Cyber stalking

Cyber stalking is a crime in which the attacker harasses a victim using electronic communication, such as e-mail or instant messaging (IM), or messages posted to a Web site or a discussion group. A cyber stalker relies upon the anonymity afforded by the Internet to allow them to stalk their victim without being detected.

Social Engineering

Social engineering is the art of manipulating people to acquire confidential information. The types of information these criminals are seeking can vary, but when individuals are targeted the criminals are usually trying to trick you into giving them your passwords or bank information, or access your computer to secretly install malicious software–that will give them access to your profile or bank information or control over your computer.

Example:

Phishing: Phishing is a cybercrime in which a target or targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords.

Spoofing: A spoofed is one that appears to originate from one source but actually has been sent from another source

Online Fraud

Making friends by chatting with trusty words using messaging application such as Viber, WhatsApp, etc. Later they send the photos and images of expensive goods as friendship gift to the users. In order to receive the gift, they force to pay/clear custom duty and will be delivered in time but nothing will be delivered. This is the behavior how unknown person extort someone online.

Internet Society Nepal

Anamnagar-32, Kathmandu, Nepal
Tel: +977 1 **5705841**
Email: **info@isoc**.org.np
Web: www.**internetsociety**.org.np

Central Investigation Bureau (CIB)
Police Headquarters
Contact No# 4411776
Mobile No# 9851283140
email - cib@nepalpolice.gov.np

"TOGETHER WE CAN COMBAT CYBER CRIME"

Central Investigation Bureau (CIB) Central Investigation Bureau (CIB) Central Investigation Bureau (CIB) Central Investigation Bureau (CIB) Central Investigation Bureau (CIB)

नेपाल प्रहरी
केन्द्रीय अनुसन्धान ब्यूरो
Central Investigation Bureau (CIB)

Cybercrime:

Cybercrime is any illegal act committed by using a computer and network.

OR,

Simply, Where a Computer is involved in the facilitation or commission of a criminal act.

OR

Even simply, Unlawful acts wherein the computer is either a tool or a target or both.

How to be safe from Cybercrime

You've probably heard the adage "information is power," and that is certainly true when it comes to cybercrime. Access to your personal information is what gives hackers the power to tap into your accounts and steal your money or your identity. But the right information can also empower you to protect yourself from being caught up in the thriving industry that is cybercrime.

With that in mind, here is our Top 10 list of steps you can take to avoid becoming a victim of cybercrime.

Use a full-service internet security suite

Use real-time protection against existing and emerging malware including ransomware and viruses, and helps protect your private and financial information when you go online. Do not use pirated software as it may harm your computer.

Use strong passwords

Don't repeat your passwords on different sites, and change your passwords regularly. Make them complex. That means using a combination of at least 8 letters or more, numbers, and symbols. Do not use family name, date of birth or common words as your passwords.

Keep your software updated

This is especially important with your operating systems and internet security software. Cybercriminals frequently use known exploits, or flaws, in your software to gain access to your system. Patching those exploits and flaws can make it less likely that you'll become a cybercrime target. Use genuine software which gets updates patches.

Manage your social media settings

Keep your personal and private information locked down. Social engineering cybercriminals can often get your personal information with just a few data points, so the less you share publicly, the better. Never share your information and location on social sites.

Secure your wireless network at home or office

Hackers can access data while it's in transit on an unsecured wireless network. You can keep the hackers out by enabling the firewall on your router and changing the router's administrator password. Cybercriminals often know the default passwords and they can use them to hack into your network. You may also want to set up your router so it only allows access to people with passwords that are encrypted. Check your owner's manual for instructions on setting up encryption. Change your password every few months.

Keep an eye and talk to your children about the internet

You can teach your kids about acceptable use of the internet without shutting down communication channels. Talk to your kids about the internet and make sure they know that they can come to you if they're experiencing any kind of online harassment, stalking, bullying or identity theft. Cyber criminals often look at the information what is shared. It's also smart to know what to look for that might suggest your child's identity has been compromised.

Keep up to date on major security breaches

If you do business with a merchant or have an account on a website that's been impacted by a security breach, find out what information the hackers accessed and change your password immediately. Be vigilant during doing business online.

Take measures to help protect yourself against identity theft

Identity theft occurs when someone wrongfully obtains your personal data in a way that involves fraud or deception, typically for economic gain. Never share your personal information to other and secure your personal data. Never click unknown links.

Know what to do if you become a victim

If you believe that you've become a victim of a cybercrime, you need to alert the local police and concerned department. This is important even if the crime seems minor. Your report may assist authorities in their investigations or may help to thwart criminals from taking advantage of other people in the future.

Social Engineering attacks

Social engineering is the art of manipulating people so they give up confidential information. The types of information these criminals are seeking can vary, but when individuals are targeted the criminals are usually trying to trick you into giving them your passwords or bank information, or access your computer to secretly install malicious software–that will give them access to your passwords and bank information as well as giving them control over your computer. To be safe first consider the source, delete any request for financial information or passwords, reject requests for help or offers of help, set your spam filters to high and secure your computing devices.

Cyber Crime Trend in Nepal

Social Site Issues

Social media has become one of the most important communication channels now-a-days. Use of Social media has increased. There are many benefits that can be taken from social sites such as connecting friends, sharing information and news. But some persons may use bad benefit of information that has been shared in social sites such as imposter, morphing, fake news, etc.

Piracy/Intellectual Property Crimes

Any content which has been copied with the intention to make a duplicate copy without the permission of original author or creator is known as Piracy. This is related to Intellectual Property Rights. Any unlawful act by which the owner is deprived completely or partially of his/her rights is an offence. For instance, software piracy, infringement of copyright, trademark, patents, designs, theft of computer source code etc.

Hacking Computer System

Hacking is one of the main cybercrime around the globe. It is getting access into a website, programme, server, service, or other system using someone else's account is done mainly for financial gain or to damage the reputation of an individual or company.

Cyber Defamation

Cyber Defamation is one of the latest weapon used by other party to damage or injure a person's or company's reputation using online media such as blogs, social media, online videos, and other internet forums/sites.