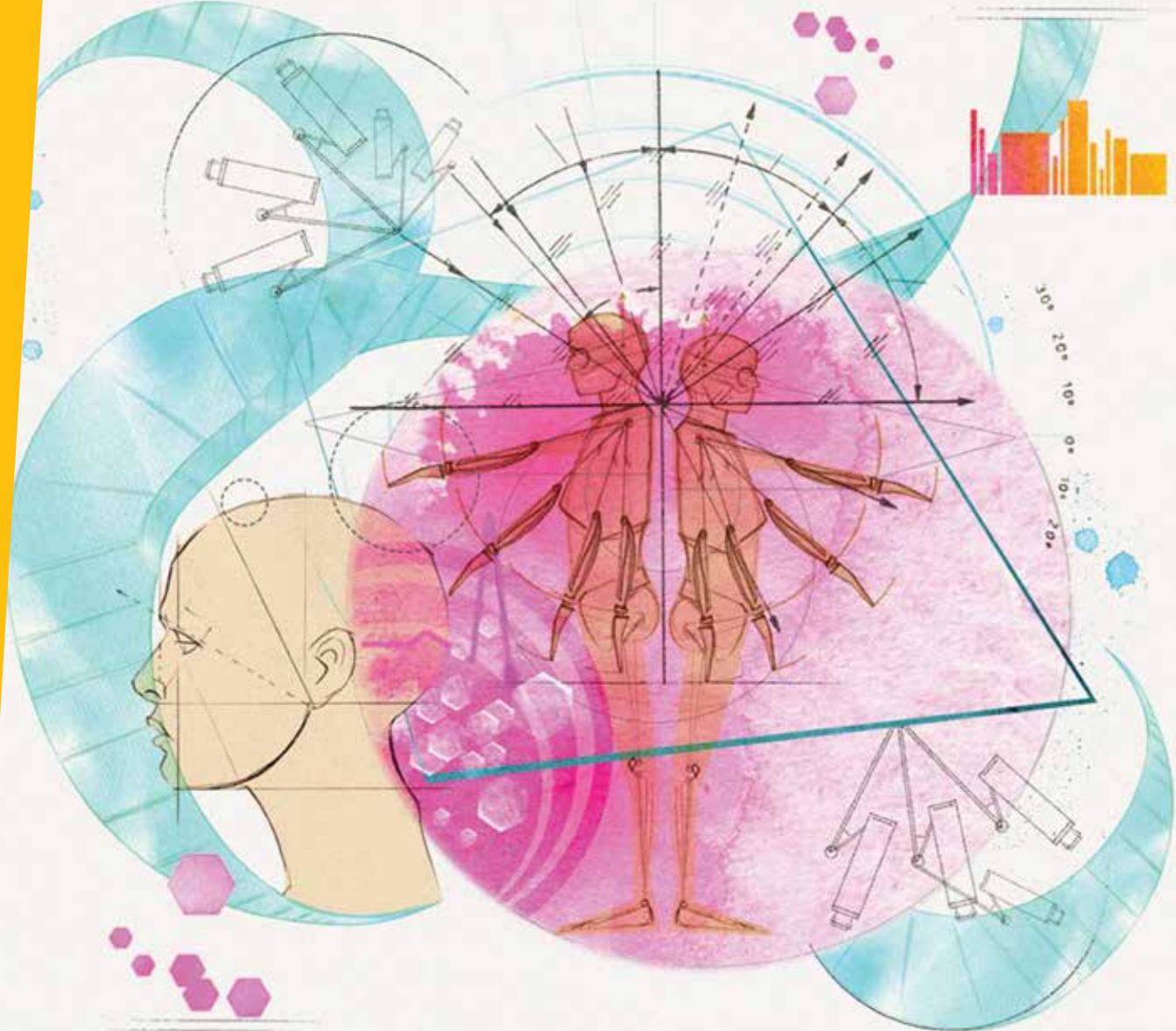


सचेत बनाँ !

सूचना र प्रविधिको
सही प्रयोग

सेन्टर फर मिडिया
रिसर्च - नेपाल



सचेत बनाँ !

सूचना र प्रविधिको
सही प्रयोगबारे
युवालक्षित मिडिया
र सूचना साक्षरता
हातेपुस्तिका



सचेत बनाँ ! : सूचना र प्रविधिको सही प्रयोग

सामग्री संयोजक : उज्ज्वल आचार्य

प्रकाशित मिति : २०८०, असोज



सेन्टर फर मिडिया रिसर्च - नेपाल, काठमाडौँ

वेब : <https://research.butmedia.org>

सामाजिक सञ्जाल : CMRNepal

ईमेल : cmrnepal@butmedia.org

सहयोग

TACTICAL TECH



लेआउट : बिक्रम चन्द्र मजुमदार

कभर : Illustration by Ann Kiernan for Technologies of Hope and Fear by Tactical Tech

यो हातेपुस्तिका ट्याक्टिकल टेक (Tactical Tech) र ओपन सोसाइटी फाउन्डेशन (Open Society Foundations) को सहयोगका कारण सम्भव भएको हो । यसका कतिपय सामग्री र ग्राफिक्सहरू ट्याक्टिकल टेकका प्रकाशनहरूबाट साभार गरिएका छन् भने कतिपय सेन्टर फर मिडिया रिसर्च - नेपालका प्रकाशनहरूबाट साभार गरिएका छन् । यस पुस्तिकाको विषयवस्तुको छ्नोट, विषयवस्तु र सामग्री भने सिएमआर नेपालका एकल जिम्मेवारी हुन् । अन्य सहयोगी संस्थाको विचार प्रतिबिम्बित गर्नेन् भन्ने जरुरी छैन ।

यो हातेपुस्तिका क्रियटिभ कमन्स CC BY 4.0 अन्तर्गत प्रकाशन गरिएको छ । यसका सामग्रीहरू मूल कुरा फरक नपर्ने गरी पुनः प्रकाशन गर्न पाइन्छ ।

हाम्रो भनाइ

सूचना प्रविधिको तीव्र विकाससँगै अवसर र चुनौती थपिएका छन् । सूचना प्रविधिले गर्दा छिटो र छरितोरूपमा सूचना तथा ज्ञानलाई व्यापक बनाउन सहज भएको छ । साथसाथै उपलब्ध सूचना तथा जानकारी सही हुन् कि होइनन् भन्ने छुट्याउन कठिन भइरहेको छ । आवश्यकताअनुसार सूचना तथा जानकारी केलाउन नसकदा र प्रविधिको सदुपयोग गर्न नजान्दा अन्योल सिर्जना हुने मात्र होइन, गलत नतिजा पनि आएका छन् । त्यसैले यतिबेलाको आवश्यकता सूचना प्रविधिको सही प्रयोग र सही सूचना छनोट गर्नु हो । त्यो क्षमता विकासका लागि मिडिया र सूचना साक्षरताबारे जानकारी हासिल गर्नु जरुरी हुन्छ ।

सेन्टर फर मिडिया रिसर्च-नेपालले विगतदेखि नै मिडिया र सूचना साक्षरतासम्बन्धी काम गर्दै आएको छ । यसै क्रममा यसअधि विद्यालय शिक्षकलाई लक्षित गरी मिडिया र सूचना साक्षरतासम्बन्धी स्रोत पुस्तिका प्रकाशन गरिएको थियो । यसलाई विस्तार गर्ने क्रममा सचेत बनाउँ! सूचना र प्रविधिको सही प्रयोग नामक पुस्तिका प्रकाशन गरेका छौं । पुस्तिकामा मिथ्या सूचना, मिडिया, सोसल मिडिया, इन्टरनेट, कम्प्युटर, मोबाइल फोन, तथ्य जाँच, डिजिटल डिटक्स, एआइलगायतका विषय समावेश गरेका छौं ।

अन्त्यमा पुस्तिकाको संयोजन गर्ने उज्ज्वल आचार्य, पुस्तिका प्रकाशनमा सहयोग गर्ने ट्याक्टिकल टेक र ओपन सोसाइटी फाउन्डेशनप्रति हार्दिक धन्यवाद व्यक्त गर्दछु ।

तृष्णा आचार्य

अध्यक्ष

सेन्टर फर मिडिया रिसर्च - नेपाल

हात्रो भनाइ	५
यो पुस्तिका केका लागि ?	९
• यो पुस्तिका कसका लागि ?	
• यो पुस्तिकाको प्रयोग कसरी गर्ने ?	
भाग १ : परिभाषा र उचित प्रयोग.....	११
Unit 1 → Information सूचना/जानकारी.....	१२
Unit 2 → Misinformation मिथ्या सूचना.....	१४
Unit 3 → Media मिडिया.....	१७
Unit 4 → Social Media सोसल मिडिया.....	२०
Unit 5 → Internet इन्टरनेट.....	२३
Unit 6 → Chat/Messenger/Email च्याट/मेसेन्जर/ईमेल.....	२६
Unit 7 → Computer/Mobile Games कम्प्युटर/मोबाइल गेम.....	२९
Unit 8 → Mobile Phone मोबाइल फोन.....	३२
Unit 9 → Password पासवर्ड.....	३४
Unit 10 → Photo/Video फोटो र भिडियो.....	३६
Unit 11 → Our Data हात्रो डेटा.....	३८
भाग २ : परिभाषा र जानकारी.....	४१
Unit 12 → Media and Information Literacy मिडिया तथा सूचना साक्षरता.....	४२
Unit 13 → Fact-Checking तथ्य जाँच.....	४४
Unit 14 → Digital Safety डिजिटल सुरक्षा.....	४६
Unit 15 → Digital Detox डिजिटल डिटॉक्स.....	४८
Unit 16 → Artificial Intelligence एआइ	५०
भाग ३ : प्रयोगात्मक सुझाव.....	५३
Unit 17 → टु स्टेप भेरिफिकेसन.....	५४
Unit 18 → सोसल मिडियालाई रिपोर्ट	५६

यो पुस्तिका केका लागि ?

यो पुस्तिका कसका लागि ?

यो पुस्तिका विशेषगरी विद्यालय र कलेजमा अध्ययनरत किशोर-किशोरी/युवालाई ध्यानमा राखी बनाइएको हो । त्यस्ता किशोर-किशोरी/युवा एवं उनीहरूका शिक्षक र अभिभावकलाई यो पुस्तिका उपयोगी हुन्छ ।

तर यो पुस्तक मिडिया र सूचना साक्षरता अथवा डिजिटल सुरक्षाबारे चासो हुने वा इन्टरनेटलगायतका विषयबारे जान्न चाहने सबैले प्रयोग गर्न सक्नुहुन्छ । यसलाई यी विषयबारे तालिम वा कार्यशालाहरूमा पनि प्रयोग गर्न सकिन्छ ।

यो पुस्तिका तपाईंले पढिसकेपछि आफैसँग राख्न पनि सक्नुहुन्छ वा भाइ/बहिनी वा साथीलाई दिन पनि सक्नुहुन्छ ।

पढिसकेपछि यस पुस्तिकाका कुनै पनि विषयबारे आफ्ना साथी, परिवार, अभिभावक वा शिक्षकसँग वा सबैसँग छलफल गर्नुहोस् । त्यसो गर्दा हामी सबैजना इन्टरनेट र मिथ्या सूचनाका नराम्रा कुराबाट जोगिन सक्छौं ।

यो पुस्तिकाको प्रयोग कसरी गर्ने ?

यो पुस्तिका विशेषगरी ३ कुरामा केन्द्रित छ ।

- मिडिया र सूचना साक्षरता
- डिजिटल सुरक्षा र
- इन्टरनेटसम्बन्धी प्रविधिको सुरक्षित र सही प्रयोग

यो पुस्तिकाका २ भाग छन् ।

पहिलो भागमा माथि भनिएका ३ विषयमा विभिन्न अन्तर्निहित प्रविधि वा प्रयोगबारे जानकारी दिइएको छ । प्रत्येक खण्डमा त्यो के हो र के होइन अनि त्यस विषयमा हामीले के गर्दा र के नगर्दा राम्रो हुन्छ भन्ने कुरा समेटिएका छन् । उदाहरणका लागि मिथ्या सूचनाको खण्डमा मिथ्या सूचना के हो, मिथ्या सूचनाको प्रभावबाट बच्न र बचाउन हामीले के गर्नुपर्छ र के गर्नुहुन्न भन्ने कुरा सङ्क्षेप र सजिलो भाषामा दिइएको छ ।

दोस्रो भागमा चाहिँ मिडिया र सूचना साक्षरता, तथ्य जाँच, डिजिटल सुरक्षा एवं डिजिटल डिटक्स गरी ४ विषयमा जानकारी दिइएको छ ।

प्रविधिले परिवर्तन गरेको आजको संसारमा पहिलो भागमा रहेका कुराहरू जान्न अत्यावश्यक छन् भने दोस्रो भागका धेरै कुरा जानिराख्दा राम्रो हुन्छ ।

यो पुस्तिका सुरुदेखि अन्त्यसम्म पढे पनि हुन्छ र आफूलाई जान्न मन लागेको विषयअनुसार पढे पनि हुन्छ । यसका सबै विषय अन्तर्निहित भए पनि प्रत्येक खण्ड छुट्टाछुट्टै पढ्न मिल्छ ।

भाग १

परिभाषा र उचित प्रयोग

Unit 1

Information

सूचना / ज्ञानकारी

यो पुस्तिकामा सूचनालाई कुनै माध्यम प्रयोग गरी एक व्यक्तिबाट अर्को व्यक्तिसम्म पुगेको कुनै व्यक्ति वा घटना वा विषयका बारेमा विवरण वा विचार वा अङ्क हो भनी मानिएको छ । ती लिखित वा मौखिक वा चित्रित कुनै पनि प्रकारका हुन सक्छन् । उदाहरणका लागि ती सूचना अक्षर, भिडियो, अडियो, एनिमेसन, चित्र वा गेम पनि हुन सक्छन् ।

हामीले धेरै स्रोतबाट सूचना प्राप्त गरिरहेका हुन्छौं ।
हामीले सूचना प्राप्त गर्ने स्रोत यी हुन सक्छन् :

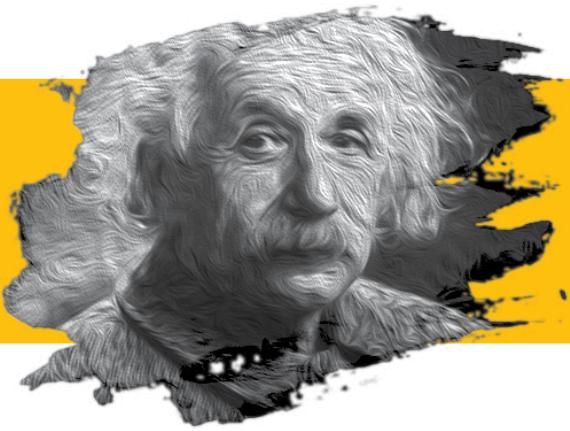
- ▶ परम्परागत मिडिया (पत्रपत्रिका, रेडियो र टेलिभिजन)
- ▶ सोसल मिडिया (फेसबुक, युट्युब, टिवटर, टिकटक)
- ▶ अनलाइन मिडिया (वेबसाइट वा पडकास्ट)
- ▶ सन्देश आदान-प्रदान गर्ने एपहरू (ह्वाट्सएप, फेसबुक मेसेन्जर, भाइबर, इमो)
- ▶ मोबाइल एपहरू (हाप्पो पात्रो)
- ▶ भिडियो गेम वा विज्ञापन
- ▶ फिल्म, नाटक वा प्रदर्शनी
- ▶ किताब (कथा/उपन्यास/कविता), इतिहास वा अन्य विषयका पुस्तक वा कमिक्स

▶ व्यक्ति (साथीभाइ, अभिभावक, शिक्षक र अन्य) वा संस्था/समूह

सूचना तथ्यपरक नहुन पनि सक्छन् । ती विचार मात्रै पनि हुन सक्छन् । ती तोडमरोड गरिएका तथ्य पनि हुन सक्छन् र हामीलाई भुक्त्याउनका लागि बनाइएका पनि हुन सक्छन् ।

सूचना गलत हुन सक्छन् । कसैले देखै नदेखेका कुरा पनि हुन सक्छ । देखेकै भनेर भनिएका सूचनामा पनि पूर्ण जानकारी नहुन सक्छ वा त्यसलाई गलत बुझिएको वा व्याख्या गरिएको हुन सक्छ ।

सूचना मिथ्या हुन सक्छन् । कसैले जानी/जानी वा नजानी/नजानी त्यसलाई प्रसार गरेका हुन सक्छन् ।



सूचना ज्ञान होइन ।

- अल्बर्ट आइन्स्टाइन, वैज्ञानिक



20°

Unit 2

Misinformation

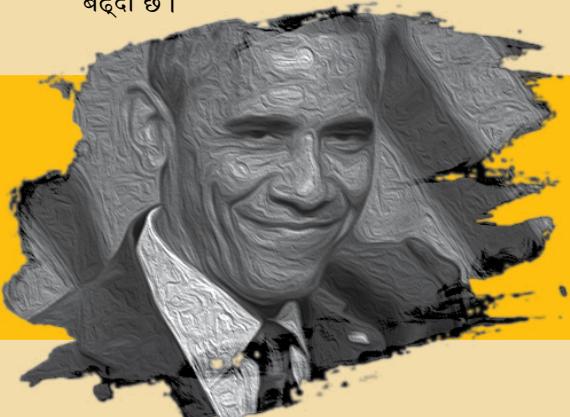
मिथ्या सूचना

मिथ्या सूचना (अड्डेजीमा मिसइन्फरमेसन/डिसइन्फरमेसन) भनेको मूलतः भुटो वा गलत वा भ्रमपूर्ण वा अनर्थस्तुपमा घटना, अभिव्यक्ति, तथ्याङ्क र तर्क प्रयोग गरेर वा व्याख्या गरिएका सूचना हुन्।

यस्ता सामग्रीको मूल उद्देश्य हाप्रो विचार वा सोच वा कामलाई प्रभावित गर्नु हुन्छ।

इन्टरनेटको विकास र विशेषगरी आममानिसले सहजस्तुपमा सामग्री प्रकाशन र वितरण गर्न सक्ने सोसल मिडियाको विस्तारका कारण मिथ्या सूचनाको प्रयोग अझ बढी सहज र धेरैबीच पुग्न सक्ने भएको छ।

मिथ्या सूचना जुनसुकै विषयमा पनि हुन सक्छ। तर विश्वभर निर्वाचनका क्रममा मिथ्या सूचनाको प्रयोग बढ्दो छ।



यस्ता सूचना सबै मिथ्या सूचना हुन् :

- ▷ कुनै हानि गर्ने उद्देश्य नभएका तर पाठकलाई मूर्ख बनाउने व्यङ्यातमक सामग्री।
- ▷ शीर्षक वा तस्विरसँग मूल लेख मेल नखाने सामग्री।
- ▷ भ्रम सिर्जना गर्ने सामग्री।
- ▷ सही सूचनालाई गलत सन्दर्भमा प्रयोग गरिएको सामग्री।
- ▷ कसैले भन्दै नभनेकोलाई भनेको भनिएका सामग्री।
- ▷ तथ्य वा तथ्याङ्क वा घटना वा तर्क वा तस्विरलाई तोडमरोड गरिएका सामग्री।
- ▷ हुँदै नभएका घटना वा तथ्य वा अभिव्यक्ति।



यहाँ यति धेरै सक्रिय मिथ्या सूचना छन् र तिनलाई यति राम्ररी प्रस्तुत गरिएका छन् कि तपाईँ त्यसलाई फेसबुक पेज वा टिभीमा उस्तै देख्नुहुन्छ।

- बाराक ओबामा, अमेरिकाका पूर्वराष्ट्रपति

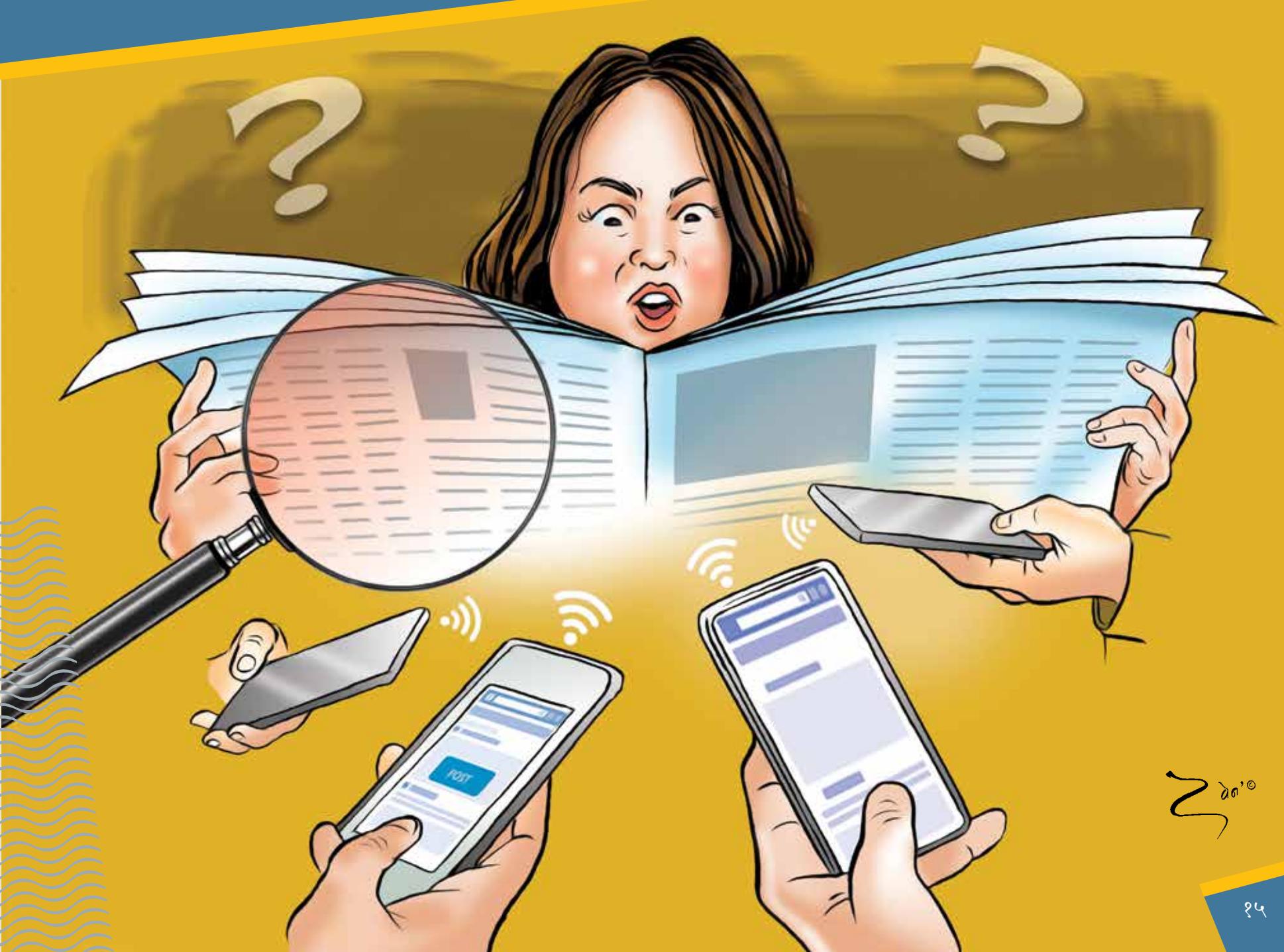
के गर्ने ?

शङ्का गर्ने

हामीले जुनसुकै माध्यमबाट प्राप्त गरेको भए पनि त्यो सूचना मिथ्या हुन सक्छ भनेमा सचेत हुनुपर्छ।

कुनै सामग्री गज्जब छन् वा खुसी, रिस वा दुःख जस्ता मानवीय आवेगलाई तुरन्तै जागृत गर्नेखालका छन् भने ती सामग्री शङ्कास्पद हुन्छन्।

कुनै पनि सामग्री भट्ट विश्वास गर्न नसकिनेखालको वा आश्चर्यचिकित पार्नेखालको वा होइन होला लाग्नेखालको वा सारै रमाइलोखालको छ भने त्यस्ता सामग्रीमा पनि शङ्का गर्नुपर्छ।



Misinformation

मिथ्या सूचना

आलोचनात्मक दृष्टि दिने

सूचना दिने व्यक्ति वा संस्था विश्वास गर्न लायक छ ?
सूचना दिने व्यक्ति वा संस्थाको पूर्वाग्रह वा संलग्नता के छ ? उसले किन हामीलाई यो सूचना दिइरहेको छ ?
शीर्षक वा तस्विरअनुसारको सामग्री छ ? 'एउटा साथी', 'नाम भन्न मिल्दैन', 'त्यहाँ भएका एकजना', 'एक उच्च अधिकारी', 'हाम्रो स्रोत' वा 'एक विज्ञ' भन्ने भनेको कुरा पो हो कि ? त्यो व्यक्ति वा संस्थाले पहिले दिएका अन्य सूचना मिथ्या थिए कि थिएनन् ?

अन्यत्र खोज्ने

हामीले प्राप्त गरेका सूचना अन्य स्रोतमा छ कि छैन ?
गुगल गरेर खोज्दा पनि धेरै कुरा थाहा हुन सकछ ।
समाचार बन्न सक्ने कुरा कुनै सञ्चार माध्यममा छैन

वा समाचार एउटा साइटमा मात्रै छ भने त्यो मिथ्या हुने संभावना धेरै हुन्छ । समय छ भने सामग्री सही छन् कि छैनन् भनेर परीक्षण गर्नुहोस् । यस्तो पुष्टि गर्नका लागि सम्बन्धित व्यक्ति वा संस्थासँग सोधन सकिन्छ एवं इन्टरनेट वा सोसल मिडियामा खोज्न सकिन्छ ।

रिपोर्ट गर्ने

कुनै सामग्री मिथ्या भए त्यो प्रकाशित सोसल मिडियामा मिथ्या हो भनी रिपोर्ट गर्नुहोस् । (रिपोर्ट गर्नेबाटे थप जानकारीका लागि यो पुस्तकको अन्तिम अध्याय हेर्नुहोस् ।)

के नगर्ने ?

- ▷ कुनै पनि सूचना प्राप्त गरेपछि तुरुन्तै विश्वास नगर्नुहोस्, ती मिथ्या हुन सक्छन् भनेर सचेत हुनुहोस् ।
- ▷ कुनै पनि सूचना आफ्नो सोसल मिडियामा सेयर गर्न वा त्यस्ता सूचनाका आधारमा आफ्नो विचार राख्न हतार नगर्नुहोस् ।
- ▷ शीर्षकमा शङ्का लागेका वा गलत साइटमा प्रकाशित सामग्री पढन खोजेर समय खेर नफाल्नुहोस् ।
- ▷ सोसल मिडियामा सेयर गरिएका विचार वा सामग्री को र कति जनामा पुछ भन्ने कुराको अनुमान गर्न कठिन हुन्छ । यसर्थे अनावश्यक कुरा वा गलत सूचना रमाइलो वा अन्य कुनै कारणले पनि लेख्ने वा सेयर गर्ने नगर्नुहोस् ।
- ▷ कुनै सूचना मिथ्या हो भने थाहा पाउनेबित्तिकै आफ्नो सोसल मिडियामा त्यो मिथ्या हो भनेर जानकारी गराउनुहोस् ।
- ▷ सोसल मिडियामा लेखेपछि त्यसमा आएका प्रतिक्रिया हेर्नुहोस् र कसैको भनाइले शङ्का उत्पन्न गरेमा तुरुन्तै सच्याउनुहोस् । अरु कसैले सेयर गरेको सामग्री मिथ्या भएको थाहा भए कमेन्टमार्फत जानकारी गराउनुहोस् ।

Unit 3

Media

मिडिया

मिडिया भन्नाले सामान्यरूपमा हामी समाचारका स्रोतका रूपमा रहेका संस्थागत आमसञ्चार माध्यमलाई बुझ्छौं । आमसञ्चार माध्यम यस्ता हुन सक्छन् :

- छापा माध्यम : अखबार, पत्रपत्रिका र म्यागेजिन
- विद्युतीय माध्यम : रेडियो र टेलिभिजन
- अनलाइन माध्यम : वेबसाइट र समाचार एप

कतिपय अवस्थामा छापा र विद्युतीय माध्यमलाई परम्परागत माध्यम अनि अनलाइन माध्यमलाई नयाँ माध्यम पनि भनिएका छन् ।

सोसल मिडिया भनिने फेसबुक, टिकटक, टिकटक वा युट्युब जस्ता माध्यमहरू भने संस्थागत समाचार संस्था जस्ता मिडिया होइनन् । मिडियामा आउने सूचनालाई समाचार वा विचारका रूपमा आए पनि त्यसलाई पत्रकारिताका विभिन्न चरणहरू पार गरेर धेरै मानिसले सत्यतथ्य छ कि छैन भनी पुष्टि गरेको हुनुपर्छ । त्यसैले मिडिया बढी विश्वसनीय हुन्छन् ।

मिडियामा सामग्री तथ्यपरक, समाजका लागि उपयोगी, निष्पक्ष, कसैको दबाबमा नपरी लेखिएका र आमहितका लागि हुन्छन् भन्ने मान्यता छ । मिडियाका सामग्री पत्रकारिताका उत्पादन हुन् र पत्रकारिता पेसा निश्चित प्रक्रिया, मापदण्ड र आचारसंहिताअन्तर्गत चल्नुपर्छ ।

पत्रकारिता र मिडिया देश र प्रजातन्त्रका लागि अपरिहार्य छ भन्ने मानिन्छ ।

तर मिडियामा काम गर्नेहरू पनि मानिस नै हुन् । उनीहरूले सूचना प्राप्त गर्ने पनि मानिस नै हुन् । उनीहरू सबैको पूर्वाग्रह हुन्छ । त्यसैले जति प्रयास गरे पनि मिडियामा केही कमजोरी रहन्छन् ।

पूर्वाग्रह भनेको कुनै विषयमाथि हाम्रो पहिलेदेखि भएको धारणा हो जुन हामीलाई विश्वास लागेको हुन्छ । सूचना प्रवाह र ग्रहणको कुरामा पनि यसले भूमिका खेल्छ । हामी हाम्रो पूर्वाग्रहसँग मिल्दोजुल्दो सूचना भए सजिलै ग्रहण गर्छौं भने अमिल्दो सूचना भए त्यसलाई ग्रहण गर्न कमै मात्र प्रयास गर्छौं ।

“
मिथ्या समाचार उत्पादन सस्तो छ ।
राम्रो पत्रकारिता महँगो छ ।

- टमस हेन्रिक इल्भिस, इस्टोनियाका पूर्वराष्ट्रपति



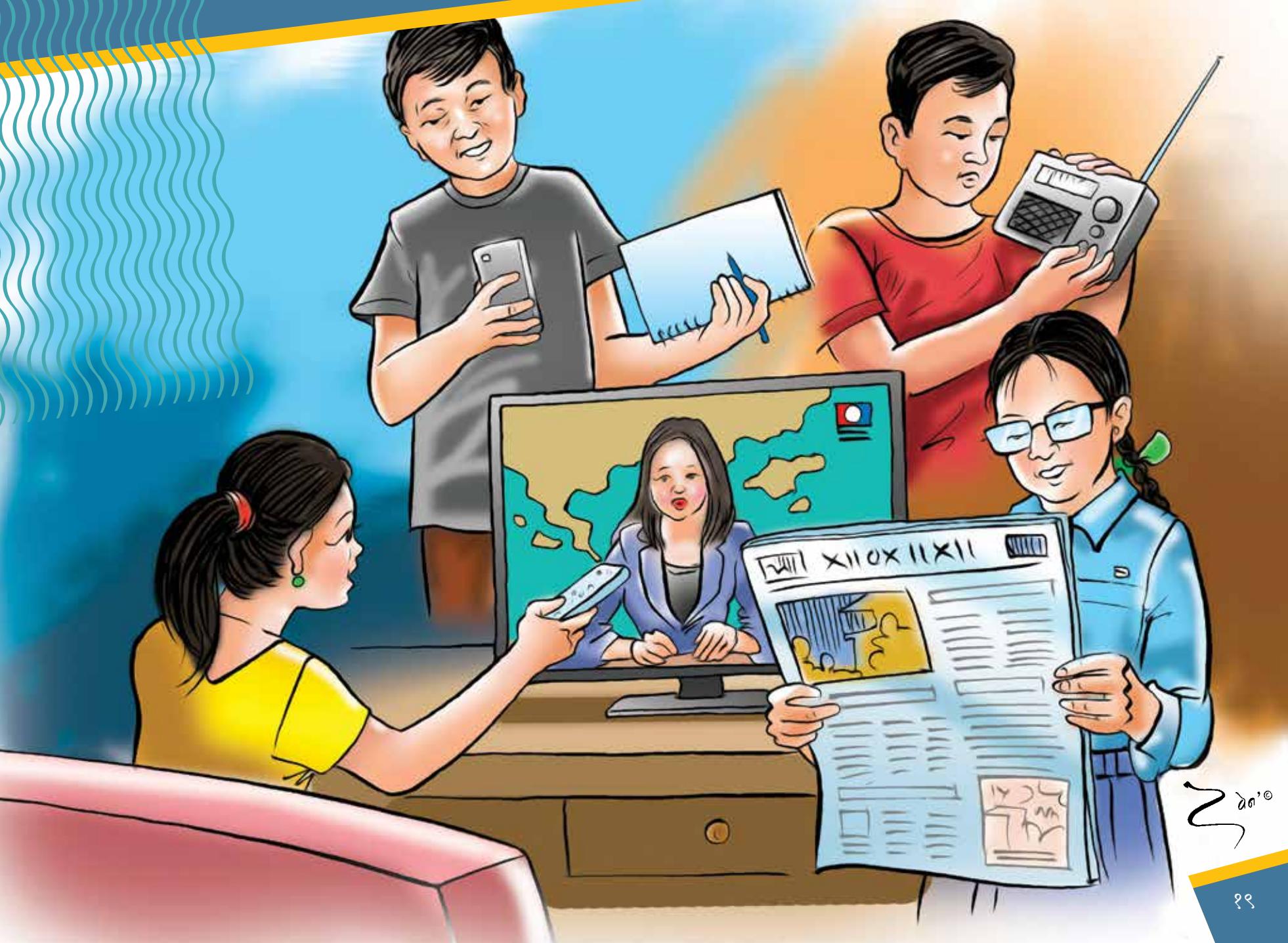
के गर्ने ?

- सकेसम्म धेरै मिडियामा पहुँच बनाउने जसले गर्दा विविध विचारका सामग्री हामीले प्राप्त गर्छौं ।
- मिडियाका सामग्रीलाई अन्य सूचना भन्दा अलि बढी विश्वास गर्ने तर आलोचनात्मक दृष्टिले पनि हेरिहनुपर्छ ।
- कतिपय मिडिया निश्चित उद्देश्य बोकेका हुन्छन् । कतिपय मिडियाको राजनीतिक धारणा हुन्छन् । ती सार्वजनिक पनि हुन सक्छन् वा लुकाइएका पनि हुन सक्छन् । मिडिया कसको हो र कस्तोखाले विचार प्रवर्द्धन गर्दै सोच्नुपर्छ ।
- अन्यत्र देखिएका समाचार जस्ता सूचनाको पुष्टि गर्ने मिडियामा तीवारे समाचार आएका छन् कि छैनन् हेर्नुपर्छ ।
- मिडियामा कुनै सामग्रीमा शइका लागेमा वा पूर्वाग्रही देखिएमा वा पूर्ण नलागेमा वा

पत्रकारिताका मूल्य/मान्यता बाहिर भएको लागेमा प्रश्न गर्नुपर्छ । यस्तो प्रश्न मिडियालाई सिधा वा सोसल मिडियामा लेखेर गर्नुपर्छ । नागरिकले प्रश्न उठाउँदा मिडियालाई जिम्मेवार बन्न कर लाग्छ ।

के नगर्ने ?

- मिडिया भन्दैमा त्यसका सबै सामग्रीलाई आँखा चिम्लेर विश्वास गरिहाल्नु हुँदैन । मिथ्या सूचना मिडियामा पनि आउँछन् ।
- केही मिथ्या समाचार आउँछ वा आफ्नो विचारसँग नमिल्ने सामग्री आउँछ वा आफूले भने जस्तो सामग्री आउँदैन भनेर पत्रकारिता वा मिडियालाई बदनाम गर्ने हिसाबले होच्याउने वा आलोचना गर्नुहुँदैन । तथ्यपरक र तर्कसङ्गत आलोचनाले मिडियालाई सुधार्छ तर पूर्वाग्रही आलोचनाले मिडिया बदनाम हुँदा समाज र प्रजातन्त्रलाई हानि हुन्छ ।



Unit 4

Social Media

सोसल मिडिया

सोसल मिडियामा मिडिया शब्द भए पनि ती संस्थागत पत्रकारिता जस्तो मिडिया भने होइनन् ।

सन् २००० यता इन्टरनेट बिस्तारै सूचना र सञ्चारको एकतर्फी माध्यम भन्दा प्रयोगकर्ताहरू सक्रिय हुने गरी दुईतर्फी वा बहुतर्फी माध्यमका रूपमा विकास हुन थाल्यो । जसलाई “वेब २.०” भनियो ।

यो परिवर्तनले सोसल मिडियाको आगमन भयो र आज हजारौँको सङ्ख्यामा सोसल मिडिया भन्न सकिने सेवाहरू इन्टरनेटमा उपलब्ध छन् र तिनलाई करोडौँ मानिसले प्रयोग गरिरहेका छन् । टिकटक, फेसबुक, ट्रिवटर, युट्युब, इन्स्टाग्राम, ब्लग वा स्न्यापच्याट जस्ता वेबसाइट वा एपहरू सोसल मिडिया हुन् ।

सामान्यरूपमा दुईजनाबीच वा सानो समूहबीच कुराकानी हुने स्काइप वा भाइबर वा ह्वाट्सएप वा इमो अथवा समाचार वेबसाइट, जस्तै- अनलाइनखबर वा सेतो पाटी वा इकान्तिपुर वा नागरिकन्युज सोसल मिडिया होइनन् । तर भाइबर र ह्वाट्सएपलाई केही अवस्थामा सोसल मिडियाका रूपमा प्रयोग गर्न सकिन्छ ।

सोसल मिडिया	फेसबुक, ट्रिवटर (एक्स), युट्युब, इन्स्टाग्राम, टिकटक, स्न्यापच्याट वा पिन्ट्रेस्ट
च्याट/मेसेन्जर जसलाई सोसल मिडियाका रूपमा प्रयोग गर्न पनि मिल्छ	भाइबर (ग्रुप वा कम्युनिटी वा च्यानल), ह्वाट्सएप (कम्युनिटी वा ग्रुप) वा टेलिग्राम (ग्रुप वा च्यानल)
मिडिया वेबसाइट जुन सोसल मिडिया होइनन्	अनलाइनखबर, सेतो पाटी, इकान्तिपुर आदि

कुनै वेबसाइट वा एप सोसल मिडिया हुन् भने तिनले तलका ४ सुविधा दिन्छन् :

- क. हाम्रो सामग्री (अक्षर वा फोटो वा भिडियो वा आवाज वा अन्य केही कुरा) प्रकाशन गर्ने सुविधा
- ख. हाम्रो सामग्री कसैले सम्पादन नगरी वा नहेरी तुरन्तै प्रकाशित हुने व्यवस्था



सोसल मिडियाको शक्ति र प्रभाव चाखलाग्दो कुरा छ, त्यसैले हामीले सोसल मिडियालाई सहीरूपमा प्रयोग गर्नुपर्छ ।

- मलाला युसुफजाई, नोबेल शान्ति पुरस्कार विजेता





Social Media सोसल मिडिया

ग. हाम्रो सामग्री हामीले चाहेको बेला सम्पादन गर्ने वा
मेट्रो सुविधा र

घ. हाम्रो सामग्री हाम्रो सञ्जालमा रहेका व्यक्तिहरूमाझ
सार्वजनिक हुने अवस्था

नेपालमा सबै भन्दा बढी प्रयोग भइरहेका सोसल
मिडियामा फेसबुक, युट्युब र टिकटक छन् । दिवाटर पनि
लाखौं नेपालीले प्रयोग गरिरहेका छन् ।

के गर्ने ?

- ▷ सोसल मिडिया सदुपयोग गरेर धेरै फाइदा लिन
सकिन्छ । त्यसैले सकारात्मक हिसाबले सोसल
मिडिया प्रयोग गर्नुपर्छ ।
- ▷ आफूसँग सरोकार राख्ने विषयमा आफ्नो विचार
लेख्न, साथीभाइ र आफन्तसँग सम्पर्क कायम राख्न
एवं अन्य कार्यलाई असर नपर्ने गरी मनोरञ्जनका
लागि सोसल मिडियालाई प्रयोग गर्नुपर्छ ।
- ▷ प्रत्येक सोसल मिडियाका बारेमा जानकारी राखेर
त्यसको प्रयोग गर्दा फाइदाजनक हुन्छ । उदाहरणका
लागि वृत्ति विकास र व्यावसायिक जीवन उन्नति
प्रयोजनका लागि लिङ्गडइन, विचार व्यक्त गर्ने र
व्यक्तिगत कुराहरूका लागि फेसबुक, सूचनाका
लागि टिकटर, मनोरञ्जनका लागि टिकटक एवं
सद्गीत र शिक्षाप्रद कुराका लागि युट्युब बढी
उपयोगी हुन सक्छ ।
- ▷ प्रत्येक सोसल मिडियामा आफ्ना व्यक्तिगत
जानकारी सकेसम्म कम राख्नुपर्छ अनि त्यसका
गोपनीयताहरूसम्बन्धी सेटिङ्हरू हेरेर आफ्नो
जानकारी पराइ हातमा जानबाट सकेसम्म सुरक्षित
बनाउनुपर्छ ।
- ▷ बीलयो पासवर्ड प्रयोग गर्नुपर्छ र सबैमा 2-step
verification राख्नुपर्छ ।
- ▷ अरूको तस्बिर प्रकाशन गर्दा सोधेर मात्रै हाल्नुपर्छ ।
जथाभावी अरूको तस्बिर वा भिडियो खिचेर हाल्नु
ठीक होइन ।

के नगर्ने ?

- ▷ जथाभावी नचिनेका मानिसलाई साथी बनाउनु
हुन्न । इन्टरनेटमा नाम र तस्बिर हेरेर मान्छे चिने
जस्तो गर्नुहुन्न किनभने कसैले गलत नाम र तस्बिर
राखेर खाता खोलेको हुन सक्छ ।
- ▷ सोसल मिडियाका साथीलाई अन्य साथी जस्तो
विश्वास गर्नुहुन्न ।
- ▷ सोसल मिडियामा देखिएका सबै लिङ्ग किलक
गर्नुहुन्न ।
- ▷ आफ्ना तस्बिर, व्यक्तिगत जानकारी र अन्य
सम्वेदनशील कुराहरू सबैको पहुँचमा हुने गरी
हाल्नुहुन्न ।
- ▷ नागरिकता, पासपोर्ट, प्लेनका टिकट वा परीक्षा
प्रवेशपत्र जस्ता व्यक्तिगत जानकारी हुने वस्तुहरूको
तस्बिर हाल्नुहुन्न ।
- ▷ अरू कसैलाई पनि आफ्नो खाता चलाउनु दिनुहुन्न ।
- ▷ साइबर अपराध वा दुरुपयोग हुने कार्य गर्नुहुन्न ।

थप जानकारीका लागि उज्ज्वल आचार्य र सन्तोष सिंग्देलले लेखेको र फ्रिडम फोरम नेपालले प्रकाशन गरेको “इन्टरनेट र यसको सुरक्षित प्रयोग : शिक्षक, अभिभावक र प्रयोगकर्ताको लागि
हातेपुस्तिका” हेर्नुहोस् । यो पुस्तिका www.freedomforum.org.np मा निःशुल्क उपलब्ध छ ।

Unit 5

Internet

इन्टरनेट

हामी सबैले इन्टरनेट चलाउँछौं । यसको मतलब हामी विश्वभर फैलिएको कम्प्युटरको सञ्जालमा जोडिन्छौं ।

इन्टरनेटमा विश्वका करोडौं कम्प्युटर र उपकरण सानादेखि ठूला, निजीदेखि सार्वजनिक वा सरकारी, व्यापारिकदेखि शैक्षिक कम्प्युटर सञ्जालहरूमा ताररहित वा तारसहितका विभिन्नखाले प्रविधिले सूचना आदान-प्रदान वा सञ्चार गर्न सक्ने गरी जोडिएका छन् ।

इन्टरनेटमा अनगिन्ती सूचना स्रोत वा सञ्चार एवं अन्य प्रकारका सेवा प्रयोग गर्न सञ्जिलो गरी जोडिएका छन् । प्राविधिकरूपमा जटिल भए पनि सामान्यरूपमा बुझ्दा

यसमा जोडिएका कुनै पनि एक उपकरणबाट अर्को उपकरणसम्म सम्बन्ध स्थापित हुन्छ ।

प्रयोगकर्ताका लागि इन्टरनेट, मोबाइल फोन वा कम्प्युटरबाट सूचना आदान-प्रदान गर्न मिल्ने र विश्वका अन्य जुनसुकै कुनामा रहेका भए पनि अन्य प्रयोगकर्तासँग सञ्चार सम्बन्ध स्थापित गर्न सकिने धेरैखाले सुविधा प्रदान गर्ने प्रविधि हो ।

इन्टरनेटको विकास सञ्चार सञ्जालका रूपमा भए पनि हाल यसको प्रयोग र सम्भावनाका कारण यो प्रविधिमा मात्रै सीमित छैन । इन्टरनेटले हाम्रो काम, सामाजिक उपस्थिति र व्यवहार, सूचना आदान-प्रदान एवं मानिस,

विचार र वस्तुहरूको व्यवस्थापन गर्ने तरिकालाई परिवर्तन गरेको छ ।

इन्टरनेटको प्रयोग

इन्टरनेट प्रयोग भइरहेका केही क्षेत्र यसप्रकार छन् :

- सूचना र समाचार
- सञ्चार
- शिक्षा र स्वास्थ्य
- कारोबार र व्यापार
- मनोरञ्जन
- अनुसन्धान
- किनमेल
- वृत्ति विकास
- व्यक्तिगत र लेखन
- सामाजिक सञ्जाल

इलेक्ट्रोनिक युगमा गोपनीयता सबै भन्दा ठूलो समस्या हो ।

- एन्डी ग्रोभ, इन्टेल कपोरिसनका पूर्वप्रमुख

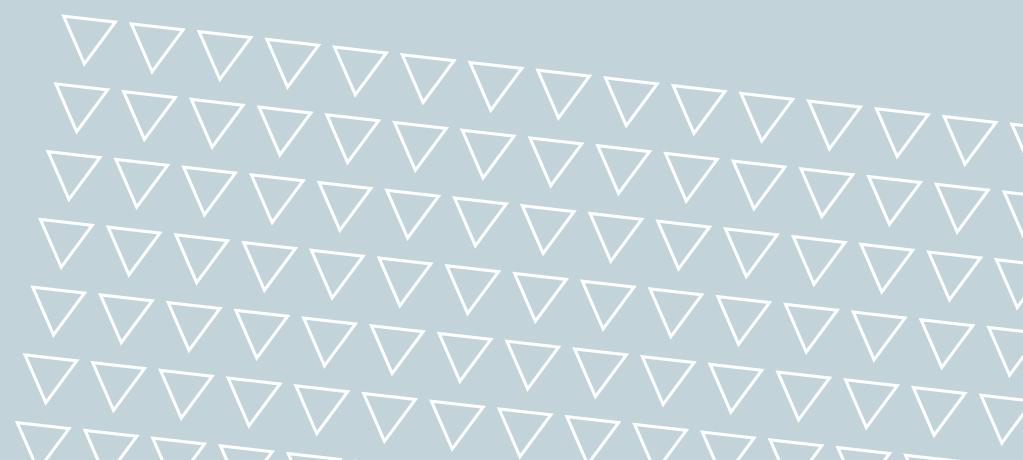
Internet इन्टरनेट

के गर्ने ?

- ▷ अध्ययन, अनुसन्धान र शिक्षाका साथै मनोरञ्जन एवं विभिन्न सरकारी र अन्य सेवा लिनका लागि प्रयोग गर्नुपर्छ ।
- ▷ इन्टरनेटका प्रयोग र जोखिमका बारेमा साथीभाइ र परिवारसँग नियमित छलफल गर्नुपर्छ एवं सुरक्षित प्रयोगका उपायहरू अपनाउनुपर्छ ।
- ▷ इन्टरनेट प्रयोगको नियम बनाउनुपर्छ । इन्टरनेटमा गरेका कामहरूबारे कुरा गर्ने, इन्टरनेट वा सोसल मिडियामा राख्न हुने/नहुने सामग्रीहरू निश्चित गर्ने, इन्टरनेटबाट डाउनलोड गर्न हुने/नहुने सामग्रीहरू र प्रयोगबारे जानकारी राख्नुपर्छ ।
- ▷ इन्टरनेट प्रयोग गर्दा कुनै शाङ्कास्पद वा नरमाइलो अनुभव भएमा साथीभाइ वा शिक्षक/अभिभावकलाई भन्नुपर्छ र सल्लाह लिनुपर्छ ।
- ▷ नियमितरूपमा केही समय इन्टरनेट र उपकरणबाट टाढा रहने अभ्यास डिजिटल डिटक्स गर्नुपर्छ ।

के नगर्ने ?

- ▷ अश्लील र अन्य गैरकानुनी सामग्रीहरूमा पहुँच बनाउने वा त्यस्ता सामग्री डाउनलोड गर्ने वा अरूसँग सेयर गर्ने गर्नकहुन्न ।
- ▷ इन्टरनेट ब्राउजरमा आफ्ना पासवर्डहरू सेभ गर्नुहुँदैन र अरूले चलाउन मिल्ने कम्प्युटरमा इन्टरनेट चलाउनुभएको छ भने आफू उद्देने बेला ब्राउजरको इतिहास मेट्नुपर्छ ।
- ▷ इन्टरनेटको ज्यादा प्रयोग पनि एकखालको मनोरोग भएको हुँदा यसलाई कुलत बनाउनुहुँदैन । त्यो भनेको चौबीसै घण्टा इन्टरनेटमा रहनुहुँदैन र इन्टरनेटबाहिरको काम र सम्बन्धलाई पनि समय दिनुपर्छ ।
- ▷ इन्टरनेटको प्रयोग गरी जुवा खेल्ने, धम्की दिने, उत्पीडन दिने, गाली/बेइज्जती गर्ने, ह्याकिड गर्ने, पैसा चोर्ने जस्ता गैरकानुनी कार्यहरू गर्नुहुँदैन ।





Unit 6

Chat/Messenger/Email

च्याट / मेसेन्जर / ईमेल

हामी सन्देश आदान-प्रदान गर्न इन्टरनेट प्रयोग गर्छौं । साथीभाइ वा आफ्नतर्सँग सम्पर्क राखिराख्न, एवं चिठ्ठीपत्र पठाउन वा प्राप्त गर्न इन्टरनेटले सहज बनाएको छ । यस्ता सन्देश आदान-प्रदान च्याटमा पनि हुन सक्छ वा ईमेलमा पनि हुन सक्छ । च्याट भनेको हामीले कुनै अन्य व्यक्ति वा समूहसँग लिखित वा आवाज वा भिडियोमा कुराकानी गर्ने हो भने ईमेल विद्युतीय चिठ्ठी हो ।

च्याटका लागि सर्वाधिक प्रयोग हुने एप्हरू फेसबुक मेसेन्जर, ह्वाट्रसएप, भाइबर, स्न्यापच्याट, इमो, र जुम हुन् भने ईमेलका लागि हामी धेरै जिमेल वा आउटलुक वा हटमेल प्रयोग गर्छौं । च्याट वा ईमेलमा हामीले गोप्य र निजी राख्नुपर्ने संवेदनशील जानकारीहरू धेरै हुन्छन् । अनलाइन गेमहरूमा पनि च्याटको सुविधा हुन्छ ।

के गर्ने ?

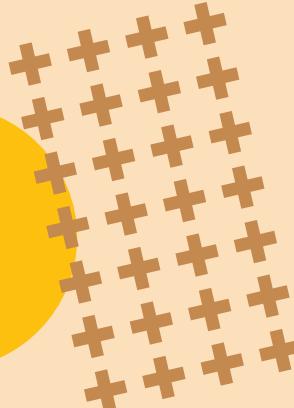
- ▷ आफ्ना च्याट वा ईमेल खाताहरूमा बलियो पासवर्ड र 2-step verification राख्नुहोस् ।
- ▷ च्याट वा ईमेलको सुरक्षा र गोपनीयतासम्बन्धी सेटिङमा गई राप्ररी अध्ययन गर्नुहोस् र आफू एवं आफ्नो तथ्याङ्कसम्बन्धी प्रावधानहरू परिवर्तन गर्नुहोस् ।
- ▷ सुरक्षा बढी भएका सन्देश आदान-प्रदान एप्हरू प्रयोग गर्नुहोस् । दुईतर्फी इन्क्रिप्सन भएका च्याट एप प्रयोग गर्दा तपाईंको सन्देश बीचमा अस्त्वे हेर्न सक्दैन । यस्ता एप्हरूमा सिनल, वायर वा ह्वाट्रसएप प्रयोग गर्नुहोस् ।

- ▷ अनावश्यक च्याट र ईमेलहरू मेट्नुहोस् । विशेषगरी अरूका संवेदनशील जानकारी भएका च्याट वा ईमेलहरूको प्रायोजन सकिनेबित्तिकै मेट्नुपर्छ ।
- ▷ च्याटमा प्रापकले हेरेपछि आफै मेटिने सुविधा हुन्छन् । संवेदनशील वा अरूले थाहा पाउँदा आफूलाई अफ्टेरो पर्ने कुराहरू च्याट गर्दा त्यो सुविधा प्रयोग गर्नुहोस् ।
- ▷ च्याट वा ईमेलमा कसैले तपाइँलाई यौनजन्य सामग्री पठाउँछ वा माघ्छ, तपाइँलाई तनाव हुने वा असहज बनाउने कुरा गर्दा भन्ने त्यस्ता खाता ब्लक गर्नुहोस् र साथीभाइ वा शिक्षक/अभिभावकलाई भन्नुहोस् ।



पहिले कुनै कुरा सार्वजनिक गर्न महँगो र त्यसलाई निजी राख्न सस्तो हुने गर्थ्यो । अहिले कुनै कुरा निजी राख्न महँगो र त्यसलाई सार्वजनिक गर्न सस्तो भएको छ ।

- क्ले सिर्की, सोसल मिडिया प्राध्यापक





Chat/Messenger/Email

च्याट / मेसेन्जर / ईमेल

- च्याटका लागि सकिन्छ भने निश्चित समय तोक्नुहोस् र अन्य काम एवं निन्दालाई असर पारेर च्याटमा व्यस्त हुनु स्वास्थ्यलाई राप्रो हुँदैन भने बुझ्नुहोस् ।
- धेरै संवेदनशील ईमेल आदान-प्रदानका लागि इन्क्रिप्सन प्रयोग गर्नुपर्छ ।

के नगर्ने ?

- चिनजान नभएका वा अनावश्यक मानिससँग च्याट नगर्नुहोस् ।
- ईमेल वा च्याटमा सकेसम्म संवेदनशील कुराहरू लेखेर नपठाउनुहोस् । नपठाए पनि हुने कुरा नपठाएकै बेस हुन्छ र पठाउनैपर्ने छ भने च्याटमा प्रापकले हेरेपछि आफै मेटिने सुविधा प्रयोग गर्नुहोस् ।
- नम वा यौनजन्य तस्बिर वा भिडियो नपठाउनुहोस् । आफै प्रेमी/प्रेमिका वा श्रीमान्/श्रीमतीलाई पनि

त्यस्तो तस्बिर नपठाउनुहोस् । पठाउनैपर्ने अवस्थामा अनुहार जस्ता पहिचान खुल्ने कुरा नभएका पठाउनुहोस् ।

- अन्य व्यक्तिका बारेमा खराब वा नराप्रो कुराहरू नलेख्नुहोस् । हाम्रा प्रत्येक च्याट र ईमेल सार्वजनिक हुन सक्छ भने कुरामा सचेत रहनुहोस् ।
- आफ्ना व्यक्तिगत पहिचानका र गोप्य जानकारीहरू सकेसम्म कम पठाउनुहोस् ।
- यौनजन्य कुराकानीबाट सकेसम्म परै बस्नुहोस् ।
- अनलाइन सम्पर्क भएका अपरिचित व्यक्तिहरूसँग नभेद्नुहोस् । भेटैनैपर्ने भए साथी लिएर बजार जस्ता सार्वजनिक स्थानमा भेद्नुहोस् । एकान्त हुन सक्ने होटल वा रेस्टुरेन्ट वा घर जस्ता स्थानमा नभेद्नुहोस् ।
- च्याट वा ईमेलमा आएका लिङ्क नखोल्नुहोस् । खोल्नै पर्ने भएमा कपी गरेर अर्को ब्राउजरमा खोल्नुहोस् ।



Unit 7

Computer/Mobile Games

कम्प्युटर/मोबाइल गेम

इन्टरनेटको प्रयोग मनोरञ्जनका लागि पनि हुन्छ र मनोरञ्जनको एउटा माध्यम भनेको फोर्टनाइट वा पब्जी जस्ता अनलाइन गेम खेल्नु पनि हो । अनलाइन गेमहरू मानसिक विकास र समय बिताउन उपयोगी हुन सक्छन् तर यसका खतरा पनि छन् ।

अनलाइन गेम धेरैजसो समूहमा खेलिन्छ र यसको आफै समुदाय हुन्छन् । यस्ता समुदायमा अपरिचितहरू पनि हुन्छन् । अनलाइन गेममा धेरैजसो च्याट वा कुराकानी गर्न सकिन्छ । गेमअनुसार कतिपय अवस्थामा कोड भाषा पनि प्रयोग हुन्छ ।

कतिपय गेममा भर्चुअल रियालिटी वा अगमेन्टेड रियालिटी प्रयोग हुन्छ जसले ती गेम खेल्ने प्रयोगकर्तालाई साँच्चैको अवस्थामा भएको भान गराउँछ ।

अनलाइन वा मोबाइल गेमको खतरा भनेको यसको कुलत, यसमा हुन सक्ने उत्पीडन, यसका हिंसा वा अन्य दृश्यले पार्न सक्ने मानसिक आघात र हाप्रो गोपनीयता राख्नुपर्ने कुराहरू सार्वजनिक हुन सक्ने अवस्था हो ।



भिडियो गेमहरूको एउटै उद्देश्य मात्रै हुन्छ:
रमाइलो । सबैका लागि रमाइलो ।

- इवाता सातरू, भिडियो गेम प्रोग्रामर

Computer/Mobile Games

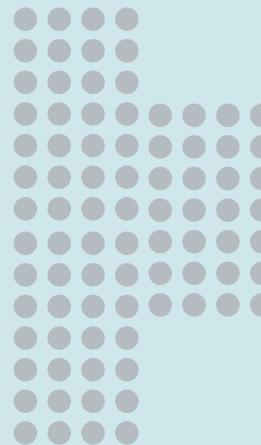
कम्प्युटर / मोबाइल गेम

के गर्ने ?

- ▷ आफ्नो उमेर र रुचिअनुसारका गेम छानेर खेल्नुपर्छ । अरूले खेलेको भन्दैमा ठूला उमेर समूहका लागि बनाइएका खेलहरू वा हिंसात्मक खेलहरू छान्नुहुँदैन ।
- ▷ गेमका लागि प्रोफाइल बनाउँदा व्यक्तिगत जानकारी नदिने गरी बनाउनुपर्छ । नाम वा तस्विर फरक छान्न सकिन्छ । गेमिङका लागि नाम नखुल्ने छुटै इमेल बनाउन सकिन्छ ।
- ▷ खाता बनाइसकेपछि खेल्नुअघि गेमका सुरक्षा र गोपनीयतासम्बन्धी सेटिङहरू हेरेर आवश्यक परिवर्तन गर्नुपर्छ ।
- ▷ हिंसा वा यौन वा अन्य दृश्यले असहज बनाउँछ भने त्यस्तो गेम खेल्न छोड्नुपर्छ । बारम्बार त्यसको सम्भन्ना आइरहने अवस्था भए शिक्षक वा अभिभावकको सहयोग लिनुपर्छ ।
- ▷ अनलाइन गेमिङका लागि निश्चित समय तोक्नुपर्छ । रातभर वा लामो समयसम्म खेलेर यसलाई कुलत बनाउनुहुँदैन ।

के नगर्ने ?

- ▷ गेमका च्याट वा कुराकानीमा आफ्नो वास्तविक नाम, ठेगाना वा अन्य असान्दर्भिक व्यक्तिगत जानकारीहरू भन्नुहुँदैन ।
- ▷ गेमिङ समुदायलाई सकेसम्म त्यहीं सीमित राख्नुपर्छ ।
- ▷ गेमका बेला उत्पीडन हुन सक्ने बोली वा धम्कीहरू आएमा सहनुहुन्न र त्यस्तो समुदायबाट बाहिरिनुपर्छ । आफूमाथि उत्पीडन भएको अवस्थामा रिपोर्ट गरेर शिक्षक / अभिभावकलाई भन्नुपर्छ ।
- ▷ गेमका विषयमा चिटकोड या अन्य यस्तै भनी आएका फाइलहरू डाउनलोड गर्नुहुँदैन । ती भाइरस वा जासुसी एप पनि हुन सक्छन् ।
- ▷ चोरी गरिएका वा क्र्याक गरिएका गेम डाउनलोड गर्नुहुँदैन ।





Unit 8

Mobile Phone

मोबाइल फोन

हामी सबैको हातमा मोबाइल फोन छ । हामी धेरैजसो इन्टरनेट मोबाइल फोनबाटै चलाउँछौं र मोबाइलमा हाम्रा कल रेकर्ड र एसएमएस सन्देशहरू अनि तस्बिर र भिडियो मात्रै होइन, हामीले चलाउने एप र तिनका डेटा पनि हुन्छन् ।

हाम्रो सबै भन्दा धेरै तथ्याङ्क भण्डारण भएको उपकरण मोबाइल फोन हो । यो अरू कसैले हात पारे हाम्रो सबै भन्दा धेरै गोपनीयता भज्ञ हुने कुराहरू थाहा पाउन सक्छ ।

मोबाइल फोनका विषयमा जानुपर्ने पहिलो कुरो भनेको हाम्रो फोनको प्रयोगसम्बन्धी धेरै तथ्याङ्क फोन कम्पनीमा हुन्छ भन्ने हो । त्यस्तो तथ्याङ्कमा हामीले कसलाई कहिले फोन गच्छौं र कर्ति समय कुरा गच्छौं, हामीले कसलाई के

एसएमएस पठायौं, हामीले कतिबेला कतिबेर इन्टरनेट चलायौं र कुन समयमा हामी कहाँ छौं, अनि हाम्रा फोन सम्वादहरू हामीले फोन गरेको व्यक्तिले रेकर्ड गर्न सक्छ र सन्देशहरू ऊसँग पनि हुन्छ भनेर जानुपर्छ ।

मोबाइल फोनमा करिपय एफहरूले पनि ती सबै तथ्याङ्कमाथि पहुँच बनाएका हुन्छन् र तिनका निर्माणकर्ता कम्पनी वा व्यक्तिले ती तथ्याङ्क प्राप्त गर्न सक्छन् ।

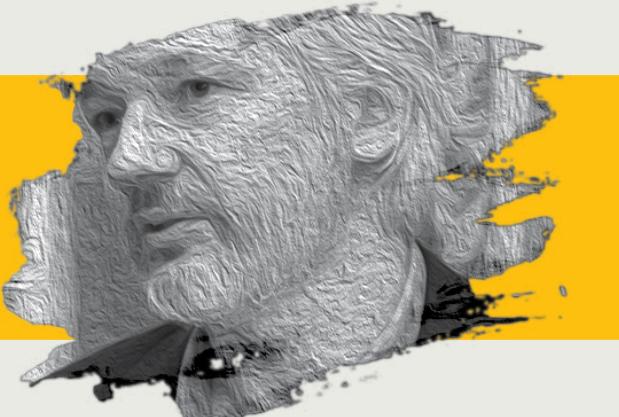
मोबाइल फोनमा सोसल मिडिया, ईमेल, च्याटका पासवर्डहरू सेभ हुन्छन् भने हामीले करिपय अवस्थामा पासवर्ड वा ब्याङ्क कार्डको पिन जस्ता आफ्ना गोप्य जानकारी राखेका हुन सक्छौं । त्यस्तै त्यसमा हामीले खिचेका तस्बिर र भिडियो मात्रै नभई हामीलाई अरूले पठाएका तस्बिर वा भिडियोहरू पनि हुन सक्छन् ।

के गर्ने ?

- ▷ फोनमा बलियो पासवर्ड राख्नुपर्छ । पिन वा प्याट्रन भन्दा पासवर्ड बढी सुरक्षित हुन्छ ।
- ▷ फोनको सेटिङ्गमा गएका लोकेसन सेयरिडलाई अफ गर्नुहोस् । अनि सुरक्षा र गोपनीयतासम्बन्धी प्रावधानहरू राम्रारी हेरेर आवश्यक परिवर्तन गर्नुहोस् ।
- ▷ फोनमा पनि एन्टीभाइरस र एन्टीस्पाइवेयर एप राखेर बेलाबेलामा अपडेट र स्क्यान गर्नुपर्छ ।
- ▷ घर वा सुरक्षित स्थानमा भएको बेला फोनलाई सकेसम्म हातले सजिलै नभेट्ने स्थानमा वा अन्य अवस्थामा हातमा लिनु भन्दा खल्तीमा राख्नुहोस् ।
- ▷ फोनको सिस्टम र भएका एफहरूलाई नियमित अपडेट गर्नुहोस् ।
- ▷ प्रयोग नहुने अवस्थामा यसको ब्लुटुथ र वाइफाइ अफ गरेर राख्नुहोस् ।

मोबाइल फोन एउटा निगरानी राख्ने यन्त्र हो जसबाट फोन गर्न पनि मिल्छ ।

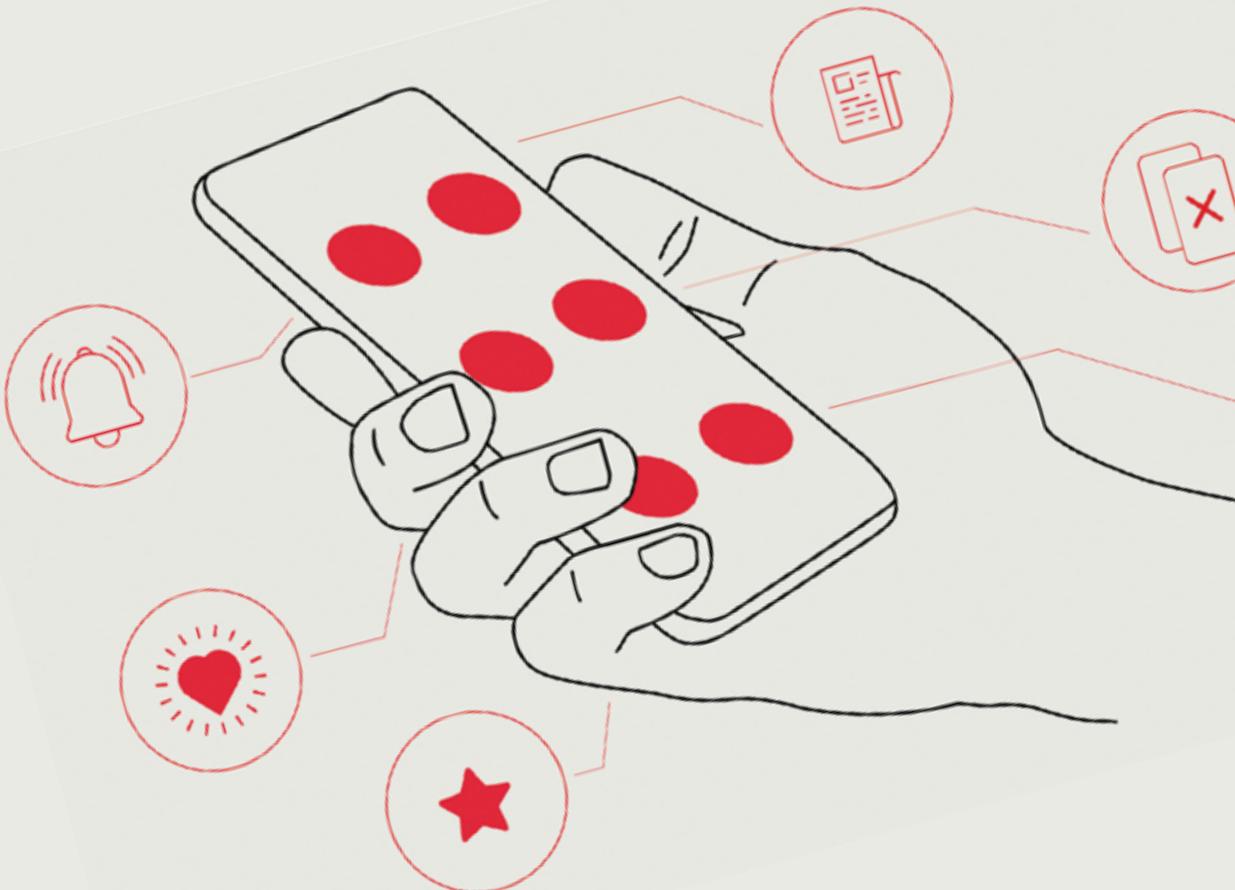
- जुलियन असान्ज, विकिलिक्सका संस्थापक



- ▷ फोनमा भएका महत्वपूर्ण कुराहरू कम्प्युटर वा क्लाउड स्टोरेजमा ब्याकअप गरेर राख्नुहोस् ।
- ▷ फोनका संवेदनशील डेटालाई सकेसम्म मेमोरी कार्डमा भण्डारण हुने सेटिङ गर्नुहोस् ।

के नगर्ने ?

- ▷ फोनमा अनावश्यक र थाहा नभएका एफहरू राख्नुहुँदैन । निःशुल्क भनिएका धेरै एप्ले हाप्रो तथ्याङ्कमा पहुँच बनाउँछन् । अझ जथाभावी डाउनलोड गरिएका एफहरू त खतरनाक हुन सक्छन् ।
- ▷ आफै फोन त हो भनेर त्यसमा संवेदनशील तस्क्रिप्ट, भिडियो वा जानकारीहरू राख्नुहुँदैन । राख्नैपर्ने अवस्थामा सेक्युर फोल्डर भने सुविधा प्रयोग गरेर बलियो पासवर्ड भित्र राख्नुपर्छ ।
- ▷ आफू भएको स्थानको गोपनीयता राख्नुपर्ने अवस्थामा फोन नलिइ जानुपर्छ । तर सुरक्षाका हिसाबले कमजोर ठाउँमा फोन नहुँदा सहयोग मान्न सकिँदैन भन्ने पनि रुखाल राख्नुपर्छ ।
- ▷ मर्मतका लागि दिनुपर्ने अवस्थामा फोन नछाड नुहोस् । आफै अगाडि मर्मत गर्न लगाउनुहोस् । सकेसम्म विश्वसनीय स्थानमा मात्रै मर्मत गर्न दिनुहोस् । छाइनुपर्ने अवस्थामा त्यसको मेमोरी कार्ड निकालेर राख्नुहोस् ।
- ▷ आफ्नो मोबाइलमा एसएमएस वा मेसेजिङ एप्मार्फत आएका कुनै पनि नम्बर अरू कसैलाई नभनुहोस् । ओटिपी भनिने यस्ता नम्बरहरू लिएर अरूले हाप्रो खाता ह्याक गर्न सक्छन् ।



Unit 9

Password

पासवर्ड

पासवर्ड साँचो जस्तै हो जसले हाम्रो कम्प्युटर जस्ता उपकरण वा सोसल मिडिया वा अन्य खातामा लागेको ताल्चा खोल्छ । सामान्यतया इन्टरनेटका कुनै पनि सुविधा प्रयोग गर्दा युजरनेम र पासवर्ड राख्नुपर्छ । युजरनेम सार्वजनिक हुन्छ भने पासवर्ड गोप्य हुन्छ ।

हाम्रा खाता र तथ्याङ्क त्यतिबेला सुरक्षित रहन्छ जतिबेलासम्म हाम्रो पासवर्ड अरूले थाहा पाउँदैनन् । तर कतिपय सोसल मिडियामा पासवर्डहरू ह्याक गरेर लिक गरिएका छन् । त्यसैले हामीले सुरक्षित राख्नदैमा मात्रै हाम्रो पासवर्ड सुरक्षित हुन्छ भन्ने निश्चित हुँदैन ।

पासवर्ड बलियो बनाउनुपर्छ । बलियो पासवर्ड बनाउन निम्न कुरा ख्याल राख्नुपर्छ :

- पासवर्ड कम्तीमा १२ अक्षरको हुनुपर्छ ।
- पासवर्डमा अङ्क, अक्षर र सङ्केत चिह्नहरू हुनुपर्छ ।
- पासवर्डमा शब्दकोशमा भेटिने शब्दहरू प्रयोग गर्नुहुन्न ।
- पासवर्डमा फोन नम्बर वा स्थान वा व्यक्तिको नाम वा घर नम्बर वा जन्म मिति प्रयोग गर्नुहन्न ।
- पासवर्ड आफूले भने सजिले सम्झन सकिने हुनुपर्छ ।

सबैतिर एउटै वा १-२ वटा पासवर्ड प्रयोग गर्नु भन्दा फरक-फरक पासवर्ड प्रयोग गर्नु उत्तम हुन्छ । सम्झन गाह्रो हुने भए उसैखाले तर २-४ अक्षर फरक भएका पासवर्ड प्रयोग गर्न सकिन्छ ।

अहिले सबैजसो इन्टरनेट सुविधामा 2-step verification को प्रावधान हुन्छ, त्यसलाई प्रयोग गर्नुपर्छ । यो भनेको कुनै खातामा पहुँच बनाउन पासवर्ड र थप अर्को कदम राख्ने हो । थप कदममा एसएमएसमा आउने नम्बर प्रयोग गर्ने वा अथेन्टिकेटरमा मिनेटैपिच्छे परिवर्तन हुने नम्बर प्रयोग गर्ने वा युएसबी साँचो प्रयोग गर्ने हुन सक्छन् । एसएमएस राख्नदाको फाइदा भनेको कसैले आफ्नो पासवर्ड थाहा पाएर आफ्नो खाता खोल्न चाहेको थाहा हुने अवस्था हो ।

के गर्ने ?

- अङ्क, अक्षर र सङ्केत चिह्न मिलाएर लामो र बलियो पासवर्ड बनाउनुपर्छ ।
- इन्टरनेटका खाताहरूमा 2-step verification प्रयोग गर्नुपर्छ ।

- ▶ प्रत्येक खाताका लागि सकेसम्म छुट्टाछुट्टै पासवर्ड प्रयोग गर्नुपर्छ ।
- ▶ पासवर्ड समय/समयमा परिवर्तन गर्नुपर्छ ।

के नगर्ने ?

- ▶ पासवर्ड कसैलाई दिनुहुँदैन । आफ्ना पुराना पासवर्ड पनि गोप्य राख्नुपर्छ ।
- ▶ पासवर्ड कतै लेखेर राख्नु पनि हुँदैन ।
- ▶ पासवर्ड बनाउँदा सजिलो हुन्छ भनेर किबोर्डमा लहरै भएका अक्षरहरू राख्नुहुँदैन ।
- ▶ सकेसम्म निःशुल्क वाइफाइ चलाउनु हुँदैन र चलाएको अवस्थामा पनि सकेसम्म पासवर्ड हालेर खाता खोल्ने जस्ता काम गर्नुहुँदैन ।
- ▶ सेभ पासवर्ड भन्ने सुविधा प्रयोग गर्नुहुँदैन । यसरी सेभ गरिएका पासवर्ड तपाइँको कम्प्युटरमा सजिलै हेर्न सकिन्छ ।
- ▶ अरूले पनि चलाउने कम्प्युटरमा पासवर्ड हाल्दा ख्याल पुऱ्याउनुपर्छ । काम सकेपछि लगआउट गरेर ब्राउजर बन्द गरेर मात्रै उठनुपर्छ ।



पासवर्डलाई टुथब्रस मान्नुहोस् । अरूलाई प्रयोग
गर्न नदिनुहोस् र समय/समयमा बदल्नुहोस् ।

- किलफोर्ड स्टल, अमेरिकी लेखक

३५
१००^०



Unit 10

Photo/Video

फोटो र भिडियो

हामी सबै सोसल मिडियामा आफ्ना तस्बिर र भिडियो हाल्छौं। फेसबुक र इन्स्टाग्राममा तस्बिर एवं टिकटकमा भिडियो धेरै हालिन्छ।

तस्बिर र भिडियोबाट हामी एकआपसलाई अपडेट गर्छौं, त्यसमा आउने कमेन्ट वा लाइकबाट खुसी हुन्छौं। कतिपय कार्यक्रम र समारोहमा हामी राम्रा तस्बिरका लागि मेहनत पनि गर्छौं। टिकटकका लागि त हामी सार्वजनिक स्थान वा समारोहमा समेत भिडियो खिचिरहेका हुन्छौं। नाचगान वा अन्य कुनै घटना हामी फेसबुकमा लाइभ गर्न वा टिकटकमा भिडियो बनाउन खिच्ने गर्छौं।

इन्टरनेट वा सोसल मिडियामा तस्बिर वा भिडियो हाल्दा सचेत हुनुपर्ने विषय भने छन्। ती विषय भनेको व्यक्तिगत गोपनीयता, उत्पीडन वा दुरुपयोगको सम्भावना र हाप्रो मानसिक स्वास्थ्यसँग सम्बन्धित छन्।

के गर्ने ?

- ▷ तस्बिर वा भिडियो हाल्दा ती कुरा इन्टरनेटमा स्थायी हुन्छन्, मेर्टेंडैन भने सम्भनुपर्छ।
- ▷ तस्बिर वा भिडियोमा अरु व्यक्ति छन् भने त्यस्ता

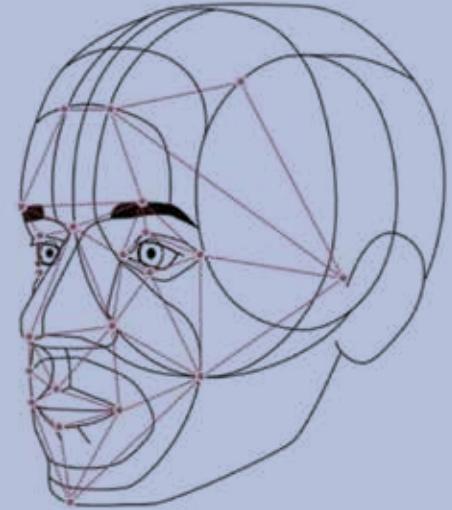
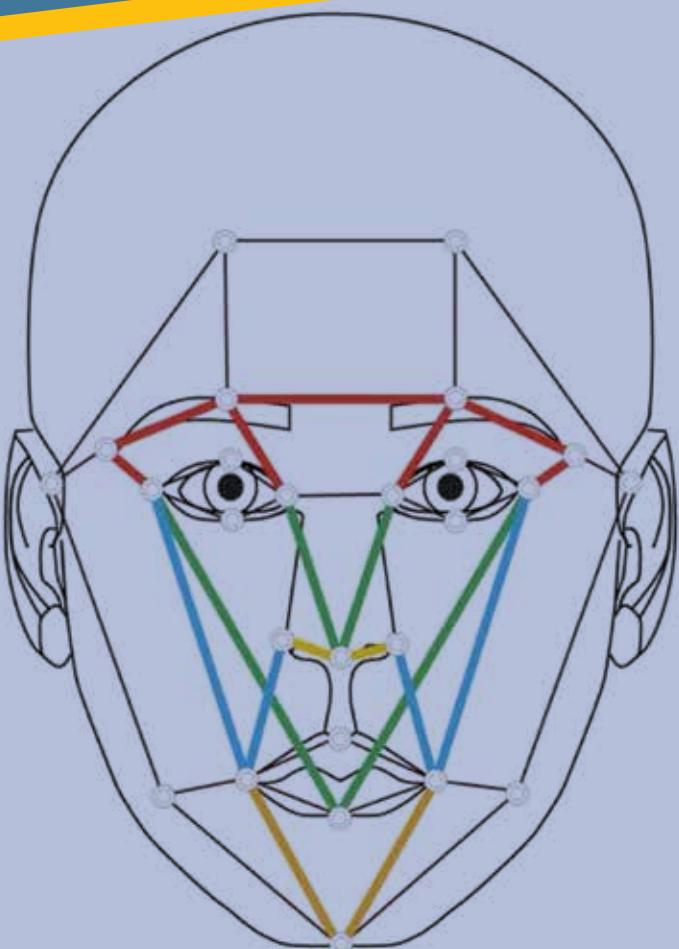
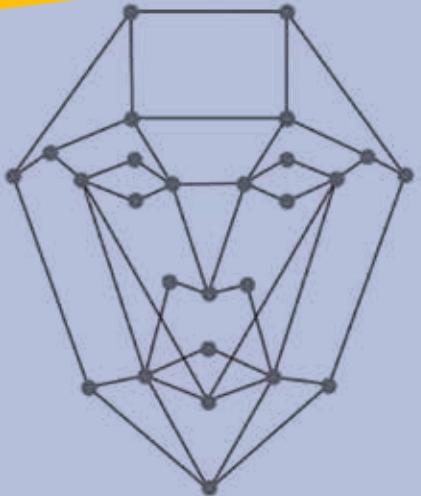
तस्बिर वा भिडियो इन्टरनेटमा हाल्नुअघि उनीहस्तको अनुमति लिनुपर्छ। कम्तीमा तस्बिर खिच्ने बेला वा हाल्ने बेला म यो इन्टरनेटमा हाल्छु है भन्नुपर्छ।

- ▷ कतिपय सोसल मिडियामा तस्बिर वा भिडियो कसले हेर्न पाउँछ भनेर सेटिङ गर्न मिल्छ। फेसबुक वा टिकटकमा आफ्ना साथीहस्तले मात्रै हेर्न मिल्ने गरी हाल्नुपर्छ।
- ▷ फोटो र भिडियो हालेको महिना दिन वा यस्तै निश्चित समयपछि तिनलाई प्राइभेट बनाउनुपर्छ।
- ▷ बालबालिकाको तस्बिर वा भिडियो हाल्दा विशेष सचेत रहनुपर्छ। सकेसम्म बालबालिकाका तस्बिर वा भिडियो नहाल्नु ठीक हुन्छ।
- ▷ तस्बिर वा भिडियो हालिसकेपछि त्यसमा आएका कमेन्टहरू हेर्नुपर्छ, असहज हुनेखालका कमेन्टहरू आएका छन् भने त्यस्तालाई मेट्नुपर्छ वा रिपोर्ट गर्नुपर्छ।
- ▷ आफ्नो तस्बिर वा भिडियो कसैले दुरुपयोग गरेको थाहा भएमा सकेसम्म छिटो प्रहरी वा शिक्षक/अभिभावकको सहयोग लिनुपर्छ।

के नगर्ने ?

- ▷ सकेसम्म इन्टरनेटमा तस्बिर हाल्दा दुरुपयोग हुन सक्नेखालका तस्बिरहरू हाल्नुहुँदैन। मूलत: एकलै भएका वा टाउको वा शरीरलाई सजिलै परिवर्तन गर्न सकिनेखालमा तस्बिरहरू हाल्दा ध्यान दिनुपर्छ।
- ▷ तुरुन्तै वा भविष्यमा सार्वजनिक हुँदा आफूलाई अफेरो पर्न सक्ने तस्बिर र भिडियोहरू हाल्नुहुँदैन।
- ▷ अरुका तस्बिर वा भिडियोको अधिकार हामीसँग हुँदैन त्यसैले अरुको सर्वाधिकार भएका तस्बिर वा भिडियो हाल्नुहुँदैन।
- ▷ विशेषगरी गीत/सङ्गीत वा चलचित्र वा टिभी कार्यक्रमका भिडियोहरू अनुमतिबिना इन्टरनेटमा राख्नु हुँदैन।
- ▷ तस्बिर वा भिडियो लाइक वा कमेन्टका लागि नराख्नुहोस् वा तिनमा आएका लाइक वा कमेन्टलाई धेरै महत्त्व दिनुहुँदैन।

आफ्नो गोप्य तस्बिर वा भिडियो दुरुपयोग भएको थाहा भएमा त्यसलाई इन्टरनेटबाट हटाउन www.stopncii.org प्रयोग गर्न सकिन्छ। स्टप नन-कसेन्सुअल इन्टिमेट इमेजको वेबसाइटमा गाएर प्रत्येक त्यस्ता तस्बिरका लागि क्रियट द केस थिचेर प्राप्त निर्देशन अनुसार गर्नुपर्छ।



तपाइँका १४ तस्बिर देखाउनुहोस्, हामी
तपाइँलाई चिन्नेछौं।

- एरिक सिमट्स, गुगलका पूर्वप्रमुख



Unit 11

Our Data

हाम्रो डेटा

इन्टरनेट, मोबाइल फोन, कम्प्युटर वा स्मार्ट उपकरणमा हाम्रोबारे के/कस्ता जानकारी भण्डारण हुन्छ ?

हाम्रो कम्प्युटरमा हाम्रा फाइलहरू, हाम्रो कम्प्युटर प्रयोग बानीबेहोरा, कुन/कुन साइट हेच्याँ भन्ने जानकारी र पासवर्डहरू पनि भण्डारण भएका हुन सक्छन् ।

मोबाइलमा कम्प्युटर भन्दा धेरै जानकारी हुन्छ र धेरैजसो एपहरूमा पासवर्ड हाल्नै नपर्ने गरी चल्ने हुन्छन् ।

मोबाइलमा फेसबुक वा मेसेन्जर जस्ता एपहरूका पासवर्ड सेभ भएका हुन्छन् । कसैले हाम्रो फोन खोल्न सक्यो भने उसले लगभग हाम्रो सबै एपमा पहुँच पाउँछ ।

हामीले चलाउने सोसल मिडियाको कम्पनीसँग हामीले राखेका सबै अक्षर, तस्बिर, लाइक वा साथीका बारेमा जानकारी हुन्छ । हामीले मेटे पनि ती उनीहरूसँग हुन्छ । त्यस्तै हाम्रा बानीबेहोरा, हामीलाई मन पर्ने र नपर्ने कुराहरू, हामीले पढेका लिङ्गहरू वा हेरेका विज्ञापनका आधारमा हाम्रो मनोविज्ञान र विचारका बारेमा पनि उनीहरूलाई धेरै जानकारी हुन्छ । त्यसको विश्लेषण गरेर हाम्रा व्यक्तिगत रुचि/भुकाव आदिसम्बन्धी थप सूचनासमेत थाहा पाउँछन् ।

फेसबुक मात्रै होइन, हामीले चलाउने अन्य सोसल मिडिया वा मोबाइल एपहरूमा पनि हाम्रा व्यक्तिगत सूचना उत्तिकै हुन्छन् । एन्ड्रोइड फोन प्रयोग गर्नेहरूको धेरै जानकारी गुगलसँग हुन्छ र हामीले हामी कुन स्थानमा छौं भनेर थाहा पाउने जस्ता कतिपय कुरा बन्द गरे पनि ती पूर्णरूपमा बन्द भएका हुँदैनन् । गुगलले चाहेमा त्यस्तो जानकारी प्राप्त गर्न सक्छ ।

हाम्रा मोबाइल फोन कम्पनीसँग हामीले कस/कसलाई कतिबेला कहाँबाट फोन गच्याँ वा के मेसेज पठायाँ वा कुन बेला इन्टरनेट चलायाँ र कुन साइट हेच्याँ भन्ने जानकारी हुन्छ ।

के गर्ने ?

यो कुरा थाहा पाउनैपर्छ : इन्टरनेटमा गोपनीयता हुँदैन । इन्टरनेटमा हामीले राखेका कुरा स्थायी हुन्छन् । कुनै पनि कुरा मेटिँदैनन् । हामीले मेटे पनि ती हामीले नदेखिने मात्रै हुन्छन् तर इन्टरनेटबाट मेटिएका हुँदैनन् ।

इन्टरनेट प्रयोगमा सावधानी अपनाउँदा केही गोपनीयता सम्भव हुन सक्छ ।

इन्टरनेटमा कुनै पनि नयाँ सुविधाको प्रयोग सुरु गर्दा सेटिङ्मा गाएर गोपनीयताका बारेमा भएका कुराहरू राम्रारी पढ्ने र सम्भव भएसम्म गोपनीयता कायम राख्ने व्यवस्था छनोट गर्ने गर्नुपर्छ ।

इन्टरनेटमा कुनै पनि कुरा लेख्दा, कुनै फोटो वा भिडियो हाल्दा त्यो कुरा आवश्यक नै हो कि हैन भनेर एकपटक सोच्ने गर्नुपर्छ । जहिले पनि आवश्यक कुरा मात्र त्यहाँ लेख्ने या राख्ने गर्नुपर्छ ।

इन्टरनेटमा सामग्री राख्दा वा लेख्दा यी सामग्री ५, १० वा २० वर्षपछि कसैलाई देखाउँदा वा कसैले हेर्दा के होला भन्ने सोचेर हाल्नुपर्छ ।

फेसबुक वा अन्य कुनै पनि सेवाको प्रयोग बन्द गर्नुअगाडि त्यो सेवामा भएका आफ्ना सबै कुरा मेट्नुपर्छ ।

धेरै व्यक्तिगत कुरा, जस्तो- फोन नम्बर वा घर नम्बर वा परिवार वा साथीभाइका कतिपय जानकारीहरू वा आफ्ना सोचाइ, विचार वा मुडका कुरा पनि इन्टरनेटमा



लेख्नुअगाडि सोच्नुपर्छ किनभने त्यस्ता
कुरा महत्वपूर्ण मात्रै होइन, हाप्रा
कमी/ कमजोरी र मनोविज्ञान उजागर
गरिदिने माध्यम र दुरुपयोग हुन सक्ने
'सूचना- औजार' पनि हुन् ।

इन्टरनेटमा एकपटक राखिएका कुरा
पूर्णरूपमा हटाउन असम्भव छ ।
त्यसैले इन्टरनेट वा सामाजिक सञ्जाल
वा मेसेन्जरमा केही कुरा लेखदा वा तस्बिर
भिडियो राख्दा सोच्नुहोस् : यो कुरा कुनै
पनि बेला सार्वजनिक हुन सक्छ ।



गोपनीयताको मृत्यु भयो, सोसल मिडियाको
हातमा बन्दूक छ ।

- पिट क्यासमोर, म्यासएबलका संस्थापक

भाग २

परिभाषा र जानकारी

Unit 12

Media and Information Literacy

मिडिया तथा सूचना साक्षरता

अहिलेको विश्वमा सूचनाको संसार भ्रामक बनेको छ । हामीलाई सूचनाका विभिन्न स्रोतबाट जातातै थरीथरीका सूचना द्वात गतिमा प्राप्त भइरहेका छन् । सूचनाको गति र सझुया धैरे भएको हुँदा हामीलाई सूचनाको परख गर्ने समय असाध्यै कम मिल्छ । सूचनाको परख गर्नु आफैमा सजिलो र छिटो हुने काम पनि होइन ।

मिडिया साक्षरता भनेको सामान्यरूपमा मिडियाका विभिन्न रूपका सामग्रीहरू प्राप्त गर्न, मूल्याइकन गर्न र निर्माण गर्न जाने क्षमता हो । त्यसबाहेक मिडियाका सामग्रीका सन्देश बुझन सक्ने, त्यस्तो सन्देश किन दिइरहेको छ भनेर सोचन सक्ने र त्यसबाट हामीलाई के प्रभाव पर्छ भनेर मूल्याइकन गर्न सक्ने सिप पनि मिडिया साक्षरता हो ।

यस हिसाबले मिडियाबाट वा अन्य माध्यमबाट प्राप्त सूचनालाई परख गर्न आवश्यक सिपहरूलाई नै मिडिया तथा सूचना साक्षरता भनिन्छ । मिडिया तथा सूचना साक्षर हुनका लागि निम्न ज्ञान र सिप आवश्यक पर्छ :

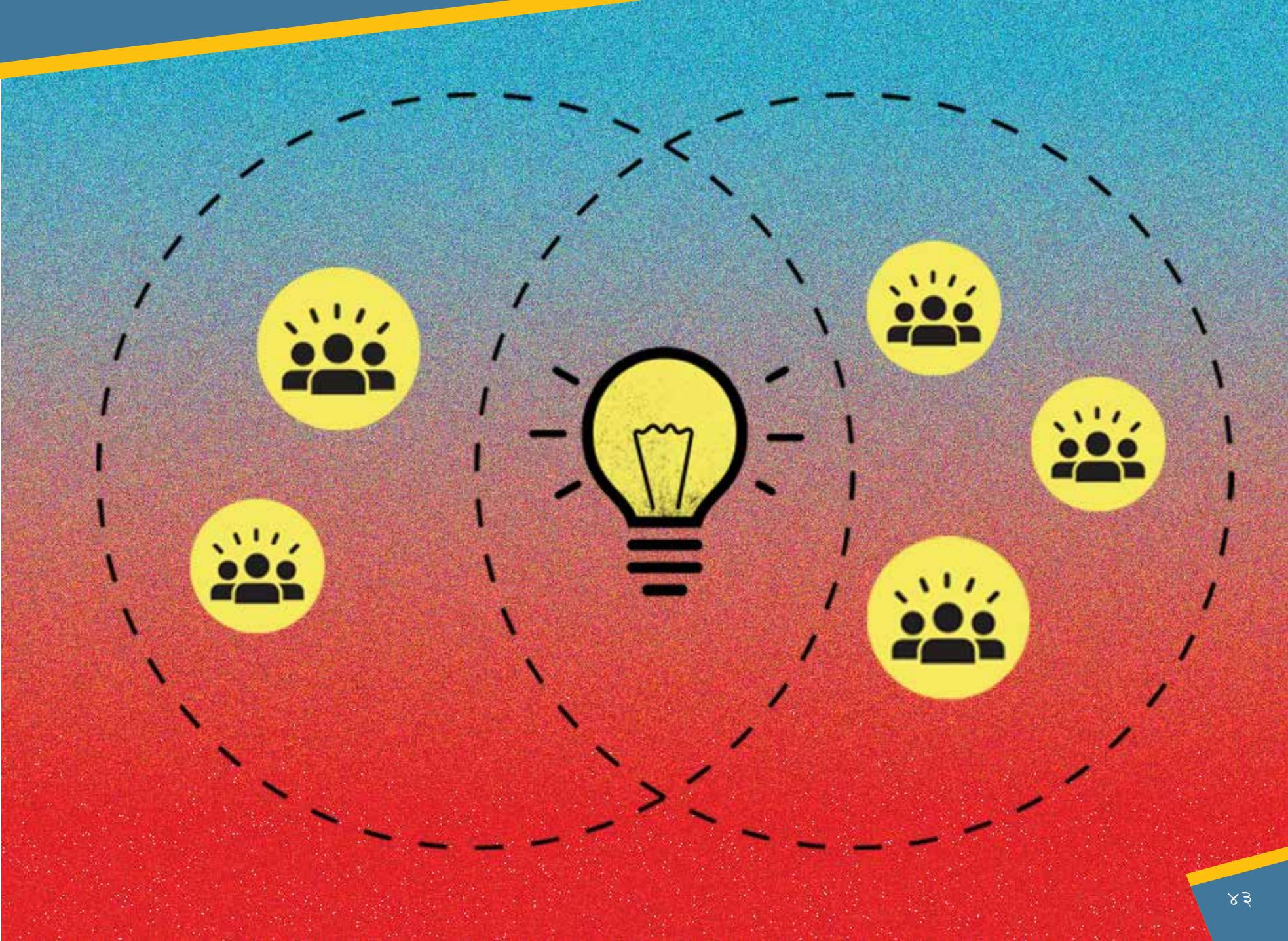
- ▷ मिडिया र सूचनासम्म पहुँच : सूचना प्राप्तिका स्रोत र उपकरणसम्म पहुँच, सूचना प्राप्त गरेपछि त्यसको मूल स्रोतबाटे जानकारी ।

- ▷ सूचनाको मूल्याङ्कन : प्राप्त सूचनामाथि यो सूचना किन यो रूपमा वा यो तरिकाबाट दिइयो र स्रोतका रूपमा किन कसैलाई प्रयोग गरियो भन्ने जस्ता प्रश्नको उत्तर खोज्ने प्रयास ।
- ▷ सूचना निर्माण/प्रकाशन : रेडियो, टिभी वा पत्रपत्रिकाका सामग्री कसरी कसले बनाउँछ वा सोसल मिडियाका सामग्री कसले कसरी बनाउँछ भन्ने ज्ञान र सिप ।
- ▷ सूचनामाथि आलोचनात्मक दृष्टि : प्राप्त सूचनाले के र कस्तो प्रभाव पार्न सक्छ वा ती सूचना कसले कुन प्रयोजनका लागि दिएको हुन सक्छ भन्ने आलोचनात्मक प्रश्न ।
- ▷ सूचनाको छनोट : माथिका चरण पार गरिसकेपछि सूचनाका सही स्रोत छाने र सूचना प्राप्तिपछि के गर्ने भन्ने कुराको अभ्यास ।

मिडिया र सूचना साक्षर व्यक्तिले

- ▷ शीर्षक पढेर, लेखक चिनेर र सूचनाको मिति हेरेर मिथ्या सूचना चिन्छन्
- ▷ सूचना परीक्षणका लागि फरक स्रोतहरू प्रयोग गर्छन्
- ▷ भाषाशैली हेरेर सूचना फैलाइएको कारण अध्ययन गर्छन्
- ▷ सूचनामा भएका अङ्क वा तथ्याङ्क कहाँबाट र कसरी आयो भन्ने विचार गर्छन्
- ▷ तस्विर वा चित्रहरू किन प्रयोग गरियो र त्यसले हामीलाई के असर गर्छ भन्ने थाहा पाउँछन्
- ▷ सूचना सामग्रीहरू आफै तयार गर्न सक्छन्
- ▷ सूचना सामग्रीको पक्ष/विपक्ष वा आग्रह/पूर्वाग्रह छुट्टाउन सक्छन्
- ▷ सूचना स्रोतको भरपर्दो सूची बनाउन सक्छन्

थप जानकारीका लागि सेन्टर फर मिडिया रिसर्च - नेपालको मिडिया र सूचना साक्षरता : प्रशिक्षक स्रोत पुस्तिका हेनुहोस् । यो पुस्तिका research.butmedia.org मा निःशुल्क उपलब्ध छ ।



Unit 13

Fact-Checking

तथ्य जाँच

तथ्य जाँच (fact-checking) एउटा विशिष्ट प्रकारको अभ्यास हो जसमा उपलब्ध प्रमाण वा तथ्याङ्क वा वैज्ञानिक आधार बन्न सक्ने अनुसन्धानका आधारमा कुनै सूचना तथ्यगत भए/नभएको परीक्षण गरिन्छ ।
तथ्य जाँचका लागि सामान्यरूपमा यीमध्ये सबै वा धेरै उपाय अवलम्बन गरिन्छ :

- इन्टरनेटमा खोजी,
- विज़हरूसँग सरसल्लाह,
- सम्बन्धित व्यक्ति वा निकाय वा संस्था वा समूहसँग जानकारी,
- प्रमाण (अडियो, भिडिओ वा दस्ताबेज, अध्ययन/अनुसन्धान वा तथ्याङ्क) को खोजी,
- आधिकारिक स्रोतको खोजी ।

तथ्य जाँचको नतिजा उपलब्ध तथ्यमा भर पर्छ । कुनै कुरा उपलब्ध नहुँदैमा त्यो मिथ्या नहुन पनि सक्छ वा तथ्य जाँच गर्दा फेला पार्न नसकिएको पनि हुन सकछ ।

तथ्य जाँच सिद्धान्तमा जसरी कुनै प्रमाणिवाना कुनै जानकारी तथ्य हुन सक्दैन, त्यसैगरी प्रमाण नभएका कुरा पनि मिथ्या हुन सक्दैनन् ।

कसरी गरिन्छ तथ्य जाँच ?

तथ्य जाँच फरक तरिकाले गर्न सकिन्छ । मिडिया र सोसल मिडियामा भाइरल भएका सूचनाहरूको तथ्य जाँच गर्ने नेपालप्याक्टचेक (NepalFactCheck.org) ले भने तथ्य जाँच गर्दा निम्न तरिका अपनाउँछ :

- ▶ नेपालप्याक्टचेकले सामाजिक सञ्जाल वा सञ्चार माध्यममा भाइरल भएका जानकारी वा सूचनाको तथ्य जाँच गर्छ । सामान्यतया तथ्य जाँचकीहरूले आफै भेटेका वा पाठकहरूबाट अनुरोध भइरहेका सामग्रीहरूबाट स्विवेकले छानेर तथ्य जाँच गर्छन् ।
- ▶ सामान्यतया स्विवेक प्रयोग गर्दा ती भाइरल छन्/छैनन्, ती जानकारी वा समाचारले नागरिकको अधिकार वा लोकतन्त्र वा अन्य नकारात्मक असर गर्छ/गर्दैन र ती सामग्रीको तथ्य जाँच गर्न सकिने अवस्था छ/छैन भने आधारमा गर्छन् ।

- ▶ तथ्य जाँचकीले स्विवेकले गर्न सक्ने जरि छानेर तथ्य जाँच गर्छन् । करिपय तथ्य जाँच भएका सामग्रीहरू प्रकाशन हुँदैन । धेरैजसो अवस्थामा तथ्य जाँचमा सही देखिएका सामग्रीका तथ्यबारे सार्वजनिक वार्दिवाद छैन भने ती प्रकाशन गरिरहनु आवश्यक हुँदैनन् ।
- ▶ तथ्य जाँचका लागि सामान्यरूपमा यीमध्ये सबै वा धेरै उपाय अवलम्बन गरिन्छ : इन्टरनेटमा खोजी, विज़हरूसँग सरसल्लाह, सम्बन्धित व्यक्ति वा निकाय वा संस्था वा समूहसँग जानकारी, प्रमाण (अडियो, भिडिओ वा दस्ताबेज, अध्ययन/अनुसन्धान वा तथ्याङ्क) को खोजी, आधिकारिक स्रोतको खोजी । इन्टरनेटमा खोजी गर्नका लागि विभिन्न उपकरण र सफ्टवेयर प्रयोग गरिन्छ ।



20°^o

84

Unit 14

Digital Safety

डिजिटल सुरक्षा

इन्टरनेटको सुरक्षित प्रयोग गर्ने भनेको डिजिटल सुरक्षाका लागि सावधानी अपनाउनु हो । ल्यापटप, मोबाइल र हामीले प्रयोग गर्ने अन्य स्मार्ट भनिने इन्टरनेट जोडिएका वा हाम्रो तथ्याङ्क भण्डारण हुने इलेक्ट्रोनिक उपकरणहरू, त्यसमा रहेका तथ्याङ्क र इन्टरनेटमार्फत हुने सञ्चार सन्देशको सुरक्षाका उपायहरू डिजिटल सुरक्षा हो ।

इन्टरनेटमा सुरक्षित रहने उपायका कुरा गर्दा ल्यापटप वा मोबाइल फोन वा स्मार्टवाच जस्ता उपकरणको सुरक्षाको कुरा पनि महत्वपूर्ण हुँच किनभने तिनीहरूमा हाम्रा धैरै सूचना र तथ्याङ्क हुँच्नु जुन सजिलै चोर्न, व्याक गर्न वा बिगार्न सकिन्छ । कसैका बारेमा सूचना चाहनेका लागि सबै भन्दा सजिलो माध्यम नै हाम्रा उपकरण वा सोसल मिडिया हुन सक्छ । आधारभूत डिजिटल सुरक्षाका लागि आवश्यक अभ्यास निम्न छन् :

- ▷ आफ्नो कम्प्युटर वा मोबाइलमा पासवर्ड राख्नुहोस् र कसैलाई पनि आफ्नो उपकरण प्रयोग गर्न नदिनुहोस् ।
- ▷ पासवर्ड क्यापिटल र स्मल अक्षर, नम्बर र सङ्केत चिह्न मिसाएर राख्नुहोस् । इमेल र सामाजिक सञ्जालमा अनिवार्य 2-step verification

राख्नुहोस् अनि आफ्नो पासवर्ड (पुरानो पनि) कसैलाई नभनुहोस् ।

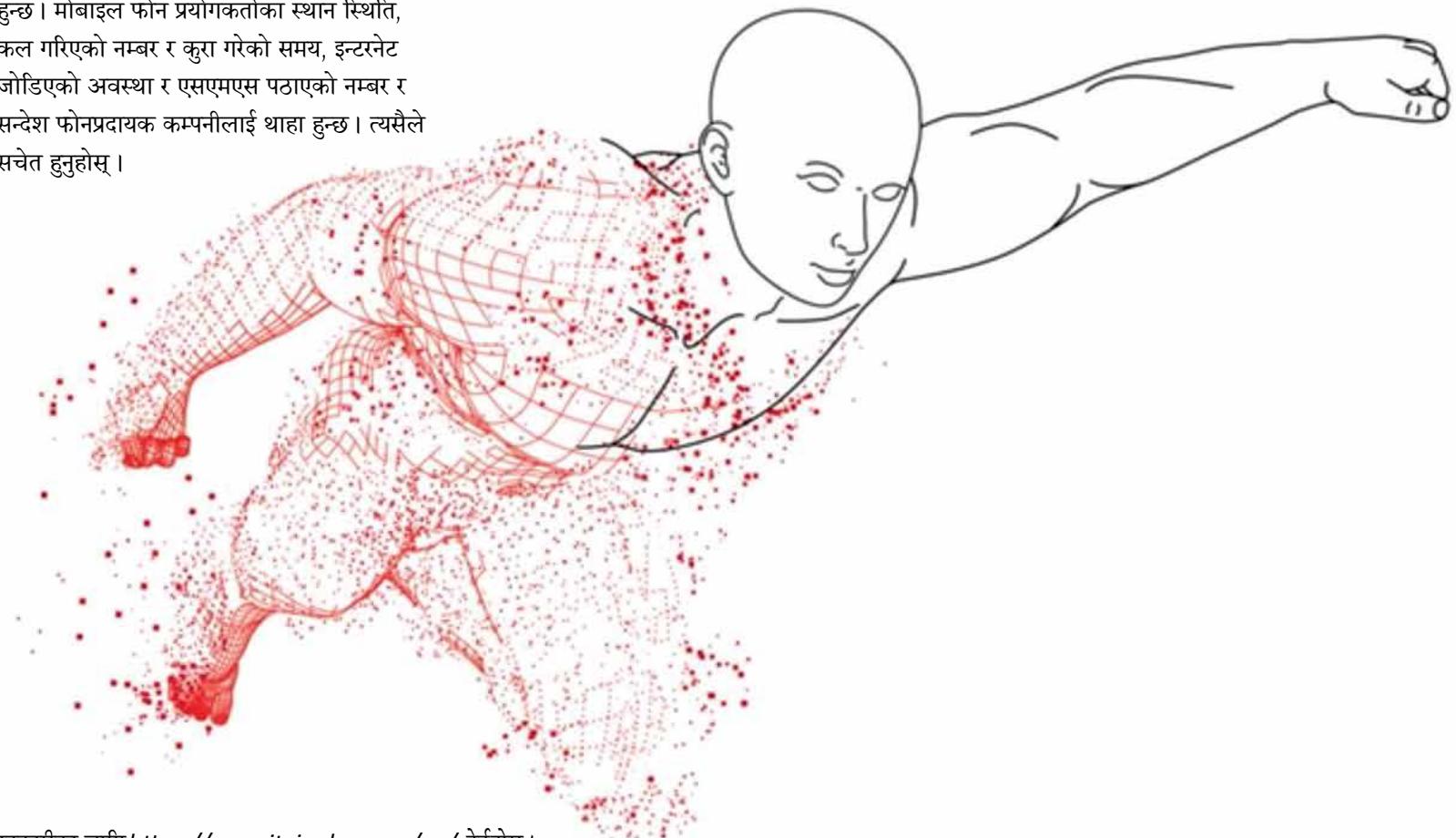
- ▷ कसैलाई पनि (प्रेमी/प्रेमिका, साथी वा अन्य कोही) कुनै पनि अवस्थामा आफ्नो नम वा अर्धनम वा अरूलाई देखाउन नमिल्ने तस्बिर मेसेन्जर वा इन्टर नेटमा कुनै पनि हालतमा नपठाउनुहोस् । पठाउनपर्ने भए अनुहार नदेखिने तस्बिर पठाउनुहोस् ।
- ▷ आफ्ना उपकरणलाई भाइरस र अन्य हानिकारक सफ्टवेयरबाट बचाउनुहोस् । यसका लागि जे पायो त्यही डाउनलोड र इन्स्टल नगर्नुहोस्, अरूको पेन ड्राइभ प्रयोग नगर्नुहोस्, इमेलमा आएका एट्रयाचमेन्ट नखोल्नुहोस् र भरपर्दो एन्टीभाइरस राखेर समय-समयमा अपडेट गर्नुहोस् ।
- ▷ जसरी मिति गुज्रेको औषधिले काम गर्दैन त्यसैगरी समय-समयमा अपडेट नगरिएको एन्टीभाइरसले पनि काम गर्दैन । अनि जसरी खल्तीमा औषधि राखेर रोग निको हुँदैन त्यसैगरी कम्प्युटरमा एन्टीभाइरस राख्नैमा भाइरस हट्ने भन्ने हुँदैन । त्यसैले एन्टीभाइरस समय-समयमा अपडेट गर्नुहोस् अनि त्यसलाई चलाएर स्क्यान गर्नुहोस् ।
- ▷ लोभ नगर्नस् । तपाईंलाई नकिनेको चिङ्गा पर्दैन, तपाईंलाई कुस्त पैसा छोडेर विदेशमा कोही मर्दैन,

त्यसैले त्यस्ता इमेल देख्नेबित्तिकै मेट्नूहोस् । खोल्दै नखोल्नुहोस्, खोलिहाले पनि त्यसका लिङ्कमा नथिच्नूहोस् ।

- ▷ कुनै लिङ्कमा किलक गर्दा वा चलाइरहेकै बेला फेसबुक वा इमेल वा अन्य सेवा लगआउट भएको जस्तो भएर फेरि लगइन गर्न पासवर्ड माथ्यो भने कुनै पनि हालतमा पासवर्ड नहाल्नुहोस् । पासवर्ड हाल्ने एक मात्र अवस्था भनेको आफैले वेब एड्रेस टाइप गरेको बेला हो ।
- ▷ क्रि वाइफाइ पाइयो भन्दैमा खुसी नहुनुहोस् । सार्वजनिक इन्टरनेटबाट तपाईंको व्यक्तिगत तथ्याङ्क, अन्य जानकारीहरू र गोपनीयता भज्न हुने सम्भावना रहन्छ । सकेसम्म यस्तो इन्टरनेट नचलाउनुहोस् र चलाए पनि त्यहाँबाट ब्याङ्क एप जस्ता सम्वेदनशील कुराहरू आवश्यक पर्ने साइट वा एप नचलाउनुहोस् ।
- ▷ कहीं पनि किलक गर्नु भन्दा पहिले ३ पटक सोच्नुहोस् कि यो ठीक हुँच कि हुन ? यो इन्टर नेटका लिङ्क, इमेल वा मेसेन्जरमा आएका लिङ्क र सामाजिक सञ्जालका लाइक वा सेयरसम्म सबैमा लागु हुँच । नथिची नहुने अवस्थामा बाहेक किलक नगर्नुहोस् ।
- ▷ इन्टरनेट साधारणतया गोप्य हुँदैन तर केही गोपनीयता राख्न सकिन्छ । इन्टरनेट चलाउँदा

ब्राउजरले कतिबेला के/के चलायो भन्ने इतिहास
राख्छ भने गुगल जस्ता सेवा चलाउँदाको इतिहास
राख्छ । त्यसैले समय-समयमा ब्राउजरको इतिहास
मेट्नुपर्छ ।

- ▷ मोबाइल फोनमा धेरै सम्बेदनशील जानकारी र डेटा
हुन्छ । मोबाइल फोन प्रयोगकर्ताका स्थान स्थिति,
कल गरिएको नम्बर र कुरा गरेको समय, इन्टरनेट
जोडिएको अवस्था र एसएमएस पठाएको नम्बर र
सन्देश फोनप्रदायक कम्पनीलाई थाहा हुन्छ । त्यसैले
सचेत हुनुहोस् ।



थप जानकारीका लागि <https://securityinabox.org/en/> हेर्त्तहोस् ।

Unit 15

Digital Detox

डिजिटल डिटक्स

कुनै निश्चित समयका लागि इन्टरनेट र विद्युतीय उपकरणबाट टाढा बस्ने अभ्यास डिजिटल डिटक्स हो ।

यसलाई डिस्कनेक्ट टु रिकनेक्ट (पुनर्सम्बन्धका लागि सम्बन्ध विच्छेद) पनि भनिन्छ ।

इन्टरनेटको ज्यादा प्रयोग वा कुलतले त्याउने प्रभावहरू जस्तै तनाव र एकाइकीपनबाट बचाएर सामाजिक जीवनलाई पुनर्जीवन दिनका लागि आजको युगमा यो अत्यावश्यक मानिन थालेको छ । यसलाई ध्यानसँग तुलना गर्न सकिन्छ ।

डिजिटल डिटक्स गर्न सामान्यतया एक हप्ताको समय ठीक हुन्छ तर हप्तैभरि इन्टरनेट हेँहैं हुन भन्ने होइन, खाली प्रयोग कम गर्ने र प्रकृतिसँग नजिक हुने अभ्यास हो । यो समयमा इन्टरनेट सुरक्षाका लागि गर्नैपर्ने अभ्यासहरू पनि गर्न सकिन्छ ।

डिजिटल डिटक्सको अभ्यास गर्दा सुरुको दिन असहज वा खालीपन वा केही छुटे जस्तो महसुस हुनु सामान्य हो ।

डिजिटल डिटक्स कसरी गर्ने ?

- फोनबाट सोसल मिडियाका सबै एप मेट्नुहोस् । सोसल मिडिया त्यापटप वा कम्प्युटरमा मात्रै चलाउनुहोस् ।

- फोनमा आगमन कल र एसएमएसबाहेकका अरू सबै नोटिफिकेशन अफ गर्नुहोस् ।

- साथी वा परिवारसँग गफ गर्दा, खाना/खाजा खाँदा वा सामाजिक भेटघाटमा फोन हातमा नलिनूस्, खल्तीमै राख्नूस् ।
- शौचालय जाँदा फोन बाहिरै छाडेर जानुहोस् ।

नमुना अभ्यास

दिन	इन्टरनेट अभ्यास	सामाजिक अभ्यास	इन्टरनेट सुरक्षा अभ्यास
आइतबार	राति फोन शयनकक्षमा नराखी अन्य कोठामा राख्नुहोस् ।	साथीहरू भेटेर सँगै चिया पिउँदे गफ गर्नुहोस् ।	गुगलमा आफ्नो नाम सर्च गर्नुहोस् र के के दैखिन्छ विचार गर्नुहोस् । ब्राउजरको इतिहास मेट्नुहोस् ।
सोमबार	घरमा हुँदा फोन आफूसँग नराखी बैठक कोठामा राख्नुहोस् र फोन प्रयोग आवश्यक हुँदा त्यहींबाट गर्नुहोस् ।	आफन्तसँग भेटघाट गर्नुहोस् ।	इमेल र सोसल मिडियाका सबै पासवर्ड परीर्वतन गर्नुहोस् ।
मझगलबार	घरमा सोसल मिडिया प्रयोग नगर्नुहोस् ।	घरमा सबैजना सँगै वा भाइ/बहिनीसँग बसेर ठिभी वा सिनेमा देनुहोस् ।	क्रोमलाई इनकमिन्टो र फ्रायर फक्सलाई इनभिजिवल मोडमा मात्रै चलाउनुहोस् । गुगलको स्ट्रो डकडकगो चलाउनुहोस् ।
बुधबार	घरमा इन्टरनेटको प्रयोग नगर्नुहोस् । यसका लागि घरको इन्टरनेट राउटर अफ गर्न सकिन्छ ।	घर नजिकैको चोक या पार्क जानुहोस् र बाटोमा भेटिएका चिनजानका मानिससँग केही क्षण कुरा गर्नुहोस् ।	मोबाइल फोनको सेक्युरिटी र प्राइभेसी सेटिङ्हरु हेर्नुहोस् ।
बिहीबार	फोन घरमै छाडेर काम वा विद्यालय जानुहोस् ।	एउटा पुस्तक (छापिएको) पढ्न सुरु गर्नुहोस् ।	फेसबुकको सेक्युरिटी र प्राइभेसी सेटिङ्हरु हेर्नुहोस् ।
शुक्रबार	फोनलाई एयरप्लेन मोडमा राख्नुहोस् र आफूलाई आवश्यक पर्दा मात्रै केही क्षणलाई त्यो मोड अफ गर्नुहोस् ।	परिवारसँग रातिको खाना खान बाहिर जानुहोस् वा सबैजना सँगै मिलेर भाल्यामा मीठो खानेकुराहरू पकाउनुहोस् ।	myactivity.google.com मा जानुहोस् अनि त्यहाँ भएका आफ्नो गुगल प्रयोगको इतिहास हेर्नुहोस् । गुगल इतिहास मेट्नुहोस् ।
शनिबार	शुक्रबार राति १० बजेदेखि शनिबार रातिसम्म फोन अफ गर्नुहोस् ।	परिवारसँग दिनभरको पिकनिक वा पार्क भ्रमण गर्नुहोस् । प्रकृतिसँग दिन बिताउनुहोस् ।	परिवारसँग इन्टरनेटको प्रयोग, जोखिम र बच्चे उपायबारे छलफल गनुहोस् ।



आईतबार
सोमबार
मंगलबार
बुधबार
विहीनबार
शुक्रबार
शनिबार

Unit 16

Artificial Intelligence

एआइ

कृत्रिम बौद्धिकता भनिने एआइ यान्त्रिक सुभवुभमा आधारित प्रविधि हो । यसमा मेसिनले ठूलो तथ्याङ्कका आधारमा त्यसलाई मानिसले जस्तै छुट्टाउन वा त्यसबाट सूचना निकाल्न वा त्यसको आधारमा सुभवुभ विकास गर्न वा कुनै कार्य गर्न सकछ ।

अहिले एआइ प्रविधि चर्चामा छ । अन्य प्रविधिमा एआइको प्रयोग बढ्दो छ । उदाहरणका लागि एउटा निश्चित तापक्रम पुरोपार्छ फ्रिजले आफैं कम ऊर्जा प्रयोग गर्ने प्रविधि पनि एआइमा आधारित हो भने कुनै व्यक्तिको तस्विरलाई राप्रो बनाउने फोनको सुविधा पनि एआइ हो । अनुहार चिन्ने प्रविधिदेखि इमेल लेखिदिने वा कथा बनाइदिने वा चित्र वा भिडियो बनाइदिने एआइमा आधारित प्रणाली अहिले चर्चामा छन् ।

एआइलाई अहिले च्याटिजिप्टीले चर्चित बनाएको छ भने गुगल र माइक्रोसफ्ट जस्ता ठूला कम्पनीले हामीलाई दिएको सुविधामा यसको प्रयोग गर्न थालेका छन् ।

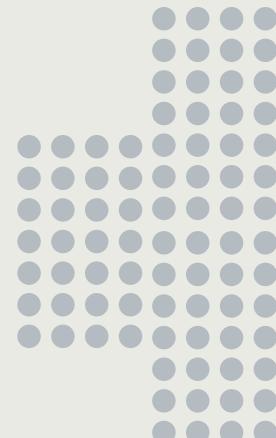
यो नयाँ र विकासक्रममै रहेको प्रविधि भएकाले यसको प्रयोगका विषयका कठितपय नैतिक कुराहरू अलमलमै छ तर यसको प्रयोग व्यापक हुँदै जाने देखिएको छ ।

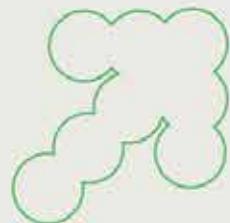
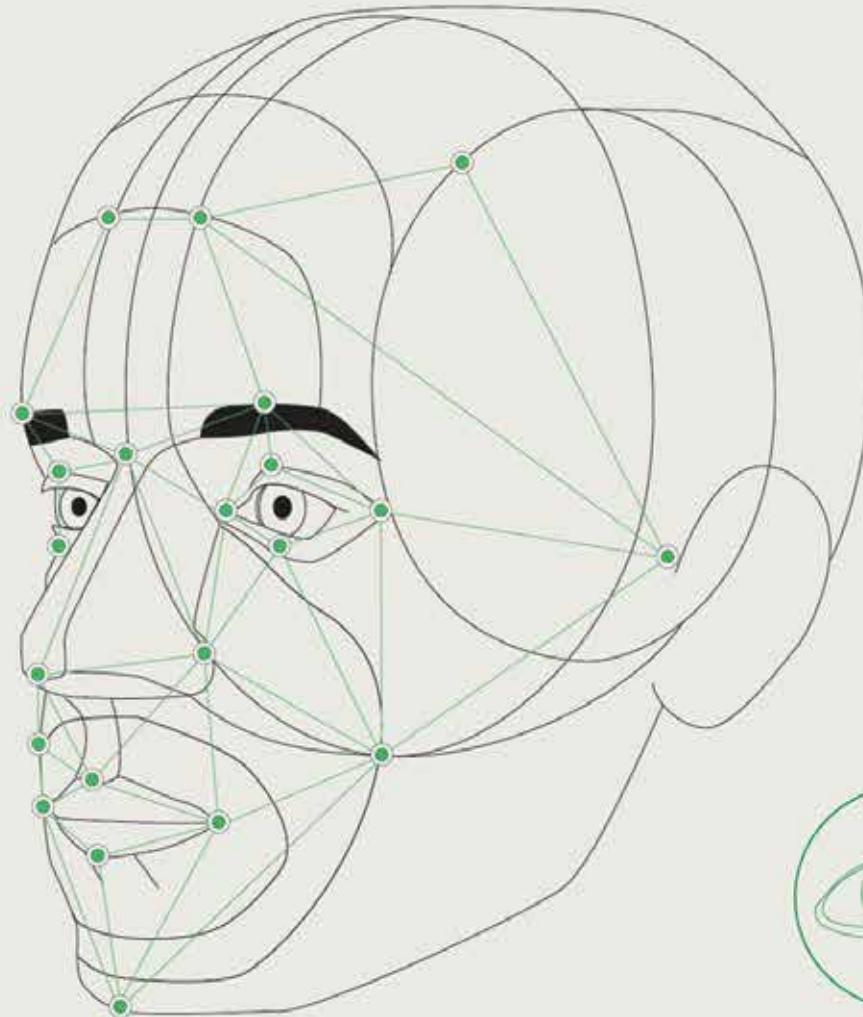
के गर्ने ?

- ▷ एआइ प्रविधिमा आधारित कुराहरू प्रयोग गर्दा होसियारी अपनाउनुपर्छ । आफ्मा व्यक्तिगत जानकारीहस्तारेमा सचेत रहनुका साथै यो पूर्ण विकसित प्रविधि नभएकाले यसबाट आएका कुराहरू सबै विश्वसनीय नहुन सक्छन् ।
- ▷ शिक्षाप्रद कुराहरूका लागि एआइ प्रविधि प्रयोग गर्न सकिन्छ । कुनै कुरा कसरी गर्ने भनेर च्याटिजिप्टीमा सोधन सकिन्छ । पद्धनुपर्ने कुराहरू एआइ प्रविधिलाई सारांश बनाउन लाउन सकिन्छ ।
- ▷ एआइको सहयोगबाट आएका कुराहरूलाई त्यसैअनुरूप खुलस्त पार्नुपर्छ । उदाहरणका लागि एआइ प्रविधि प्रयोग गरी बनाइएका तस्विर वा भिडियो वा चित्रलाई त्यस्तै जनाउनुपर्छ ।
- ▷ एआइ प्रविधिका फाइदा र बेफाइदा दुवैबारे लेखिएका छन् । दयाकै यो प्रविधि कस्तो हुन्छ कसैलाई थाहा छैन तर यो प्रविधि अब बन्द हुँदैन । त्यसै भएर यसलाई चिन्नु र बुझ्नुपर्छ अनि फाइदा लिने हिसाबले प्रयोग गर्दै जानुपर्छ ।

के नगर्ने ?

- ▷ एआइबाट निकालिएका कुराहरूलाई आफ्मो दाबी गरेर राख्नु वा बुझाउनुहुँदैन । उदाहरणका लागि विद्यार्थीले गृहकार्यका रूपमा एआइलाई निबन्ध लेख्न लगाएर बुझाउनु हुँदैन ।
- ▷ एआइ आधारित प्रणालीमा अनैतिक कामहरू गर्नुहुँदैन । जस्तो तस्विर बनाउने एआइ प्रविधिलाई गलतखालका तस्विरहरू बनाउन लगाउनु हुँदैन ।
- ▷ एआइ प्रविधि प्रयोग गर्दा पनि व्यक्तिगत जानकारीहस्त सकेसम्म कम राख्नुपर्छ ।
- ▷ अप्रमाणित वा मिथ्या सूचना फैलाउन एआइको प्रयोग गर्नुहुँदैन ।





भाग ३

प्रयोगात्मक सुझाव

Unit 17

दु स्टेप भेरिफिकेसन

पासवर्ड जतिसुकै बलियो भए पनि त्यो सार्वजनिक हुने वा अरूले थाहा पाउने सम्भावना हुन्छ । अरूले पासवर्ड थाहा पाए पनि अकाउन्टमा पहुँच नदिन मुरक्खाको दोस्रो तह प्रयोग गर्न सकिन्छ । यस्तो दोस्रो तहलाई दु-स्टेप भेरिफिकेसन वा दु फ्याक्टर अथेन्टिकेसन भनिन्छ ।

दु-स्टेप भेरिफिकेसनमा सही पासवर्ड प्रयोग गरिसकेपछि तलकामध्ये थप एक चरण पार गरेपछि मात्रै अकाउन्ट खुल्छ :

- ▷ मोबाइलमा एसएमएस आउने नम्बर हाल्ने
- ▷ मोबाइलमा अथेन्टिकेटर भनिने एपमा प्रत्येक मिनेट परिवर्तन हुने नम्बर हाल्ने
- ▷ फिजिकल कि भनिने युएसबीमा छिराउन मिल्ने वा अन्य स्मार्ट उपकरण प्रयोग गर्ने

यीमध्ये मोबाइलमा एसएमएस आउने विधि प्रयोग गर्दा अरू कसैले आफ्नो पासवर्ड थाहा पाएर अकाउन्ट खोल्न प्रयास गरेको थाहा हुन्छ । तर यो विधिमा आफूसँग मोबाइल नहुँदा वा विदेशमा यात्रा गर्दा अकाउन्ट खोल्न नसकिने समस्या ल्याउन सक्छ ।

दु-स्टेप भेरिफिकेसन सुरु गर्न वा बन्द गर्ने सुविधा सोसल मिडियाको सेटिङ्गभित्र रहेको सेक्युरिटीमा हुन्छ ।

अथेन्टिकेटर एपहरूमा गुगल अथेन्टिकेटर वा माइक्रोसफ्ट अथेन्टिकेटर वा दुएफएएस जस्ता कुनै पनि एप प्रयोग गर्न सकिन्छ । एउटै एपमा सबै अकाउन्टको दु-स्टेप भेरिफिकेसन राख्न मिल्छ ।

उदाहरणका लागि फेसबुकमा दु-स्टेप भेरिफिकेसन सुरु गर्ने तरिका यस्तो छ :

- ▷ फेसबुक खोलेपछि दाहिनेतर्फ माथिल्लो कुनामा देखिने आफ्नो तस्विरमा थिचेर सेटिङ एन्ड प्राइभेसीमा जानुहोस्
- ▷ आफ्नो सेक्युरिटी एन्ड लगिन सेटिङमा जानुहोस्
- ▷ त्यसमा रहेको युज दु फ्याक्टर अथेन्टिकेसनसँगै रहेको एडिटमा थिच्नुहोस्
- ▷ दोस्रो मुरक्खा तरिका छानुहोस् (सेक्युरिटी कि वा अथेन्टिकेटर एप वा एसएमएस)
- ▷ त्यसपछि प्राप्त निर्देशनअनुसार एकपटक गर्नुपर्ने सेटिङ गर्नुहोस् ।

यदि तपाईंलाई कुनैबेला दोस्रो चरणको सुरक्षा चरण पार गर्न गाहो हुने अवस्था छ भने सबैजसो सोसल मिडियाले १० वटाक रिकभरी कोड दिन्छन् । एकपटक प्रयोग गर्न मिल्ने त्यो कोडलाई दु स्टेप भेरिफिकेसनको कोडका रूपमा प्रयोग गरेर अकाउन्टमा पहुँच पाउन सकिन्छ ।



Unit 18

सोसल मिडियालाई रिपोर्ट

धैरेजसो सोसल मिडिया प्लेटफर्ममा रिपोर्ट गर्ने तरिका एकै हुन्छ । तलको चरण फेसबुक, इन्स्टाग्राम, टिवटर (एक्स) र लिङ्गडइनमा लागु हुन्छ :

- ▷ रिपोर्ट गर्नुपर्ने पोस्ट वा तस्बिरको माथि दाहिने कुनामा रहेको ३ थोप्लोमा थिच्नुपर्छ ।
- ▷ त्यसपछि देखिएको मेनुमा रिपोर्ट वा रिपोर्ट पोस्ट वा रिपोर्ट फोटो छानुपर्छ ।
- ▷ त्यसपछि दिइएको निर्देशानुसार किन रिपोर्ट गरेको हो लेख्नुपर्ने हुनसक्छ ।
- ▷ कुनै प्रोफाइल वा पेज रिपोर्ट गर्नका लागि त्यो प्रोफाइल वा पेज खोलेपछि माथि दाहिने कुनामा देखिने ३ थोप्लोमा थिच्नुपर्छ र आएको मेनुमा रिपोर्ट भन्ने लिङ्ग छानुपर्छ ।

स्न्यापच्याटमा भने पोस्टको तल त्यस्तो ३ थोप्लो देखिन्छ ।

युट्युबमा पनि भिडियो वा सर्ट्सको तल त्यस्तो ३ थोप्लो हुन्छ ।

टिकटकको भिडियो वा भिडियोमा आएको कमेन्ट रिपोर्ट गर्न तिनलाई थिचिराख्दा आउने मेनुमा रिपोर्ट छानुपर्छ । डाइरेक्ट मेसेज रिपोर्ट गर्नचाहिँ त्यसको माथि दाहिने कुनामा ३ थोप्लोमा थिचेर आएको मेनुमा रिपोर्ट भन्ने प्रावधान हुन्छ ।

ह्वाट्सएप, भाइबर, फेसबुक मेसेन्जर जस्ता सन्देश आदान-प्रदान गर्ने एपमा आएका मेसेज वा पठाउने व्यक्तिलाई पनि रिपोर्ट गर्न सकिन्छ । कि त्यस्ता सन्देशका वरपर भएका ३ थोप्लो थिचेर वा त्यस्ता सन्देशलाई केही क्षण थिचिराख्दा आउने मेनुबाट रिपोर्ट गर्न सकिन्छ ।





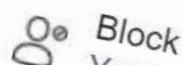
You selected

✓ Hate Speech

✓ Social Caste

If you think this post goes against our Community Standards, please also report it. You may want to block this person instead.

Other steps you can take



Block

You won't be able to see or contact each other.



Unfollow

Stop seeing posts but stay friends.



Report comment

Submit to Facebook for review.



Unfriend

You'll no longer be friends on Facebook.

Done

प्रयोग भएका चित्रहरूको सर्वाधिकारबारे जानकारी

कभर चित्र: Ann Kiernan for Technologies of Hope and Fear by Tactical Tech

पृष्ठ १३, १५, १९, २७, ३१, ३५, ४५ र ४९ का चित्रहरू सिएमआर नेपालका लागि देवेनले कोरेका हुन्। ती चित्रहरूको सर्वाधिकार सिएमआर नेपालसँग छ।

पृष्ठ १७, २९, ३३, ३७, ३९, ४३, ४७ र ५१ मा प्रयोग भएका चित्रहरू ट्याक्टिकल टेकको दी ग्लासरम परियोजनाबाट अनुमति लिएर साभार गरिएका हुन्। ती चित्रहरूको सर्वाधिकार ट्याक्टिकल टेकसँग छ।

अन्य चित्रहरू सर्जकले सबै प्रयोगका लागि खुला राखेका सर्वाधिकाररहित सिर्जनाहरू हुन्।

