Internet Safety Guidelines

Stay safe in school, home and office by following simple security rules and protect yourself from being tomorrow's headline.

DREAMS
NEPAL

Strong Passwords

Passwords are a primary means to control access to systems and should therefore be selected, used and managed to protect against unauthorized discovery or usage. Passwords provide the first line of defense against improper access and compromise of sensitive information.

Weak passwords are passwords that are easily guessable, crackable and vulnerable to attacks. Weak passwords make it very easy for hackers to gain access to an account and could lead to substantial financial loss and identity theft.

Strong passwords should include the following best practices:

- Should not be left blank.
- Must be at least eight characters in length.
- Must contain a character from three of the following four character sets:

- Lower case characters (e.g. a to z)
- Upper case characters (e.g. A to Z)
- Numeric digits (e.g. 0 to 9)
- Character symbols (e.g. + = ( ) &% ! ? ><)

Passwords do Not's

- Should not include three or more consecutive characters from your login or full name.
- Should not be a word in any language, slang, dialect, jargon, etc. (e.g. the word 'password' is a weak password).
- Should not include your name, common names of people or places, technical jargon, repeating sequences and keyboard sequences.
- Should not be written down or stored on-line.
- Should be easily remembered. Do not use the same password on multiple accounts. If one account is breached, the others will be at risk as well.
- Do not enter passwords when others can observe what you are typing.
- Do not reveal your password to anyone.
- Do not share your password with your supervisor, manager, partner, your children, your friends, etc.
- Do not walk away from a shared computer without logging off.

- Always log out of systems / applications when they're not in use
- Lock your computer when not in use
- Do not leave an application unattended if it is logged in or unless a password protected screen saver is in place
- Change your password immediately if you suspect that others know your password

Other considerations to take note of:
Remember: If someone has your password, the intruder can commit criminal acts using your account.

E-Mail Use Guidelines

E-mail is an efficient and timely communication tool used to conduct business within government, businesses and citizens. E-mail has become an important component of any office automation system. E-mail facilitates the exchange of information, speeds up the decision making process and reduces paperwork, resulting in increased productivity, reduced costs and ensures better delivery of services. Please be guided by the following good practices:

Do's

- Check the address line before sending a message and check you are sending it to the right person/s.
- Respect the legal protections to data and software provided by copyright and licences.
- Treat all e-mail with suspicion. What you see in the e-mail body can be forged, the sender's address or return address can be forged and the e-mail header can also be manipulated to disguise its true origin.

Do Not’s

- Do not use e-mail to send or forward material that could be seen as confidential, political, obscene, threatening, offensive or libelous.
- Do not auto forward government e-mails to any private e-mail accounts.
- Do not forward chain letters, junk mail, jokes or news flashes.
- Do not use e-mail for monetary gain, political purposes or illegal activities.
- Do not use the Government data or computing resources/systems to violate state laws and regulations.
- Do not download and/or distribute copyrighted materials including print, audio, and video.
- Do not download e-mail attachments from unknown sources.
- Do not include any confidential information in an e-mail message.
- Do not send offensive, defamatory, racist, obscene, pornographic, harassing or threatening messages, hate mails, discriminatory remarks and other anti-social behaviour messages.
- Do not use e-mail to spread computer viruses, damage or destroy data, infiltrate systems, damage hardware or software, or in any way degrade or disrupt the network performance.
- Do not send e-mail messages using another person's e-mail account.
- Do not disguise or attempt to disguise your identity when sending out an e-mail.
- Do not use e-mail for private business.

Internet Use Guidelines

Do's

- Be careful when using the Internet - remember you're representing the Government of Nepal and follow ETA of Nepal.
- Verify that before installing any software, the software has been obtained from a reputable source and legally.
- Do viruses scan check on any downloaded files prior to opening.

Don'ts

- Do not visit sites that contain obscene, hateful, pornographic or otherwise illegal material.
- Do not store confidential Government data on third party sites as you do not know where these documents might end up.
- Do not perpetrate any form of fraud or piracy.
- Do not send offensive or harassing material to other users.
- Do not hack into unauthorized areas.
- Do not disclose your password.
- Do not use the Internet to conduct any personal business or for commercial or promotional purposes.
- Do not install or use peer-to-peer (P2P) software.
- Do not redistribute downloaded material unless the owner has given permission in the copyright/license terms.
- Do not use someone else's password to gain access to the Internet.

Physical Access Security

Do's

- Ensure that your visitors have signed the visitor's log book and that they are escorted at all times.
- Report a lost, stolen or damaged electronic identification tag to the department concerned.
- Escort visitors in restricted areas of information resource facilities.
- Notify administration/security with any abnormal movements of unfamiliar individuals within the premises.
- Report to administration/security any violations, namely:

- Refusal to wear the electronic identification tag visibly;
- Manipulation of the automatic door closing mechanism;
- Use of another person's electronic identification tag;
- Unescorted visitors.

- Access to computer rooms can only be given when an authorized staff member is inside and will supervise the visitor's movements completely or hand over to successive staff.
- Restrict physical access to servers to authorized staff.

Do Not's

- Do not follow closely behind another person so as to gain access to an area requiring the use of an electronic identification tag (tailgating).
- Do not give, share or loan your electronic identification tag.

Phishing

Phishing is a technique used to gain personal information for purposes of identity theft by using fraudulent e-mail messages that appear to come from legitimate sources. The message may look quite authentic, featuring corporate logos and formats similar to the ones used for legitimate messages.

In any working environment, different people hold information that can be considered sensitive or else can be particularly useful to outside parties. A Phishing attacker will make use of non-technical methods *(such as **Social Engineering** which is the practice of deceiving someone into revealing passwords or other information that compromises the security of a system)* to gain that information.

A good number of Phishing attempts make use of e-mail to reach out to millions of possible victims. Such e-mails look very similar to the website of the company that these e-mails claim to be coming from.

When you think of Phishing, think of fishing. Similar to how anglers used to lure fish, online scammers use certain tactics to lure us into giving them our valuable information under false pretenses. Since information is so readily available to everyone via the Internet, recognizing online threats will help prevent us from falling victims to such attempts.

- *What you see in the e-mail body can be forged, the sender’s address or return address can be forged and the e-mail header can also be manipulated to disguise its true origin. Unless the e-mail is digitally signed you can't be sure it wasn't forged or 'spoofed'.*
- *Never reveal information, such as passwords, to anyone making contact with you.*
- *Do not forward any credit card details and/or bank account numbers through e-mail.*
- *Do use anti-virus and anti-spyware software, as well as a firewall, and update them all regularly.*
- *Do not reply to any e-mail asking to verify your personal data. You will find that legitimate vendors and merchants do not send such requests via e-mail.*
- *Never send personal or financial information to any one via e-mail.*
- *Ensure that all of your software is up to date - for instance, if you use Microsoft Windows, run Windows Update every day when you first connect to the internet. If you use other operating systems or browsers then check daily for patches or updates. Security loop-holes are regularly discovered in software.*
- *Make sure you're on a secure Web server when submitting credit card or other sensitive information via your Web browser. Check the beginning of the Web address in your browser’s address bar - it should be "https://" rather than just http://.*
- *Report any Phishing incidents immediately to your supervisor or line manager.*

Clear Desk and Clear Screen

Papers and computer media containing classified information must be stored safely when not in use. This will reduce the risks of compromise, unauthorized access and disclosure, loss of, and damage to government information.

Employees must lock their computers when leaving their desk and log-off when leaving for an extended period of time. This ensures that the contents of the computer are protected from prying eyes and the computer is protected from any unauthorized use. Computers left unattended provide the opportunity for malicious data input, modification, or deletion, often with a negative consequence to the actual employee.

Remember, users are held accountable for all their PC activities entered through the User ID whether or not the user was present at the time.

Clear Desk

- All classified information must be removed from the desk and locked away in a drawer or in a filing cabinet.
- Passwords must not be written down and stored near a computer or in any other accessible location.
- Copies of documents containing classified information must be immediately removed from printers/fax machines.
- Documents or magnetic media, or other removable media such as CDs, DVDs etc should be safely stored away.
- Desks must be cleared at the end of each working day (excluding 24 hour environments).
- Personal items (i.e. keys, handbags, wallets, etc) must be locked away safely for security purposes. It is the responsibility of the owner to ensure that all security precautions are taken.

Clear Screen

- Users must shut-down their computers at the end of the working day. Locking the screen not only prevents someone else from using the PC, which is logged on in the user's name, but it also prevents someone from reading classified information left open on the screen.
- Lock workstations (computers, laptops and windows terminals) when unattended by pressing Ctrl-Alt-Del. At the end of the working day close down all the applications and log off/shutdown the workstation.
- Laptops must be stored securely and not left on desks when the user is not in attendance at the office. Laptops are not to be left at any site or premises where the user cannot be sure of its security.
- Laptops must be either locked with a locking cable or locked away in a drawer or cabinet when the work area is unattended or at the end of the working day.
- All knowledge, information and access to information should be handled responsibly. It is the responsibility of each user to consider the security of the information they have access to and to protect that information accordingly.

- Remember that the laptop and the information stored on it is the user’s responsibility.
- Electronic data and equipment shall not be treated differently from manual records and equipment, as they contain the same type of classified and/or personal information. Computer and all other equipment containing data should therefore be treated with the same level of security as paper based resources.
- Computers and laptops must not be left logged on when unattended, and must be protected by passwords, screensavers and other security controls that are available.
- Screens must be locked by the user when leaving their computer terminal, irrespective of the amount of time spent away from the unattended screen.
- Don’t position your screen in a way that sensitive information may be read by others.

SMSishing

Identity thieves have found a new way to get to your personal information through your cell phone by pretending to be legitimate businesses or financial institutions. This practice is known as **SMSishing** and you don't have to use your computer to be vulnerable to online scammers.

SMSishing is a type of social engineering that uses cell phone text messages to persuade victims to provide personal information such as credit/debit card details, PINs, etc. SMSishing is a derivative of Short Message Service *(SMS, which is the communications protocol used for sending text messages on cell phones*) - plus Phishing. The incoming text message, which contains a virus, will be a legitimate looking website address or more commonly, a phone number that connects to an automated voice response system, which then asks to confirm your personal details.

Herewith are some examples about how an individual can protect himself/herself against SMSishing:

§ Never reply to SMSs, calls or e-mails on transactions that you did not perform.

§ Never reply to a text message asking you for confidential information.

§ Never click on any website links found in unsolicited SMS or Multi-Media Messages (MMS) from unknown sources. Do not reply to such SMSs and delete them immediately.

§ Call your cell phone service provider to unsubscribe you from the list that sent you the original text message.

§ Keep your cell phone number confidential and share it only with known sources such as friends and relatives. If you put it on your business card, be careful whom you give it to.

§ Avoid entering your cell phone number on websites to get free ringing tones or other free offers.

§ Always remember that your cell phone is just as susceptible to SMSishing as your computer is to Phishing.

§ Use your password to secure your handset. Apart from the default factory settings create a combination that won't easily be guessed by others, and set up the device to automatically lock up if not used for a few minutes.

§ Do not enable automatic log-in because it will store your username and/or password in the device itself.

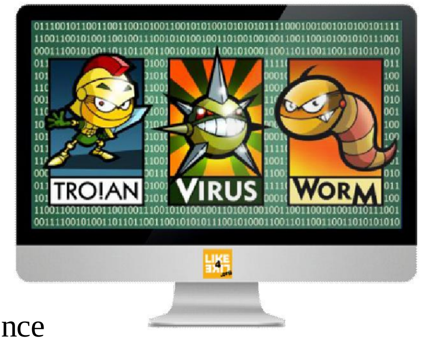
- Never store reminders of your username and/or password in your contacts list or as a text message.
- Download applications from a trusted site. Do not download illegal software as this might contain a virus.
- Check regularly for security patch updates on your phone. Enable automatic updates and install anti-virus software and other security software such as firewalls, where possible. Make sure the sources are genuine.
- Be aware that message headers can be forged easily, so the posing sender may not be the real sender.
- Avoid connecting to unencrypted wireless access points. Use encrypted wireless connections of known sources.
- Where possible, encrypt data on your cell phone.
- Ensure that a Website is secure by checking whether there is an "s" after the http in the address and a lock icon at the bottom of the screen. Both are indicators that the site is secure (e.g. https://www.abc.com)

Be extra careful about clicking on embedded internet links in text messages. You should also use your common sense if you get an unexpected text message. That free anti-virus software could turn out to be a virus in itself.

Viruses

What is Malware?

Malware (or MALicious softWARE) is software which gets onto your PC and causes viruses, worms or Trojans to run without you even knowing. You will never know that you have Malware on your PC until you begin to experience system degradations or system crashes.



How does Malware work?

Malware hijacks your PC and uses it for malicious activities. Once Malware sneaks into your PC, it is capable of:

- Spying on your surfing habits,
- Logging your passwords by observing your keystrokes,
- Stealing your identity,
- Reading your e-mail,
- Hijacking your browser to web pages that phish for your personal information and a variety of other invasive tactics.

How does Malware get onto my PC?

Basically, Malware is a computer program that invades your system when you open e-mail attachments, visit websites, open instant messaging sessions or during file-sharing sessions.

Why is Malware used?

It is difficult to know why people write these malicious programs. Everyone has his/her own reasons. Some general reasons are to experiment how to write viruses or to test their programming abilities and talents. Some people just like to see how the virus spreads and gets 'famous' around the world.

What is Spyware?

Spyware, sometimes called a **spybot**, a program which installs itself on your PC (usually without your permission) in order to monitor (spy) all your activities on your PC and online.

How does Spyware work?

Spyware works by running a program behind the scenes on your PC. You are unlikely to know that you're being monitored. Some types of Spyware will run to cause a nuisance on your machine by launching advertising pop-ups or changing the browser homepage. Other things which come under the Spyware spectrum include tracking cookies, which collect information from thousands of sites to see who visits what and when, along with other things which bury themselves deep into the PC memory and track other data.

How does Spyware get onto my PC?

Spyware is software that is downloaded on your PC as a result of clicking on certain ads on the Internet. Spyware will bombard you with pop-ups and will place hyperlinks on websites for Spyware advertisements instead of the real advertisements.

The developers of Spyware use the weaknesses of internet browsers and the naivety of inexperienced PC user's advantage to get their Spyware downloaded on the PC. If the Spyware program is particularly malicious it will bury itself into the machine. This means that even if you delete it from the machine, it will come back again unless removed professionally or by using specialized removal software.

Why is Spyware used?

The aim of some Spyware programs, as the name suggests, is to spy on your PC activities. The intent is to capture personal data (i.e. passwords, credit card details, etc.) and transmit that data back over the Internet to a malicious source. When you enter information, it is transmitted to a server and this information can then be used, for example, to purchase goods by using your bank account details or to use your information for other fraudulent purposes.

What is Spam?

Spam is any unsolicited communication received electronically. Typically, we think of e-mail but instant messaging can also be a source of Spam. Spam can be an entry point for Spyware or Malware.

How does Spam work?

Spam is the mass mailing of a single e-mail to thousands or millions of recipients. The Spam perpetrator, known as the spammer, obtains a list of valid e-mail addresses from one of several sources, then fires out as many e-mails as the spammer wants, hoping to get a percentage of profitable responses. The spammer can send out thousands of e-mails in a very short period with really no expense other than the bandwidth necessary to mail out all those e-mails or just the cost of the Internet connection itself.

The second most common source of Spam is many e-mail propagating viruses, or 'worms' on the Internet. Once a PC is infected with one of these programs, it will e-mail a copy of the virus accompanied by a deceptive message, to every e-mail address known by the system (on your address book). If these e-mails are opened, the worm will reproduce itself exponentially creating more junk e-mail.

How does Spam get onto my PC?

Many companies have special software that can extract e-mail addresses and put them into a database to sell. Many companies also search the web looking for web addresses containing the symbol @. From these, they can find valid e-mail addresses.

Why is Spam used?

Many spammers can buy a database from companies with millions of valid e-mail addresses and use them to advertise. These e-mail addresses are composed of addresses used on websites, newsgroups, chat rooms, etc.

What is Adware?

Adware is software that displays advertising banners, re-directs you to websites and otherwise conducts advertising on your PC.

How does Adware work?

Adware is software which installs itself onto your PC with the intention of promoting adverts depending on the information it captures about the victim.

How does Adware get onto my PC?

There are many ways in which Adware can get on your PC. The most common way is through attachments in unsolicited e-mails. When you open the attachment, it will install itself on your PC and might give someone else access to your computer while you are connected to the Internet.

Why is Adware used?

Adware programs will often pop up adverts depending on the searches you conduct. This is a source of revenue for Adware authors as they will get a small amount of money every time an advert shows. If this operates on a global scale, the authors will soon become rich in a very short time.

Summary of possible problems caused by these threats:

- Lots of pop-up windows in the web browser
- Cascading windows that cannot be closed
- Slows PC and gets worse over time
- Takes up large amounts of hard disk space
- Reduces Internet speed;
- Cannot access the Internet
- Restarts PC on its own
- Freezes up Web browser
- Home page changed in web browser and cannot be reset

- Changes in web browser such as unfamiliar links in Favourites, different default search engine and new buttons on toolbar
- New shortcuts appear on the desktop, the task bar, or even the system tray that the user did not put there
- Firewall and anti-virus software mysteriously turned off
- Firewall alerts the user to an unknown program or process trying to access the Internet, or one trying to access the PC.

Protect your Data

Update Your Operating System and Applications Regularly

Every computer uses a piece of software called an Operating System (OS). An OS is the most important software that runs on your computer. The OS performs many essential tasks for your computer such as storing and retrieving data, interfacing with other programs and hardware, and other functions. It controls the memory needed for computer processes, manages disk space, controls peripheral devices, and allows you to communicate with your computer. As systems are used and new technologies are released, the OS requires software patches and upgrades to resolve any security issues that are discovered. An unpatched OS can become an entry point for an intruder attack. You need to update your OS, your security software and all other programs on your computer on a regular basis.

Install and Update Anti-Virus Software

Anti-virus software programs are developed to detect and remove computer viruses and other virus-related software from your PC. Anti-virus software protects your PC from viruses that can destroy your data, slow down your PC's performance, cause a crash, or even allow spammers to send e-mail through your account. Anti-virus software works by scanning your computer and your incoming e-mail for viruses and then deleting any effected mails. Ensure that your anti-virus definition files are up-to-date and ensure that automatic update settings are configured and that updates are being applied.

Install and Update Anti-Spyware Software

Spyware software monitors or controls your computer use and is usually installed on your computer without your consent. It is used to send you pop-up ads, redirect your computer to websites, monitor your Internet surfing or record your keystrokes to obtain your passwords, which in turn could lead to the theft of your personal information.

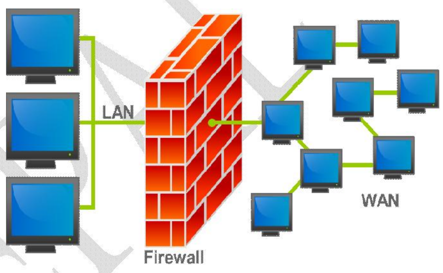
A computer may be infected with spyware if it:

- **Slows down, malfunctions, or displays repeated error messages;**
- **Won't shut down or restart;**
- **Serves up a lot of pop-up ads, or displays them when you're not surfing the web;**
- **Displays web pages or programs you didn't intend to use, or sends e-mails you didn't write.**

Use Care when reading E-mail with attachments

Do not trust any attachment to be what it claims to be or from whom it says it is from. All of the information in the header of the e-mail, including the identity of the sender can be forged and the true identity of the attached file may also be disguised. It is best to treat all incoming attachments with suspicion. Never open any attachments unless you are expecting them and know who they are from. If you are in doubt, do not open the attachment and contact the sender asking him/her to confirm what they have sent you.

Install a Firewall



A firewall helps in keeping hackers away from using your computer to send out your personal information without your permission. A firewall is like a guard, watching for outside attempts to access your system and blocking traffic to and from sources you do not permit. A firewall comes between you and the Internet, monitoring what comes in and what goes out. By configuring your firewall to disallow all traffic except what you are aware of and have specifically permitted, you can protect yourself from both hostile intruders and information leaks. A firewall is an essential part of your on-line security.

Make Back-ups of Important Files and Folders

Any kind of digital storage is susceptible to failure. It cannot be predicted, but one can certainly plan for it. It is worth the while to get into the habit of making periodical back-ups. Back-ups are the last line of defence against hardware failure, damage caused by a security breach or just accidental deletion of data. Keep a copy of important files on removable media. Use software back-up tools if available and store the back-up disks in another location in a safe place.

Safeguard Your Password

A good password should not only be difficult to crack but also easy to be remembered. Passwords are an important aspect of computer security. They provide front line protection to computer accounts. It is your responsibility to safeguard your password. Never share your password(s) with anyone. If you share your password, you are granting someone else access to your information. You are responsible for protecting your own password/s and for the responsible use of your accounts.

Protect your Personal Information

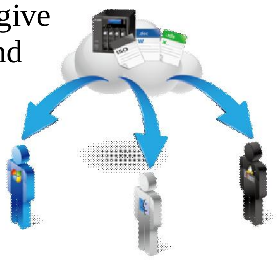
To an identity thief, your personal information can provide instant access to your financial accounts, your credit record and other assets. If you think no one would be interested in your personal information, think again. Anyone can be a victim of identity theft. Millions of people become victims of identity theft every year. One way by which criminals get your personal information is by lying about who they are, to convince you to share your account numbers, passwords, and other information so they can get your money or buy things in your name. *The scam is called phishing*. Criminals send e-mails, text, or pop-up messages that appear to come from your bank, a government agency, an on-line seller or another organization with which you do business. The message asks you to click to a website or call a phone number to update your account information or claim a prize or benefit. It might suggest something bad will happen if you don't respond quickly with your personal information.

Avoid Phishing Scams

Some identity thieves have stolen personal information by hacking into large databases managed by large corporations. Don't give out your personal information unless you first know how it's going to be used and how it will be protected. If you are shopping on-line, don't provide your personal or financial information through a company's website until you have checked for indicators that the site is secure, like a lock icon on the browser's status bar or a website URL that begins "https:" (the "s" stands for "secure"). Unfortunately, no indicator is foolproof; some scammers have forged security icons. And some hackers have managed to breach sites that took appropriate security precautions.

Beware of File-Sharing

Every day, millions of computer users share files on-line. File-sharing can give people access to a wealth of information, including music, games, and software. File-sharing will connect your computer to an informal network of other computers. Millions of users could be connected to each other through this software at one time. However, file-sharing can have a number of risks. If you don't check the proper settings, you could allow access not only to the files you intend to share, but also to other information on your hard drive, like your e-mail messages, photos and other personal documents. In addition, you may be unknowingly downloading malware or pornography labeled as something else. Or you may download material that is protected by copyright laws, which would mean you could be breaking the law.



Don't Let Your Computer Become Part of a BotNet

Some spammers search the Internet for unprotected computers they can control and use anonymously to send spam, turning them into a robot network, known as a botnet (also known as a zombie army). A botnet is made up of thousands of home computers sending e-mails by the millions. Most spam is sent remotely this way. Malware may be hidden in free software applications. It can be appealing to download free software like games, file-sharing programs, etc. But sometimes just visiting a website or downloading files may turn your computer into a bot.

Secure your Wireless Network

An unsecured wireless network can give hackers access to your computer in order to steal your personal information or to upload malware onto your computer. In order to secure your wireless network, be sure to enable encryption, change the default password that comes with your wireless device, change the Service Set Identifier name (SSID), turn off SSID broadcasting and use MAC filtering. Your wireless device manual should guide you on how to implement these security settings.