and implement awareness campaigns to educate users, businesses and organisations based on the feedback from the questionnaires and interviews conducting with the stakeholders. The National Cybersecurity Awareness Programme can take the lead in the creation of cybersecurity awareness campaigns with the aim of educating users and reducing incidents.

9.2 Policy and Legal Measures

Electronic Transaction Act was implemented in 2006, which legalizes all electronic transactions and digital signatures. The law defines and sets penalties for computer and cybercrimes, such as hacking, piracy, and computer fraud. Other relevant acts and regulations for information technology and communications are the Telecommunications Act 1997, Telecommunications Regulations 1997 and Telecommunications Policy 2004.

Specific legislation on child online protection has been enacted through the following instruments:

- Section 47 of the Electronic Transaction ordinance
- Section 2(c1) under Some Public (Crime and Punishment) Act
- Section 16(2) and (3) of the Children's Act, 2048 – only for children under 16.

¹ www.cbs.gov.np

² NTA MIS Report (16 June-16 July 2015)

Most respondents were not aware of the current laws, legal measures and policies related to cybercrimes or that allows for prosecution of someone committing cybercrime against a person, business or organisations.

9.2.1 Recommendations

Stakeholders should consider the process of amending or passing of comprehensive cybersecurity laws because delays give cybercriminals the chance to exploit legal loopholes and take advantage of lack of provision for such. Such legal framework should address not only national issues, but also facilitate international cooperation which is critical in times of crisis. Nepal must ensure that national cybersecurity laws are developed within international cooperation principles.

9.3 Current threat landscape and incidents

Currently there are no proper organisation or mechanism dealing with detection, tracking and mitigation of cyberattacks and cybercrime at national level. Isolated cases are treated on an ad-hoc basis either by the Police, ISPs or computer related departments in the government. There are no mechanism or an institution to track or monitor cybercrimes in the country. The people of Nepal are not aware of who to report computer related crimes or breaches and most of them go to the Police. Currently cybersecurity incidents are handle by the police and organisations which has some the capability. The questionnaire findings clearly indicate the need for a national Cybersecurity Awareness Programme that will act as a focal point in managing incidents and as a coordination centre to manage information sharing and information flows so that all relevant parties can report incidents to this central point. The National Cybersecurity Awareness Programme will also provide knowledge of available best practices that can be shared and implemented on the various networks.

Some of the common types of cybercrimes are related to:

- Finance
- Scams
- Phishing
- Viruses and worms
- Frauds

9.3.1 Recommendation

Nepal needs to have focal point for incident reporting and handling such as a National Computer Incident Response Team (CIRT). While there is a definite need for a National Cybersecurity Awareness Programme, there is a need for dedicated agency for incident handling and response as such formal institution will have able to provide proactive and reactive services with highly specialised knowledge and skillset. As the National CIRT will also act as trusted party to the government, businesses and people at large as it is seen as critical service provider. They will also act as a channel for communicating awareness messages and provide advisory services for organisations, including sharing of best practices and guidelines.

9.4 Current Awareness among corporate users, businesses and organisations

Currently there are no formal cybersecurity awareness programme reported by the respondents. Most of the IT savvy respondent were able to manage to keep their computer secure by having antivirus, firewall and applying software updates to their computer. Some were responsible enough not to open suspicious email and those with attachments from unknown sources. Most companies reported that they don't have security policies and acceptable use policies and guidelines. There were reported cases on the use of pirated software due lack of budget and general awareness. Software updates are often not done on such systems which make the computer vulnerable to current attacks.

9.4.1 Recommendation

To develop and deliver awareness programme that will raise awareness on cybersecurity current issues and threats, and how to mitigate them at organisational level. The security awareness programme is appropriately formulated to effectively deliver the key messages tailored to meet each of the target audience.

The awareness programme shall meet the requirements of the organisation and the training needs of the organisation. In today's business environment, security remains a critical component of business operation. Therefore it is crucial that all staff are made aware of the security best practices, processes and policies to safeguard their information resources and remain resilient. The key objective is to design, develop and implement appropriate cybersecurity awareness programme for employees focusing on their role to maintain confidentiality, integrity and availability of information assets.

9.5 Access to Awareness resources

Currently there are no known and formal access to awareness programmes, materials or resources. They may be personal consultation or informal discussions among the IT savvy people on some of the common issues such as malwares, phishing, scams, online privacy but most importantly the larger part of the population are still not aware based on the feedback and assumptions made. With Nepal having a high internet penetration rate, it is critical that internet safety tips and best practices are developed and disseminated to all users.

9.5.1 Recommendation

With Nepal having a high internet penetration rate, it is critical that internet safety tips and best practices are developed and disseminated to all users. The awareness message should be tailored to meet the needs of each target audience including kids and teenagers, parents and adults and organisations. The awareness resources should be customised to local language to overcome language barriers. This should be included in the development process once the English version is completed. Outreach programmes should be developed to sensitise the public about the dangers associated with cyberthreats. Training and education should be conducted to teach users basic steps for dealing with IT security issues.

9.6 Constituency/stakeholder participation

A constituency is the specific community that the National Cybersecurity Awareness Programme is established to serve. Stakeholders are the people who will be involved in the planning, strategizing and decision making of the National Cybersecurity Awareness Programme. Stakeholder organisations can also be a part of the constituency. The National Cybersecurity Awareness workshop was organised by Ministry of Information and Communication (MoIC) and Nepal Telecommunications Authority (NTA) under the technical collaboration of the International Telecommunication Union (ITU).

The list of stakeholders and participants whom attend the workshop are as below:

- Ministry of Information and Communications Senior Management Team
- Nepal Telecommunications Board Members and Senior Management team
- Central Investigation Bureau (CIB) of Nepal Police
- United Telecom Limited (UTL)
- Nepal Telecom

Cybersecurity Awareness Assessment Report for Nepal

- ISP Associations
- Ncell
- Smart Telecom
- Federation of Computer Association of Nepal
- Laliput District Court
- National Information Technology Center
- Office of Controller of Certification
- ITSERT-NP
- Nepal Army
- Prime College
- Institute of Engineering
- Sanima Bank

9.6.1 Recommendations

Stakeholders should adequately manage the confidentiality, integrity and availability of ICT infrastructure, information systems and computers used by people and organisations to connect to the Internet. ISPs, e.g., need to deploy and maintain proper monitoring systems at the international gateways to track and block malicious traffic from infecting the information infrastructure of the country. This, to a certain extent, ensures the availability of services, systems and data for the user and subscribers. ITU recommends Nepal Telecommunications Authority (NTA) to take the project lead on this important initiative, subjected to agreement by all related stakeholders. Stakeholders need to ensure proper cybersecurity governance, policies and procedures are implemented based on international best practices and standards. This is critical component of e-government services, as it is considered to be part of national critical information infrastructure.

10. Cybersecurity Awareness Programme Development and Proposed Deliverables

The cybersecurity awareness programme development and implementation will contribute to:

- Building a strong and resilient cybersecurity culture for Nepal
- Increased confidence in ICT and government services
- Minimizing cybersecurity threats to users in private and public sector organisations in Nepal

Cybersecurity Awareness Assessment Report for Nepal

- Reducing threats and vulnerabilities facing end-users such as Kids and Teenagers, Parents and Adults and Senior citizens.
- Reduced incidents due to informed and educated internet users

The design and development of cybersecurity awareness programme is recommended to be led by Nepal Telecommunications Authority with assistance from ITU. As the development team and the resources are based in Nepal, most of the development will take place and delivered in the country. ITU will visit, based on the project plan for meeting, presentations, trainings and site visits. ITU will communicate directly with appointed Project Director and Steering Committee.

The key deliverables for this project will consist of:

- The report describing the methodology, project implementation plan and findings from initial assessment on the current cybersecurity awareness posture
 - Conducting a series of cybersecurity awareness workshop with a selected private and public sector organisations
 - Identify priorities and resources required to ensure that the awareness plan will respond to and be aligned with national needs
 - Cybersecurity awareness communication strategy and approaches
 - Develop and recommend a proposed strategy for cybersecurity awareness dissemination in Nepal through knowledge transfer and training
 - Design and development of Cybersecurity awareness materials and training programmes including:
 - Conducting cybersecurity awareness trainings for a target group of employees selected from private and public sector organisations
 - Train the trainer programmes for school teachers and private and public sector organisations.
 - Cybersecurity awareness content development for online media including web portal, video and social media, and print media including brochures, posters and banners (for exhibitions).
 - Cybersecurity awareness materials for kids and teenagers and home users, including parents and adults.
 - Cybersecurity video and audio development to be used for TV and Radio campaign

- Conducting cybersecurity awareness Train the Trainer (ToT) programme for future trainers and school teachers
- Conducting Child Online Protection workshop and sharing of resources
- Final project report

11. Target Groups and Communication Strategy

National Cybersecurity Awareness programme shall be formulated to suit the need of the each target audience taking into consideration their age group, social demographics, geographic location, language, job profiles and organisations. The main objective of any awareness programme is to ensure that the target audience to understand the intended message based on the work they do online and the threats that they likely to face. The better you understand the threat, the more precise the topics will be and users will be in a better position to understand the message. The level of depth and technicality should also be considered as awareness programme are for the general users and efforts should be made to keep it simple, precise and concise. It is also to important not create many target groups as there will be redundancy and also the users generally use the same applications such as email, social media, online gaming, online transactions, etc. The difference is what they perceive and their understanding of the threat. Social media application such as Facebook is used by many user ranging from kids to senior citizens but the attacker look for their victim based on the age group and profile. The threat vector varies according to the user profile, there the awareness message should be tailored based on the age group accessing the platform. As for organisations, the target groups can vary from general staff and executives, managers and head of department, to senior manager. The focus will be on security policies, best practices and guideline in protecting organisation's information and physical asset and classifying them, dealing with third party, remote access, bring you own device (BYOD), user acceptance policy and more.

For the awareness campaign to be developed and implemented successfully, following are the key consideration for the project team.

- Determine the Aims and Objectives
- Identify Target Group
- Justifications for the campaign
- Key issues to be addressed and why?
- Establish metrics to measure performance

Cybersecurity Awareness Assessment Report for Nepal

- Develop lesson learnt
- Establish partnership to have better reach and to share resources
- Ensure common message and shared opinions and views

Establishing message for each target group

- To target a specific group that has similar interest and priorities
- Different audiences place different emphasis on different risks
- Ask questions that is relevant and grab their attention, why should they care and what they should do
- Understand the audience
- Know what they care about
- Understand their needs and their concerns
- Inform them where to get the information and know what they like to receive.
- Catch their attention alerting the risks
- Evaluate responses from groups, interview and surveys

11.1 Kids and Teenagers

The awareness programme shall be formulated based on their common activities and application they use online while focusing on acceptable behaviour and internet safety tips which includes the following topic areas and concentrations:

- Dealing with strangers
- Protecting your personal information
- Creating and protecting your password
- Cyberstalking and Harassment
- Social media
- Posting information online
- Protecting your computer
- Installing applications
- Acceptable Use
- Sharing internet experience with their parents or teachers
- Chatting and Instant Messaging
- Dealing with Emails
- Making friends online
- Online gaming
- Knowing who to report incidents

11.2 Parents and Adults

The awareness programme shall be formulated based on their common activities and application they use online while focusing on acceptable behaviour and internet safety tips which includes the following topic areas and concentrations:

- Creating and Protecting your Password
- Conducting online transactions – E-Banking, Auction, Online Shopping
- Social Engineering: Phishing and Scam
- Protecting and updating your computer
- Protecting your information
- Social Media threats and Privacy setting
- Teaching and monitoring your kids online
- Knowing who to report incidents
- Protecting your mobile devices
- Accessing internet in public places
- Internet addiction
- Dealing with Malware and suspicious activities on your Computer.
- Chat and Instant Messaging
- Protecting your personal information

11.3 Organisations

Awareness programme for organisations including the private and public sector, dealing with internal and external factors. Internal factors include the staff, protection of information and physical assets, process and dealing with third parties. There many international best practices and guidelines, including information security management standard such as ISO/IEC27001. The awareness programme for organisation aims educate the staff on current threats and vulnerabilities and how to identify, manage and mitigate them based on accepted behavioural aspect to remain resilient. Every staff shall be at all time maintain confidentiality and integrity of information asset but unfortunately due to negligence, lack of understanding and human, breaches and compromises occurs. Senior management directive and policies will ensure staff take responsibility in managing assets with utmost care.

Considerations and challenges for raising cybersecurity awareness for organisations:

- Expected change of change of behaviour may not work with all staff as they see it as a hindrance to their productivity
- Cybersecurity seen as an IT department problem and not as everyone responsibility
- Lack of management support due to business priorities
- Lack of resources and funding can't be justified
- Investment can't be justified

Cybersecurity Awareness Assessment Report for Nepal

- Failure to develop consistent processes and strategies related securing information and physical assets
- Awareness programme are only considered as a “Check box approach” due regulatory and compliance requirements
- Most unaware that it is part of the cyber incident response process

Who should lead for Organisations?

The following staff are the recommended lead for organisational cybersecurity awareness programmes:

- Information security officers / ISMS managers
- Information security awareness officers
- CIOs / CISOs / CSOs / CTOs
- Security auditors, and governance and compliance officers
- Training managers / Human resource managers
- Anyone responsible for planning and executing security awareness programs

The following are some of the awareness topics and areas of concentration for staff:

- Acceptable use policy
- Protecting your password
- Information Management and Classification
- Bring your own device policy (BYOD)
- Remote Access/Public Access
- Dealing with Third Party/Vendor
- Social Engineering : Phishing and Scam
- Protecting and updating your Computer
- Email Security and Spam
- Reporting Incidents
- Detecting suspicious visitors
- Backup

12. Communication Channels

National Awareness programme shall be designed, developed and delivered in a manner that is most cost effective manner to reach the intended audience. The development of awareness materials and resources can be done in phases by considering the most effective to least effective medium of communication. There must be a balance between the cost and effectiveness focusing on the desired outcome. Refer to Fig. 1 for Communication mediums

Mobile/Online	Print	In Person/Live	Public Media
<ul style="list-style-type: none"> •Email •SMS •Web Portal •Newsletter •Screensavers •Phone App 	<ul style="list-style-type: none"> •Brochure •Magazine •Comic •Poster •Leaflet/Fact Sheet •Newspaper •Education Pack •Teaching Materials 	<ul style="list-style-type: none"> •Fairs •Exhibition •Meeting •Seminar •Conference 	<ul style="list-style-type: none"> •TV •Radio •Video •Billboards •Posters •Bus Ads •Taxi Ads

Figure - Communication mediums

13. Critical Success Factor for raising National awareness

National cybersecurity awareness programmes are intended to reach the target audience in the most effective manner. Understanding the current posture and the threats faced by the audience allows for more accurate programme that will be accepted by the audience. Awareness campaigns can't be delivered by a single party across the country. Strategic partnership with organisations must be established in order to deliver the messages to the target audience using multiple channels and measuring their performance. For organisations, it can be more challenging as there may be organisational culture or not supported by the management due to business priorities. Often security awareness is seen as an afterthought as organisations focus is on their daily operations and their clients. Staff many not give full cooperation to awareness programme as they may not see tangible value in committing to such programmes.

14. Project Timeline

Cybersecurity Awareness Assessment Report for Nepal

The proposed activities and timeline will be further discussed and fine-tuned, once the project kick-off date has been agreed and project lead have been identified. Once agreed, a detailed project proposal will be produced.

Phase/Duration	Task/Activity	Stakeholder
Plan & Assess (1-3 Months)	<ul style="list-style-type: none"> • Pre Assessment Questionnaire • Conduct Awareness Programme for interested parties/stakeholders • Post Assessment Report • Identify Stakeholder/Project Lead • Produce Project Proposal • Seek for Funding and Support • Setup Project Team • Identify Target Groups • Identify Materials needed • Evaluate Potential Solutions • Define Goals and Objectives • Define Communication Plan • Prepare Work Plans 	ITU ASP RO, NTA, MoIC, ITU Expert
Execute & Manage (6 months)	<ul style="list-style-type: none"> • Re-confirm Project Team • Review Work Plans • Confirm Communication Channels • Develop Awareness and Training Materials • Launch Awareness Campaign • Deliver via identified Communication Channels • Conduct Awareness Training • Conduct Train the Trainer Programme • Develop Measurement for Evaluation • Review the Initial Materials • Documentation and Reports 	ITU ASP, NTA, ITU Expert
Evaluate and Adjust (3 months)	<ul style="list-style-type: none"> • Conduct Evaluations • Incorporate Communication Feedback • Review Programme Objectives • Improve Programme as appropriate • Management Documentations and Report 	ITU ASP, NTA, ITU Expert

15. Financial Plan

National Cybersecurity Awareness programmes are generally not commercially profitable as the focus is on raising cybersecurity awareness among identified target groups. The project costing and

expenditure will be proposed once the project has been agreed by the identified project lead and stakeholder. The costing for the awareness campaign will vary according to the selected awareness materials to be developed and the communication channel to be utilised, e.g. website, TV and Radio, posters, brochures and training number of trainings to be conducted. Once the budget have been allocated, the project document will be developed and proposed.

16. Project Team

The following is the proposed project team (Fig.2) will formulate, administer, manage and implement the cybersecurity awareness training for Nepal. Nepal Project Team will work with ITU expert that is assigned for this project. The Nepal Project Team will produce the deliverables of this project to the Project Steering Committee under the coordination of the Project Director. ITU will produce the requirements for each deliverable and assign the tasks involved to the Development Team. The Instructors will be responsible for the delivery of all required awareness trainings in this project.

The roles and responsibilities of each team member:

- Project Director – Oversees the entire project and ensures the development and delivery is going smoothly according to the project plan
- Project Steering committee – This team works with ITU and relevant stakeholders to ensure the project resources are available based on the allocated budget, and keeps track of the progress. They will also act as an advisory panel for the entire project
- Public Relations – the PR team will provide advice on appropriate channels for communicating the awareness message to various target groups. They will also be involved in editing and proof-reading the awareness content for accuracy, while meeting the desired branding scheme.
- Finance and Administration – This personnel will ensure sufficient funds are made available, monitor expenses and budgets to ensure the project is not affected by any shortfall. The administration of the overall project will be handled by this as well to ensure deliverables are met with allocated resources.
- Trainers – Trainers will be responsible for formulating and delivering the content to various target group in classroom style setting. They will also work out the training schedule for the organisations to conduct the awareness trainings.

- Developer – This team will be involved in concept, design and development of the awareness content for each of the identified awareness material customised for identified communication channel including online and offline materials.

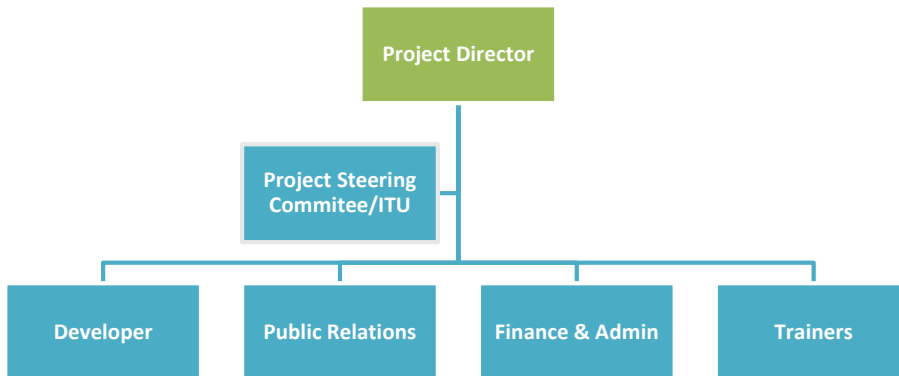


Figure - Project Team

17. Assumptions

There are many factors that can make security awareness difficult to fully achieve. These factors either affect attitudes toward security or the ability to make the right decisions about protecting information assets. The expected outcome of any awareness programme is change of behaviour and approach to internet safety, that to ensure the objective of the of cybersecurity awareness programme is met. The success of cybersecurity awareness programme is to be measured at a pre-defined time once it is deployed or implemented.

The following are the factors to be considered when attempting to improve security awareness in organisation:

People in organisations are busy

People in organisations usually don't have the time to attend formal cybersecurity awareness training or have the time to read security policies and stay current on them. Organisation embarking on cybersecurity awareness programme must seek upper management and department head commitment, support and approval. It has to be organisational wide initiative and not an individual or the IT department initiative. Regular security awareness sessions must be conducted and best practices

must be easily attainable and made available to all staff. Displaying security awareness messages in appropriate locations in an organisation is one example of how security messages can be relayed.

Computer Literacy

For most, an internet-enabled computer is a device or system used for creating documents, gathering information, to conduct business or personal transactions, for communication, store customer information, etc. The level of understanding varies from users and environment they are in and often used based on their needs. It is therefore difficult for computer users to understand or be concerned about the threats, vulnerabilities and exposures and of computers and the information on them.

People don't understand the risk

Risk is often intuitively rather than critically assessed. The components of security risk - threats, vulnerabilities and the value of information - are also poorly understood and often misjudged. Security decisions, the benefactor of security awareness, require a consideration of risk because there is usually a trade-off between security and cost, performance, availability and other concerns.

Financial

There are financial factor that need to be considered which can affect the cybersecurity awareness programme. Often public and private organisation are faced with limited budget to implement security awareness programme as it is perceived as an investment that does not bring financial gain to the organisation. Since organisations exist to serve their customers and constituents with products and services, information assets are critical for their existence and appropriate policies and procedures are to be implemented to protect information from insider and outsider threats. Therefore it should be budgeted for and commitment is required from the senior management. If information or system is compromised due to staff negligence or ignorance, the organisation reputation will be at stake. Prudent investment in security awareness can reduce the probability of an incident. The business benefits (resulting from increased compliance, improved control, reduced risks and reduced losses through security breaches) will substantially outweigh the costs of the programme.

Developing security awareness material

The development of security awareness materials are often influenced by the budget availability. Security awareness materials and resources are to be tailored to meet the needs of the audience and their concerns. Security awareness material must reach the intended audience using the most effective communication channel and platforms. To reach a mass audience, TV and Radio announcements, Billboards, Community events are seen to the most effective medium but it is costly. If the campaigns

are funded and supported by governments and private organisations, the security awareness project the benefit will outweigh the cost. If both public and private organisations, and end-users such parents and adults, kids and teenagers are made aware of the threats on the Internet, they will know how to be safe and remain resilient, which in the longer term, would bring societal wellbeing and wealth creation benefiting the country as a whole.

18. International Partnership

National Cybersecurity Awareness Programme shall be developed with partnership with organisations with similar capacity and resources that are made available. This would help Nepal in developing high quality content for the awareness materials in the shortest time possible by leveraging on accurate, trusted and relevant resources. One of the highly recommended partner is the U.S Department of Homeland Security, whom have developed the Stop.Think.Connect. awareness programme, with collaborative effort from the National Cyber Security Alliance, the Anti-Phishing Working Group (APWG), key industry leaders, government agencies, and non-profit organisations.

The Stop.Think.Connect. is a national awareness campaign that communicates the current threats for the American society and organisations in order to be more safer and secure while online. This campaign has reached thousands of Americans and has been providing useful safety tips on how computer users can protect themselves both at home and the organisations they work for.

19. Critical Success Factors

There are vast amounts of media coverage and reports of security breaches, incidences of information theft and scandals. This is raising the importance of IT security awareness and education among computer user both at home and organisations. As these threats are real and are affecting all computer users, it would be detrimental if users not informed in a timely manner. By increasing awareness and education, it prepares individuals and organizations to secure their involvement in cyberspace. Every individual whether at home or at work is a user of information and securing that information is vital in order to protect the privacy and prevent from threats.

For home-users, the internet is very much becoming part of everybody's life and the individual would need to be educated on internet safety and best practices which would further enable them to educate their peers and siblings. In order to ensure that this target group is addressed, their needs are to be

understood so appropriate awareness programme can be developed and implemented. This target group is comprised of kids and teenager, and parents and adults.

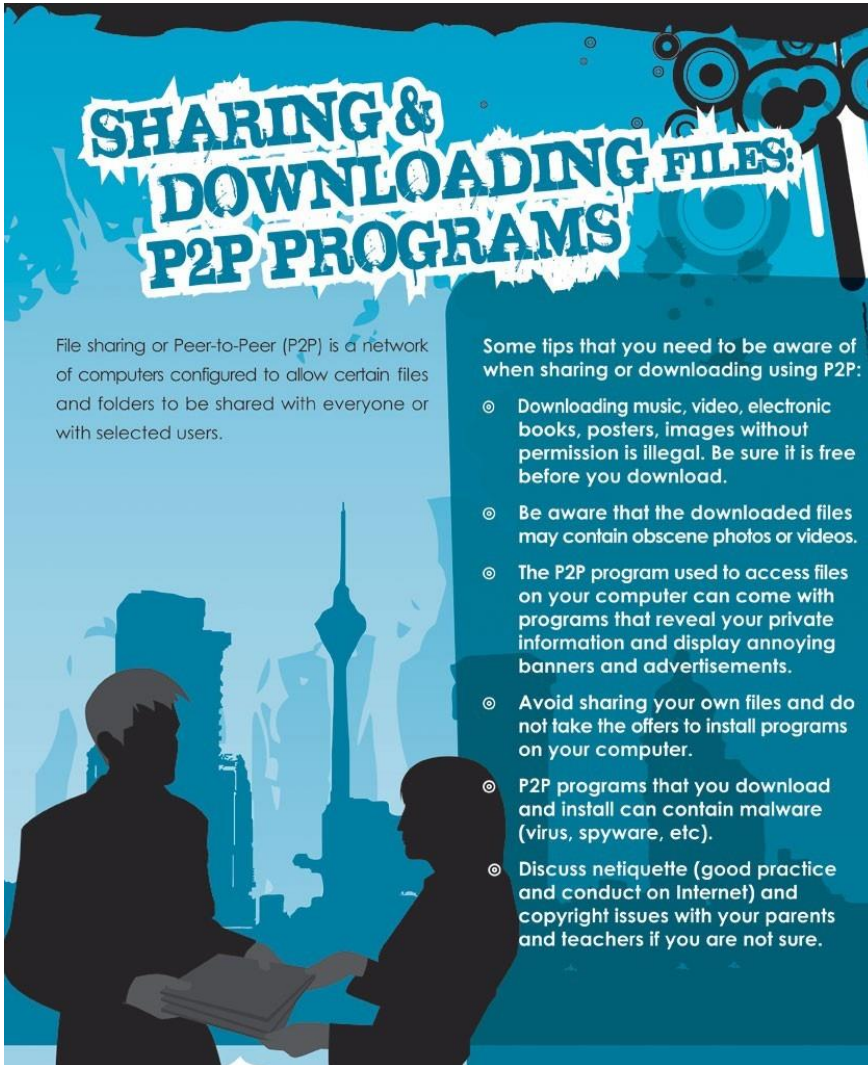
For organisations, the attention has created the need for both the profile and importance of corporate governance and accountability organizations. However, little is known in the current IT security awareness and the existence of information security department in organizations. Organisations need to adopt and use security policies, employ skilled information security staff and deploy security awareness programme for their staff. IT departments are expected to provide evolving solutions that ensures a secure and resilient environment for employees, partners and clients by protecting information assets – complex networks and a wider variety of access points – from more sophisticated attacks, self-replicating viruses and social engineering tactics. Although maintaining effective IT security solutions can save money, but to justify the continuing investment to non-technical decision makers can be a challenge. In today’s business environment, security remains a critical component of business operation. Therefore all staff in any organisation needs to be well aware of the security best practices and policies implemented to safeguard information resources.

20. References

Stop Think Connect	https://stopthinkconnect.org/
ENISA	https://www.enisa.europa.eu/
CyberSafe	http://www.cybersafe.my/en/
Nepal Telecommunications Authority	http://www.nta.gov.np/en/ NTA MIS Report (16 June-16 July 2015)
Ministry of Information and Communications Technology	http://www.moic.gov.np/en/
Nepal Central Bureau of Statistics	www.cbs.gov.np
Implementation of WSIS Action Line C5	http://www.itu.int/wsis/c5/index.html
ITU Global Cybersecurity Agenda	http://www.itu.int/osg/csd/cybersecurity/gca/
ITU Activities related to Cybersecurity	http://www.itu.int/cybersecurity/
COP Guidelines	http://www.itu.int/osg/csd/cybersecurity/gca/cop/index.html

Appendix 1: Sample Awareness Materials

Posters



SHARING & DOWNLOADING FILES: P2P PROGRAMS

File sharing or Peer-to-Peer (P2P) is a network of computers configured to allow certain files and folders to be shared with everyone or with selected users.

Some tips that you need to be aware of when sharing or downloading using P2P:

- ⦿ Downloading music, video, electronic books, posters, images without permission is illegal. Be sure it is free before you download.
- ⦿ Be aware that the downloaded files may contain obscene photos or videos.
- ⦿ The P2P program used to access files on your computer can come with programs that reveal your private information and display annoying banners and advertisements.
- ⦿ Avoid sharing your own files and do not take the offers to install programs on your computer.
- ⦿ P2P programs that you download and install can contain malware (virus, spyware, etc).
- ⦿ Discuss netiquette (good practice and conduct on Internet) and copyright issues with your parents and teachers if you are not sure.

MAKING FRIENDS ONLINE: SOCIAL NETWORKING

A social networking site is an online place where a user can create a profile and build a personal network that connects him or her to other users.

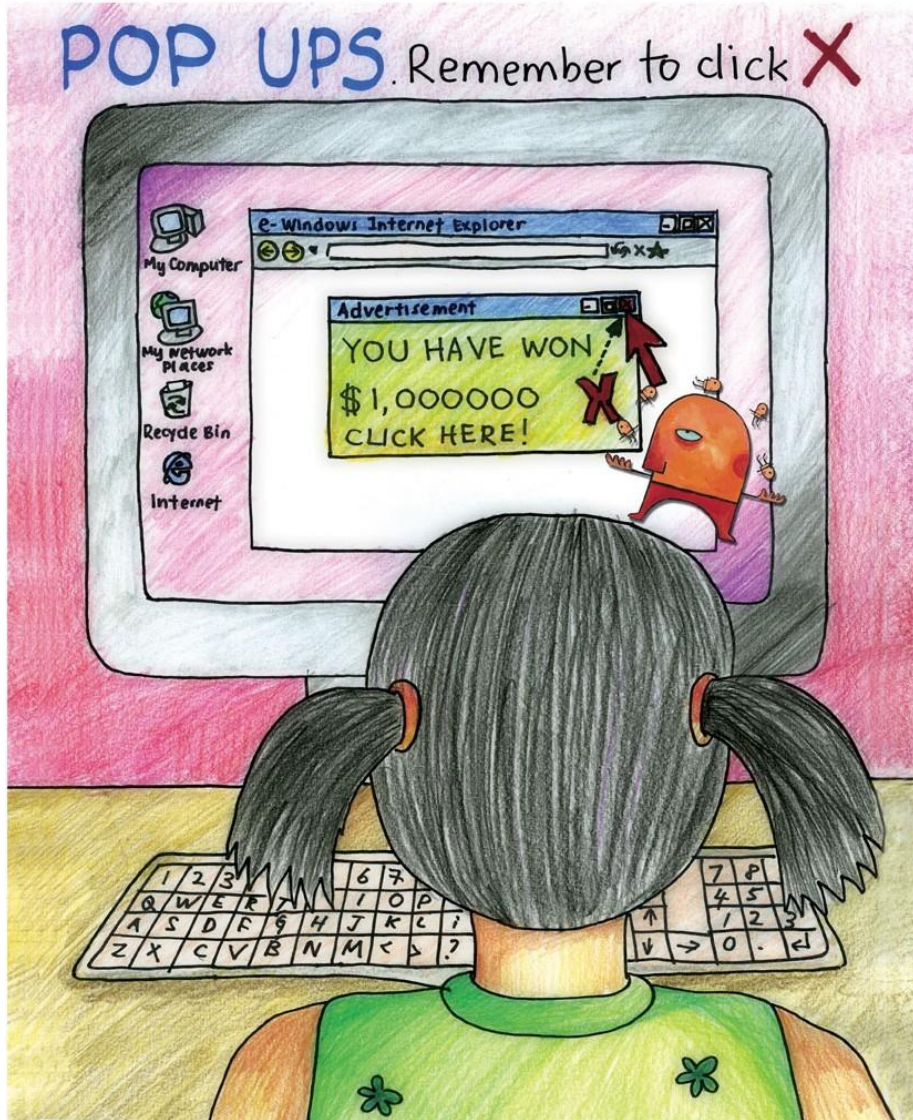
Some tips for safe social networking:

- ⦿ Don't reveal too much information about yourself on the "Your Profile".
- ⦿ Be careful when communicating with people you've only met recently online, especially those asking personal questions.
- ⦿ Add people as friends to your site if you know them in person.
- ⦿ Delete any messages of those who write comments that may not be appropriate.
- ⦿ Check the rules on social networking sites such as *Friendster*, *MySpace*, *Facebook* before using it to make friends.
- ⦿ Do not post information about your friends as you could put them at risk.
- ⦿ Remember, what you post online are not private and can be seen by anyone.

13 STEPS TO SAFE INTERNET BANKING

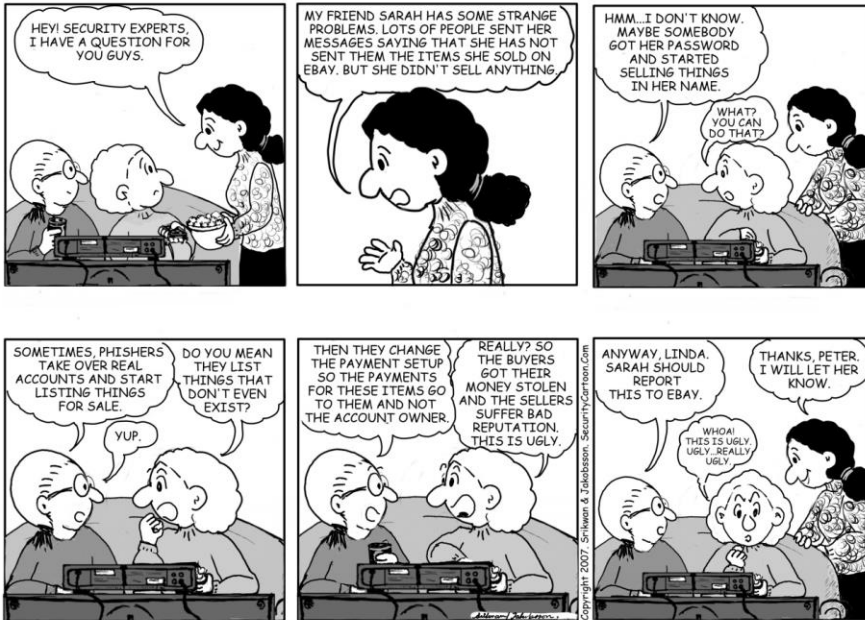
1. Keep your password/PIN code safe every 3 months. If you conduct Internet banking, create unique passwords for each website. Create unique passwords for each website.
2. How do you know the website is secure?
 - Look for https:// in the URL
 - Look at the status bar of the browser on the padlock and ensure it is locked
3. Log out immediately after completing your Internet banking session and history (refer to your bank's Internet banking session and history).
4. Never leave your computer unattended.
5. If you are unsure of the security of a website, do not use it.
6. Use an anti-virus, anti-spyware software that is always up-to-date and available on the Internet.
7. Ensure that your PC and browser are up-to-date with the latest security feature of your Operating System.
8. Do not be influenced by attachments in your emails. Do not click on links to surf or use your **Bookmark**.
9. Do not respond to emails as requested. Report to your bank.
10. If you decide to go to other websites, do not provide any personal information of that website.
11. Always check your account regularly.
12. When visiting your Internet banking site, always log out when you last signed in.
13. If your bank account has been compromised, report to your bank immediately.

WEB BROWSER	SECURED
Microsoft Windows Platform	
Internet Explorer	
Netscape Navigator	
Firefox	





Security Cartoons



Cybersecurity Awareness Assessment Report for Nepal

Brochures



What are the benefits of using the Internet?

- Access to information using multimedia (text, sounds, pictures, and video).
- Convenient communication tool for sending messages.
- Obtain most up-to-date information on anything of your interest.
- Learn to understand and compare information written/posted by many people.
- Interact with people (experts) over great distances for specific information or conduct discussion.
- Platform to seek for views and opinions on your area of interest.
- Play fun and educational games.
- Gain knowledge and skills that may be useful in your hobby or your future jobs.

What can you do as a Parent?

- Learn about the Internet and the possible risks. Visit www.esecurity.org.my.
- Spend time with your child and get involved in their life to learn about their online interest and experience.
- Keep the computer in the family area to better monitor your child's activity.
- Teach your child to end any online activity when he or she feels uncomfortable or scared by logging off or telling you or a trusted adult (school teacher) as soon as possible.
- Discuss with your children the difference between advertising and educational or entertaining content and show them an example of each.
- Help them to choose a login name and make sure it doesn't reveal any personal information about them.
- Insist that your children respect the property of others online. Explain to them that making illegal copies of other people's work (music or movie), video games, and other programs is just like stealing it from a store.
- Tell your children that they should never meet online friends in person. Explain that online friends may not be who they say they are.
- Control your children's online activity with advanced internet software. Parental controls can help you filter out harmful content, monitor the sites your child visits, and find out what they do there.
- Teach your kids that not everything they read or see online is true. Encourage them to ask you if they're not sure.
- Tell them to never reveal their personal information about themselves or their family to anyone.

What you need to know

The Internet is a great place that comes with enormous amounts of information and resources for everyone. But for parents it poses new challenges as the Internet medium is highly interactive and very much people-oriented when it comes to personal communication, unlike with TV and radio. Some people use the Internet to promote things that we do not want our children to be exposed to, e.g. pornography, illegal gambling and other unsuitable materials.

You need to know what are your children exposed to on the Internet and how best go about talking to your children about them. You also need to observe their change in behaviour, e.g. they are spending too much time on the Internet, they have not been happy lately, etc.

Your child can be exposed to:

- Websites with sexually explicit images and text.
- Websites promoting hatred, violence, drugs and other things not appropriate for children.
- Information that is inaccurate, misleading, and not true.
- Marketing companies that collect personal information from kids in order to sell products to them or their parents.
- Requests for personal information from appealing contests, surveys, to be used in unauthorized ways.
- Easy access to games with excessive violence.

Should you stop your children from using the Internet?
No, the Internet is useful for them to communicate with people (classmates, friends and family); do research for their studies, playing games and much more. It is rich source of information but also poses dangers if they are not careful and made aware. There are things that you can do to protect your children, just like dealing with real life problems.

Sample: Electronic Mail Acceptable Use Policy

Electronic Mail Acceptable Use Policy

User Responsibilities

These guidelines are intended to help you make the best use of the electronic mail facilities at your disposal. You should understand the following.

The Organisation provides electronic mail to staff to enable them to communicate effectively and efficiently with other members of staff, other companies and partner organisations. When using the Organisation's electronic mail facilities you should comply with the following guidelines.

DO

- Do check your electronic mail daily to see if you have any messages.
- Do include a meaningful subject line in your message.

Cybersecurity Awareness Assessment Report for Nepal

- Do check the address line before sending a message and check you are sending it to the right person.
- Do delete electronic mail messages when they are no longer required.
- Do respect the legal protections to data and software provided by copyright and licenses.
- Do take care not to express views, which could be regarded as defamatory or libellous.

DO NOT

- Do not print electronic mail messages unless absolutely necessary.
- Do not expect an immediate reply, the recipient might not be at their computer or could be too busy to reply straight away.
- Do not forward electronic mail messages sent to you personally to others, particularly newsgroups or mailing lists, without the permission of the originator.
- Do not use electronic mail for personal reasons.
- Do not send excessively large electronic mail messages or attachments.
- Do not send unnecessary messages such as festive greetings or other non-work items by electronic mail, particularly to several people.
- Do not participate in chain or pyramid messages or similar schemes.
- Do not represent yourself as another person.
- Do not use electronic mail to send or forward material that could be construed as confidential, political, obscene, threatening, offensive or libellous.

Please note the following:

All electronic mail activity is monitored and logged.

All electronic mail coming into or leaving the Organisation is scanned for viruses.

All the content of electronic mail is scanned for offensive material.

If you are in any doubt about an issue affecting the use of electronic mail you should consult the I.T. Department. Any breach of the Organisation's Electronic Mail Acceptable Use Policy may lead to disciplinary action.