JOL Established by INASP in 2007. Managed by Tribhuvan University Central Library.

Ganeshman Darpan

A Peer-Reviewed, Open Access Journal

साइबर अपराध मौलाउँदै यसको सुरक्षामा संवेदनशीलता र बढ्दो चुनौती

सुदीप रैला [a,*]

[a] Ganeshman Singh Multiple Campus, Kathmandu

Article Info

Received: October 16, 2024
Accepted: December 18, 2024
Published: May 22, 2025
Available online: May 29, 2025

DOI: https://doi.org/10.3126/gd.v10i1.80608

Keywords: *सूचना, प्रविधि, साइबर अपराध, डिजिटल, कम्प्युटर, एन्ड्रोइड मोबाइल, नेटवर्क, इमेल, इन्टरनेट, बुलिङ, ब्ल्याकमेलिङ, इन्ट्रानेट, एक्स्ट्रानेट, सामाजिक सञ्जाल, एप्लिकेशन, अर्पानेट, वर्ल्ड वाइड वेब, भर्चुअल*

Abstract

प्रस्तुत लेख साइबर अपराध र यसबाट कसरी सुरक्षित रहन सकिन्छ भन्ने विषयसँग सम्बन्धित छ । विश्वव्यापी रुपमा माकुराको जालो झैँ गरी जेलिएको इन्टरनेटको सहायतामा कम्प्युटर तथा कम्प्युटर नेटवर्कमार्फत विभिन्न गैरकानुनी क्रियाकलापहरु विश्वभर फस्टाउँदै गएका छन । अहिले नेपालमा पनि डर लाग्दा किसिमबाट साइबर अपराधका गतिविधिहरु हुँदै आएका छन । यस अध्ययनले अबका दिनमा इन्टर नेटको प्रयोग के कसरी गर्ने, साइबर अपराध हुनबाट कसरी सुरक्षित रहने, कस्ता विषयहरु साइबर अपराध हुन भन्ने विषयबारे इन्टरनेटका प्रयोगकर्तालाई सचेत गराई सही दिशातर्फ उन्मुख गराउने लक्ष्य रहेको छ । मैले यस अध्ययनको लागि विभिन्न क्षेत्रका बौद्धिक व्यक्तिहरु र इन्टरनेट प्रयोगकर्ताहरुसँग साइबर अपराध भनेको के हो र यस्ता गैरकानुनी क्रियाकलापबाट बच्न के गर्नुपर्ला भनी छलफल तथा अन्तर्वार्ता विधिको अवलम्बन गरी विश्लेषणसहित यो अनुसन्धानमूलक लेख प्रस्तुत गरेको छु ।

सूचना प्रविधिको विकाससँगै विश्वभर आपराधिक गतिविधिहरु पनि विभिन्न स्वरुपमा विकसित हुँदै गएको छ । अहिले कम्प्युटर तथा कम्प्युटर नेटवर्कमार्फत इमेल तथा वेबसाइट ह्याकिङ गर्ने, व्यक्तिको चरित्र हत्या गर्ने, तथ्याङ्क तथा पासवर्ड चोरी गर्ने, फेसबुक तथा अन्य सामाजिक सञ्जालबाट ब्ल्याकमेलिङ गर्ने, इन्टरनेट बैंकिङ जालसाजी गर्ने, अर्काको नाम, तस्विर, भिडियो तथा रेकर्ड गरिएका श्रव्यदृश्य सामग्रीलाई अनधिकृत रुपमा प्रयोग गर्ने, क्रेडिट कार्ड तथा एकाउन्टको चोरी गर्ने, इन्टरनेटमार्फत महिला तथा बाल यौनहिंसालगायत फेक आइडी बनाएर विभिन्न सामाजिक सञ्जालमार्फत गाली बेइज्जती गर्ने, अश्लील फोटो तथा भिडियो बनाएर पठाउने जस्ता इन्ट्रानेट र एक्स्ट्रानेटसँग सम्बन्धित सबै गैरकानुनी गतिविधिहरु भइरहेका छन । यी र यस्ता सबै गैरकानुनी क्रियाकलापहरु आज विश्वभर फस्टाउँदै जानाले विकसित तथा कम विकसित मुलुकहरुमासमेत ठूलो समस्याको विषय बनेको छ । अहिले विश्वभर नै सबै नागरिकले भो गदै आएको साझा समस्या साइबर अपराध हो । साइबर अपराधबाट बच्न स्वयम् इन्टरनेट प्रयोगकर्ता सचेत हुनुपर्ने र राज्यतर्फबाट कडाभन्दा कडा कानून बनाएर लागू गर्नुपर्ने देखिन्छ । त्यसका साथै इन्टरनेटको प्रयो गमा साइबर अपराध एक देशभित्र मात्र नभएर विश्वको जुनसुकै राष्ट्रको एक कुनाबाट गर्न सक्ने भएकाले अन्तर्राष्ट्रिय स्तरमै साइबर समन्वय हुनु जरुरी छ । यसोभएमा मात्र सबै मुलुकबाट साइबर अपराधका गतिविधिहरु कमी हुनसक्छ ।

परिचय तथा पृष्ठभूमि

सन् १८८५ मा Babbage designs 'computer' को विकास भएको नब्बे (९०) वर्षपछि सन् १९७५ मा Gray Kildall ले PC Operating System को विकास गरे । यसरी वैज्ञानिक खोज अनुसन्धानबाट नयाँ नयाँ सूचना प्रविधिको विकास हुने क्रममा सन् १९६९ मा अमेरिकाको रक्षा विभागका अनुसन्धान विशेषज्ञहरुले चारओटा कम्प्युटरको नेटवर्कबाट प्रयोगात्मक रुपमा सूचना सम्प्रेषण गर्न शुरु गरे . जसलाई अर्पानेट 'Advance Research Project Agency Network' (ARPANET) को नाम दिएका थिए । त्यसै गरी सन् १९७२ मा इमेलको विकास हुनपुग्यो । सन् १९६९ मा विकास भएको अर्पानेट (ARPANET) लाई सन् १९७४ मा आएर गैरसरकारी शैक्षिक नेटवर्कको अवधारणाअनुसार "इन्टरनेट" भनेर प्रयोग गर्न थालियो । त्यसपश्चात् कम्प्युटरबाट मेल आदानप्रदान गर्न सकिने भयो । त्यसैगरी सन् १९८९ मा बेलायतका वैज्ञानिक टीम बर्नर्स ली (Tim Berners-Lee) ले वर्ल्ड वाइड वेब (World Wide Web) को विकास गरे । त्यसको एक वर्षपछि सन् १९९० मा (Hyper Text Transfer Protocols) 'HTTP' को विकास भयो ।

त्यसैगरी सन् १९९८ सेप्टेम्बर ४ तारिखका दिन ल्यारी पेज र सर्जी ब्रिन मिलेर संयुक्त राज्य अमेरिकाबाट गुगल (Google) को विकास गरे । इन्टरनेटको सहायतामा गोगलमा कुनै पनि सामग्रीहरु राख्न तथा राखिएको सामग्रीलाई तुरुन्तै पत्ता लगाउन सकिन्छ । इन्टरनेटबिना यो कार्य सम्भव छैन । इन्टरनेटको विकास नेपालमा पनि सन् १९९० पछि मात्र भएको पाइन्छ । नेपालमा इन्टरनेटको शुरुआत गर्ने पहिलो संस्था मर्कन्टाइल (Merchantile) हो । सन् १९९४ मा मर्कन्टाइल कम्युनिकेसन प्रा.ली. (Merchantile Communication Pvt.Ltd) ले इमेल सेवा उपलब्ध गराएको थियो । त्यसपछि नेपालमा पनि सरकारी तथा गैरसरकारी कार्यालयहरुले एक कार्यालयबाट अर्को कार्यालयमा महत्वपूर्ण सूचनाहरु मेलमार्फत पठाउन र पाउन सकिने भयो । त्यसका साथै सर्वसाधारण व्यक्तिहरुले पनि इन्टरनेटको सहायतामा आफ्ना महत्वपूर्ण सूचनाहरु आफ्ना साथीभाइलाई मेलामार्फत पठाउन थाले । यसरी सन् १९९० को दशकबाट इन्टरनेटको सहायतामा मेलमार्फत सन्देश आदानप्रदान गर्ने र Yahoo तथा Google मा राखिएका सामग्रीहरु हेर्न सकिने भयो ।

सन् २००० पछि त संसारभर इन्टरनेटको विकासले माकुराको जालो झैँ फैलियो । अनेकन सूचना प्रविधिको विकास भयो । यसले व्यक्तिको दैनिकीलगायत एक स्थानबाट अर्को स्थानसम्म चाहेको समयमा सन्देश आदानप्रदान गर्न सकिने भयो । अझ एन्ड्रोइड मोबाइलको विकास भएपछि त्यसमा भएको प्ले स्टोर (Play Store) मार्फत अनेकन एप्लिकेशनहरु डाउनलोड गरी त्यसबाट आफूसँग साथी भएका व्यक्तिहरुलाई श्रव्यदृश्यका सामग्रीहरु तथा सन्देश आदानप्रदान गर्न सकिने भयो ।

* Corresponding author.
E-mail addresses: sudipraila@gmail.com

आजका मानिस भर्चुअल संसारमा बाँचेका छन भन्दा फरक नपर्ला । इन्टरनेटको विकासले सञ्चार जगतमा कायापलट नै भएको छ । आज नेपालको कुनै एक विकट मानिने जिल्लाबाट अमेरिका, अष्ट्रेलिया, जापान तथा जर्मनमा रहेका छोराछोरीसँग श्रव्यदृश्यमा कुराकानी गर्न पाएका छौ । सूचना प्रविधिमा भएको विकास के यो सानो हो र ? पक्कै होइन । अहिले भर्खरै इजरायलमा बस्ने नेपाली चेलीसँग नेपालबाट उसको मोबाइल नम्बर डायल गरेर तुरुन्तै कुरा गर्न सकिन्छ । यसलाई अलिक घोत्लिएर सोच्नुहोस् त कसरी सम्भव भयो होला । यस्तो विकास मानवले मात्र गर्न सक्दछ । अहिलेका मानवले यी र यस्ता कयौं प्रविधिहरुको विकास गरेका छन जुन सबै मानिसको पहुँचसम्म नपुगेको पनि हुनसक्छ ।

सूचना प्रविधिको विकासमा न्युमिडियाको उदयले राजनीतिक भौगोलिक सीमाबाहिरसमेत पुगेर समष्टिगत विश्वलाई नै मानवग्रामको रुपमा परिणत गरिदिएको छ । त्यसैले आजको युगलाई सूचना प्रविधिको युग भन्ने गरिन्छ । हिजोका परम्परागत सञ्चार माध्यमले यस्तो अतुलनीय कार्य गर्न सकेको थिएन । यसोभन्दैमा रेडियो र टेलिभिजनले किन गरेको थिएन भनेर प्रश्न गर्नेहरु निस्कन सक्दछन । तर न्युमिडियाले झैं विश्वभर सूचना आदानप्रदानमा परम्परागत मिडियाबाट सहज थिएन । यसमा कसैको दुईमत नहोला ।

सूचना प्रविधिको विकासमा अहिले विश्व नै डिजिटल युगमा छ । नेपाल पनि यस युगभन्दा बाहिर रहन सकेको छैन । नेपालमा छोटो समयमै आमनागरिकहरु डिजिटल प्रविधिमा अभ्यस्त भए । अझ एन्ड्रोइड मोबाइलको विकास भएपछि त झनै मोबाइलको प्ले स्टोरमा उपलब्ध सामाजिक सञ्जालका विभिन्न एप्लिकेशनहरु डाउनलोड गरेर इन्टरनेटको सहायतामा एक व्यक्ति र अर्को व्यक्तिकाबीच सूचना आदानप्रदान गर्न सहज भयो । यो राम्रै पक्ष हो । त्यसैले बालक, युवा तथा बृद्धबृद्धाहरुलाई समेत सूचना र शिक्षा दिने लिने र मनोरञ्जन गर्ने माध्यमको रुपमा न्युमिडिया सबै माझ परिचित छ । तर यसको प्रयोगमा व्यापकता भएसँगै विक्रिति र विसंगति पनि उत्तिकै बढ्दो छ ।

देश तथा विदेशमा भएगरेका विविध विषयवस्तुबारे चाहेअनुरुप सूचना तथा सन्देश सम्प्रेषण गर्न सकिने सुविधाले यसको प्रयोगकर्ताको संख्यामासमेत वृद्धि भएसँगै साइबर अपराध पनि बढ्न थालेको पाइन्छ । यसरी साइबर अपराधबारे मातृकाप्रसाद लम्साल, गोविन्दप्रसाद भण्डारी र विष्णुबहादुर कार्कीले संयुक्त रुपमा “विद्युतीय माध्यमको प्रयोग गरेर गरिने अपराध नै साइबर अपराध हो” (लम्साल, भण्डारी र कार्की, वि.सं. २०८१:११६) भनी परिभाषीत गरेका छन । इन्टरनेटबाट गरिने उच्छृङ्खलता, गुमनामी तथा छद्मभेषबाट फाइदा उठाई विद्युतीय प्रविधिलाई दुरुपयोग गर्ने प्रवृत्ति नेपालमा मात्र नभई संसारभर मौलाउँदो छ । विकसित राष्ट्रहरुमा साइबर अपराध गतिविधिलाई रोक्न साइबर सुरक्षा योजना, साइबर थ्रेट एनालाइसिस, आइटी अनुसन्धान रणनीति, साइबर आतंकवाद अनुसन्धान, साइबर सुरक्षा सेवा जस्ता कार्यक्रमहरु सञ्चालन गरेर सर्वसाधारणलाईसमेत सचेत र जागरुक गराउने काम गरेका छन । तर नेपालमा भने यस प्रकारका कार्यक्रमहरु देखिंदैनन् र यस विषयमा खासै अनुसन्धानमूलक लेख तयार गरेको पनि पाइदैन । यसै अभावलाई पूर्ति गर्ने उद्देश्यका साथ यो लेख तयार गरिएको छ । प्रस्तुत लेखमा यसको विकासक्रम र यसले पारेका राम्रा नराम्रा प्रभावबारे व्याख्या तथा विश्लेणात्मक ढङ्गबाट प्रस्तुत गरिएको छ । साइबर अपराधबारे अध्ययन गर्न चाहने अध्येताका लागि यो प्रस्तुत अध्ययन उपयोगी हुनेछ ।

उद्देश्यहरु

यस अध्ययनको मुख्य उद्देश्यहरु निम्नानुसार रहेका छन :

१. इन्टरनेटका प्रयोगकर्तालाई साइबर अपराधबारे बुझाउन,

२. साइबर अपराधबाट कसरी सुरक्षित रहने भन्ने सचेत गराउन र

३. साइबर अपराध न्यूनीकरण गर्न ।

अध्ययन विधि

सूचना प्रविधिको विकासले ल्याएको सञ्चार साधनहरुमार्फत विभिन्न गैरकानुनी क्रियाकलापहरु बढेसँगै साइबर अपराध बढ्न थालेको हो । यसै कुरालाई आधार मानेर यस अनुसन्धानमूलक लेख तयार गर्दा मैले “साइबर अपराध मौलाउँदै यसको सुरक्षामा संवेदनशीलता र बढ्दो चुनौती” शीर्षकको यो लेख गुणात्मक प्रकृतिको अध्ययनमा आधारित भएर तयार गरेको छु । प्रस्तुत अनुसन्धानमूलक लेखको अध्ययन विधिमा सामग्री सङ्कलन विधि, सैद्धान्तिक ढाँचा, सामग्री विश्लेषण, अन्तर्वार्ता र प्रश्नावली विधिको अवलम्बन गरिएको छ ।

प्रविधिको प्रयोग गरेर अपराध गतिविधि बढाउने कार्य एक प्राविधिक कार्य हो । तर त्यसले पार्ने प्रभाव व्यक्ति, परिवार, समाज तथा राष्ट्रको विभिन्न पक्षमा पर्ने हुँदा यसलाई परिमाणात्मक भन्दा पनि गुणात्मक अनुसन्धान विधिको अवम्बन गर्दा बढी अर्थापन हुने भएकाले गुणात्मक विधिको उचित प्रयोग गरी यसको व्याख्या तथा विश्लेषण गरिएको छ । तसर्थ यसबारे चिन्तन मनन गर्ने बौद्धिक व्यक्ति तथा इन्टरनेट प्रयोगकर्तासँग छलफल, अन्तर्वार्ता तथा खुल्ला प्रश्नावली विधिको अवलम्बन गर्दै विभिन्न विद्वानहरुले तयार पारेका पुस्तकहरु, जर्नल, प्रज्ञा नेपाली बृहत् शब्दकोश, इन्साक्लोपेडिया ई. प्राथमिक र द्वितीय स्रोतको प्रयोग गरेको छु । यस लेखमा प्रयोग गरिएका स्रोतहरु मिश्रित छन । केही महत्वपूर्ण विषयको जानकारीका लागि इन्टरनेटको सहायतामा यसै विषयसँग सम्बन्धित लेख, रचना, विचारहरुलाई स्रोतको रुपमा लिइएको छु । यसरी सङ्कलन गरिएका सामग्रीको छफलका लागि विश्लेषणात्मक विधिको उपयोग गरिएको छ । यो अनुसन्धानमूलक लेख गुणात्मक विश्लेषणमा आधारित लेख हो ।

परिणाम र विमर्श

पहिले पहिले विज्ञान वरदान भनेर भन्ने गरिन्थ्यो भने अहिले अभिषाप पो होकी भन्ने कुरा साइबर अपराधका गतिविधिबाट भान हुन थालेको छ । अहिले डिजिटल प्रविधिमार्फत अनेकन आपराधिक गतिविधिहरु बढ्दो छ । यसै विषयमा आधारित हुँदै यस अनुसन्धानमूलक लेख तयार पारिएको छ । यस लेख तयार पार्न विभिन्न क्षेत्रका १५ जना बौद्धिक व्यक्तिहरु र ५५ जना इन्टरनेटको प्रयोगकर्ताहरुसँग सोधखोज, छलफल, अन्तर्वार्ता र खुल्ला प्रश्नावली विधिको अवलम्बन गरिएको छ । यिनै व्यक्तिहरुका भनाई तथा धारणालाई आधार मानेर विश्लेषण गरी प्रस्तुत गरिएको छ ।

साइबर अपराध भनेको के हो ?

साइबर अपराधको परिभाषा गर्नु निक्कै जटिल र महत्वपूर्ण पक्ष हो । कम्प्युटर र इन्टरनेटबाट गलत मनसायले कसैको चरित्र हत्या, वेबसाइट तथा इमेल ह्याकिङ, फेसबुक तथा अन्य सामाजिक सञ्जालबाट ब्ल्याकमेलिङ, पासवर्ड चोरी, इन्टरनेट बैंकिङ जालसाजी, अर्काको नाम, तस्बिर, भिडियो तथा रेकर्ड गरिएका श्रव्यदृश्य सामग्रीलाई अनधिकृत रुपमा प्रयोग, बौद्धिक सम्पत्ति चोरी, क्रेडिट कार्ड क्लोनिङ, झुटा इमेल, साइबर बुलिङ, घृणापूर्ण अभिव्यक्ति, कम्प्युटर तथा विद्युतीय उपकरणलाई नेटवर्कमा पुऱ्याउने कार्य सबै साइबर अपराध हुन । तर इन्टरनेटमा भएका सबै विषयहरु अपराध होइनन् । त्यसैगरी कम्प्युटर नेटवर्कको प्रयोग गरेर हुने इन्टरनेट, इन्ट्रानेट तथा एक्स्ट्रानेटसँग सम्बन्धित आपराधिक क्रियाकलापहरु सबै साइबर अपराधको कोटीमा दर्ज भएका छन । त्यसै गरी प्रज्ञा नेपाली बृहत् शब्दकोशले “साइबर” को अर्थ : “विद्युतीय सञ्चारको सञ्जाल” (नेपाल प्रज्ञा–प्रतिष्ठान,वि.सं. २०७९: १९४५) भनी बताएको छ ।

त्यसैगरी हरी आचार्यले साइबर अपराधबारे : “सूचना प्रविधिको उपयोग मार्फत अनधिकृत पहद्दँच स्थापित गरी व्यक्तिगत, संस्थागत र सार्वजनिक सुरक्षामा गम्भीर खलल पार्ने विषय साइबर अपराध” (२०८०, आश्विन १४, आइतबार) प्रशासन डठकममा æसाइबर अपराध : समस्या, चुनौती र समाधान” शीर्षकको लेखमा बताएका छन । तसर्थ साइबर अपराध कम्प्युटर नेटवर्कको सहायताबाट गरिने जुनसुकै आपराधिक क्रियाकलाप हो । अहिले विश्वभर इन्टरनेटको प्रयोग बढेसँगै साइबर अपराध पनि बढ्न थाले को छ । कम्प्युटर तथा कम्प्युटरजन्य प्रविधिका विभिन्न नेटवर्कमार्फत साइबर आक्रमण हुने क्रम बढ्दो छ ।

नेपालमा साइबर अपराधका स्वरुपहरु

सन् १९८९ मा बेलायतका वैज्ञानिक टीम बर्नर्स ली (Tim Berners-Lee) ले वर्ल्ड वाइड वेब (World Wide Web) का तीन डब्लुको विकास गरे । त्यसपछिका यिनै तीन डब्लुको वरिपरि ३६ वर्ष लाग्दासम्म संसारका मानवजातिलाई नचाइरहेको छ । अहिले यस्तो क्षेत्र पाउन मुस्किल छ जसलाई इन्टरनेट प्रविधिले प्रभाव पारेको नहोस । अहिले कम्प्युटर तथा कम्प्युटरजन्य प्रविधिमार्फत व्यक्ति आफूले चाहेअनुरुप खबर आदानप्रदान गर्न सक्दछ । यसरी विश्वभरका मानिसले कतिपय सन्देश व्यक्ति व्यक्तिका बीच आदानप्रदान गर्दछन त कतिपय संस्थागत रुपमा । यसरी अहिले हरेक व्यक्ति तथा संस्थाले आआफ्ना महत्वपूर्ण विषयहरु कापी तथा डायरीमाभन्दा पनि कम्प्युटर, ल्यापटप, मोबाइल, इमेल तथा विभिन्न एप्लिकेशनमा राख्ने गर्दछन⁄गरिन्छ जस्तै : विभिन्न व्यक्ति तथा संस्थाले पठाएका मेलहरु, सामाजिक सञ्जाल फेसबुकमा आफूलाई मन परेका विभिन्न विषयवस्तुहरुका तस्बिर, लेख, फिचरलगायतका सामग्रीहरु ई. (लक गरेर तथा कतिपय सार्वजनिक रुपमा) राखिएका हुन्छन ।

विश्वभरमै साइबर अपराध र सुरक्षामा संवेदनशीलता बनेको सन्दर्भमा नेपालमा पनि यसको समस्या उक्तिकै बनेको छ । पछिल्ला समयमा द्रुत गतिमा डिजिटाइजेसन अगाडि बढेसँगै इन्टरनेटको पहुँचमा विभिन्न प्रकारका गेमहरु खेल्ने र अनेकन प्रकारका घटनाहरु सामाजिक सञ्जालमार्फत आउने गरेका छन । यसरी डिजिटल रुपमा गैरकानुनी गतिविधिमार्फत व्यक्ति वा संस्थालाई तनाव सिर्जना गर्नु नै डिजिटल अपराध हो । डिजिटल रुपमा आउने सबै प्रकार विक्रिति तथा विसंगतिलाई नै साइबर अपराध भनी बुझ्नु पर्दछ ।

हामीले विभिन्न सञ्चारमाध्यम मार्फत सुन्दै आइरहेका छौ दूरसञ्चार र इन्टरनेट सेवा प्रदायक, एयरलाइन्स, गैरसरकारी संस्था, आइएसपी, वित्तीय संस्थालगायतका विभिन्न कम्पनीका शिष्टममा साइबर आक्रमण भएका विषयहरु . त्यतिमात्र नभएर विदेशी नागरिक ह्याकरहरुले नक्कली एटीएम कार्ड बनाएर पैसा निकालेका विषयहरु अझैं डरलाग्दा किसिमका छन । “इन्टरनेशनल टेली कम्युनिकेसन युनियन (आईटीयु) को ग्लोबल साइबर सेक्युरिटी इन्डेक्समा नेपाल ९४ औं स्थानमा छ, दक्षिण एसियामा भुटनापछि सबैभन्दा कमजोर (नयाँ पत्रिका, २०७९ माघ १७)” भनी शैलेन्द्र गिरीले कान्तिपुर अनलाइनबाट फाल्गुन ७, वि.सं. २०७९ मा “साइबर सुरक्षा र बढ्दो चुनौती” शीर्षकको लेखमा बताएका छन ।

त्यसैगरी नेपालमा कम्प्युटर तथा कम्प्युटर नेटवर्कमार्फत आपराधिक गतिविधिहरु तथा नकारात्मक विषयहरु फैलाउने क्षेत्रको रुपमा सामाजिक सञ्जाललाई प्रयोग गरेको पाइन्छ । कतिपयको फेसबुक ह्याक भएका, मोबाइलमा अनेकन किसिमका विजयी तथा लक्की ड्र⁄चिठ्ठा परेका र त्यसका लागि केही रकम दिनुपर्ने र पछि ठूलो धनराशि आउने भनी विभिन्न आस देखाएर कल गर्ने⁄आउने, वैदेशिक रोजगारीको आश्वासन दिने, ब्ल्याकमेल गर्ने जस्ता आपराधिक गतिविधिले मानिसको मनोवैज्ञानिक पक्षमा ठूलो सन्ताप उत्पन्न गरेको छ ।

अर्को कुरा:“साइबर समस्याको मूल जड भने अधिकांश इन्टरनेट तथा कम्प्युटर प्रयोकर्तामा साइबर थ्रेटबारे आधारभूत जानकारी नहुनु नै हो जसले साइबर सुरक्षाको चुनौती बढ्दै गएका छ” (उप्रेती, तोमनाथ, वि.सं. २०८० माघ १८, बिहीबार १६:३२) भनी इकर्मचारी डट कम को एक लेखमा बताएका छन । यो नै सबैभन्दा विडम्बनाको विषय हो । कसैले आफूलाई कुनै थ्रेटदिँदा पनि मलाई चिन्ने आफन्त तथा साथीभाइले के भन्लान भन्ने डरका कारण त्यसै चुपचाप बस्नुले पनि यस्ता गतिविधिहरु मौलाउँदै गएका छन । त्यसैले त अहिले नेपालमा पनि साइबर अपराध र यसको सुरक्षामा चुनौती उत्पन्न भएको छ । हुनत यसको समस्या नेपालमा मात्र नभएर विश्वभर नै संवेदनशीलताको विषय बनेको छ । यसोभन्दै गर्दा हामीले सबैतिर यस्तै रहेछ भनी त्यसै बस्ने होइन । यसको सुर क्षामा हामी पनि जागरुक हुनुपर्छ . कतिखेर यसबाट हामीलाई थ्रेट आउने हो पत्तो नै हुन्न । विशेषत नेपालमा विभिन्न स्वरुपमा साइबर अपराधहरु हुने गरेको छ जसलाई निम्नानुसार प्रस्तुत गरिएका छन :

- भर्दै नभरेको चिट्ठा पऱ्यो भनी रकम ठगी गर्ने,
- पार्सल तथा उपहार पठाइदिन्छु भनी ठगी गर्ने,
- अनलाइन सपिङको आवरणमा पूर्व भुक्तानी लिई सामान डेलिभरी नगर्ने,
- गोप्य तस्बिर तथा भिडियोहरु सार्वजनिक गरिदिने भनी आर्थिक लाभ लिने तथा प्रेममा धोका पाएपछि वा प्रेम प्रस्ताव अश्वीकार भएका कारण बदलाको भावनाले नग्न फोटो तथा भिडियामा अनुहार देखाई सामाजिक सञ्जालमा पोष्ट गर्ने,
- कुनै लोभ, ईर्ष्या, डाहा तथा रिसमा अर्काको मानहानी तथा चरित्र हत्या गर्ने,
- वेबसाइट तथा इमेल ह्याकिङ,

- फेसबुक तथा अन्य सामाजिक सञ्जालबाट ब्ल्याकमेलिङ गर्ने,
- डाटा तथा पासवर्ड चोरी गर्ने,
- इन्टरनेट बैंकिङ जालसाजी गर्ने,
- अर्काको नाम, तस्बिर, भिडियो तथा रेकर्ड गरिएका श्रव्यदृश्य सामग्रीलाई अनधिकृत रुपमा प्रयोग गर्ने,
- क्रेडिट कार्ड तथा एकाउन्टको चोरी गर्ने,
- इन्टरनेटमार्फत माहिला यौनहिंसा, बाल यौन तथा चरित्र हत्या गर्ने,
- फेक आइडी बनाएर विभिन्न सामाजिक सञ्जालमार्फत गाली बेइज्जती गर्ने,
- अश्लील फोटो तथा भिडियो बनाएर पठाउने,
- विभिन्न किसिमबाट तनाव सिर्जना गराउने,
- गलत कागजात तयार गर्ने,
- इन्टरनेटको प्रयोग गरेर जुवा खेल्नु वा खेलाउनु (अनलाइन ग्याम्बलिङ),
- गैरकानुनी अवरोध,
- तथ्याङ्कमाथि हस्तक्षेप,
- उपकरणको दुरुपयोग,
- कम्प्युटर प्रणालीमा हस्तक्षेप,
- कम्प्युटर माध्यमबाट गरिने जालसाजी, दुराचार, किर्ते ई. ।

बैकिङ घोटलाका विषयहरु जस्ता अनेकन प्रकारका साइबरको माध्यममार्फत अपराधहरु दिनप्रतिदिन बढ्दै गइरहेका छन । यस्ता अपराधहरुको अनुसन्धान गरी दोषीलाई कानुनी कठघरामा उभ्याउन तथा नागरिकमा इन्टरनेट सदुपयोग गरी सुरक्षित रहन नेपाल प्रहरी चौबिसैंघण्टा खटिरहेका छन ।

साइबर बुलिङ

न्युमिडियाले आजको समयमा हाम्रो जीवनलाई सहज बनाउनुका साथै धेरैजना व्यक्तिको जीवनमा बाधा समेत पुऱ्याएको छ । अंग्रेजीमा रहेको 'Cybelbullying' साइबर बुलिङलाई नेपालीमा अर्थ्याउँदा : आफूभन्दा साना तथा कमजोरलाई इलेक्ट्रोनिक माध्यमको प्रयोगबाट कुनै डर, धम्की तथा उत्पीडनमा पार्नु, हेच्याउनु, अरुलाई गिज्याउनु, गलत ढङ्गबाट विश्लेषण गरेर हल्ला फिजाउने वा हेपाइ प्रवृत्ति हो ।

खासमा साइबर बुलिङलाई अनलाइन बुलिङ पनि भन्ने गरिन्छ । SMS, Text, Apps, Social Media, Forum, Gaming, Moboile Phone Call आदिमा मानिसहरुले हेर्न, भाग लिन तथा सामग्री साझेदारी गर्न कुनै पनि इलेक्ट्रोनिक्स माध्यममार्फत हुनसक्छ । यस्ता माध्यमबाट कसैमाथि अमर्यादित ढङ्गबाट गाली गर्नु, अश्लील भाषाको प्रयोग, अश्लील फोटो, भिडियो तथा नकारात्मक शब्दावलीमा रेकर्ड गरिएका सामग्रीहरु, अवैध र आपराधिक क्रियाकलाप, धम्की तथा डर देखाउने, चिढ्याउने तथा लज्जित तुल्याउने सबै कार्यहरु साइबर बुलिङ हुन ।

विशेषत साइबर बुलिङको मुख्य उद्देश्य व्यक्तिको असत्य विषय तथा नभएका विषयलाई गलत ढङ्गबाट फैलाउनु, छद्म रुपमा स्वार्थी चरित्रका व्यक्तिहरुले सोझा, सादा तथा कमजोर मानिसलाई उनीहरुले नचाहेका कार्य गर्न इलेक्ट्रोनिक प्रविधिको प्रयोगमा सामाजिक सञ्जालबाट धम्की तथा डर देखाएर जबरजस्ती रुपमा त्यस कार्य गर्न बाध्य पार्ने, कसैलाई समूहबाट एक्ल्याउने, हाँसोको पात्र बनाउँने, अनावश्यक विषय ल्याएर कुरा काट्ने जस्ता गलत क्रियाकलापहरु हुने गरेको अनुसन्धानको क्रममा पाइयो ।

साइबर बुलिङको मुख्य प्रवृत्ति : फोनमा कल गरेर यसो हो उसो हो भनेर डर देखाउँने, अश्लील फोटो तथा भिडियो अपलोड गर्ने, कुनै कमेन्ट तथा गलत म्यासेज पठाउँने वा पोष्ट गर्ने गरेको पाइयो । साइबर बुलिङबारे विशेषत स्कूल तथा विद्यालयका साना साना केटाकेटी तथा युवायुवतीहरु सबैभन्दा बढी समस्यामा परेको देखियो । यस्तो समस्या अहिले दिनानुदिन विश्वभर बढ्दो क्रममा रहेको पाइन्छ ।

साइबर बुलिङ त्यतिखेर हुन्छ जब डिजिटल मिडियामार्फत कसैले अर्को व्यक्तिलाई डर तथा धम्की दिइन्छ । यसले बालबालिकादेखि युवापिडिमासमेत उनीहरुको मनोवैज्ञानिक, सामाजिक तथा शैक्षिक पक्षमा नराम्रो प्रभाव पार्दछ । साइबर बुलिङ भयानक तथा डरलाग्दो अनलाइन घटना हो यसले किशोर किशोरी तथा साना बालबच्चाहरुलाई जानाजानी लक्षित गरी डर, धम्की तथा मानसिक यातना दिने गरेको पाइयो । साइबर बुलिङ मुख्यतया निम्न कारणहरुबाट भएको देखिन्छ :

- विशेषत प्रतिशोध तथा बदलाको भावना,
- घरायसी, सामाजिक तथा राजनीतिक समस्या,
- आफ्नो प्रभुत्व स्थापित गर्न,
- डाह, घृणा तथा ईर्ष्याका कारण,
- अरुलाई दुःख दिएर मज्जा लिने प्रवृत्ति,
- आक्रमक व्यक्तित्व वा स्वभाव ई. ।

नेपालमा पनि पछिल्लो समयमा साइबर बुलिङका घटनाहरु बढ्दै गएका छन । यसबाट बच्ने सबैभन्दा राम्रो उपाय भनेको यसलाई पूर्ण रुपले बेवास्ता गर्नु तथा आफूले नचिनेकालाई साथी नबाउनु हो . त्यसका साथै आफूले सामाजिक सञ्जालमा कद्रनै फोटो, भिडियो वा कुनै स्टाटस पोस्ट गर्दा सबैले सहजै देख्न नसक्नेगरी प्राइभेसी सेटिङ मिलाउनु पनि यसबाट टाढा रहनु हो। यसको अलवा अपरिचित व्यक्तिसँग नजोडिने, फलोइङ सिस्टमा नरहने तथा अनफ्रेण्ड तथा अनफलो गर्दा साइबर बुलिङबाट बच्न सकिन्छ ।

त्यसैगरी कसैले गलत नियवश अनलाइनमा दूर्व्यवहार गर्ने प्रयास गरेमा त्यसलाई ब्लक गर्नु बढी बुद्धिमानी हुन्छ किनकि पछि आफूले अरुलाई यसो भो उसो भो भनेर पछुताउनु पर्दैन । यदि तपाईंले विशेषत फेसबुकमा अश्लील भिडियो, तस्बिर तथा कुनै टिप्पणी देख्नुभयो भने फेसबुकमा रिपोर्ट गर्नुहोस् र त्यसका साथै तपाईंले ती भिडियो, फोटो तथा टेक्स्टलाई प्रमाणको रुपमा कानुनी कारवाही

गर्न नजिकको प्रहरी चौकी (साइबर ब्यूरो) मा जानकारी दिनुहोस् ताकी त्यस्तालाई कारवाहीको दायरमा ल्याउन सकियोस् । नेपालमा साइबर बुलिङमा संलग्न भएकाको खोजी कार्य गरी उचित दण्ड, सजाँय तथा जरिवाना लगाउने कार्यमा नेपाल प्रहरीले तदारुकताका साथ लागिरहेको छ । यदी कसैले साइबर बुलिङ Bulling भनेर त्यसको खोजी गर्नुछ भने पहिला साइबर ब्यूरोमा एफआइआर दर्ता गरेपश्चात् प्रहरीद्धारा त्यस्ताको खोजी कार्य गरी कारवाही हुन्छ ।

घृणापूर्ण अभिव्यक्ति

विशेषत निर्वाचन नजिक आउदैगर्दा तथा कुनै आन्दोलनको बेलामा दलहरुका बीचमा आरोप प्रत्यारोपका विषय र कुनै दल तथा पार्टी टुक्रदा एक दलका नेताले अर्काको विरुद्ध पहिले गरेका कमीकमजोरी/कर्तुतलाई उजागर गर्दै पढ्न र सुन्नसमेत नसकिने गरी तीन पुस्तालाई पुग्नेगरी विषवमन गर्ने गरेका विषयहरु सञ्चारमाध्यममार्फत प्रकाशन तथा प्रसारण हुने गरेको अध्यनमा पाइयो । यस्ता विषयहरु नेपाली राजनीतिमा देखिरहेकै विषय हुन । तर यसरी कसैमाथि घृणा भावले बोल्दा आफ्नो मान, मर्यादामा आँच आउनुका साथै जनतामा गलत सन्देश जाने हुन्छ । आफ्नो मान, सम्मान तथा प्रतिष्ठामाथि बेवास्ता गर्दै आवेशमा आएर कसैमाथि नराम्ररी खनिनु बुद्धिमानी कहलिदैन । त्यसले फाइदाभन्दा पनि बेफाइदा गर्दछ । यस विषयमा हामी सबैले हेक्का राख्नुपर्दछ ।

त्यसैगरी नेपालमा बेलाबेलामा अभियान्ताहरुले मिडियामा स्पेस पाइन्छ की भनेर सरकारमा बसेका दलका नेता, मन्त्री, प्रधानमन्त्री तथा राष्ट्रपतिलाईसमेत विभिन्न भएनभएका विषयको लाञ्छना लगाई घृणापूर्ण अभिव्यक्तिहरु श्रव्दृश्यमा सामाजिक सञ्जालमा छ्यापछुयाप्ती पाइन्छन । अझ कतिपयले डिजिटल मिडियाका विभिन्न मञ्चबाट आफ्ना परिवार, साथीभाइ, इष्टमित्रसँग बसेर सुन्न नसकिने शब्दहरुको प्रयोग गर्दै आरोप प्रत्यारोप गर्ने गरेको अध्ययनमा पाइयो । त्यतिमात्र नभइ कतिपय घृणा पैदा गराउने कार्टुनका दृश्यहरुसमेत न्युमिडियाका विभिन्न मञ्चमार्फत सम्प्रेषण गर्ने गरेको विषय इन्टरनेटका प्रयोगकर्ताले बताए ।

विशेषत नेपालमा डिजिटल मिडियाबाट नेता तथा अभियान्ताले एकअर्कालाई सिध्याउँने गरी भ्रष्टाचारी, राष्ट्रद्रोही, धर्म विरोधी, हत्यारा, गुण्डाका नाइके, सुन तस्करी, मानव तस्करी, शहकारी ठग, अमेरिकि तथा "र" को एजेन्ट जस्ता दर्जनौ उपमा दिएर भएनभएका आरोप लगाई गाली गर्ने तथा गलत सन्देशहरु सम्प्रेषण गर्ने गरेको पाइयो । त्यसैगरी एकओटा उदाहरण लिउ : दुर्गा प्रसाईको महाअभियान "सडक प्रदर्शन वि.सं २०८० मंसिर ०७ गतेबाट फाल्गुन १ गतेसम्म" भनी प्रचारप्रसार गर्दै संघीयता खारेज, धर्म निरपेक्षताको साटो वैदिक सनातन राज्य बनाउनुपर्ने, देशमा नागरिक तथा व्यावसायिकलाई गरिखाने वातावरण दिनु पर्ने भनी विभिन्न दलका नेता तथा ठुला व्यावसायि र लघु वित्तका सञ्चालकलाई आरोप प्रत्यारोप गरेका विषयले जनतामा नेता तथा व्यावसायिप्रति घृणा पैदा गरेको देखिन्छ ।

नेपालमा साइबर अपराध बढ्नुको कारण

कम्प्युटर तथा कम्प्युटर नेटवर्कमार्फत ट्वीटर, इन्स्टाग्राम, वीच्याट, फेसबुक, इमो, भाइबर, स्काइप, बोटीम, फेसबुक म्यासेन्जर, युट्युब, टिकटक जस्ता सामाजिक सञ्जालमा व्यक्तिको इच्छा विपरीतका कार्य गर्नुलाई साइबर अपराध भनी बुझ्नु पर्दछ । सबै कुराको फाइदा मात्र हुन्न त्यसले बेफाइदा पनि गर्दछ । बिरामीको लागि औषधि फाइदाको विषय हो तर रोग के हो ? त्यसको लागि कुन औषधि खाने भन्ने विषय महत्वपूर्ण हुन्छ । टाउको दुखेको बेलामा पेट दुखेको औषधि खायौ भने त्यसले असर गर्दछ । त्यसैगरी हरेका चिजको फाइदा र बेफाइदा हुन्छ भने झैं मानिसले निर्माण गरेको इन्टरनेट प्रविधि र अनेकन डिजिटल एप्लिकेशनका पनि उत्तिकै राम्रा र नराम्रा पक्षहरु रहेका छन । आज विश्वभर इन्टरनेट प्रविधिमार्फत अनेकन अपराधहरु हुन थालेको छ । यो विश्वभरका मानिसको चिन्ताको विषय बनेको छ ।

सूचना प्रविधिको विकासमा न्युमिडियाले व्यक्तिका दैनिक कामलगायत शिक्षा, स्वास्थ्य, मनोरञ्जन, सार्वजनिक सेवा प्रवाह तथा सञ्चार आदानप्रदानमा ठूलो टेवा पुऱ्याएको छ । तर इन्टरनेटमार्फत राखिएका तथा पठाइएका सूचनाहरु कतिखेर कहाँ कस्ले के गर्ने हो भन्ने त्रास पनि उत्तिकै रुपमा रहन थालेको छ । विश्वभर विद्युतीय माध्यमबाट हमाला बढेसँगै नेपालमा पनि यसको त्रास उत्तिकै रुपमा रहेको छ । अहिले नेपालमा पनि इन्टरनेटको प्रयोग पहिलेको तुलनामा अध्याधिक मात्रामा बढेको पाइयो । यसले एकातर्फ मानिसलाई जोडेको छ भने अर्कोतिर टाढा पनि बनाएको छ । सोफामा सँगै बसेका पति र पत्निबीच राम्रोसँग कुराकनी हुन छाडेको छ । एक कोठामा रहेको छोराछोरीलाई भान्छाबाट आमाले खानापाक्यो खानाखान आउनु भनेर म्यासेज पठाउने विषय अब सामान्य भइसक्यो ।

साइबर अपराध हुनबाट बच्नका लागि इन्टरनेटको प्रयोगकर्ताले विशेषत सूचना प्रविधिको प्रयोग के कसरी गर्ने, के राख्न हुने, के राख्न नहुने, कस्ले के भनेको हो, त्यो व्यक्ति परिचित हो वा होइन, आफूसँग कुराकानी गरिरहेको व्यक्तिलाई आफ्ना निजी विषयबारे के कति भन्ने नभन्ने जस्ता विविध विषयबारे सचेत हुनुपर्दछ । इन्टरनेटबाट त हो नी, कस्ले देखेको तथा सुनेको छ र भनी अफ्ना महत्वपूर्ण निजी जीवनका विषयहरु प्रदान गऱ्यौ भने त्यसले आउँदा समयमा तिनै विषयहरु साइबर अपराधीहरुका लागि ठुला प्रमाणहरु बन्नेछन । यि र यस्ता कयौं कमिकमजोरीका कारणले आपराधिक गतिविधिमा लाग्ने व्यक्तिहरुलाई सजिलो हुनेहुँदा कयौं साइबर अपराधका घटनाहरु घट्ने गरेको पाइयो ।

अहिले नेपालमा साइबर स्पेस निकै जोखिममा रहेको छ जसले गर्दा नेपालको राष्ट्रिय सूचना तथा व्यक्तिगत गोपनीयताको संरक्षणमाथि नै जटिलता उत्पन्न भएको छ । नेपालमा साइबर अपराध बढ्नुका मुख्य कारणहरुमा :

- ☞ साइबर अपराध सम्बन्धी कुनै नीति, नियम तथा नियमन गर्ने ऐन तथा दह्रो कानून नबन्नु,
- ☞ आइटी सम्बन्धी विज्ञता हासिल गरेका व्यक्तिको अभाव/न्यून,

- आमनागरिकमा साइबर सुरक्षाबारे पर्याप्त ज्ञानको कमीले व्यक्तिगत तथ्याङ्कहरुलाई सुरक्षा गर्न जटिलता,
- अधिकांश इन्टरनेटको प्रयोगकर्तामा मिडिया साक्षरता र साइबर थ्रेटबारे ज्ञानको कमी,
- राज्यको विद्युतीय सुरक्षा नीति र व्यवस्थापनमा कमजोरी,
- साइबर अपराध विरुद्धको अभियानमा राज्यको लगानी न्यून रहनु,
- साइबर सुरक्षा सम्बन्धी अमनागरिकलाई जागरुक गराउन राज्यको तर्फबाट साझा अभियानको रुपमा अघि नबढाउँनु,
- डिजिटल साक्षरताको विकासमा राज्यले जोड नदिनु,
- नेपालमा सञ्चालित अधिकांश सामाजिक सञ्जालको नियन्त्रण संयन्त्र नेपालमा नहुनु ई. ।

अन्य विविध कारणले गर्दा देश तथा बिदेशबाटसमेत नेपालको साइबर स्पेसमा मोबाइल, कम्प्युटर तथा विभिन्न नेटवर्कमा आपराधिक गतिविधिहरु बढेको पाइन्छ ।

साइबर अपराधी तथा ठगी हो भनेर कसरी थाहा पाउँने ?

- यदि तपाइँलाई अपरिचित व्यक्तिले उपहार पठाएको छ भन्दै कुनै म्यासेज र मोबाइलमा कल तथा सामाजिक सञ्जालमार्फ जानकारी गराएमा शंका गर्ने,
- बजार मूल्यभन्दा न्यून मूल्यमा कुनै पनि सामानको प्रस्ताव गरेमा,
- उसले प्रयोग गरेको आधिकारिक वेबसाइट हो/होइन अर्थात युआरएल (URL) राम्रोसँग जाँचबुझ गर्नुपर्दछ,
- जहिले पनि https// बाट शुरु भएका लिङ्क मात्र खोल्नुपर्दछ,
- प्रयाः ठगीका वेबसाइटहरु अस्पष्ट जानकारी, गैरव्यावसायिक र व्याकरणमा त्रुटि भेटिन्छन ।

किन र कसरी फैलन्छ साइबर ठगी ?

- विशेषत कुनै उपहार जस्ता प्रलोभन र सीमित समयको अफर छ भनेर सोझा र विशेषत कमजोर महिला तथा व्यक्तिलाई ततकालै निर्णय गर्न बाध्य पारेर,
- प्राय : नेपाली इन्टरनेट प्रयोगकर्ताहरु प्रविधिको सुरक्षित प्रयोग कसरी गर्ने भन्ने विषयमा अनभिज्ञ भएका कारण उनीहरुले जटिल र अप्ठ्यारा पासवर्ड राख्न नसक्नु, राम्रो फोटो तथा भिडियो देख्ने बित्तिकै अपरिचित लिङ्कलाई पनि क्लिक गरिहाल्ने र असुर क्षित नेटवर्क प्रयोगबाट,
- नक्कली वेबसाइट, मोबाइल एप्स तथा कुनै पनि सामाजिक सञ्जालमार्फत फर्जी अकाएन्टको प्रयोग गरेर व्यक्तिको विश्वास जित्न अभ्यास गर्दछन र
- सस्तो मूल्यमा ब्राण्डेड सामान, उच्च लाभ दिने लगानीको योजना र केही दिनमै रकम दोब्बर हुने/गरिदिने आश्वासनहरु दिएर ई. ।

साइबर अपराधबाट कसरी बच्ने वा जोगिने ?

इन्टरनेटको प्रयोग गर्दा हामीले आफ्नो पासवर्ड हालीसकेपछि हामी सबै त्यसको निगरानीमा रहन्छौ । कतै न कतै त्यसको सञ्चालन अरु कसैले गरिरहेको हुन्छ । त्यसैले म जतिखेर पनि अप्ठ्यारोमा पर्न तथा असुरक्षित हुनसक्छु, म ठगिन सक्छु, म विरुद्ध ठूलो अपराध लाग्नसक्छ भन्ने विषयप्रति सजग हुनुपर्दछ । तसर्थ साइबर अपराधबाट बच्न निम्न विषयहरुमा ध्यानदिन सकेको खण्डमा यसबाट जोगिन सक्छौ :

- सकेसम्म आफूले प्रयोग गर्ने सामाजिक सञ्जालमा व्यक्तिगत जानकारी सार्वजनिक नगर्ने अथवा व्यक्तिगत सूचनालाई गोप्य राख्ने,
- आफ्नो महत्वपूर्ण सामग्रीलाई सामाजिक सञ्जालमा अपलोड नगर्ने,
- प्राइभेसी र सेक्युरिटी सेटिङ मिलाउने । कुनलाई पब्लिक गर्ने र कुनलाई नगर्ने भन्ने विषयमा ध्यानदिने,
- सामाजिक सञ्जालमा आफूले चिनेक र परिचित व्यक्तिलाई मात्र जोड्ने,
- स्टाटस तथा कुनै कमेन्ट गर्दा निक्कै सोचविचार गरेर त्यसले पछि अप्ठ्यारो नपार्नेगरी कमेन्ट तथा म्यासेज गर्ने,
- यदि तपाइँलाई कसैले लोभ लालचा देखाएर अश्लील कार्य गर्न आदेश गर्दैछ अथवा डर र धम्की दिँदै छ भने त्यस्ता व्यक्तिको आइडिलाई लिस्टबाट हटाउने, ब्लक गर्ने तथा तुरुन्तै प्रहरीलाई जानकारी गराउँने,
- कतिपय शङ्कास्पद सन्देश तपाइँको कुनै पनि सामाजिक सञ्जालमा आएमा त्यस्तालाई नहेर्ने (नखोल्ने) तथा बेवास्ता गर्ने,
- आफ्नो इमेल, कुनै लिङ्क अथवा एप खोल्नु अगाडि सावधानी भएर खोल्ने,
- कप्युटर तथा ल्यापटपमा एन्टिभाइरस, इन्टरनेट सेक्युरिटी राखेर समय समयमा स्क्यान गर्दै गर्ने,
- सकेसम्म आफूले प्रयोग गर्ने पासवर्ड बलियो, अप्ठ्यारो अथवा जटिल पासवर्डको प्रयोग गर्ने,
- कुनै भुक्तानी अनलाइनमार्फत गर्दा आधिकारिक र सुरक्षित प्लेटफर्मको प्रयोग गर्ने,
- सेवा प्रदायक वा व्यवसायको प्रामाणिकता प्रमाणित गर्ने र
- कुनै पनि बैंक तथा संस्थाले तपाइँलाई कहिल्यै ओपीटी (OPT) वा पासवर्ड सोध्दैन त्यसबारे ख्याल गर्ने र
- विद्यालय तहबाट पाठ्यक्रममा डिजिटल साक्षरताको व्यवस्था गर्ने (यो राज्यको काम हो) ई. ।

त्यसका साथै साइबर अपराधको सुरक्षामा नेपाल प्रहरीले पनि समुदाय प्रहरी साझेदारी कार्यक्रममार्फत साइबर अपराधका विरुद्धमा विभिन्न जनचेतनाका कार्यक्रमहरु विभिन्न निकायहरुसँग सहकार्य गरेर विद्यालयहरुमा, समुदायहरुमा प्रवाह गरिरहेको छ । त्यसैगरी सामाजिक सञ्जालहरु, फेसबुक, इन्स्टाग्राम तथा नेपाल प्रहरीको वेबसाइदेखि विभिन्न विज्ञेप्तिहरु जारी गरेर यसको सम्बन्धका छुट्टै विशिष्टिकृत व्यूरोको रुपमा नेपाल प्रहरीसँग साइबर व्यूरो पनि रहेको छ ।

तसर्थ इन्टरनेटको प्रयोगकर्ताले सदैव म असुरक्षित हुन्छु, ठगिन्छु, लुटिन्छु की भन्ने विषयलाई आत्मसाथ गर्दै अगाडि जानुपर्दछ । त्यसका साथै आफ्ना बालबालिकाहरुलाई पनि यसबारेमा जानकारी गराउँनु पर्दछ । आफू पनि सुरक्षित हौ र यस्ता घटनाहरु यदि कतै जानकारीमा छन भने नजिकको प्रहरी कार्यालय तथा १०० नम्बरमा सम्पर्क गरेर सूचना दिन सकिन्छ ।

नेपालमा साइबर अपराध सम्बन्धी कानुनी व्यवस्था

सूचना प्रविधिको विकासले नागरिकको दैनिकीलाई सरल तथा सहज त बनाएको छ। तर यसको प्रयोगमा सावधानी नअपनाउँदा विभिन्न किसिमका साइबरजन्य घटनाहरुको शिकार हुनेको संख्या पनि उत्तिकै रुपमा बढ्दो छ।

नेपालमा विद्युतीय कारोबार ऐन, २०६३ को परिच्छेद–९ को दफा ४४ देखि दफा ५५ सम्मका अधिनमा रही साइबरसम्बन्धी अपराध उपरको अनुसन्धान तथा अभियोजन हुँदै आएको पाइन्छ (बशिरा , वि.सं. २०७९ असार ५, १०:५७) भनी अन्नपूर्णपोष्ट डट कममा "चुनौती बन्दै साइबर अपराध" शीर्षकको लेखमा बताएका छन।

साइबर अपराधका गतिविधिहरुको अध्ययन तथा अनुसन्धान गरी त्यसको कारवाही गर्न विद्युतीय (इलेक्ट्रोनिक) कारोबार ऐन, २०६३ देखि लागू गरिदै आएको छ।

विद्युतीय कारेबार ऐनको परिच्छेद –९ को

दफा ४४ मा : कम्प्युटर स्रोत सङ्केतको चोरी, नष्ट वा परिवर्तन गर्ने,
दफा ४५ मा : कम्प्युटर सामग्रीमा अनधिकृत पहुँच,
दफा ४६ मा : कम्प्युटर र सूचना प्रणालीमा क्षति पुऱ्याउने र
दफा ४७ मा : विद्युतीय स्वरुपमा गैरकानुनी कुरा प्रकाशन गर्ने (विद्युतीय (इलेक्ट्रोनिक) कारोबार ऐन, २०६३: १८–१९) भनी तो किएबमोजिम कारवाही गर्दै आएको छ। यो नै नेपालको पहिलो साइबर कानून हो।

नेपालमा साइबर अपराधको नियमनको लागि विद्युतीय कारेबार ऐनको दफा ४७ विद्युतीय स्वरुपमा गैरकानुनी कुरा प्रकाशन गर्ने : (१) कम्प्युटर, इन्टरनेट लगायतका विद्युतीय सञ्चारमाध्यमहरुमा प्रचलित कानूनले प्रकाशन तथा प्रर्दशन गर्न नहुने भनी रोक लगायतका सामग्रीहरु वा सार्वजनिक नैतिकता, शिष्टाचार विरुद्धका सामग्री वा कसैप्रति घृणा द्धैष फैलाउने वा विभिन्न जातजाति र सम्प्रादायबीचको सुमधुर सम्बन्धलाई खलल पार्ने किसिमका सामग्रीहरु प्रकाशन तथा प्रदर्शन गर्ने, महिलालाई जिस्क्याउने, हैरानी गर्ने, अपमान गर्ने वा यस्तै अन्य कुनै किसिमको अमर्यादित कार्य गर्ने वा गर्न लगाउने व्यक्तिलाई एक लाख रुपैयाँसम्म जरिवाना वा पाँच वर्षसम्म कैद वा दुवै सजाय हुनेछ।

(२) कुनै व्यक्तिले उपदफा (१) बमोजिमको कसूर पटक पटक गरेमा त्यस्तो कसूर बापत अघिल्लो पटक भएको सजायको डेढी सजाय हुनेछ ((विद्युतीय (इलेक्ट्रोनिक) कारोबार ऐन, २०६३:१९) भनी व्यवस्था गरेको छ।

यसभन्दा अगाडि केही सार्वजनिक (अपराध र सजाय) ऐन, २०२७ मा जम्मा चार पेजमा उल्लेख गरिएका सजायअनुसार कार वाही गरिन्थ्यो।

त्यसैगरी नेपालमा फौजदारी अपराध संहिता, २०७४ को भाग –३ को वैयक्तिक गोपनीयता तथा प्रतिष्ठा विरुद्धको कसूर अन्तर्गत परिच्छेद–२ को गाली बेइज्जती सम्बन्धी कसूर दफा ३०५ मा गाली गर्न नहुने, दफा ३०६ बेइज्जती गर्न नहुने र दफा १०७ मा बे इज्जती गरेमा हुने सजाय (फौजदारी अपराध संहिता, २०७४: १३४–१३६) को व्यवस्था उल्लेख गरेको छ।

त्यसैगरी वि.सं. २०८० मा नेपाल सरकारले “राष्ट्रिय सरकार सुरक्षा नीत २०८०” जारी गरेको छ। यस नीतिमा दफा ६ को : दीर्घकालीन सोचमा : सुरक्षित एवम् उत्थानशील साइबर स्पेश (Resilient Cyber Space) को निर्माण गर्ने (राष्ट्रिय सरकार सुरक्षा नीत २०८०:४) भनी उल्लेख गरेको छ।

अहिले नेपालको ७ प्रदेश र ७७ जिल्लामा रहेको जिल्ला अदालतमध्ये काठमाडौँको बबर महल स्थित काडमाडौँ जिल्ला अदालतबाट मात्र साइबर अपराधको मुद्दा हेर्दै आइरहेको छ भने साइबर अपराधको अनुसन्धान तथा नियन्त्रणलाई प्रभावकारी बनाउँन नेपाल प्रहरीले विशिष्टीकृत एकाइको रुपमा वि.सं. २०७५ जेठ २७ गते साइबर व्यूरोको स्थापना गरेर साइबर अपराधहरुको अनुसन्धान गरी दोषीलाई कानुनी कठघरामा उभ्याउन तथा नागरिकमा इन्टरनेट सदुपयोग गरी सुरक्षित रहन नेपाल प्रहरी चौबिसैघण्टा खटिरहेका छन। हाल यस व्यूरोले काठमाडौँको भोटाहिटीमा रहेको कार्यालयबाट साइबर अपराध सम्बन्धीका घटनाहरुको प्रभावकारी अनुसन्धान गर्दै आइरहेको छ।

नेपालमा साइबर सुरक्षमा संवेदनशीलता

- प्राइभेसी कानून र तथ्याङ्क संरक्षण कानून (डाटा प्रोटेक्सन ल) समेट्न सकेको छैन,
- आइसिटी प्रयोगकर्ताले आत्मसुरक्षाको उपाय अपनाउन नसक्नु,
- डिजिटल अपराध विरुद्धको सुरक्षाका लागि उचित शिक्षा तथा ज्ञानको कमी,
- नेपालमा अधिकांश इन्टरनेटको प्रयोगकर्तामा साइबर थ्रेटबारे ज्ञानको कमी,
- विभिन्न प्रकारका सामाजिक सञ्जाल (ह्वाट्सएप, स्न्यापच्याट, भाइबर, फेसबुक, ट्वीटर, इन्स्टाग्राम ई.) मार्फत नाम परिवर्तन गरेर, फोटो एडिट गरेर तथा छद्‌म भेषमा साइबर अपराध हुने गरेको पाइयो।

एनआईसी बैंक ह्याक प्रकरणमा उत्तर कोरियाको ह्याकरले स्वीफ्ट प्रणालीबाट ह्याक गरेर अन्य देशका आठओटा बैंकमा रुपै याँ सारेको प्रकरण। त्यसैगरी भर्खरै विवाह भएको नव दाम्पत्य जोडिको महिना दिन नबित्दै विवाहित महिलाको पहिलाको प्रेमीले सामाजिक सञ्जाल फेसबुकमा पोष्ट गरेको फोटोको कारण सम्बन्धमा खलल उत्पन्न भएको विषय जस्ता दर्जनौ विषयहरु आज दिन दुगुना रात चौगुनाका दरले वृद्धि हुँदै गएको पाइन्छ। नेपालमा आजसम्म साइबर अपराध सम्बन्धी छुट्टै कडा कानून निर्माण नगर्नुले पनि नेपालमा साइबर अपराध बढ्दै गएको पाइयो।

निष्कर्ष

वास्तवमा साइबर अपराध विषयमा खोज अनुसन्धान गर्नु निकै कठिन विषय हो। जहाँ संसारभरका मानिसहरुले इन्टरनेटको माध्यमबाट विभिन्न सूचना तथा सन्देशहरु ग्रहण तथा सम्प्रेषण गर्दछन। तीनबारे नियन्त्रण गर्नु तथा कस्ले कस्लाई के गऱ्यो वा भन्यो भन्ने विषयको अनुसन्धान विश्वको एक कुनामा बसेर सम्मभव हुने विषय होइन। तर यस विषयमा सबै इन्टरनेटको प्रयोगकर्ता आफै सचेत र मिडिया साक्षर हुने हो भने स्वःतह न्यून भएर जानेछ। तसर्थ हामी सबैले सूचना प्रविधिको प्रयोग के कसरी गर्नुपर्दछ भनी

समयमै सचेत भयौ भने साइबर अपराधबाट बच्न सक्दछौ । अन्यथा हेलचेकयाइँ गऱ्यौ भने एकदिन हामी आफै यसको शिकार बन्न नपुगिएला भन्न सकिन्न ।

विकसित राष्ट्रमा समेत अहिले साइबर अपराध टाउको दुखाइको विषय बनेको बेलामा मिडिया साक्षरता कम भएको नेपालमा नहुने कुरै भएन । विशेषगरी सामाजिक सञ्जालको प्रयोगकर्ता जो साझा र बेसहारा व्यक्तिहरुलाई निशाना लगाएको पाइन्छ । यस्तो हुनुको कारण राज्यको विद्युतीय सुरक्षा नीति र व्यवस्थापनमा कमजोरी र साइबर अपराध विरुद्धको अभियानमा राज्यको लगानी न्यून रहनुले साइबर अपराध बढेको देखिन्छ । यसका लागि नेपाल सरकारले जापान, चीन तथा बेलायत सरकाले झैँ मिडियाको दुरुपयो गलाई निरुत्साहित गर्न साइबर अपराध र तथ्याङ्क सुरक्षा सम्बन्धी अलग अलग ऐन तथा कानून बनाउन सके मात्रै यसको नियन्त्रण हुन सक्ला नत्र कारवाहीको नाममा केही हजार धरौटी लिएर छाडेपछि अपराधिहरु झनै हौसियर अरुहरुलाई समेत ह्याकिङ गर्ने तथा धम्काएर पैसा असुल गर्ने, गाली बेइज्जती गर्ने, अश्लील फोटो तथा भिडियो पोष्ट गरेर व्यक्तिलाई मानसिक तनाब दिने जस्ता अनगिन्तीका समस्याहरु सिर्जना गर्न र गराउन सक्ने सम्भावना प्रबल रहन्छ । त्यसका साथै नेपाल सरकारले साइबर अपराध, यसको खतरा, सुरक्षा र रणनीतिहरुको व्यावसायिक विश्लेषण गर्नंपर्ने देखिन्छ ।

त्यसैगरी नेपालमा इन्टरनेट प्रयोगकर्ताको नाम, अस्थायी/स्थायी ठेगाना र फोटोसहित राख्ने तथा अश्लील वेबसाइडहरु बन्द गर्ने कानून बनाउनु आवश्यक छ । यदि साइबर अपराध सम्बन्धी इन्टरनेटको प्रयोगकर्ता सचेत नहुने र नेपाल सरकारले पनि कडा कनून निर्माण गरी कार्यन्वयनमा नल्याउने हो भने नेपाल छिट्टै नै साइबर हब बन्ने विषयमा दुईमत छैन । बेलैमा सबैको यसतर्फ ध्यानजानु जरुरी छ ।

सन्दर्भ सामग्री (References)

नेपाल प्रज्ञा–प्रतिष्ठान । वि.सं. २०७९ । प्रज्ञा नेपाली बृहत् शब्दकोश । कमलादी, काठमाडौं ।

लम्साल, मातृकाप्रसाद, भण्डारी, गोविन्दप्रसाद र कार्की, विष्णु बहादुर । वि.सं. २०८१ । सामाजिक अध्ययन । काठमाडौं । रिडमोर ।

उप्रेती, तोमनाथ । २०८० माघ १८, १६:१३ । साइबर सुरक्षामा संवेदनशीलता र बढ्दो चूनौती । इकर्मचारीडट कम । *https://ekarmachari.com/archives/46561?fbclid=IwY2xjawH3F2tleHRuA2FlbQIxMQABHZKT2tFAq5W6XKY_UZQGcc_UolzVlljW3M8fZYmBa-fiBR-8kudyijSlGQ_aem_9MQ3o9Rc2vh61-HTq7-sjw*

बशिरा । वि.सं. २०७९ असार ५, १०:५७ । चुनौती बन्दै साइबर अपराध । अन्नपूर्णपोष्ट डट कम । *https://annapurnapost.com/y/206650/?fbclid=IwY2xjawH3GiBleHRuA2FlbQIxMQABHfru8YjI7ug3JyTnY3hJ8svIxNF9qS1NwcShsUfZrt7jfoTrAAIIQ1mo4A_aem_pEvap0yXEnAoWjLH4GJN9A*

आचार्य, हरी । २०८०, आश्विन १४, आइतबार । साइबर अपराध : समस्या, चुनौती र समाधान । प्रशासन डट कम । *https://www.prasashan.com/2023/10/01/476345/?fbclid=IwY2xjawH3HWdleHRuA2FlbQIxMQABHUMTBlrE3OWar58m0vn5-iKoIDIgg9N1B07Yij6zz5H19gTJ7ZwuYqPAiQ_aem_pHJ2quNFtLuRBkyDndFgcw*

गिरी, शैलेन्द्र । फाल्गुन ७, २०७९, ०७:५० । साइबर सुरक्षा र बढ्दो चुनौती । ईकान्तिपुर डट कम । *https://ekantipur.com/opinion/2023/02/19/167677232426013865.html?fbclid=IwY2xjawH10BVleHRuA2FlbQIxMQABHaJRk1plmRd46e1BMB3F5pRf_e45ntSp0APorasbXF6EmWSb9pbns24aUw_aem_forQSTMjuSFMTqW0urhO9Q*

Ministry of Law [MOL] (2015). Constitution of Nepal.