साइबर सुरक्षाका लागि

जनहितमा जारी सन्देश

नेपाल दूरसञ्चार प्राधिकरण
जमल, काठमाण्डौ

प्रकाशक: नेपाल दूरसञ्चार प्राधिकरण
कान्तिपथ, जमल, काठमाण्डौ
प्रकाशन मिति: वि. सं. २०७८
प्रकाशन प्रति: ५००
सर्वाधिकार: प्रकाशकमा सुरक्षित

शुभकामना

नेपाल सरकार

सञ्चार तथा सूचना प्रविधि मन्त्रालय

मा. ज्ञानेन्द्र बहादुर कार्की
सञ्चार तथा सूचना प्रविधि मन्त्री

सिंहदरबार, काठमाडौं
नेपाल

शुभकामना

सूचना तथा सञ्चार प्रविधिको क्षेत्रमा भएको तीव्र विकासले आधुनिक विश्वलाई एक गाउँमा परिणत गरिदिएको छ। प्रविधिको विकासले मानव जीवनका हरेक क्षेत्रमा प्रभाव पारेको छ। सूचना तथा समाचारको सहज उपलब्धता, पारिवारिक तथा सामाजिक सम्पर्कमा सहजता र सरकारी, निजी तथा नागरिकका तहबाट सेवा लिन र दिन समेत सञ्चार तथा सूचना प्रविधिको क्षेत्रमा भएको विकासले थप मदत गरेको छ। यस अर्थमा सूचना तथा सञ्चार प्रविधि मानव सभ्यताको बहुआयामिक विकासको एक अभिन्न अङ्ग बनिसकेको छ।

सूचना प्रविधिको विकास सँगसँगै आर्थिक, सामाजिक, शैक्षिक लगायतका क्षेत्रहरूमा इन्टरनेट सेवाको प्रयोग बढेको छ, जसले साइबर सुरक्षाको महत्त्व पनि झन् बढ्दै गएको छ। नेपालमा इन्टरनेटको प्रयोग हुन थालेको दुई दशकभन्दा बढी भए पनि इन्टरनेट तथा साइबर स्पेसमा आफूलाई सुरक्षित राख्ने बारेमा चेतना र ज्ञानको अभाव छ। कतिपय नागरिक अज्ञानताकै कारणले साइबर आक्रमणबाट पीडित हुने गरेका छन्। यस सन्दर्भमा इन्टरनेट तथा साइबर स्पेसमा भएका विवरण तथा डाटालाई सुरक्षित राख्ने सम्बन्धमा चेतना जगाउन नेपाल दूरसञ्चार प्राधिकरणबाट साप्ताहिक रूपमा जारी भएका चेतनामूलक सन्देशहरू समावेश गरी पुस्तकको रूपमा प्रकाशन गर्न लागेकोमा निकै हर्षित भएको छु। यसबाट इन्टरनेट तथा सूचना प्रविधिको प्रयोग गर्दा हुनसक्ने साइबर हमला, गोपनीयता भङ्ग हुने अवस्था र साइबर आक्रमणबाट बच्ने बचाउने सम्बन्धमा आम नागरिकले यथार्थ सनदेश प्राप्त गर्नेछन् भन्ने मेरो विश्वास छ।

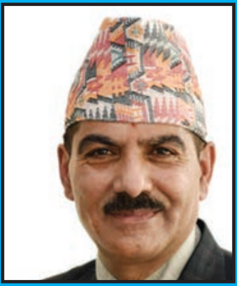
यसका साथै नेपाल सरकारले परिकल्पना गरेको डिजिटल नेपालको कार्यान्वयनका क्रममा आम नागरिकलाई सुरक्षित तवरमा सहभागी बनाउन समेत यस पुस्तकले मदत गर्दछ भन्ने मेरो अपेक्षा छ। अन्त्यमा, साइबर सुरक्षा सम्बन्धमा जनचेतनामूलक सन्देशको पहुँच वृद्धि गर्ने नेपाल दूरसञ्चार प्राधिकरणको पहलकदमीका लागि हार्दिक बधाई तथा शुभकामना व्यक्त गर्दछु।

धन्यवाद ।

ज्ञानेन्द्र बहादुर कार्की
मन्त्री

फोन नं.: ९७७-४२११५५५, ४२११७०१, ४२११६४० (कार्यालय), फ्याक्स: ९७७-१-४२११६००
वेब साइट: www.mocit.gov.np

शुभकामना



नेपाल सरकार

सञ्चार तथा सूचना प्रविधि मन्त्रालय

प.स.
च.न.

सिंहदरबार, काठमाडौं

शुभकामना

विश्वव्यापी रूपमा सूचना प्रविधिमा भएको विकास र विस्तारले आममानिसको जीवनयापनलाई सहज र सरल बनाउनुका साथै सरकारी र निजी क्षेत्रबाट प्रवाह हुने सेवाको पहुँच वृद्धि गर्न ठूलो भूमिका खेलेको छ । सूचना प्रविधिको प्रयोगले सेवा प्राप्तिको समय तथा लागत कटौती गरी सेवाको गुणस्तर बढाएको छ । आर्थिक, सामाजिक, शैक्षिकलगायत सबै क्षेत्रमा सूचना प्रविधिको बढ्दो प्रयोगले सूचना प्रविधिलाई प्रत्येक व्यक्तिको जीवनको अभिन्न अङ्गको रूपमा स्थापित गरेको छ ।

सूचना प्रविधिको प्रयोग बढ्दै जाँदा यससँग जोडिएका जोखिम सँगै यसको दुरूपयोग गरी हुने अपराध समेत बढ्दै गएका छन् । आफ्नै असावधानीका कारण वा साइबर हमलाकारहरूको योजनामा फँसेर व्यक्ति प्रताडित बन्ने र सामाजिक एवं नैतिक समस्यामा पर्ने गरेका छन् । तसर्थ यस्ता घटनाहरूलाई न्यून गर्दै आमजनतालाई साइबर सुरक्षाका बारेमा जानकारी गराउनुपर्ने आवश्यकता एकातिर छ भने साइबर सुरक्षाका लागि संरचनात्मक र नीतिगत व्यवस्था गर्नुपर्ने आवश्यकता अर्कातिर छ ।

साइबर सुरक्षाका लागि पहिलो र महत्त्वपूर्ण भूमिका प्रयोगकर्ता स्वयंमको नै हुन्छ। सूचना प्रविधिको प्रयोग गर्दा अपनाउनुपर्ने सावधानी, साइबर स्पेसमा राख्ने विवरण र सामग्री, एकअर्काको गोपनीयताजस्ता विषयहरूमा प्रयोगकर्ता आफैं जागरूक हुनुपर्दछ । साथै साइबर हमलाकार तथा अन्य पक्षबाट हुनसक्ने अवाञ्छित क्रियाकलाप तथा आक्रमणबाट बच्नका लागि चाल्नुपर्ने कदमहरूका बारेमा समेत जानकार हुनुपर्दछ । नेपाल दूरसञ्चार प्राधिकरणले यिनै विषयलाई ध्यानमा राखी साप्ताहिक रूपमा जनचेतानमूलक सामग्री प्रकाशित गर्दै आइरहेको छ । यसबाट साइबर सुरक्षाका बारेमा जनचेतना जगाउन यथेष्ट सहयोग पुगेको छ। यसै प्रयासलाई थप सबल बनाउन प्राधिकरणले साप्ताहिक रूपमा प्रकाशन गर्दै आइरहेको जनचेतनामूलक सन्देश तथा सामग्रीहरूलाई एकत्रित गरी पुस्तकको रूपमा प्रकाशन गर्न लागेकोमा मलाई खुशी लागेको छ ।

यस किसिमको प्रकाशनले छरिएर रहेका सामग्रीहरूलाई एउटै पुस्तकमा समावेश गर्ने हुँदा आमपाठकलाई यससम्बन्धी सूचना प्राप्त गर्न र आफ्नो तर्फबाट सावधानी अपनाउन सहज हुनेछ भन्ने मेरो विश्वास छ । यस पुस्तकमा प्रकाशन भएका सामग्रीहरूको अध्ययन गरी यिनले दिएका सन्देशको मर्मअनुरूप सूचना प्रविधिको प्रयोग गर्न सकेमा साइबर सुरक्षाका लागि महत्त्वपूर्ण सहयोग हुनेछ । यस कार्यमा लिएको अग्रसरताका लागि नेपाल दूरसञ्चार प्राधिकरणलाई हार्दिक बधाई दिँदै प्राधिकरण साइबर सुरक्षाका सम्बन्धमा थप क्रियाशील हुन सकोस् भन्ने शुभकामना समेत दिन्छु।

धन्यवाद ।

वैकुण्ठ अर्याल
सचिव

२०७८ माघ १८

फोन नं. : ४२११५५६, ४२११६५०, ४२११६१५, फ्याक्स नं.: ४२११७२९, ४२११६१०
Email : info@mocit.gov.np, Website: www.mocit.gov.np

मन्तव्य

नेपाल दूरसञ्चार प्राधिकरण
(अध्यक्षको सचिवालय)

प.सं.:-०७८/०७९
च.नं.:- ३९५२

मिति:-२०७८/१०/२०

मन्तव्य

सूचना तथा संचार प्रविधिको विकाससँगै मानव सभ्यताले ठूलो फड्को मारेको छ । नेपालमा दुई दशक अघिदेखि नै इन्टरनेट सेवा उपलब्ध हुँदै आइरहेकोमा हाल करिब ८५% नागरिकमा मोवाइल ब्रोडब्याण्ड इन्टरनेटको पहुँच पुगिसकेको अवस्था छ । देशको दूरदराजमा दूरसञ्चार सेवाको पहुँच पुर्याउनका लागि नेपाल दूरसञ्चार प्राधिकरणले राष्ट्रिय स्तरमा दूरसञ्चारको पूर्वाधार निर्माणमा जोड दिंदै आएको छ। विद्यमान कोभिड–१९ महामारीको अवस्थामा सूचना प्रविधिको महत्व झन् उजागर भएर आएको छ। विभिन्न क्षेत्रका सेवाहरु सूचना प्रविधिमैत्री भई इन्टरनेटको प्रयोग दिनानुदिन बढिरहेको छ।

इन्टरनेटको बढ्दो प्रयोगसंगै देखिएको साइवर सुरक्षा जोखिमलाई न्यूनीकरण गर्न तथा आम इन्टरनेट प्रयोगकर्ताहरुलाई डिजिटल सुरक्षाको प्रत्याभूति दिलाउन नेपाल दूरसंचार प्राधिकरणले Cyber Security Byelaw, 2020 जारी गरी कार्यान्वयनमा ल्याएको छ। यसै विनियमावली अनुसार गठित Cyber Security Task Force ले नियमित रुपमा जनचेतनामुलक साइबर सुरक्षा सम्बन्धी सन्देशहरु प्राधिकरणको वेबसाइट मार्फत प्रवाह गर्दै आइरहेको छ। साइबर सुरक्षाको निम्ति यस प्राधिकरणको Cyber Security Task Force ले चालेका कदमहरु रचनात्मक एवं प्रशंसनिय छन्। उपरोक्त जनहितमा जारी चेतनामुलक सन्देशहरुलाई पुस्तकको रुपमा प्रकाशन गरी दूरदराजमा पु-याई बढी भन्दा बढी इन्टरनेट प्रयोगकर्ताहरुलाई साइबर सुरक्षा साक्षर बनाउन यस पुस्तकले महत्वपूर्ण भूमिका खेल्ने छ भन्ने अपेक्षा गरेको छु ।

पुरुषोत्तम प्रसाद खनाल
अध्यक्ष

जमल (राष्ट्रिय नाचघर –भवन), काठमाडौं, नेपाल
फोन नं. +९७७-५३५४६८१ ई-मेल:info@nta.gov.np, वेबसाइट: www.nta.gov.np

प्रकाशकीय

संयोजक
विजय कुमार राय
निर्देशक

सदस्य
रोजा किरण बासुकला
उपनिर्देशक

सदस्य
हिरण्य प्रसाद बास्ताकोटी
उपनिर्देशक

आधुनिक युगमा सूचना तथा सञ्चार प्रविधि समाजको लागि एक आधारभूत आवश्यकताको विषय बनिसकेको छ । सूचना तथा सञ्चार प्रविधिले सिंगो विश्वलाई जोडी Global Village को रुपमा स्थापित गरेको छ । ब्रोडब्याण्ड इन्टरनेटको बृहत्तर विस्तार, हरेक क्षेत्रमा यसको बढ्दो उपयोगिता र सामाजिक संजालले गर्दा मानिसहरु धेरै समय अनलाइन नै रहने गरेका छन् । कोभिड-१९ महामारीले झन् सम्पूर्ण विश्वजगत इन्टरनेट र साइबर स्पेसमा केन्द्रीकृत भएको छ । साइबर स्पेस शैक्षिक, सामाजिक, राजनीतिक, आर्थिक देखि जनस्वास्थसँग सम्बन्धित क्रियाकलापहरुको लागि अपरिहार्य मञ्च बन्न पुगेको छ । नेपालमा करिब ८५ प्रतिशत नागरिकको मोबाइल ब्रोडव्याण्ड इन्टरनेटमा र करिब ११३ प्रतिशत नागरिकको तारसहित वा ताररहितका प्रबिधिहरुको माध्यमबाट इन्टरनेटमा पहुँच पुगिसकेको छ ।

इन्टरनेट मार्फत आदान-प्रदान हुने प्रत्येक सूचना स्थायी प्रकृतिको हुन्छ । डिलिट गरिएका विवरणहरु समेत कतै न कतै भण्डारण भैरहेको हुन्छ । इन्टरनेट चलाउँदा कसरी सुरक्षित रहने

सदस्य
सुगन शाक्य
सहायक निर्देशक

सदस्य सचिव
ओम प्रकाश महतो
सहायक निर्देशक

र इन्टरनेट मार्फत संवेदनशील जानकारी तथा सूचना सेयर गर्दाका परिणाम के कस्तो हुन सक्छ ? यस विषयमा औपचारिक तथा अनौपचारिक रूपमा सचेतना अभियान चलाउन जरुरी भइसकेको छ। इन्टरनेट तथा साइबर स्पेस प्रयोगकर्ताहरुको गोपनीयता तथा सूचनाको सुरक्षा सुनिश्चित गर्न, जोखिम कम गर्न, क्षति न्यूनीकरण गर्न लगायत साइबर दुर्व्यवहार तथा सम्भावित अपराधहरु नियन्त्रण गर्न अपरिहार्य भैसकेको छ । यसै सन्दर्भमा प्राधिकरणको Cyber Security Task Force ले आम नागरिकहरुका लागि नियमित रुपमा साइबर सुरक्षा सम्बन्धीत चेतनामूलक सन्देशहरु जारी गर्दै आइरहेको छ। प्राधिकरणको वेबसाइटमा प्रकाशित उपरोक्त जनहितमा जारी चेतनामूलक सन्देशहरुलाई देशको कुनाकाप्चासम्म पुर्याउने र नेपाली नागरिकलाई साइबर सुरक्षाको बिषयमा जागरुक बनाउने प्रयास स्वरुप उपरोक्त सन्देशहरुको संग्रहलाई पुस्तकको रुपमा प्रकाशन गरिएको छ। आशा छ, यस पुस्तकमा भएका सन्देशहरुले सुरक्षित साइबर समाज र राष्ट्र निर्माणमा सहयोग पुग्नेछ।

विजय कुमार राय, निर्देशक
संयोजक
साइबर सेक्युरिटी टास्क फोर्स
(Cyber Security Task Force)

यस भित्र:

सि.नं.	विषय	पाना नं.
१	पासवर्डसँग सम्बन्धित	१
२	फिशिंग स्क्याम (Phishing scam) सँग सम्बन्धित	२
३	सोसियल इन्जिनियरिंग (Social Engineering) संग सम्बन्धित	४
४	घरको वाइफाइ (Home WiFi) लाई कसरी सुरक्षित राख्ने ?	८
५	सार्वजनिक वाईफाई (Free/Pubic WiFi) प्रयोग गरेर इन्टरनेट चलाउँदा कसरी सुरक्षित रहने ?	९
६	सामाजिक संजालहरु (Social Media) जस्तै Facebook, Twitter, LinkedIn आदि प्रयोग गर्दा कसरी सुरक्षित रहने ?	११
७	Online Banking (Mobile Banking/ Internet Banking) सेवा कसरी सुरक्षित साथ प्रयोग गर्ने ?	१३
८	मालवेयर (Malware) के हो ?	१५
९	अनलाइन बाल सुरक्षाका लागि जारी सन्देश	१९
१०	मोबाइल सुरक्षा (Mobile Security) संग सम्बन्धित	२१
११	Licensed/Open Source Software को प्रयोगसंग सम्बन्धित	२३
१२	रान्समवेयर (Ransomware) संग सम्बन्धित	२५
१३	पासवर्डलाई कसरी सुरक्षित साथ राख्ने ?	२८
१४	भिसिंग (Vishing) सँग सम्बन्धित	२९
१५	फारमिंग आक्रमण (Pharming Attack) संग सम्बन्धित	३१
१६	स्निफिंग आक्रमण (Sniffing Attack) संग सम्बन्धित	३३

यस भित्रः

सि.नं.	विषय	पाना नं.
१७	म्यान इन द मिडल आक्रमण (Man in the Middle Attack: MITM) सँग सम्बन्धित	३५
१८	कार्यालयको Corporate Network को सुरक्षासँग सम्बन्धित	३७
१९	डिस्ट्रिब्युटेड डिनायल अफ सर्भिस आक्रमणसंग सम्बन्धित	३९
२०	कुकिज सूरक्षा (Cookies Security) संग सम्बन्धित	४२
२१	इमेल सूरक्षा (Email Security) संग सम्बन्धित	४५
२२	Removable Media Security संग सम्बन्धित	४८
२३	सूचना प्रणाली (Information System) को भौतिक सुरक्षा (Physical Security) संग सम्बन्धित	५०
२४	Desktop/Laptop Computer Security संग सम्बन्धित	५२
२५	Cloud मा राखिने डाटाको सुरक्षा (Cloud Data Security) संग सम्बन्धित	५४
२६	वेबसाइट सुरक्षा (Website Security) संग सम्बन्धित	५६
२७	कम्प्युटर ह्याकिंग (Computer Hacking) संग सम्बन्धित	५८
२८	कम्प्युटर ह्याकिंग (Computer Hacking) बाट कसरी बच्ने ?	६०
२९	साइबर सुरक्षाका लागि अपनाउनु पर्ने दश असल बानीहरु (Ten Good Habits for Cyber Security) संग सम्बन्धित	६२

१ पासवर्ड (Password) सँग सम्बन्धित

१. पासवर्ड कम्तीमा दस(१०) अक्षरको राखौं ।

२. पासवर्ड बनाउँदा Capital Letter (A–Z), Small Letter (a–z), Number(0–9), Special Character (!, @,#,$,%,^,&,*,–,+={}() आदि समावेश गरौं ।

३. पासवर्ड र प्रयोगकर्ताका नाम (Username) एउटै नराखौं ।

४. पासवर्ड बनाउँदा शब्दकोषमा भएको शब्दहरुको प्रयोग नगरौं ।

५. घर परिवार, साथीभाई, आफन्त आदिको नाम,मोबाईल नम्बर, फोन नं, ठेगाना, जन्ममिति जस्ता सजिलै अनुमान लगाउन सकिने शब्दहरु पासवर्डमा प्रयोग नगरौं ।

६. एउटै पासवर्डलाई धेरै वटा खातामा (Digital Account) प्रयोग नगरौं ।

७. पासवर्डलाई कम्तीमा पनि तीन/तीन महिनामा परिवर्तन गरौं ।

८. पहिले नै प्रयोग गरीसकेको पासवर्डलाई पुनः प्रयोग नगरौं ।

९. कुनै पनि प्रणालीमा रहेको Default(स्वतः) पासवर्डलाई परिवर्तन गरौं ।

१०. पासवर्डलाई अरु कसैसँग आदान प्रदान नगरी गोप्य राखौं । पासवर्डलाई कुनै सामाजिक सञ्जाल वा सञ्चार माध्यमबाट आदान प्रदान नगरौं ।

११. आफ्नो खाता (Digital Account)लाई सुरक्षित राख्न Multi–factor Authentication (जस्तै 2–Factor Authentication, Password को साथै Fingerprint, PIN code, Mobile Number, OTP, Facial Identity इत्यादि) को प्रयोग गरौं ।

२ फिशिंग स्क्याम (Phishing scam) सँग सम्बन्धित

(१) फिशिंग स्क्याम (Phishing scam) अथवा फिशिंग हमला (Phishing Attack) के हो ?

यो एक प्रकारको साइबर हमला (Cyber Attack)हो जसको प्रयोग गरेर साइबर अपराधीहरुले (Cybercriminals) इन्टरनेट प्रयोगकर्ताहरुको (Internet users) व्यक्तिगत विवरण, इमेल तथा पासवर्ड, बैंकको खाता नम्बर तथा पिन कोड आदि प्राप्त गर्ने साथै कुनै प्रलोभन वा डर धम्की देखाई बैंकबाट आफ्नो खातामा रकम जम्मा गर्न लगाउने जस्ता प्रयासहरु गर्छन र सोझासाझा व्यक्तिहरुलाई त्यस्तो जालमा पार्न सफल पनि हुन्छन् । यसको लागि साइबर अपराधीहरुले इमेल पठाउने, असली जस्तै देखिने नक्कली वेबसाइटको (Fake Website) प्रयोग गर्ने, संदेश (Message) पठाउने र फोनकलको समेत प्रयोग गर्छन् ।

(२) फिशिंग स्क्याम (Phishing scam) अथवा फिशिंग हमला (Phishing Attack) बाट कसरी बच्ने ?

फिशिंग स्क्याम (Phishing scam) अथवा फिशिंग हमला (Phishing Attack) बाट बच्न निम्न उपायहरु अपनाऔ :-

१. अपरिचित व्यक्ति वा ठेगानाबाट आएको शंकास्पद इमेललाई नखोलौं ।

२. अपरिचित व्यक्ति वा ठेगानाबाट आएको शंकास्पद इमेलको Attachment लाई नखोलौं ।

३. अपरिचित व्यक्ति वा ठेगानाबाट आएको इमेलमा रहेको Link हरुमा Click नगरौं र नखोलौं ।

४. अपरिचित व्यक्ति वा ठेगानाबाट आएको इमेल वा शंकास्पद इमेललाई तत्काल

Delete अथवा Block गर्नौं ।

५. इमेल Reply/Response नै गर्नुपरे Browser मा वेबसाइटको नाम Type गरेर मात्र गरौं ।

६. पुरस्कार(Prize), उपहार (Gift), चिठ्ठा (Lottery) लगायत विभिन्न प्रलोभन देखाएर पठाईएको वा डर धम्की दिई पठाईएको इमेल, संदेश फोनकल लगायतलाई Reply/Response नगरौं ।

७. परिचित वा अपरिचित व्यक्ति/संस्थाबाट आएको Email मा PDF, TEXT, CSV जस्ता Standard Format बाहेकका exe, vbs जस्ता extension का File हरु Click नगरौं र नखोलौं ।

८. आफूसँग सम्बन्धित नभएका Country domain/sub–domain बाट आएका इमेलहरुलाई नखोलौं र Delete गर्नौं ।

९. अनावश्यक Mailing List मा Subscribe नगरौं र अनावश्यक Mailing list मा Subscribed भएमा Unsubscribe गर्नौं ।

१०. इमेलबाट आफ्नो Password, OTP, Bank Account Number, PIN code जस्ता विवरणहरु नपठाऔ ।

११. कुनैपनि वेबसाइटको राम्रोसँग पहिचान नगरी Login Credentials (User Name and Password), बैंकको क्रेडिट कार्ड नम्बर, नागरिकता नम्बर लगायतका Personally Identifiable Information (PII) हरु Share नगरौं । आधिकारिक वेवसाइटको राम्रोसँग पहिचान गरेर मात्र आफ्नो विवरण Share गर्नौं ।

१२. प्राप्त हुन आएको कुनै इमेल वा वेबसाइटको विषयमा शंका लागेमा सम्बन्धित संस्थामा फोन सम्पर्क गरेर, इमेल पठाउने व्यक्ति वा संस्थाको राम्रोसँग पहिचान गरेर मात्र Reply/Response गरौं ।

१३. आफ्नो Computer/Laptop/Mobile Device आदिमा Antivirus को प्रयोग गरौं

३ सोसियल इन्जिनियरिंग (Social Engineering) सँग सम्बन्धित

(१)सोसियल इन्जिनियरिंग (Social Engineering) के हो ?

यो एक प्रकारको साइबर हमला (Cyber Attack) हो जसमा साइबर आक्रमणकर्ता (CyberAttacker) ले मनोवैज्ञानिक युक्तिहरू/रणनीतिहरू र मानिसहरूसँग भएको आफ्नो सम्बन्धको समेत प्रयोग गरेर पासवर्ड, बैंकको खाता नम्बर तथा पिनकोड, रकम प्राप्त गर्ने प्रयास गर्छन र सफल पनि हुन्छन् ।

सामान्यतया ह्याक गर्ने तरिकाहरू पत्ता लगाउन भन्दा मानिसको आर्कषण/झुकावलाई आफुतिर तानी उसको विश्वास जित्न सजिलो हुने हुँदा आक्रमणकर्ता (CyberAttacker) ले लोभ्याउने खालको सन्देश, संगीत, चलचित्रहरु सितैमा डाउनलोड गर्न दिने र सोही समयमा कम्प्युटरमा गोप्यरूपमा मालिसियस सफ्टवेयर स्थापना गरी कम्प्युटर प्रयोगकर्तासम्म पहुँच बनाउने गर्छन र कम्प्युटरलाई नियन्त्रण गर्ने गर्छन ।

त्यस्तै साइबर आक्रमणकर्ता(CyberAttacker) ले इन्टरनेट प्रयोगकर्तालाई झुक्याई पासवर्ड दिनको लागि मूर्ख बनाई, डर धम्की देखाई बैंकबाट आफनो खातामा रकम जम्मा गर्न लगाउने जस्ता प्रयासहरु गर्छन र सोझासाझा व्यक्तिहरुलाई त्यस्तो जालमा पार्न सफल पनि हुन्छन् ।

तसर्थ यसरी साइबर आक्रमणकर्ताहरुले इमेल पठाउने, असली जस्तै देखिने नक्कली वेबसाइटको (Fake Website) प्रयोग गर्ने, सन्देश (Message) पठाउने र फोनकलको समेत प्रयोग गर्ने र मनोवैज्ञानिक संगत क्रियाकलापबाट मानिसको विश्वास जित्न सफल भई सोझासाझा व्यक्तिहरुलाई ठगी गर्ने, डाटा चोर्ने तथा बेच्ने, संस्थाको मान प्रतिष्ठा तथा वित्तमा क्षति पुर्याउने जस्ता कार्य नै सोसियल इन्जिनियरिंग (Social Engineering) हो ।

(२)सोसियल इन्जिनियरिंग हमला (Social Engineering Attack) मा प्रयोग हुने माध्यम (Means)के के हुन सक्छन ?

सोसियल इन्जिनियरिंग (Social Engineering Attack) मा प्रयोग हुने माध्यमहरुः-

१. इमेल (Phishing Email)
२. टेलीफोन/मोवाइलवार्ता (Vishing)
३. पेनड्राइभ (USB Sticks)
४. वेभसाइट(Internet freebies)
५. भौतिक पहुँच (Physical impersonation)
६. इलेट्रोनिक फोहोर (Electronics Waste)

(३)सोसियल इन्जिनियरिंग हमला (Social Engineering Attack) बाट कसरी बच्ने ?

सोसियल इन्जिनियरिंग हमला (Social Engineering Attack) बाट बच्न निम्न उपायहरु अपनाऔ :-

(क)इमेल (Phishing Email)

१. शंकास्पद इमेललाई reply/response नगर्ने ।
२. इमेलको शंकास्पद attachments तथा प्राप्त भएका लिंकलाई नखोल्ने ।
३. Sender's email address तथा इमेलको embedded links लाई Cursor hovering गरी त्यसको आधिकारिकताको खोजविन तथा पहिचान गर्ने ।

(ख) टेलीफोन/मोवाइलवार्ता (Vishing)

१. सामान्यतया फोनमा संवेदनशील जानकारी प्रदान नगर्ने ।
२. उपहार(Gift)/चिठ्ठा (Lottery)/Working Visa बहानामा फोन गर्नेलाई

आफ्नो व्यक्तिगत विवरण नदिने ।

३. Caller ID, Text Message Sender ID, Short Code उपर शंका लागेमा खोजविन तथा आधिकारिकता पहिचान गर्ने ।

४. फोन गर्नेको नाम, संगठनात्मक एकाई वा बाह्य कम्पनीको नाम शंका लागेमा केही समय लिई खोजविन तथा आधिकारिकता पहिचान गरेर मात्र आफ्नो विवरण पठाउने ।

(ग) पेनड्राइभ (USB Sticks)

१. पेनड्राइभ(USB Sticks)मा Virus, Key loggers, Trojans, Ransomware जस्ता Malicious Software राखी हमला गर्न सक्ने भएकोले उक्त पेनड्राइभ (USB Sticks)लाई Virus Scan गरेर मात्र प्रयोग गर्ने ।

२. अति महत्वपूर्ण पूर्वाधारहरु (Critical Infrastructures e.g. Server)मा सामान्यतया पेनड्राइभ (USB Sticks)को प्रयोग नगर्ने ।

३. कुनै अपरिचित पेनड्राइभ (USB Sticks)फेला परेमा त्यसलाई आफ्नो कम्प्यूटरमा प्रयोग नगर्ने, पेनड्राइभ (USB Sticks)को फाइल (Contents) नखोल्ने ।

(घ) वेभसाइट(Internet freebies)

१. आधिकारिक वेभसाइटको पहिचान गरेर मात्र आफ्नो व्यक्तिगत विवरण प्रदान गर्ने ।

२. Cracked/Pirated Software Download गरी प्रयोगनगर्ने ।

३. असुरक्षित वेवसाइटहरु जस्तैः eMule, BitTorrent, Ares, etc. को प्रयोग नगर्ने ।

४. सितैमा विभिन्न offer हरु जस्तै movies, songs, music video, software, books etc. उपलब्ध गराउने असुरक्षित वेभसाइट (Internet freebies) प्रयोग नगर्ने ।

(ङ) भौतिक पहुँच (Physical impersonation)

१. कार्यस्थलको कम्प्युटर Password and Physical Lock गरेर राख्ने ।
२. कुनै पनि व्यक्तिलाई Access दिनु अगाडि त्यस व्यक्तिको सही पहिचान गर्ने ।
३. सूरक्षागार्डको उचित व्यवस्थापन गर्ने ।

(च) इलेट्रोनिक फोहोर डिस्पोजल (Electronics Wastedisposal)

१. काम नलाग्ने इलेट्रोनिक सामग्रीहरुमा पनि संवेदनशील विवरणहरु हुन सक्ने भएकोले उक्त सामग्रीहरुलाई जथाभावी डिस्पोज नगर्ने । संवेदनशील विवरणहरुलाई नष्ट गरेर मात्र डिस्पोज गर्ने ।
२. म्याद सकिएको इलेट्रोनिक कार्डहरू (जस्तै आईडी कार्डहरू, एटीएम कार्डहरू, Access कार्डहरू) डिस्पोज गर्नु अघि उक्त कार्डहरुबाट कुनै पनि विवरण निकाल्न नमिल्ने गरी डिस्पोज गर्ने ।
३. काम नलाग्ने हार्ड डिस्क, पेन ड्राइभ, मेमोरी स्टिकहरू तथा USB फ्ल्यास ड्राईभहरूमा रहेको इलेक्ट्रोनिक डाटा नष्ट गरेर मात्र डिस्पोज गर्ने ।

४ घरको वाइफाइ (Home WiFi) लाई कसरी सुरक्षित राख्ने ?

घरको वाइफाइ सुरक्षित (Home WiFi Security) राख्न निम्न उपायहरु अपनाऔं ।

१. इन्टरनेट सेवा प्रदायकले Home WiFi जडान गरिसकेपछि इन्टरनेट सेवा प्रदायकसंग WiFi Router को Admin Username तथा Password प्राप्त गरौं र उक्त पासवर्ड परिवर्तन गरौं ।

२. Wireless Home Network को Default Name (SSID) परिवर्तन गरौं र WiFi को लागि बलियो पासवर्ड राखौं ।

३. आफ्नो Home WiFi को SSID अरुले पहिचान गर्न नसक्ने बनाउन SSID लाई Hide गरौं ।

४. घरको वाइफाइलाई सुरक्षित बनाउन Network Encryption मा WPA2 / WPA3 लाई छनौट गरी Configure गरौ । साथै WiFi Protected setup (WPS) लाई Disable गरेर राखौं ।

५. Wireless Router को Software लाई नियमित अध्यावधिक (Update)हुने गरी Configure गरौं ।

६. घरको वाइफाइ प्रयोग गर्ने व्यक्तिहरुको मोबाइल, ल्यापटप, कम्प्युटर, ट्याबलेट आदि उपकरणहरुको MAC Address हरुलाई Bind गरेर WiFi प्रयोग गरौं ।

७. घरमा इन्टरनेट प्रयोग नहुने बखत वायरलेस राउटर (Router) को स्वीच अफ गरी राखौं ।

५ सार्वजनिक वाइफाइ (Free/Pubic WiFi) प्रयोग गरेर इन्टरनेट चलाउँदा कसरी सुरक्षित रहने ?

सार्वजनिक वाइफाइ (Free/Public WiFi) प्रयोग गरेर इन्टरनेट चलाउँदा सुरक्षति रहन निम्न उपायहरु अपनाऔं ।

१. कुनै सार्वजनिक संस्था/स्थान जस्तै सपिंग मल, होटेल, एयरपोर्ट, रेस्टुरेन्ट, कफी सप, सार्वजनिक यातायात आदिको आधिकारिक वाईफाईको नाम पहिचान गरी सो वाइफाइसँग दिईएको पासवर्ड प्रयोग गरेर मात्र इन्टरनेट चलाऔ । ह्याकरहरु (Hackers) ले पनि उस्तै देखिने Free Public WiFi बनाउन सक्ने भएकोले सो बाट साबधान रहौं ।

२. कुनै सार्वजनिक वाइफाई (Free Public WiFi) संग जोडिदा आफ्नो मोबाइल, ल्यापटप, कम्प्युटर, ट्याबलेट आदिको File Sharing Option बन्द गरी राखौं । साथै ल्यापटप, कम्प्युटर उपकरणमा भएको Firewall Option सधैको लागि ON गरी राखौं ।

३. पासवर्ड सुरक्षित (Password protected) नभएको खुल्ला वाइफाइ (Open WiFi) लाई प्रयोग गरी इन्टरनेट नचलाऔं ।

४. सार्वजनिक वाइफाइ/हटस्पटको प्रयोग गरेर इन्टरनेट चलाउँदा सकेसम्म VPN -Virtual Private Network) प्रयोग गरौं ।

५. सार्वजनिक वाइफाइ/हटस्पटको प्रयोग गरेर इन्टरनेट चलाउँदा सकेसम्म Encrypted (HTTPS भएको) वेभसाइट लाई मात्र Browse/Visit गरौं ।

६. सार्वजनिक वाइफाइ/हटस्पटको प्रयोग गरेर इन्टरनेट चलाउँदा व्यक्तिगत संवेदनशील विवरणहरु भएको मोबाईल एप्प (Mobile App) तथा साइटहरु जस्तैः Online Banking Site, Social Media आदि Browse नगरौं ।

७. व्यक्तिगत संवेदनशील विवरणहरु भएको मोबाईल एप्प (Mobile App) तथा साइटहरु जस्तैः Online Banking Site, Social Media आदि Browse गर्नु पर्दा आफ्नै मोवाईलको 3G/4G को डाटा प्रयोग गरौं ।

८. सार्वजनिक वाइफाइ प्रयोग गरे पश्चात आफू log in भएको प्रत्येक वेबसाइट/पोर्टलबाट तत्काल log out गरौं ।

९. सार्वजनिक स्थलमा उपलव्ध रहेको टर्मिनल/कम्प्युटरको प्रयोग गरी इन्टनेट चलाई सकेपछि आफूले Visit गरिएको Browsing History तथा Web Cache लाई delete गरौं ।

१०. सार्वजनिक वाइफाइ/नेटवर्कमा जोडिने उपकरण मोबाइल, ल्यापटप, कम्प्युटर, ट्र्याबलेट)मा अनिवार्य Antivirus राखौं ।

११. आफ्नो मोबाइल, ल्यापटप, कम्प्युटर, ट्र्याबलेट प्रयोग नभएको बेला आफ्नो उपकरणको Wi–Fi वा Bluetooth connectivity लाई बन्द गरी राखौं । साथै Wi–Fi को Auto Connection को सट्टा Manual Mode को प्रयोग गरौं ।

१२. सार्वजनिक वाइफाइ/नेटवर्कबाट Financial Transaction नगरौं । साथै सार्वजनिक वाइफाइ/नेटवर्कको प्रयोग गर्दा आफ्नो Password, OTP, Bank Account Number, PIN code/receiving tokens जस्ता विवरणहरु सम्बन्धी कुनै पनि कारेबार नगरौं ।

१३. आफ्नो डिजिटल खाता (Digital Account), इमेल खाता आदिलाई सुरक्षित राख्न कम्तिमा पनि Two Factor Authentication (2FA) को प्रयोग गरौं ।

१४. पुरानो (Old and Outdated) उपकरणहरु जोखिमयुक्त (Vulnerable) हुन सक्ने भएकोले त्यस्ता उपकरणहरु सार्वजनिक वाइफाइ (Free Public WiFi) मा जोडी इन्टरनेट नचलाऔ ।

६ सामाजिक संजालहरु (Social Media) जस्तैः Facebook, Twitter, LinkedIn आदि प्रयोग गर्दा कसरी सुरक्षित रहने ?

सामाजिक संजाल (Social Media)को सुरक्षित साथ उपयोग गर्न निम्न उपायहरु अपनाऔं।

१. छुट्टाछुट्टै सामाजिक संजाल(जस्तैः Facebook, Twitter)को आफ्नो खाता (Account) का लागि छुट्टाछुट्टै तथा बलियो पासवर्ड राखौ।
२. सामाजिक संजालको आफ्नो डिजिटल खाता (Digital Account)लाई सुरक्षित राख्न Multi–Factor Authentication (जस्तै Two Factor Authentication, Mobile Number, OTP, Fingerprint इत्यादि) को प्रयोग गरौं।
३. सामाजिक संजालको आफ्नो खाता Recovery को लागि Recovery Email तथा Mobile Number को प्रयोग गरौ।
४. सकेसम्म सामाजिक संजालको प्रयोग गर्दा आफ्नो उपकरण (मोबाइल, ल्यापटप, कम्प्युटर, ट्याबलेट) को प्रयोग गरौ। आफ्नो व्यक्तिगत डिभाइसहरु (ल्यापटप, मोबाइल आदि) लाई पासवर्ड, Pattern वा Finger Print (Biometric)वाट Lock गर्ने गरौं।
५. सामाजिक सञ्जालको प्रयोग गरिने उपकरण (मोबाइल, ट्याबलेट) हराउँदा सामाजिक सञ्जालको खाताको पासवर्ड तुरुन्तै परिवर्तन गरौं।
६. प्रत्येक सामाजिक सञ्जालमा Privacy Setting को Feature हुने भएकोले त्यसको प्रयोग गरी कुन कुन विवरणहरु सार्वजनिक गर्ने/नगर्ने Customize/Configure गरौं। जस्तैः Facebook मा आफ्नो email तथा phone number देखाउने वा लुकाउने।
७. सकेसम्म आफ्नो व्यक्तिगत विवरण जस्तैः Home Address, Phone Number इत्यादि सामाजिक सञ्जालमा नराखौ।

८. सामाजिक सञ्जालमा आफ्ना व्यक्तिगत संवेदनशील फोटो, User Name and Password, बैंकको क्रेडिट कार्ड नम्बर, पिन कोड, नागरिकता नम्बर लगायतका Personally Identifiable Information (PII) हरु Share नगरौं ।

९. कुनै पनि सन्देश, फोटो पोष्ट गर्दा सचेत रहने । (जस्तैः आफू कहाँ जाँदैछु , के गर्दैछु, को संग छु जस्ता विवरणको अरुले गलत फाइदा लिन सक्छन्) ।

१०. फोटो पोष्ट गर्न कसैले दबाब दिन्छ भने अस्वीकार गर्ने । आवश्यक परेको खण्डमा सामाजिक सञ्जालमा भएका नराम्रा साथीहरु (असहज क्रियाकलापहरु देखाउने) लाई ब्लक वा साथीको सुचीबाट हटाऔं ।

११. सकेसम्म अपरिचित व्यक्तिको Friend Request Accept नगरौ । गर्नै परे उक्त व्यक्तिले गरेको पोस्ट, व्यक्तिले राखेको विवरणलाई राम्ररी विचार गरी पहिचान गरेर मात्र सामाजिक संजालमा Friend Request Accept गरौं ।

१२. सामाजिक संजालमा साथीहरुले share गरेको लिंक तथा Attachment लाई सहि पहिचान गरेर मात्र Click/Open गरौं । उक्त लिंक तथा Attachment शंकास्पद लागेमा नखोलौं ।

१३. सामाजिक सञ्जाल मार्फत प्राप्त हुने पुरस्कार(Prize), उपहार (Gift), चिट्ठा (Lottery) लगायत बिभिन्न प्रलोभन देखाएर पठाइएको वा डर धम्की दिई पठाइएको संदेश, फोनकल लगायतलाई Reply/Response नगरौं ।

१४. सामाजिक सञ्जालको प्रयोग गर्दा यौन दुर्व्यवहारसँग सम्बन्धित केही असहज गतिविधिको महसुस गरेको खण्डमा अथवा घटना घटेको खण्डमा प्रमाण संकलन गरी प्रहरीमा उजुरी गरौं ।

७ Online Banking (Mobile Banking/ Internet Banking) सेवा कसरी सुरक्षित साथ प्रयोग गर्ने ?

Online Banking (Mobile Banking/Internet Banking) सेवाको सुरक्षित साथ प्रयोग गर्न निम्न उपायहरु अपनाऔं ।

१. Online Banking को प्रयोग गर्नु अगाडी आफ्नो बैंकको Online Banking सम्बन्धी नियम प्रक्रिया आदि बारे जानकारी लिऔं ।

२. Online Banking सेवा प्रयोग गर्दा सम्बन्धित बैंकको आधिकारिक वेबसाइट प्रयोग गरौं । Mobile Banking को लागि आधिकारिक Mobile App पहिचान गरेर मात्र Install गरी प्रयोग गरौं ।

३. Online Banking मा प्रयोग हुने Computer/Mobile/Laptop मा अनिवार्य रुपमा Password/Pattern/PIN/Biometric आदिको प्रयोग गरी Lock गर्ने गरौं ।

४. Online Banking को URL सधै टाइप गरी प्रयोग गरौं कहिलें पनि Email Link वा अन्य वेबसाइटमा रहेको Hyperlink Click गरी प्रयोग नगरौं ।

५. Online Banking को लागि Multi–Factor Authentication (जस्तै Two Factor Authentication, Mobile Number, OTP, Fingerprint इत्यादि) को प्रयोग गरौं ।

६. Banking Transaction को मोबाइल(SMS/Email) Notification सेवा अनिवार्य प्रयोग गरौं ।

७. आफ्नो Bank Statement नियमित चेक गरौं ।

८. आफ्नो Bank Account,Password, PIN Code, CVC, OTP कहिले पनि कसैलाई नदिऔं । बैंकका कर्मचारीहरुले कहिले पनि तपाइँको Password,

PIN Code, CVC, OTP जस्ता विवरण नमाग्ने हुँदा Fake Call/Scam हरुवाट बचौं ।

९. Online Banking को लागि बलियो पासवर्डको प्रयोग गरौं र पासवर्डलाई नियमित परिवर्तन गरौं ।

१०. आफ्नो Online Banking को Login Credential कहिले पनि Browser आदिमा Save नगरौं ।

११. Online Banking सेवा प्रयोग गरि सकेपछि Logout/Sign out गर्न नभुलौं ।

१२. सार्वजनिक स्थलका Computer (जस्तै Cyber Cafe etc.) वा सार्वजनिक WiFi को प्रयोग गरी Online Banking सेवा प्रयोग नगरौं ।

१३. Online Banking को लागि प्रयोग गरिने Computer/Mobile Device तथा Mobile App हरुलाई नियमित अपडेट गर्ने गरौं ।

१४. आफ्नो बैंक खातामा कुनै शंकास्पद गतिविधि देखिएमा तुरुन्त बैंकमा सम्पर्क गरौं ।

१५. Computer, Mobile, Laptop आदिमा Genuine Anti–Virus को प्रयोग गरौं ।

८ मालवेयर (Malware) के हो ?

क) मालवेयर (Malware: **Mal**icious Soft**ware**) ह्याकरद्वारा निर्माण भएको यस्तो प्रोग्राम हो जसलाई ह्याकर/साईबर अपराधीले इमेल/इन्टरनेट तथा पेन ड्राइभ (USB Stick/Driver) वा संक्रमित (Infected) कम्प्युटरको माध्यमबाट अन्य कम्प्युटर तथा कम्प्युटर प्रणालीलाई बिगार्न तथा नष्ट गर्न प्रयोग गर्ने गर्छन।
मालवेयर (Malware) विभिन्न प्रकारका हुन्छन् जस्तैः Spyware, Ransomware/Crypto–malware, Adware, Virus, Trojan, Worms, Bot & Botnets, Rootkits, Keyloggers, Spam/Phishing आदि।

ख) मालवेयर (Malware Attack) कहाँबाट आउँछ ?

इन्टरनेट प्रयोगकर्ताले

- इमेल मार्फत प्राप्त असुरक्षित फाइल Attachment तथा लिंकलाई Click गर्दा,
- संक्रमित (Infected) पेन ड्राइभ (USB Stick/Driver)लाई फाइल स्थानान्तरण (Transfer/Copy) गर्नको लागि प्रयोग गर्दा,
- Visit गरिएको वेभसाईट अन्तर्गत Pop–Up Window/Banner मा Click गर्दा,
- सामाजिक संजाल (Social Media) जस्तैः Facebook, Twitter, Linkedin तथा WhatsApp/Viber मा प्राप्त असरक्षित Attachmen तथा लिंकलाई Click गर्दा,
- Freeware/shareware तथा Pirated Software, Music/Video डाउनलोड गर्दा प्रयोगकर्ताको कम्प्युटर/मोवाइलमा मालवेयर (Malware) डाउनलोड तथा Install हुन्छ।

ग) मालवेयर (Malware) ले के हानी गर्न सक्छ ?

कम्प्युटर मालवेयर Install भए पछि यसले कम्प्युटर प्रयोगकर्ताको दैनिक क्रियाकलापलाई अवलोकन गरी प्रयोगकर्तालाई थाहै नदिई चल्ने र आर्थिक तथा व्यक्तिगत संवेदनशील डाटामा ह्याकर/साईबर अपराधीलाई पहुँच पुऱ्याई दिने देखि सम्पूर्ण महत्वपूर्ण डाटालाई प्रयोग गर्न नसक्ने गरी Encryption गरी दिने र कम्प्युटर प्रणालीलाई नचल्ने गराई दिन सक्छ ।

घ) मालवेयर (Malware) बाट कसरी सुरक्षित रहने ?

मालवेयर (Malware) बाट सुरक्षित रहन निम्न उपायहरु अपनाऔं ।

१. Freeware, Pirated software/game, Free music/video, अश्लील सामाग्री उपलब्ध हुने जस्ता असुरक्षित वेबसाइटहरुको प्रयोग नगरौं । त्यस्ता अशुरक्षित वेभसाइटहरु Visit गर्दा Pop–Up Window/Banner मा प्रचारको लागि आउने लिंकिमा Click नगरौं र त्यस्ता वेबसाइटहरुबाट Freeware/shareware तथा Pirated Software, Music/Video/games डाउनलोड नगरौं ।

२. सामाजिक सञ्जाल (Social Media) जस्तैः Facebook, Twitter, Linkedin तथा WhatsApp/Viber मा प्राप्त हुने शंकास्पद Attachment तथा लिंकलाई Click नगरौं ।

३. कम्प्युटर तथा कम्प्युटर प्रणालीमा इमेल/इन्टरनेटको लिंक तथा Attachment लाई सहि पहिचान गरेर मात्र Click/open गरौं । साथै उक्त लिंक तथा Attachment शंकास्पद लागेमा नखोलौं ।

४. असुरक्षित वेबसाइटहरुको Cookies Request लाई स्वीकार (Accept) नगरौं । त्यसलाई Ignore गरौं ।

५. कुनै कारणबश कम्प्युटर तथा कम्प्युटर प्रणाली ह्याक भई ह्याकरले डाटा (Data) Encryption गरी उक्त Data Decryption को लागि ह्याकरले पैसा भुक्तानी माग गरेमा त्यस्ता ह्याकरलाई भुक्तानी नगरौं । ह्याकरलाई भुक्तानी गर्दैमा उक्त Data Decryption हुने सम्भावना हुदैन ।
६. बेवारिसे रुपमा भेटिएको पेन ड्राइभ (USB Stick/Driver) लाई कम्प्यटुर तथा कम्प्युटर प्रणालीमा प्रयोग नगरौं ।
७. असुरक्षित वेबसाइटहरु पहिचान गर्ने Netcraft जस्ता Security Browser Add-on Tools को प्रयोग गरौं ।
८. कम्प्युटर तथा कम्प्युटर प्रणालीको भण्डारण हुने महत्वपूर्ण डाटा (Data) लाई नियमित backup राखौ ।
९. कम्प्युटर तथा कम्प्युटर प्रणालीमा Anti–Virus/Anti–Malware/Spam Filter को प्रयोग गरी नियमित स्कान (Scan) गरौं ।
१०. कम्प्युटर तथा कम्प्युटर प्रणालीको Firewall लाई सधै Active “ON” राखौ ।
११. कम्प्युटर तथा कम्प्युटर प्रणालीमा प्रयोग भएका Software लगायत Operating System, Anti–Virus/Anti–Malware/Spam Filter लाई नियमित (Update) गरौं ।
१२. सकेसम्म खुल्ला वाइफाइ (असुरक्षित वाइफाइ) को प्रयोग नगरौं ।
१३. इमेल/इन्टरनेट मार्फत फैलिने नयाँ Virus/Cyber Attack बारेमा जानकारी राखौं । सो विषयमा अरुलाई समेत जानकारी गराऔं ।
१४. कम्प्युटर, कम्प्युटर प्रणाली र डिजिटल खातामा बलियो पासवर्डको प्रयोग गरौं । उक्त पासवर्ड समय समयमा परिवर्तन अवश्य गरौं ।
१५. कम्प्यटर र कम्प्यटर प्रणालीलाई सुरक्षित राख्न Multi–Factor Authentication (जस्तैः Two Factor Authentication, Mobile Number, OTP, Fingerprint इत्यादि) को प्रयोग गरौं ।

१६. इमेल/इन्टरनेट मार्फत पुरस्कार (Prize), उपहार (Gift), चिठ्ठा (Lottery), भिषा (VISA) लगायत विभिन्न प्रलोभन देखाएर पठाईएको वा डर धम्की दिई पठाइएको संदेश, फोनकल लगायतलाई Reply/Response नगरौं ।

१७. इमेलबाट आफ्नो Password, OTP, Bank Account Number, PIN code जस्ता विवरणहरु नपठाऔ ।

१८. कुनै पनि वेबसाइटको राम्रोसँग पहिचान नगरी Login Credentials (User Name and Password), बैंकको क्रेडिट कार्ड नम्बर, नागरिकता नम्बर लगायतका Personally Identifiable Information (PII) हरु Share नगरौं । अर्थात आधिकारिक वेबसाइटको राम्रोसँग पहिचान गरेर मात्र आफ्नो विवरण Share गरौं ।

१९. प्राप्त हुन आएको कुनै इमेल वा वेबसाइटको विषयमा शंका लागेमा सम्बन्धित संस्थामा फोन सम्पर्क गरेर, इमेल पठाउने व्यक्तिको वा संस्थाको राम्रोसँग पहिचान गरेर मात्र Reply/Response गरौं ।

१ अनलाइन बाल सुरक्षाका लागि जारी सन्देश

हाम्रा बालबालिकाले अचेल मोबाईल वा कम्प्युटर वा टयाब्लेट आदिबाट अनलाइन कक्षा लिने, इन्टरनेट चलाउने, गेम खेल्ने, गीतहरु सुन्ने, भिडियो हेर्ने लगायतका कार्यहरु गरिरहेका छन् ।

इन्टरनेटको प्रयोग गर्दा हाम्रा बालबालिकाहरुलाई इन्टरनेटले सिर्जना गर्न सक्ने विभिन्न खताराहरुबाट सुरक्षित राख्नुपर्ने र सुरक्षित तबरले इन्टरनेट चलाउन सिकाउनुपर्ने हुन्छ । तसर्थ हाम्रा बालबालिकाहरुलाई इन्टरनेटबाट हुनसक्ने जोखिमबाट बचाउन निम्न उपायहरु अपनाऔं ।

१. बालबालिकाले अनलाइनमा गर्ने गतिबिधि बारे जानकारी राखौं र बालबालिकासँग खुलेर कुरा गरौं, साथै सो बारे कुरा गर्न अभिप्रेरित गरौं ।
२. बालबालिकाले हेर्ने भिडियोहरु (Youtube, Tiktok लगायत), चलाउने सामाजिक सञ्जाल (Facebook आदि), खेल्ने Game हरु र अन्य गतिबिधिहरुको बारेमा आफूले समेत जानकारी राखौं ।
३. यदि बालबालिकाले सामाजिक सञ्जालको प्रयोग गर्छन् भने उनीहरुका साथीहरु को को छन्, के के Share गर्छन्, कस्ता कुराकानी गर्छन् सो को बारेमा जानकारी राखौं ।
४. बालबालिकाले सामाजिक सञ्जालको प्रयोग गर्दा हुन सक्ने सम्भावित अनुचित गतिविधिहरुको बारेमा जानकारी राखौं र नियमित निगरानी गरौं ।
५. बालबालिकाले मोबाईल वा कम्प्युटर वा टयाव्लेटमा बिताउने समयलाई सिमीत गरौं । बालबालिकालाई खेलकुद, शारीरिक व्यायाम, ध्यान, योगा, संगीत जस्ता अतिरिक्त क्रियाकलापहरुमा पनि समावेश गराऔं ।
६. बालबालिकाले नियमित रुपमा चलाउने Online Class आदिको लिंकलाई सहज पहुँचको लागि Bookmark गरी आफ्नो बालबालिकालाई सो को प्रयोग गर्न सिकाऔं ।

७. बालबालिकाले के हेर्दै/गर्दैछन् भन्ने कुरा निगरानी गर्न उनीहरुले चलाउने कम्प्युटर वा टयाव्लेट आदिको स्क्रिनलाई सबैले देखिने गरी राखौं।

८. बालबालिकालाई आफ्नो User ID, पासवर्ड जस्ता व्यक्तिगत विवरणहरु गोप्य राख्न सिकाऔं।

९. बालबालिकालाई अनलाइन भेटेको साथीसँग सकेसम्म भौतिक रुपमा भेटन निरुत्साहित गरौं।

१०. बालबालिकाले प्रयोग गर्ने कम्प्युटरमा Antivirus, Ad Block, Netcraft आदि Tools को प्रयोग गरौं।

११. अनावश्यक तथा प्रयोग नभएका डिजिटल खाताहरु बन्द गरौ/गर्न लगाऔ ं।

१२. आफ्नो इनटरनेट सेवा, Operating System र Application मा रहेको Parental Control/Child Safety Feature प्रयोग गरौं।

१३. Freeware, Pirated software/game, Free music/video, अश्लील सामग्री उपलब्ध हुने जस्ता असुरक्षित वेबसाइटहरुको प्रयोग नगर्न सिकाऔ। त्यस्ता असुरक्षित वेबसाइटहरुले पठाउने Pop–Up Window/Banner मा प्रचारको लागि आउने लिंकमा Click नगर्न सिकाऔं।

१४. कम्प्युटरमा इमेल/इन्टरनेटको लिंक तथा Attachment लाई सही पहिचान गरेर मात्र Click/open गर्न सिकाऔ। त्यस्ता लिंक तथा Attachment शंकास्पद लागेमा नखोल्न सिकाऔं।

१५. कुनै शंकास्पद गतिविधि र असहज परिस्थिति भएमा आफ्नो अभिभावकलाई जानकारी दिन बालबालिकालाई सिकाउनु होस् र कुनै गम्भिर विषय भए सम्बन्धित निकायमा उजुरी गरौं।

१० मोबाइल सुरक्षा (Mobile Security) सँग सम्बन्धित

मोबाइल ह्याण्डसेट/स्मार्ट फोनलाई ह्याकरहरुबाट जोगाउन निम्न उपायहरु अपनाऔं।

१. गुगल प्ले स्टोर वा एप स्टोर (Official Reputed App Store) बाट मात्र Rating तथा Review को आधारमा मात्रै App Download गरी Install गरौं।

२. App Install गर्दा App ले Camera Access/Location Tracking / Contacts /Media/Audio/File Access को Permission माग गरेमा Deny गरौं।

३. कुनै पनि App Install गर्नु भन्दा अगाडि सो App संग सम्बन्धित End–User Agreement तथा App को Privacy Policy अवश्य पढौं । App ले मोबाइलको कुन कुन Data Access गर्छ र App मार्फत Third Party हरुलाई share हुने व्यक्तिगत विवरण सम्बन्धमा जानकारी राखौं।

४. मोबाइललाई बलियो पासवर्ड (Password) तथा डिजिटल औंठाछाप जस्ता Bio–metric Log In प्रयोग गरी सुरक्षित राखौं । पासवर्ड (Password) समय समयमा परिवर्तन गरौं।

५. स्मार्ट फोनलाई Jailbreak/root गरी प्रयोग नगरौं। भेटिएको स्मार्ट फोनको प्रयोग नगरी नजिकैको प्रहरी कार्यालयमा बुझाऔं।

६. प्रयोग नभएको बेला मोबाइल ह्याण्डसेटलाई Lock गरेर राखौ। साथै Idle अवस्थाको लागि Auto–Lock हुने गरी फोनको Settings मा Configure गरौं।

७. मोबाइल फोनको सफ्टवेयर (Operating System / Applications) लाई नियमित रुपमा अद्यावधिक गरौं। साथै मोबाइल फोनको सुरक्षाको लागि अनिवार्य

रुपमा Genuine Firewall/Anti Virus/Mobile Security Solutions को प्रयोग गरौं।

८. प्रयोग नहुने बेला मोबाइल फोनको WiFi, Bluetooth, Mobile Data, GPS आदि लाई बन्द (OFF) गरी राखौ।

९. अरुले मोबाइल फोनको प्रयोग गर्न नसक्ने गरी मोबाइल ट्र्याकिङ हुन सक्ने गरी, Completely Wipe out गर्न सक्ने गरी तथा सिमकार्ड परिवर्तन गरेमा कुनै निश्चित नम्बरमा Alert आउने गरी Configure गरौं। यस्ता settings ले मोबाइल हराएमा भेट्टाउन सहयोग पुऱ्याउँछ र मोबाइलमा भएका व्यक्तिगत विवरणहरु अरुको पहुँच पुग्नबाट बचाउँछ।

१०. मोबाइल मार्फत डिजिटल कारोबार गर्दा असुरक्षित Free Public WiFi/Hotspot को प्रयोग नगरौं।

११. मोबाइल ह्याण्डसेटमा हुने संवेदनशील डाटाको Backup राखौं। साथै मोबाइलमा समेत उक्त संवेदनशील डाटालाई encryption गरेर राखौं।

१२. मोबाइल ह्याण्डसेटबाट अनलाइन तथा मोबाइल बैंकिङ्ग सेवा उपभोग गर्न मोबाइल डाटा/Secure WiFi प्रयोग गरौं। साथै Multi–factor Authentication जस्तै Two Factor Authentication, Mobile Number, OTP, Fingerprint इत्यादि) को प्रयोग गरौं।

१३. अपरिचित मोबाइल नम्बर/इमेल/ Whats App/Viber/Messenger आदिबाट आएको सन्देश, फोनकल लगायतलाई Reply/Response नगरौं।

१४. Freeware, Pirated software/game, Free music/video, अश्लील सामग्री उपलब्ध हुने जस्ता असुरक्षित वेबसाइटहरुको प्रयोग नगरौं, Pop–up link मा जथाभावी Click नगरौं र Freeware/shareware तथा Pirated Software, Music/Video/games डाउनलोड नगरौं।

१५. मोबाइल फोनलाई अरुको सजिलै पहुँच पुग्ने गरी यतिकै नछाडौं।

११ Licensed/Open Source Software को प्रयोगसँग सम्बन्धित

क) Genuine/Licensed/Open Source Software को प्रयोग नगरी Cracked/Pirated Software प्रयोग गर्दा के के जोखिम हुन सक्छ ?

१. Genuine/Licensed/Open Source Operating System वा Application Software को प्रयोग नगर्दा कानून अनुसार हदै सम्मको कारबाही सक्ने सम्भावना रहन्छ।

२. अवैध रुपमा प्राप्त हुने सफ्टवेयर (Cracked/Pirated)को प्रयोग गर्दा अद्यावधिक (Patch Update) नहुने भएकोले उक्त सफ्टवेयर संक्रमित हुन सक्ने हुँदा व्यापार व्यवसायमा असर पर्ने र Vulnerabilities को कारणले व्यवसायिक संवेदनशील विवरणहरुमा ह्याकरको सजिलै पहुँच हुन सक्छ।

३. Cracked/Pirated Software प्रयोगबाट पासवर्ड तथा संवेदनशील डाटा (PIN / Bank/Insurance) चोरी हुन सक्छ।

४. Cracked/Pirated Software download गरी प्रयोग गर्दा तथा अरुलाई share गर्दा खतरनाक (Dangerous) किसिमको संक्रमणहरु (Virus / Trojan /Malware/Rootkit etc.) सर्न सक्छ।

५. Cracked/Pirated Software प्रयोग भएको उपकरणबाट गृह नेटवर्क (Home Network) मा आवद्द रहेका फोन, ट्याब्लेट, र अन्य कम्प्युटरहरू जस्ता अन्य उपकरणहरुमा समेत मालवेयर सर्ने र नेटवर्कमा आवद्द रहेका उपकरणहरुमा ह्याकरको पहुँच सजिलै पुग्न गई प्रयोगकर्तालाई थाहै नदिई कम्प्युटर/उपकरण प्रयोगकर्ताको दैनिक क्रियाकलापलाई ह्याकरले अवलोकन गर्ने देखि सम्पूर्ण महत्वपूर्ण डाटालाई प्रयोग गर्न नसक्ने बनाई दिन सक्छ र कम्प्युटर प्रणालीलाई समेत नचल्ने गराउन सक्छ।

(ख) Cracked/Pirated Software वाट हुन सक्ने सम्भावित जोखिमवाट बच्ने उपायहरु :

१. Licensed वा Open Source Software को प्रयोग गरौं।

२. Cracked/Pirated Software को सट्टामा Licensed/Free trial/Free version को प्रयोग गरौं।

३. शिक्षण सिकाई तथा व्यवसायिक प्रयोजन लगायतको कार्यहरुमा Licensed/Open source Operating System तथा Application Software को प्रयोग गरौं।

४. Licensed/Open Source Software हरु उक्त सफ्टवेयर निर्माता कम्पनीको आधिकारिक वेबसाइटवाट मात्र डाउनलोड गरौं।

५. Cracked/Pirated Software को प्रयोगलाई निरुत्साहन गरौं ।

१२ रान्समवेयर (Ransomware) सँग सम्बन्धित

क) रान्समवेयर (Ransomware)के हो ?

रान्समवेयर (Ransomware) एक प्रकारको मालवेयर (Malware: **Mal**icious Soft**ware**) हो जसको प्रयोग गरेर ह्याकर/साईबर अपराधीले ईमेल/इन्टरनेट तथा पेन ड्राइभ (USB Stick/Driver) वा संक्रमित (Infected) कम्प्युटरको माध्यमबाट महत्वपूर्ण डाटा तथा कम्प्युटर प्रणालीलाई बिगार्न तथा नष्ट गर्न प्रयोग गर्ने गर्छन। साथै कम्प्युटर प्रयोगकर्ताबाट फिरौती रकम प्राप्त नगरेसम्म कम्प्युटर प्रयोगकर्ताको डाटालाई सार्वजनिक गर्ने वा महत्वपूर्ण डाटालाई प्रयोग गर्न नसक्ने गरी Encryption/Lock गरी दिने गर्छन। कतिपय अवस्थामा म्याद तोकी ह्याकर/साईबर अपराधीले कम्प्युटर प्रयोगकर्ताबाट रकम/विट क्वाइन(Crypto Currency) माग्ने तर उक्त समयावधि भित्र भुक्तानी नगर्दा महत्वपूर्ण डाटालाई सधैको लागि नष्ट(Delete) गरी दिनुको साथै ह्याकर/साईबर अपराधीले सामान्यता मागेको रकम/विट क्वाइन (Crypto Currency)भुक्तानी पाए पनि प्रयोगकर्ताको डाटालाई उपलब्ध गराउदैन। रान्समवेयर (Ransomware) धेरै प्रकारका हुन्छन् जस्तैः WannaCry, UIWIXCryptoLocker, NotPetya, Bad Rabbit, Cerber, Crysis, CryptoWall, GoldenEye, Jigsaw, Locky आदि।

ख) रान्समवेयरआक्रमण (Ransomware Attack)कहाँ बाट आउँछ ?

इन्टरनेट प्रयोगकर्ताले

- इमेल मार्फत प्राप्त असुरक्षित फाइल Attachment तथा लिंकलाई Click गर्दा,

- संक्रमित (Infected) पेन ड्राइभ (USB Stick/Driver)लाई फाइल स्थानान्तरण (Transfer/Copy) गर्नको लागि प्रयोग गर्दा,
- Visit गरिएको असुरक्षित वेभसाईटमा आएको Pop–Up Window/Banner मा Click गर्दा,
- सामाजिक संजाल (Social Media)जस्तैः Facebook, Twitter, LinkedIn तथा WhatsApp/Viber मा प्राप्त प्राप्त असुरक्षित Attachment तथा लिंकलाई Click गर्दा,
- Freeware/shareware तथा Pirated Software, Music/Video डाउनलोड गर्दा, प्रयोगकर्ताको कम्प्युटर/मोवाईलमा रान्समवेयर (Ransomware) डाउनलोड भई Install हुन्छ।

ग) रान्समवेयर आक्रमण (Ransomware Attack)बाट कसरी सुरक्षित रहने ?

रान्समवेयर (Ransomware Attack)बाट सुरक्षित रहन निम्न उपायहरु अपनाऔं।

१. कम्प्युटर तथा कम्प्युटर प्रणालीको भण्डारण हुने महत्वपूर्ण डाटा (Data) लाई नियमित backup राखौं।

२. कुनै कारणबश कम्प्युटर तथा कम्प्युटर प्रणाली ह्याक भई ह्याकरले डाटा (Data) Encryption गरी उक्त DataDecryption को लागि पैसा भुक्तानी माग गरेमा त्यस्ता ह्याकरलाई भुक्तानी नगरौं। ह्याकरलाई भुक्तानी गर्दैमा उक्त Data Decryption हुने सम्भावना हुदैन।

३. कम्प्युटर, कम्प्युटर प्रणाली र डिजिटल खातामा बलियो पासवर्डको प्रयोग गरौं। उक्त पासवर्ड समय समयमा परिवर्तन गरौं।

४. कम्प्युटर र कम्प्युटर प्रणालीलाई सुरक्षित राख्न Multi–Factor Authentication (जस्तै Two Factor Authentication, Mobile Number, OTP, Fingerprint

आदि) को प्रयोग गरौं।

५. कम्प्युटर तथा कम्प्युटर प्रणालीमा Anti–Virus/Anti–Malware/Spam Filter को प्रयोग गरी नियमित स्कान (Scan) गरौं।

६. कम्प्युटर तथा कम्प्युटर प्रणालीमा प्रयोग भएका Software लगायत Operating System, Anti–Virus/Anti–Malware/Spam Filter लाई नियमित अद्यावधिक (Update) गरौं।

७. Freeware, Pirated software/game, Free music/video, अश्लील सामग्री उपलब्ध हुने जस्ता असुरक्षित वेभसाइटहरुको प्रयोग नगरौं। त्यस्ता असुरक्षित वेबसाइटहरु Visit गर्दा Pop–Up Window/Banner मा प्रचारको लागि आउने लिंकमा Click नगरौ र त्यस्ता वेबसाइटहरुबाट Freeware/shareware तथा Pirated Software, Music/Video/games डाउनलोड नगरौं।

८. सामाजिक सञ्जाल (Social Media)जस्तैः Facebook, Twitter, LinkedIn तथा WhatsApp/Viber मा प्राप्त हुने शंकास्पद Attachment तथा लिंकलाई Click नगरौं।

९. कम्प्युटर तथा कम्प्युटर प्रणालीमा इमेल/इन्टरनेटको लिंक तथा Attachment लाई सहि पहिचान गरेर मात्र Click/open गरौं उक्त लिंक तथा Attachment शंकास्पद लागेमा नखोलौं।

१०. वेवारिसे रुपमा भेटिएको पेन ड्राइभ (USB Stick/Driver)लाई कम्प्युटर तथा कम्प्युटर प्रणालीमा प्रयोग नगरौं।

१३ पासवर्डलाई कसरी सुरक्षित साथ राख्ने ?

आफ्नो पासवर्डलाई सुरक्षित साथ राख्न निम्न उपायहरु अपनाऔं ।

१. धेरै वटा पासवर्डहरु स्मरण गरेर राख्न सम्भव नहुने भएकोले विश्वासिलो तथा भरपर्दो Password Manager को प्रयोग गरेर आफ्नो पासवर्डहरु सुरक्षित राखौ ।

२. सकेसम्म offline password manager को प्रयोग गरौं र सो को एक प्रति अन्य उपकरणमा समेत नियमित Backup गरी राखौं ।

३. Online Password Manager को प्रयोग गर्नु पर्दा Two Factor Authentication वा Multi Factor Authentication को प्रयोग गरौं ।

४. Password Manager को लागि बलियो पासवर्ड (Strong Password)प्रयोग गरौं र उक्त पासवर्डलाई स्मरण गरी राखौं । साथै, Password Recovery को लागि आफ्नो मोबाइल नम्बर वा इमेलको प्रयोग गरौं ।

५. Browser मा पासवर्डलाई Save गर्ने नगरौं । Browser को Password Auto Save लाई Disable गरौं ।

६. धेरै वटा पासवर्डहरु स्मरण गरेर राख्न सम्भव नहुने भएकोले पासवर्डहरुलाई अरुले नबुझ्ने (Encryption) गरी कागजमा लेखी समेत सुरक्षित साथ राख्न सकिन्छ ।

७. पासवर्डलाई आफ्नो इमेलमा Store/Save नगरौं । साथै, कसैलाई पनि Share नगरौं ।

१४ भिसिंग (Vishing) सँग सम्बन्धित

क) भिसिंग (Vishing)के हो ?

भिसिंग(Voice + Phishing) एउटा भ्वाईस अथवा भी.ओ.आई.पी. (VoIP) मा आधारित Phishing Attack हो जसमा साइवर अपराधीहरुले सोसियल इन्जिनियररिङ्गको प्रयोग गरेर टेलिफोन वा मोबाइल वा Viber वा Messenger वा Whatsapp वा कुनै पनि अपरिचित नम्बरबाट फोन गरी हतार (Urgency) देखाई वा कुनै प्रलोभन वा डर धम्की देखाई, बैंक खाता वा क्रेडिट कार्ड वा पिन कोड आदिमा समस्या भएका जानकारी गराउँदै सहयोग गर्ने बाहानामा कम्प्युटर वा मोबाइल प्रयोगकर्ताहरुको संवेदनशील व्यक्तिगत तथा वित्तीय विवरण, इमेल तथा पासवर्ड, पिन कोड, बैंकको खाता नम्बर आदि प्राप्त गर्ने, बैकबाट आफ्नो खातामा रकम जम्मा गर्न लगाउने जस्ता प्रयासहरु गर्छन् र आफ्नो जालमा पार्न सफल हुन्छन् ।

ख. भिसिंग(Vishing)बाट बच्न के गर्ने ?

भिसिंगबाट बच्न निम्न उपायहरु अपनाऔं ।

१. अपरचित नम्बरबाट आउने फोन नउठाऔ । साथै त्यस्ता अपरिचित नम्बरहरुमा कल ब्याक (Call Back) पनि नगरौं ।

२. झुक्किएर अपरिचित नम्बरबाट आएको फोन उठाउँदा त्यस्ता अपरिचित व्यक्तिहरुले हतारमा मागेको कुनै पनि विवरणहरु उपलव्ध नगराऔं । साथै उक्त फोनकल उपर कुनै शंका लागेमा तुरुन्तै उक्त फोनकल काटौं । उपरोक्त नम्बरहरुबारे प्राधिकरणको आधिकारिक इमेल info@nta.gov.np वा Complaint Handling System (https://complain.nta.gov.np/) मार्फत जानकारी गराऔं ।

३. कुनै अपरिचित व्यक्तिबाट विभिन्न प्रलोभन (चिठ्ठा, उपहार, भिषा, सामाजिक सुरक्षा, Loan) देखाई आएको फोनकल वा भ्वाईस सन्देश (Voice Message) लाई विश्वास नगरौं र जवाफ नफर्काऔं ।

४. कसैले आकस्मिक (Urgent) रुपमा फोन गरेर Bank Account /Credit Card Compromise भनी सहयोग गर्ने बहानामा Password, OTP, Bank Account Number, PIN code तथा मोबाइलमा आएको कोड माग गर्दा त्यस्तो संवेदनशील विवरणहरु कसैलाई पनि नदिऔं ।

५. कसैले पनि फोन मार्फत नागरिकता नम्बर, पासपोर्ट नम्बर, बिमा नम्बर, बैंक खाता नम्बर लगायतका Personally Identifiable Information (PII) हरु माग गर्दा उक्त विवरणहरु कसैलाई पनि उपलव्ध नगराऔं ।

६. कसैले फोन वा भ्वाईस सन्देश मार्फत आफ्नो उपकरणको कुनै बटन (Button) थिच्न वा कुनै लिंकमा क्लिक (Click) गर्न सुझाए अनुसार कहिले कार्य नगरौं ।

७. आफ्नो बैंकको वित्तीय विवरण, पिनकोड, पासवर्ड लगायतका कुनै पनि संवेदनशील विवरण चोरेको शंका लागेमा तत्काल पासवर्ड, पिनकोर्डहरु परिवर्तन गरौं र सम्बन्धित संस्था/बैंकलाई तत्काल जानकारी गराऔं ।

८. अपरिचित व्यक्तिबाट आउने Scam Call लाई Block गर्न आधिकारिक वा विश्वासिलो एप्स (APPS) को प्रयोग गरौं ।

१५ फारमिंग आक्रमण (Pharming Attack) सँग सम्बन्धित

क) फारमिंग आक्रमण (Pharming Attack) के हो ?

फारमिंग आक्रमण (Pharming Attack) एक प्रकारको अनलाइन ठगी (Online Fraud) हो जसमा साइबर अपराधीहरु (Pharmers/Cyber Criminals) ले प्रयोगकर्ताको कम्प्युटर तथा सर्भर (Server) मा Malicious Code Install गरी प्रयोगकर्तालाई थाहै नदिई हेर्न खोजेको Website को IP Address परिवर्तन (Computer Local Host File वा DNS Cache Corruption/ DNS server Poisoning) गरी कुनै Click विना नै प्रयोगकर्तालाई Fake/Bogus/Fraudulent Website मा स्वतः निर्देशित (Autodirect) गराई उक्त Fake/Bogus/Fraudulent Website को माध्यमबाट प्रयोगकर्ताको व्यक्तिगत संवेदनशील विवरणहरु जस्तै PIN Code, Payment Card Details, Password आदि प्राप्त गर्ने गर्दछन् । तत्पश्चात अपराधीहरुले उक्त पासवर्ड तथा पिन कोड प्रयोग गरी वित्तीय ठगी (Financial Fraud) अर्थात रकम Transfer गर्ने वा चोर्ने गर्दछन् ।

ख) फारमिंग आक्रमण (Pharming Attack) भएको कसरी थाहा पाउने ?

- यदि Browse गर्न खोजिएको वेबसाइटमा https को सट्टा http देखियो भने,
- यदि वेबसाइटमा अस्वभाविक त्रुटीहरु (जस्तैः spelling error, unfamiliar font or color) देखिने, वास्तविक भन्दा भिन्न लाग्ने, वैद्य (legitimate) साइट जस्तो नदेखिने भयो भने फारमिंग आक्रमण (Pharming Attack) भएको हुन सक्छ ।

ग) फारमिंग आक्रमण (Pharming Attack) बाट कसरी बच्ने ?

फारमिंग आक्रमण (Pharming Attack) बाट बच्न निम्न उपायहरुरु अपनाऔं ।

१. Https भएको secure वेबसाइटमा मात्र Browse वा Visit गरौं। जस्तैः https: // www.nta.gov.np

२. विश्वासिलो तथा सुरक्षित (Trusted and Safe) Browser (जस्तै Mozilla Firefox etc.) को प्रयोग गरौं।

३. शंकास्पद वेबसाइटको Browse वा Visit नगरौं।

४. कुनै पनि वेबसाइट Navigate गर्दा उक्त वेबसाइट Completely load हुन दिई उक्त वेबसाइटको URL (जस्तैः https://nta.gov.np/) मा spelling error/swapping letters भए नभएको कुरा ध्यान पूर्वक जाँच गरौं।

५. कारोवार गर्नु भन्दा अगाडि आधिकारिक वेभसाइट भए/नभएको पहिचान गरेर मात्र कारोवार गरौं।

६. Consumer–grade Routers / Access Points (AP) मा रहेको default password लाई परिवर्तन गरौं।

७. प्राय अपराधीहरु (Pharmers) ले सस्तो अथवा Free offer दिने जस्ता लोभ्याउने खालको Commercial Fake Site प्रयोग गर्ने भएकोले आधिकारिक Commercial Site मा मात्र आफ्नो व्यक्तिगत संवेदनशील विवरण share गरौं र त्यस्ता आधिकारिक Commercial Site बाट मात्र अनलाइन सपिंग/कारोवार गरौं।

८. Secure Browsing को लागि Reputed DNS Servers भएको VPN सेवा मात्र प्रयोग गरौं।

९. अपरिचित व्यक्तिबाट प्राप्त इमेलको Attachment तथा link लाई Click नगरौं।

१०. Two Factor Authentication वा Multi Factor Authentication को प्रयोग गरौं।

११. आधिकारिक तथा Reputed Anti–virus/Anti–malware वा Firewall सफ्टवेयरको प्रयोग गरौं।

१६ स्निफिंग आक्रमण (Sniffing Attack) सँग सम्बन्धित

(१) स्निफिंग आक्रमण (Sniffing Attack) के हो ?

स्निफिंग (Sniffing) भनेको इन्टरनेट प्रयोग गर्दाको बखत इन्टरनेट प्रयोगकर्ताको गतिविधिहरुको जासुसी गर्नु हो।

स्निफर (Sniffer) भनेको प्रोग्राम वा हार्डवेयर हो जसलाई साइबर अपराधीले इन्टरनेट प्रयोगकर्ताको गतिविधिहरुलाई जासुस (Spy) गर्न प्रयोग गर्छन्।

साइबर अपराधीहरुले स्निफिंग आक्रमण गरी इन्टरनेट प्रयोगकर्ताको गतिविधि/डाटा थाहै नदिई प्राप्त गर्ने र सो को विश्लेषण गरी Personally Identifiable Information (PII) (जस्तैः- User Name, Password, बैंकको क्रेडिट कार्ड नम्बर, नागरिकता नम्बर आदि) समेत प्राप्त गर्दछन्।

२. स्निफिंग आक्रमण (Sniffing Attack) भएको कसरी थाहा पाउने ?

कम्प्युटर/ल्याप्टप/मोबाइल उपकरण आदिको भण्डारण क्षमता अचानक घट्न गएको देखिएमा Sniffing Attack भएको हुन सक्छ।

३. स्निफिंग आक्रमण (Sniffing Attack) बाट कसरी बच्ने ?

स्निफिंग आक्रमण (Sniffing Attack) बाट बच्न निम्न उपायहरु अपनाऔं :-

१. असुरक्षित सार्वजनिक वाईफाई (Public Wifi) को प्रयोग नगरौं।

२. आफ्नो डाटालाई सुरक्षित रुपमा encrypt गरी स्थानान्तरण(Transfer/transmit) गर्न Reputed VPN को प्रयोग गरौं।

३. कम्प्युटर/ल्याप्टप/मोबाइल उपकरणमा Malicious Activities हुन नदिन Reputed Antivirus को प्रयोग गरौं ।

४. HTTP भएको वेबसाइट असुरक्षित हुने भएकोले सकेसम्म त्यस्तो वेबसाइटको प्रयोग नगरौं। HTTPS वा Lock Icon/Symbol सहितको URL भएको वेबसाइटको मात्र प्रयोग गरौं।

५. साइबर अपराधीहरुले सोसियल इन्जिनिरिंग (Social Engineering) वा फिसिंग इमेल (Phishing Email) वा असुरक्षित वेबसाइट मार्फत जासुसी सफ्टवेयर अर्थात Sniffer download गराई दिने भएकोले अपरिचित व्यक्ति वा ठेगानाबाट आएको शंकास्पद इमेलको Attachment वा लिंकलाई नखोलौं। साथै असुरक्षित वेबसाइटको प्रयोग नगरौं।

६. असुरक्षित सफ्टवेयर, एप, Freeware जथाभावी download नगरौं। Unencrypted/plain text messaging भएको एप्सको सकेसम्म प्रयोग नगरौं।

७. कुनै पनि वेबसाइटको राम्रोसंग पहिचान नगरी Login Credentials (User Name and Password), बैंकको क्रेडिट कार्ड नम्बर, नागरिकता नम्बर लगायतका Personally Identifiable Information (PII) हरु Share नगरौं। आधिकारिक बेवसाइटको राम्रोसंग पहिचान गरेरमात्र आफ्नो विवरण Share गरौं।

१७ म्यान इन द मिडल आक्रमण (Man in the Middle Attack: MITM) सँग सम्बन्धित

(१) म्यान इन द मिडल अट्याक क हो ?

म्यान-इन-द-मिडल अट्याकमा Sender तथा Receiver को विचमा तेश्रो पक्ष (hacker) ले प्रवेश गरी Sender को सबै Message (e.g. Password, Personally Identifiable Information, Credit Card number, Conversation etc.) प्राप्त गर्ने र सो लाई आफ्नो अनकुल परिवर्तन गरेर Receiver लाई पठाइदिने गर्दछ। साथै, Receiver बाट प्राप्त भएको Message लाई पनि आफ्नो अनकुल परिवर्तन गरी Sender लाई पठाइदिने गर्दछ। अर्थात, तेश्रो पक्ष (Hacker) ले Sender र Receiver बीचको सबै Message हरु प्राप्त गर्न र आफ्नो अनकुल परिवर्तन गरी दुरुपयोग पनि गर्न सक्छ।

(२) म्यान इन द मिडल अट्याकले कसरी काम गर्छ ?

म्यान इन मिडल अट्याक दुई चरणमा हुने गर्छन।

क) पहिलो चरणः यस चरणमा साईबर अपराधी म्यान इन मिडल अट्याकको लागि इन्टरनेट ट्राफिकलाई गन्तव्यमा पुग्नु भन्दा पहिले प्राप्त गर्दछ, जसलाई Interception भनिन्छ। यो Interception कार्य पुरा गर्न साईबर अपराधीले IP Spoofing, ARP Spoofing, DNS Spoofing आदि तरिकाहरु अपनाउने गर्छन।

ख) दोस्रो चरणः पहिलो चरणमा साईबर अपराधीले Interception लाई पुरा गर्न सफल भए पछी उक्त Intercepted Traffic लाई दोस्रो चरणमा HTTPS Spoofing, SSL Beast, SSL Hijacking, SSL Stripping लगायतका विधिहरु प्रयोग गरी traffic को Original Content प्राप्त गर्दछ।

(३) म्यान इन द मिडल अट्याकबाट कसरी बच्ने ?

म्यान-इन-द-मिडल अट्याकबाट बच्न निम्न उपायहरु अपनाऔ :-

१. आफ्नो डाटालाई सुरक्षित साथ स्थानान्तरण (Transfer) गर्न डाटालाई Secure Channel मार्फत Encrypt गरी पठाऔं।
२. आफ्नो कम्प्युटर/ल्याप्टप/मोबाइल तथा Network मा Firewall/IPS/IDS को प्रयोग गरौं।
३. असुरक्षित सार्वजनिक वाइफाइको प्रयोग नगरौं। घरको वाइफाइमा समेत WPA2/3 को mode मा प्रयोग गरौं साथै WPS Disable गरेर राखौं।
४. Browser मा Force TLS (स्वतः रुपमा HTTPS प्रयोग हुने गरी) Plugin को प्रयोग गरेर मात्र अनलाइन कारोवार गरौं
५. सुरक्षित इमेलको लागि SSL/TLS/PGP/GPG encryption को Setting राखी प्रयोग गरौं।
६. HTTPS वा Lock Icon सहित URL भएको वेबसाइटको प्रयोग गरौं।
७. आफ्नो Software (Operating System, Application Software, Browser) लाई निरन्तर Update गरौं।
८. आफ्नो कम्प्युटर/ल्याप्टप/मोबाइल उपकरणमा मालवेयरको क्रियाकलाप अथवा Malicious Activities हुन नदिन Reputed Antivirus को प्रयोग गरौं।
९. असुरक्षित सफ्टवयर, एप्स, फ्रिवेयर download नगरौं। साथै unencrypted/plain text messaging गर्ने एप्सको प्रयोग नगरौं।
१०. इमेलबाट आफ्नो Password, OTP, Bank Account Number, PIN code जस्ता विवरणहरु नपठाऔं।

१८ कार्यालयको Corporate Network को सुरक्षासँग सम्बन्धित

कुनै पनि कार्यालयको Corporate Network लाई सुरक्षित बनाउन निम्न उपायहरु अपनाऔंः

१) आफ्नो संस्थाको लागि Information System (IS) Security Policy निर्माण गरी लागु गरौं।

२) आफ्नो कर्मचारी तथा प्रयोगकर्ताहरुलाई नियमित रुपमा सूचना प्रविधि तथा साइबर सुरक्षा सम्बन्धि चेतनामूलक तालिमहरु प्रदान गरौं।

३) कार्यालयको कर्पोरेट नेटवर्कलाई Segmentation र Segregation गरौं। Critical Infrastructure भएको नेटवर्क र Publicly Access हुने नेटवर्कलाई अलग गरौं। जस्तै बैंक तथा वित्तीय संस्थाहरुले आफ्नो कारोवार गर्ने र Internet प्रयोग हुने नेटवर्कलाई अलग-अलग राख्न जरुरी हुन्छ।

४) Guest हरुको प्रयोगको लागि आफ्नो Main Network भन्दा छुट्टै Guest Network निमार्ण गरौं।

५) कार्यालयको कर्पोरेट नेटवर्कलाई सुरक्षित बनाउन विश्वासिलो तथा भरपर्दो Unified Threat Management (UTM) System / Firewall / Intrusion Prevention System (IPS) /Intrusion Detection System(IDS) को प्रयोग गरौं।

६) Network Devices (Firewall, Router Switches) हरुको Default Configuration लाई परिवर्तन गरी उचित तरिकाले configure गरौं।

७) कार्यालयको कर्पोरेट नेटवर्कको Security Assessment तथा नियमित Information Security Audit गराऔं।

८) कार्यालयको Wireless Network मा कम्तिमा पनि WiFi Protected Access 2 (WPA2) encryption को प्रयोग गरौं।

९) Network Hardware (Router, Switches, Firewall) हरुलाई भौतिक रुपमा सुरक्षित हुने गरी राखौं।

१०) कार्यालयको कर्पोरेट नेटवर्कको लागि विश्वसनीय, भरपर्दो तथा गुणस्तरीय उपकरणहरुको प्रयोग गरौं।

११) Critical Infrastructure भएको नेटवर्कमा Access प्रदान गर्दा MAC Address Binding को प्रयोग गरौं।

१२) कार्यालयको कर्पोरेट नेटवर्कमा Access Control तथा Log Maintain गर्ने व्यवस्था गरौं।

१३) कार्यालयको कर्पोरेट नेटवर्कका End Devices हरुमा Antivirus को प्रयोग गरौं।

१४) Network Devices (Firewall, Router Switches) हरुको Firmware/Software हरुलाई नियमित रुपमा update/upgrade गरौं।

१९ डिस्ट्रिब्युटेड डिनायल अफ सर्भिस आक्रमणसँग सम्बन्धित

(१) डिस्ट्रिब्युटेड डिनायल अफ सर्भिस (Distributed Denial of Service) आक्रमण के हो ?

Distributed Denial of Service(DDoS) Attack एउटा यस्तो आक्रमण हो जसमा साईबर अपराधीले नेटवर्कमा आबद्ध रहेका विभिन्न उपकरणहरुलाई संक्रमित बनाई सोही उपकरणहरुको प्रयोग गरी सेवा प्रदान गर्ने सर्भरलाई लक्षित गरी आक्रंमण गर्दछ। यसले गर्दा उक्त सर्भरबाट उद्देश्य अनुरुपको सेवा उपलब्ध हुन सक्दैन। DDoS आक्रमण सामान्यतया Volume Based Attacks, Protocol Attacks, Application Attacks गरी तीन प्रकारका हुन्छन्। साइबर अपराधीबाट भएका केही महत्वपुर्ण DDoS आक्रमणहरु यस प्रकार रहेका छन् :

- The AWS DDoS Attack(2020)
- Google Attack (2017)
- The GitHub Attack in (2018)
- The Mirai Dyn DDoS Attack(2016)
- The CloudFlare DDoS Attack(2014)
- The Spamhaus DDoS Attack(2013)
- Six Banks DDoS Attack (2012)

(२) डिस्ट्रिब्युटेड डिनायल अफ सर्भिस आक्रमणले कसरी काम गर्छ ?

साइबर अपराधीले Botnet अर्थात Zombie Computers (Network of thousands to millions of remotely controlled, hacked computers or bots) प्रयोग

गरी लक्षित वेबसाइट, नेटवर्क तथा सर्भरमा Packet Flood पठाई DDoS आक्रमण गर्ने गर्दछ। Packet Flood आक्रमणहरु मुख्यतः यस प्रकारका हुन्छन्।

क. Network Layer : Smurf Attacks, ICMP Floods, and IP/ICMP Fragmentation

ख. Transport Layer: TCP Attacks include SYN Floods, UDP Floods, and TCP Connection Exhaustion

ग. Application Layer: HTTP–encrypted attacks.

यसरी Packet Flood पठाउँदा सर्भरको सबै स्रोत साधन (Resources) प्रतिउत्तर पठाउन व्यस्त हुने र सर्भर crash समेत हुन गई उद्देश्य अनुसारको सेवा प्रदान गर्न सक्दैन।

(३) डिस्ट्रिब्युटेड डिनायल अफ सर्भिस आक्रमण भएको कसरी थाहा पाउने ?

प्रयोगकर्ताको कम्प्यूटर तथा नेटवर्कमा निम्न लक्षणहरु निरन्तर देखिएमा DDoS आक्रमण भएको हुन सक्छ।

- Locally or remotely फाइल access गर्दा ढिलो हुने।
- कुनै वेबसाइट खोल्दा लामो समयसम्म पनि नखुल्ने।
- इन्टरनेट सेवा बारम्बर अबरुद्द हुने।
- कुनै पनि वेबसाइट नखुल्ने।
- धेरै Spam इमेल प्राप्त हुने।

(४) डिस्ट्रिब्युटेड डिनायल अफ सर्भिस आक्रमणबाट कसरी बच्ने ?

१. प्रत्येक संस्थाले आफ्नो नेटवर्क तथा सर्भरको सुरक्षा कमजोरीहरु (Security Vulnerabilities) पहिचान गर्न Information Security Audit गरौं।

२. सुरक्षा कमजोरीहरु (Security Vulnerabilities) लाई यथाशिघ्र हटाऔं ।
३. DDoS आक्रमणबाट बच्न DNS सर्भरको Bandwidth लाई नियन्त्रण गरौं ।
४. Router र नेटवर्क Firewall लाई Latest Security Patch सहित नियमित रुपमा अद्यावधिक(update) गरौं ।
५. नेटवर्क ट्राफिकलाई नियमित अनुगमन (Monitor) गरौं ।
६. Malicious traffic लाई रोक्न UTM/ Next Generation Advanced Firewall /Intrusion detection systems (IDS)/ Intrusion Prevention systems(IPS) को प्रयोग गरौं ।
७. नेटवर्कमा जडित उपकरणहरुमा Default पासवर्ड हटाई बलियो पासवर्ड राखौं ।
८. Router Configuration गर्दा Security Policy Best Practices तथा Cyber Hygiene को नीति अवलम्बन गरौं ।
९. Zero Trust Security Model अपनाऔं ।
१०. DDoS Response Battle Plan सहितको Business Continuity Plan, Disaster Recovery तथा Emergency Response Plan तयार गरौं ।
११. आफ्नो नेटवर्क वा सर्भरमा DDoS आक्रमण भएको देखिएमा तत्काल इन्टरनेट सेवा प्रदायकलाई वा साइवर सुरक्षा विज्ञलाई जानकारी गराई समस्या समाधान गर्न पहल गरौं ।
१२. नेटवर्कको Critical Server को उपलब्धताको लागि Backup मा अर्को इन्टरनेट लिंक पनि राखौं ।

२० कुकिज सूरक्षा (Cookies Security) सँग सम्बन्धित

(क) कुकिज (Cookies) के हो ?

कुनै Website Browse गर्दा उक्त Web Server ले प्रयोगकर्ताको Device वा Web Browser मा राख्ने सानो Text File/Data लाई Cookies or Internet Cookies भनिन्छ। यो मुख्यतः Internet प्रयोगकर्ताको Username, ID, Email, Preference जस्ता विवरणहरु Save गरी राम्रो इन्टरनेट अनुभुति प्रदान गर्नका लागि प्रयोग गरिन्छ। यसलाई Session Management, Personalization / Tracking(User/Device) गर्ने प्रयोजनको लागि समेत प्रयोग गरिन्छ। Cookies मुख्यतः निम्न प्रकारका हुन्छन् - Session Cookies, Persistent Cookies, Third–Party Cookies, Super Cookies, Zombie Cookies।

(ख) कुकिज (Cookies) ले कसरी काम गर्छ ?

कुनै वेबसाइट पहिलो पटक Browse वा Visit गर्दा प्रयोगकर्ताको कम्प्युटरमा उक्त वेबसाइटबाट प्रयोगकर्ताको अनुमति लिई (वा नलिई) Cookies Download र Save भएर बस्छ। अर्को पटक उक्त वेबसाइट Browse वा Visit गर्दा Save भएर बसेका Cookies (Unique ID) मार्फत प्रयोगकर्ताको विवरण Server ले सजिलै प्राप्त गरी इन्टरनेट प्रयोगानुभुति बढाउन मद्दत गर्छ। Cookies मार्फत प्रयोगकर्ताको Browsing Behavior लाई Track गरी प्रयोगकर्ता सुहाउँदो विज्ञापन पठाउने गर्दछ।

(ग) कुकिज (Cookies) बाट हुन सक्ने जोखिम के के हुन ?

साधारणतया सबै वेबसाइटमा Browse वा Visit गर्दाको बखत Accept Cookies भनी प्रयोगकर्ताको सहमति माग्ने गर्छन्। कुनै वेबसाइटमा Accept Cookies लाई "Yes"

भनी सहमति दिंदा उक्त वेबसाइटसंग आबद्द रहेको Third Party ले समेत Save भएर रहेको विवरणमा पहुँच पाउँछ। यसरी कुकिजले Store गर्ने विवरण साधारणतया: Plain Text मा हुने भएकोले एउटा वेबसाइटको लागि Save भएर रहेको संवेदनशील विवरणमा (User Credentials, Bank Details, Personal Information etc) अर्को वेबसाइटको कुकिज मार्फत साइबर अपराधीले सजिलै cross site scripting प्रयोग गरी विवरणहरु सजिलै चोर्न सक्छन्। तसर्थ Cookies बाट हाम्रो गोपनीयता भंग हुने र Security Threat रहने जोखिम हुन्छ। साथै प्रयोगकर्ताको गतिविधि तथा आनीबानीलाई साइबर अपराधीले Cookies को डाटा मार्फत Track गर्न सक्छ।

(घ) कुकिज (Cookies) वाट हुन सक्ने साइबर हमलावाट कसरी बच्ने ?

Cookies बाट हुन सक्ने साइबर हमलावाट बच्न निम्न उपायहरु अपनाऔ :-

१. वेबसाइटहरु Browse वा Visit गर्दा Cookies हरुलाई नपढी सहमति प्रदान नगरौं।

२. वेबसाइटले प्रदान गर्ने कुकिजलाई सर्वप्रथम राम्रोसंग पढेर Customize गरौं।

३. कुकिजको लागि सहमति नमाग्ने वेबसाइटहरु सुरक्षा खतरा भए / नभएको पहिचान गरी Browse/Visit गरौं।

४. Trusted Website तथा Https (Lock Icon) भएको वेबसाइटको मात्र प्रयोग गरौं।

५. Browser मा उचित तरिकाले Cookies को Setting लाई Configure गरौं। जस्तै: आफुले प्रयोग गर्ने Browser को Privacy Settings मा रहेको “Do not Track” जस्ता Option को प्रयोग गरौं।

६. मोबाईलमा Third Party मार्फत सजिलै Track हुन सक्ने भएकोले सकेसम्म मोबाईलबाट हुने Web Browse लाई सिमित गरौं।

७. सम्भव भएसम्म एउटै Browser को प्रयोग नगरौं। बैंकिङ्ग कारोबार लगायतको कार्य गर्दा सुरक्षित Browser (जस्तैः Mozilla Firefox)को प्रयोग गरौं।

८. Internet चलाउँदा Browser को Private Browsing Mode को प्रयोग गरौं।

९. समय समयमा आफ्नो Browser मा भएको Cookies तथा Site Data हरुलाई Clear गरौं।

१०. कुनै वेबसाइटमा Login गरेको भएमा काम सकिने बितिक्कै Log Out गर्ने गरौं।

११. Browser मा विश्वासिलो Ad–Block गर्ने तथा Securely Browse गर्ने Plugin हरुको प्रयोग गरौं।

१२. आफ्नो कम्प्युटर, मोबाइल आदिमा Internet Security Software को प्रयोग गरौं।

२१ इमेल सुरक्षा (Email Security) सँग सम्बन्धित

(क) इमेल सुरक्षा (Email Security) के हो ?

इमेलमा अनाधिकृत पहुँच, Email Data Loss, इमेलमा प्राप्त हुने Spam Message, Phishing Message आदि लाई रोक्नको लागि वा आफ्नो इमेल खातामा अनावश्यक वा Threat Message हरुलाई आउनबाट रोक्नका लागि अपनाइने विभिन्न सुरक्षाका विधि तथा उपायहरुलाई नै इमेल सुरक्षा भनिन्छ।

साइबर अपराधीले मालवेयर, स्पाम र फिशिंग आक्रमण (Phishing/Attacks) को लागि ईमेललाई एक लोकप्रिय माध्यमको रुपमा प्रयोग गर्ने गर्छन्। इमेलमा भ्रामक सन्देशहरु पठाई, Attachment खोल्न लगाई वा लिंकमा क्लिक गर्न लगाई प्रयोगकर्ताको उपकरणमा मालवेयर स्थापित (Install) गर्ने गर्दछन्। तत्पश्चात प्रयोगकर्ताको उपकरणलाई पूर्णरुपमा आफ्नो नियन्त्रणमा लिई प्रयोगकर्ताको क्रियाकलापलाई अनुगमन गर्ने, व्यक्तिको Financial विवरण चोर्ने, कम्पनीको गोप्य तथा संवेदनशील विवरण सार्वजनिक गरिदिने जस्ता अपराधिक क्रियाकलापहरु गर्छन्। तसर्थ ईमेल सुरक्षा व्यक्तिगत र व्यापारिक ईमेल खाताहरु दुबैको लागि नै आवश्यक हुन्छ।

(ख) प्राप्त इमेल असुरक्षित इमेल (Unsecure Email) हो वा होइन कसरी छुट्याउने ?

इमेल मेसेजमा निम्न बमोजिमको संकेत देखिएमा असुरक्षित इमेल हुन सक्छ।

- अपरिचित व्यक्तिबाट आएको अस्वभाविक किसिमको इमेल भएमा।
- Prize, VISA, Lottery परेको भन्ने जस्ता लोभ्याउने खाले Content भएको इमेल भएमा।
- अस्वाभाविक किसिमको लिंक तथा Attachment पठाइएको इमेल भएमा।
- आकर्षक विज्ञापन भएको इमेल भएमा।

- आफुसंग असम्बन्धित मान्छेको इमेल प्राप्त भएमा।
- untrusted Domain जस्तै .....@afhdo3e.com देखिएमा।

(ग) इमेल (Email) कसरी सुरक्षित बनाउने ?

इमेल सुरक्षित बनाउन निम्न उपायहरु अपनाऔ :

१. इमेल सुरक्षाको लागि Email Service Provider ले प्रदान गरेको Security Features लाई Enable गरौं।

२. अनलाइन Subscription हरुमा Registration गर्दा Business वा आफ्नो महत्वपूर्ण इमेलको प्रयोग नगरौ।

३. सकभर व्यक्तिगत इमेल सार्वजनिक नगरौ। भिन्न भिन्न उदेश्यको लागि फरक फरक इमेलको प्रयोग गरौ। साथै Social Media मा राखिएको इमेल लगायतका व्यक्तिगत विवरणलाई private setting गरेर राखौं।

४. शंकास्पद देखिने इमेलबाट Phishing/ Malware/Social Engineering लगायतका सुरक्षा जोखिम हुन सक्ने भएकोले त्यस्ता शंकास्पद इमेल, Spam/Junk इमेललाई नखोलौ। साथै उक्त इमेलको Reply पनि नगरौं।

५. अनावश्यक इमेल आएमा त्यस्तो इमेललाई Spam वा Junk मा जाने वा Block गर्ने गरी Configure/Setting गरौं।

६. अनावश्यक वेबसाइटमा Subscribe नगरौ। यदि Subscribed गरेको भए उक्त वेबसाइटबाट प्राप्त इमेलमा दिईएको unsubscribe लिंक मार्फत unsubscribe गरौ।

७. इमेल सुरक्षाको लागि SPAM Filter तथा Antivirus को प्रयोग गरौ ।

८. सार्वजिनक स्थानमा राखिएको कम्प्युटरबाट इमेल login गर्दा उक्त कम्प्युटरमा भएको Keylogger को प्रयोग गरी Username तथा Password चोरी हुन सक्ने

भएकोले त्यस्ता कम्प्युटरबाट सकेसम्म login नगरौं। यदि गरेको भए पनि आफ्नो व्यक्तिगत कम्युटरबाट पासवर्ड यथासिघ्र पासवर्ड परिवर्तन गरौं।

९. शंकास्पद इमेलको लिंक तथा Attachment लाई Click नगरौ ।

१०. आफ्नो इमेलमा बलियो पासवर्ड राखौ र समय समयमा पासवर्ड परिवर्तन गरौ। साथै इमेल Recovery को लागि Multifactor Authentication को समेत प्रयोग गरौ।

११. Business इमेल वा आफ्नो महत्वपूर्ण इमेल सार्वजनिक वाइफाइबाट नखोलौ।

१२. Remotely कम्पनीको इमेल खोल्दा VPN को प्रयोग गरौ।

१३. सुरक्षित इमेल प्राप्त गर्नको लागि SSL/TLS/PGP/GPG encryption Solution लगायतको प्रयोग गरौ।

१४. कम्पनी/संस्थाको लागि Secure Email Gateway को प्रयोग गरौ ।

१५. Email Security Policy तर्जुमा गरी सो को कार्यान्वयन गरौ।

२२ Removable Media Security सँग सम्बन्धित

(क) Removable Media के हो ?

Removable Media भनेको डाटालाई भण्डारण (Data Storage) गर्ने एउटा यस्तो उपकरण (Device) हो जसलाई कम्प्युटर प्रडालीसँग (चालु अवस्थामा रहेको वा नरहेको) सजिलै जोड्न वा झिक्न सकिन्छ। USB flash drives, Removable Disk (Blu–ray disk, DVDs, CD–ROMs), Memory Cards (Compact flash card, Secure digital card, Memory stick), External hard drives, Digital cameras, Audio recorders, Smartphones आदि Removable Media का उदाहरणहरु हुन्।

(ख) Removable Media सुरक्षा के हो ?

Removable Media बाट कम्प्युटरमा Data Transfer गर्दा कम्प्युटर प्रणाली मालवेयरबाट संक्रमित (Malware Infected) हुन सक्छ। त्यस्तै कम्प्युटर प्रणालीबाट Removable Media मा Data Transfer गर्दा Removable Media पनि संक्रमित हुन सक्छ। यसरी हुन सक्ने संक्रमण (Malware Infection) बाट सुरक्षित राख्न अपनाइने उपायहरु Removable Media सुरक्षा हो।

(ग) Removable Media बाट हुन सक्ने जोखिमहरु के के हुन ?

असुरक्षित Removable Media प्रयोग गर्दा निम्न बमोजिमको जोखिमहरु हुन सक्छन।

- Removable Media, कम्प्युटर तथा नेटवर्कमा मालवेयर(Malware) प्रवेश गर्न सक्ने।
- Removable Media तथा कम्प्युटर प्रणालीको संवेदनशील तथा महत्वपूर्ण डाटा Loss हुन सक्ने।

- संवेदनशील तथा गोप्य विवरणहरु चुहावट भई वा Loss भई संस्थाको प्रतिष्ठामा क्षती (Reputation Damage) हुन सक्ने।
- Business strategy, Business plan सँग सम्बन्धित विवरणहरु Loss भई आर्थिक क्षती (Financial Damage) हुन सक्ने।

(घ) Removable Media को सुरक्षा कसरी गर्ने ?

Removable Media को सुरक्षाको लागि निम्न उपायहरु अपनाऔं :-

१. USB drives, Memory sticks, Smartphones, SD cards, External hard drives, DVDs, or other removable media लाई अरुको पहुँच नहुने गरी गोप्य स्थानमा राखौं।

२. सामान्यतया संवेदनशील डाटालाई Removable Media मा नराखौं ।

३. Removable Media मा संवेदनशील डाटा राख्नै पर्ने भए Whole disk लाई सधै Encryption गरेर राखौं।

४. Removable Media को Encryption Password वा Passphrase कसैलाई share नगरौं।

५. Removable Media मा राखिएको व्यक्तिगत Content लाई Delete गरेर मात्र अरुलाई प्रयोग गर्न दिऔं।

६. आफ्नो कम्प्युटर/ल्यापटप/मोबाइल उपकरणमा विश्वसनीय Antivirus को प्रयोग गरौं।

७. Removable Media लाई नियमित रुपमा Scan गर्ने गरौं।

८. असुरक्षित तथा सार्वजनिक कम्प्युटरमा आफ्नो Removable Media लाई प्रयोग नगरौं।

९. कतै भेटिएको वा अपरिचित व्यक्तिबाट प्राप्त शंकास्पद Removable Media लाई आफ्नो कम्प्युटरमा सिधै प्रयोग नगरौं।

१०. Removable Media मा भएका विवरणलाई Backup गरी राख्ने गरौं ।

११. कम्प्युटर प्रणालीको Auto Play/Auto Run Feature लाई Disable गरेर राखौं ।

१२. संवेदनशील डाटा भएको Removable Media लाई विसर्जन (Dispose) गर्दा निकाल्न नसक्ने गरी सुरक्षित तवरले विसर्जन (Dispose) गरौं।

२३ सूचना प्रणाली (Information System) को भौतिक सुरक्षा (Physical Security) सँग सम्बन्धित

(क) सूचना प्रणाली (Information System) को भौतिक सुरक्षा (Physical Security) भनेको के हो ?

Information System (IS) को भौतिक सुरक्षा भन्नाले Information system राखिएको भवन सहित हार्डवेयर, सफ्टवेयर, नेटवर्क र डाटाहरुलाई अनधिकृत भौतिक पहुँच, उच्च तापक्रम, High Voltage, चट्याङ, चोरी, तोडफोड, दुर्घटना, आगलागी, प्राकृतिक प्रकोपहरु जस्तै भूकम्प, बाढी आदिबाट सुरक्षा गर्नु भन्ने बुझाउँछ ।

(ख) सूचना प्रणाली (Information System को भौतिक सुरक्षा (Physical Security) कसरी गर्ने ?

Information System को भौतिक सुरक्षा (Physical Security) को लागि निम्न उपायहरु अपनाऔं :-

१. सूचना प्रणाली (Information System) हरु राख्नका लागि स्थान पहिचान गर्दा बाढी, पहिरो, भूकम्प जस्ता प्राकृतिक प्रकोपहरुको जोखिम न्यून रहेको स्थान (Site) को चयन गरौं ।

२. भूकम्प आइरहने स्थान भए भूकम्प प्रतिरोधी भवनमा र बाढी आइरहने स्थान भए भवनको माथिल्लो तल्लामा सूचना प्रणाली (Information System) राखौं ।

३. आधिकारिक व्यक्तिको मात्र प्रवेशको लागि Access Card/Access Control जस्ता प्रणाली र गार्डको व्यवस्था गरौं ।

४. High Temperature/Humidity लाई नियन्त्रण गर्न Proper Cooling System, Air Flow Circulation र उचित Ventilation को लागि HVAC (heating, ventilating, and air conditioning) व्यवस्था गरौं ।

५. सूचना प्रणाली (Information System) भएको भवनको सुरक्षाको लागि सो को वरीपरी बलियो तारबार वा पर्खाल लगाऔं तथा पर्याप्त प्रकाश (Lighting) को व्यवस्था गरौं ।

६. सूचना प्रणाली (Information System) भएको भवनमा आउने जाने व्यक्तिहरुको निगरानी गर्न भवन वाहिर तथा भित्र CCTV (Surveillance System) को व्यवस्था गरौं र जानकारीको लागि “You are under Surveillance” जस्ता सूचना लेखिएको Notice Board को व्यवस्था गरौं।

७. चोरी तथा शंकास्पद गतिविधिबाट जोगाउन Motion Detector, Sound Alarm System जस्ता Surveillance System को व्यवस्था गरौं ।

८. सूचना प्रणाली (Information System) राख्नको लागि पर्याप्त उचाई भएको र आगो प्रतिरोधी (fireproof) भवन/कक्ष को व्यवस्था गरौं।

९. Over/Under Voltage तथा Surge बाट सुरक्षाको लागि Voltage Regulator/Surge protector/UPS जस्ता प्रणालीहरुको व्यवस्था गरौं।

१०. Automatic fire–fighting system वा Manual fire–fighting equipment (i.e., fire extinguishers) को व्यवस्था गरौं।

११. सूचना प्रणाली (Information System) ले प्रदान गर्ने सेवालाई भरपर्दो बनाउन Power Backup (Generator, Solar System, UPS) को व्यवस्था गरौं।

१२. सूचना प्रणाली (Information System) को स्थापना गर्दा प्रयाप्त Current Rating तथा Insulation भएको Electrical Cable, उपकरणहरुको Grounding र Shielding , Lightning बाट बच्न Lightening Arrestor को व्यवस्था गरौं।

१३. मुसाहरु आउनबाट जोगाउन सूचना प्रणाली (Information System) भएको कक्षमा खानेकुराहरु लग्ने नगरौं र Optical Fiber लगायतका तारहरु काटिनबाट जोगाउन Anti–Rodent Fiber Optic Cable, Metal–sheating or PVC ducts आदिको प्रयोग गरौं।

१४. उपकरण तथा प्रणालीहरु (Equipment and System) को अभिलेख राखी नियमित रुपमा निगरानी गरौं।

१५. संस्थाको Security Policy तथा Emergency Response Plan/Policy तर्जुमा गरी कार्यान्वयन गरौं।

२४ Desktop/Laptop Computer Security सँग सम्बन्धित

Desktop/Laptop Computer Security को लागि निम्न उपायहरु अपनाऔ ।

१. Desktop/Laptop Computer मा Genuine/Licensed/Open Source Operating System तथा Application Software को प्रयोग गरौं ।

२. Desktop/Laptop Computer मा Genuine/Licensed Antivirus को प्रयोग गरौं ।

३. पासवर्ड सहितको Admin User Account बनाई मात्र Desktop/Laptop Computer को प्रयोग गरौं ।

४. Guest Account Create गरेर मात्र अरु कसैलाई आफ्नो Desktop/Laptop Computer प्रयोग गर्न दिऔं ।

५. Desktop/Laptop Computer मा Log In को लागि बलियो पासवर्ड वा Fingerprint Lock, Face Lock आदि राखौं ।

६. Desktop/Laptop Computer को Operating System लाई अद्यावधिक (Up to Date) गरी राखौं ।

७. Desktop/Laptop Computer को आधिकारिक Application Store/Website बाट मात्र Application हरु Download तथा Install गरौं ।

८. अनावश्यक Application हरु Download गरी Install नगरौं तथा अनावश्यक Application हरु Installed छन् भने Uninstall गरौं ।

९. आवश्यक नभएको बेला WiFi, Bluetooth आदिलाई OFF गरी राखौं ।

१०. Desktop/Laptop Computer मा Secure Web Browser (e.g. Mozilla Firefox) को प्रयोग गरौं ।

११. Desktop/Laptop Computer मा कम्तिमा दुईवटा Drive बनाएर मात्र प्रयोग गरौं।

१२. Desktop/Laptop Computer को C: Drive (Desktop Screen/Folder, My Documents, Downloads) मा महत्वपूर्ण तथा संवेदनशील File हरु नराखौं।

१३. Desktop/Laptop Computer को महत्वपूर्ण तथा संवेदनशील Data लाई नियमित रुपमा Backup गरौं।

१४. पुरानो Desktop/Laptop Computer मा भएको सम्पूर्ण Data लाई Format/Degauss/Demagnetize गरेर मात्र विसर्जन (Dispose) गरौं।

१५. Desktop/Laptop Computer मा Auto–Screen Lock हुने गरी प्रयोग गरौं ।

१६. Desktop/Laptop Computer मा असुरक्षित Removable Media/Pen Drive को प्रयोग नगरौं।

१७. Desktop/Laptop Computer मा AutoRun/AutoPlay लाई Disable गरौं।

१८. आफ्नो Personal Details, Banking Details, Password जस्ता महत्वपूर्ण विवरणलाई Desktop/Laptop Computer मा Plain Text मा save नगरी Encrypt गरेर मात्र राखौं।

२५ Cloud मा राखिने डाटाको सुरक्षा (Cloud Data Security) सँग सम्बन्धित

(क) क्लाउड डाटा सुरक्षा (Cloud Data Security) भनेको के हो ?

क्लाउड डाटा सुरक्षा (Cloud Data Security) भनेको क्लाउड (Cloud) मा राखिने डाटा (Data) लाई ह्याकर लगायत कसैको पनि अनधिकृत पहुँचबाट सुरक्षित राख्न अपनाइने उपायहरुलाई बुझाउँछ।

(ख) क्लाउड (Cloud) मा राखिने डाटाको सुरक्षा कसरी गर्ने ?

क्लाउड (Cloud) मा आफ्नो Data सुरक्षित राख्नको लागि निम्न उपायहरु अपनाऔंः-

१. क्लाउड सेवा प्रदायक (Cloud Service Provider) छान्नु पर्दा आफ्नो आवश्यकता र भविष्यमा बढ्न सक्ने Data को Volume अनुसार भरपर्दो तथा गुणस्तरीय सेवा दिन सक्ने Reputed तथा Trusted क्लाउड सेवा प्रदायकलाई मात्र छानौं।

२. क्लाउड (Cloud) मा राखिने Data लाई Encrypt हुने सुनिश्चित गरौं।

३. क्लाउड सेवा प्रदायक (Cloud Service Provider) बाट Data को नियमित रुपमा Backup हुने सुनिश्चित गरौं। साथै महत्वपूर्ण Data को Backup Locally पनि राख्ने गरौं।

४. क्लाउड सेवा प्रदायक (Cloud Service Provider) ले Data मा अनधिकृत पहुँचबाट बचाउन के कस्तो सुरक्षा व्यवस्था (Security Measures) अपनाएको छ सो विषयमा जानकारी राखौं।

५. क्लाउड सेवा प्रदायक (Cloud Service Provider) को तर्फबाट सबै सुरक्षा सम्बन्धी मापदण्ड अपनाए पनि क्लाउड प्रयोगकर्ताको कमजोरीले गर्दा पनि Data

Breach/Leak हुन सक्ने भएकोले आफ्नो उपकरण (Computer / Laptop/Mobile Device आदि) मा End–point Security (Genuine OS, Anti–virus / Anti–malware आदि) को प्रयोग गरौं ।

६. क्लाउड सेवा (Cloud Service) को User Agreements राम्रो संग पढी डाटाको सुरक्षा सुनिश्चित गरौं ।

७. सुरक्षित Data Transfer को लागि SSL Certificate तथा VPN को प्रयोग गरौं ।

८. आफूले प्रयोग गर्ने क्लाउड सेवाको Privacy Settings लाई उचित तवरले Properly Configure गरौं । साथै Recovery option हरु समेत जानी राखौं ।

९. क्लाउड सेवा (Cloud Service) को पासवर्ड बलियो राख्ने गरौं । साथै Two–Factor Authentication feature लाई Enable गरी प्रयोग गरौं ।

१०. सकेसम्म व्यक्तिगत संवेदनशील विवरण Cloud मा नराखौं ।

११. Cloud Service प्रयोग गर्दा सकेसम्म Public WiFi को प्रयोग नगरौं ।

१२. सम्बन्धित व्यक्तिहरुको लागि नियमति रुपमा Cloud Data Security तथा साइबर सुरक्षा सम्बन्धी तालिम प्रदान गरौं ।

१३. सम्बन्धित संघ संस्थाले Data Security Policy तर्जुमा गरी सो को कार्यान्वयन गरौं ।

१४. क्लाउडमा राखिएको डाटा अरुलाई share गर्दा Access Control Features (जस्तैः View only, Edit Restriction) को प्रयोग गरौं ।

१५. क्लाउड सेवा प्रदायक (Cloud Service Provider) परिवर्तन वा Data Migration गर्दा पुराने ठाउँको Data Delete भए/नभएको सुनिश्चित गरौं ।

२८ वेबसाइट सुरक्षा (Website Security) सँग सम्बन्धित

(क) वेबसाइट सुरक्षा (Website Security) भनेको के हो ?

वेबसाइट सुरक्षा (Website Security) भन्नाले कुनै पनि संस्थाको वा व्यक्तिगत वेबसाइटलाई साइबर आक्रमण (Cyber Attack) बाट बचाउन अपनाईने उपायहरुलाई बुझाउँछ ।

(ख) वेबसाइटको सुरक्षा (Website Security) कसरी गर्ने ?

वेबसाइटको सुरक्षा (Website Security) को लागि निम्न उपायहरु अपनाऔ :-

१. वेबसाइट निर्माण गर्न प्रयोग गरिएको प्लेटफर्म (जस्तैः Word Press, Django आदि) लाई नियमित अध्यावधिक गरौं ।

२. सुरक्षित Plugins (जस्तैः Polylang, Popup Builder, Shield security) को प्रयोग गरौं र त्यसलाई नियमित अध्यावधिक गरौं ।

३. वेबसाइट Host गर्दा Https तथा SSL Certificate Configure गरौं ।

४. वेबसाइटको Admin URL लाई Hide गरेर राखौं ।

५. वेबसाइटमा Login गर्न खोज्दा तीन पटक भन्दा बढी पासवर्ड नमिलेमा उक्त User Account लाई केहि समयको लागि Suspend गरौं ।

६. वेबसाइटको Login Form मा Captcha को प्रयोग गरौं ।

७. वेबसाइट Access गर्दा Multifactor Authentication (MFA) तथा सुरक्षित पासवर्डको प्रयोग गरौं ।

८. वेबसाइट Host गर्न विश्वासिलो तथा भरपर्दो (Trusted and Reputed) वेबसाइट Hosting कम्पनीको छनौट गरौं ।

९. वेबसाइटको user तथा Administrative Privileges लाई व्यवस्थित रुपले प्रयोग गरौं ।

१०. वेबसाइटको Default CMS Setting लाई अनिवार्य रुपमा परिवर्तन गरौं ।

११. वेबसाइटको अति महत्वपूर्ण डाटा तथा Configurations लाई नियमित रुपमा तथा स्वतः Backup हुने गरी व्यवस्था गरौं ।

१२. वेबसर्भरलाई उचित तवरबाट Configure गरौं र सो को Documentation गरौं ।

१३. वेबसर्भरको सुरक्षाको लागि Web Application Firewall (WAF) को प्रयोग गरौं ।

१४. प्रयोगमा नहुने तथा नआएका Module तथा Features लाई Disable गरेर राखौं ।

१५. वेबसाइटको Logs लाई नियमित रुपमा Security Monitoring तथा Audit गरौं ।

२७ कम्प्युटर ह्याकिङ्ग (Computer Hacking) सँग सम्बन्धित

(क) कम्प्युटर ह्याकिङ्ग (Computer Hacking) के हो ?

कम्प्युटर ह्याकिङ्ग (Computer Hacking) भनेको कम्प्युटर वा कम्प्युटरमा आधारित प्रणालीहरु, कार्यक्रम, सूचना वा तथ्याङ्कमा कुनै अख्तियारी नलिई पहुँच प्राप्त गर्नु हो। यसरी ह्याकरले कम्प्युटर ह्याकिङ्ग गरिसकेपछि कम्प्युटर प्रणालीलाई अवरुद्ध गर्ने, डाटाको स्वरुप परिवर्तन गर्ने, नष्ट गर्ने, डाटा विक्रि गर्ने लगायतका कार्यहरु गर्न सक्दछन्।

(ख) कम्प्युटर ह्याकिङ्ग (Computer Hacking) भएको कसरी थाहा पाउने ?

कम्प्युटरमा निम्न बमोजिमको लक्षणहरु देखियो भने कम्प्युटर ह्याक भएको हुन सक्छ :-

१. कम्प्युटरमा कम्प्युटर धनीको जानकारी बिना प्रोग्रामहरु Install भएको देखिएमा साथै, कम्प्युटर ON गर्ने वित्तिकै ती प्रोग्रामहरु स्वतः Start हुने र इन्टरनेटसँग Connect गर्न खोजेमा।

२. असामान्य रुपमा कम्प्युटरको Performance घट्ने, CPU/RAM को Usage बढ्ने तथा कम्प्युटर बेला बेलामा नचल्ने (Hang)/स्वत बन्द हुने (Crash) भएमा।

३. अनावश्यक रुपमा वेबसाइटहरुमा आफै Redirect/Visit हुने, विभिन्न सफ्टवेयर आफै Download हुने र बारम्बार Pop up Window आइरहने भएमा।

४. कम्प्युटर धनीको इमेल खाताबाट वा सामाजिक सञ्जाल खाता (Social Media Account) बाट कम्प्युटर धनीको जानकारी विना धैरै इमेल वा सन्देशहरु (Messages) पठाइएको पाइएमा।

५. कम्प्युटर धनीको जानकारी/अनुमति बिना Internet Browser को Home page परिवर्तन भएमा।

६. Windows Firewall, Antivirus, Task Manager or Registry Editor स्वतः disable भएको पाइएमा।

७. आफ्नो पासवर्डले काम गर्न छोडेमा।

८. आफ्नो Password कुनै public domain मा प्रकाशन भएको पाइएमा।

९. अस्वभाविक रुपमा धेरै Internet bandwidth को खपत भएको पाईएमा र Internet Slow भएमा।

१०. "You have been hacked" जस्ता Message प्राप्त भएमा।

११. आफ्नो इमेल आदिमा फिरौती रकम माग गरी (Ransomware) इमेल सन्देश प्राप्त भएमा।

१२. Browser मा Unwanted Toolbars हरु देखिएमा।

२८ कम्प्युटर ह्याकिङ्ग (Computer Hacking) बाट कसरी बच्ने ?

कम्प्युटर ह्याकिङ्ग (Computer Hacking) बाट बच्न निम्न उपायहरु अपनाऔं :-

१. आफ्नो नेटवर्क तथा कम्प्युटरमा हुन सक्ने अनाधिकृत पहुँचबाट बच्न इन्टरनेटमा जोडिनुभन्दा अगाडि Firewall लाई Enable गरौं।

२. Real Time Threat Detection को लागि Reputed Antivirus र Anti–spyware Software को प्रयोग गरौं।

३. Upper Case, Lower Case, Numeric / Other Special Character सहितको बलियो पासवर्डको प्रयोग गरौं। साथै, आफ्नो पासवर्ड कसैसंग पनि share नगरौ।

४. इमेल, समाजिक संजाल तथा वित्तीय खातामा Fingerprint, One–Time Password (OTP) जस्ता Multi Factor Authentication (MFA) को प्रयोग गरौं। आफ्नो पासवर्डलाई बेला बेलामा परिवर्तन गरौ। साथै विभिन्न खाताहरुको लागि फरक फरक पासवर्डको प्रयोग गरौं।

५. आफ्नो उपकरणको Operating System (OS), Apps, Browser, Antivirus लगायतका Software को नियमित Update गरी Up–to–date राखौं।

६. Spam Email लाई Click नगरौं। अपरिचित व्यक्तिबाट आएको Spam ईमेलमा रहेको Attachment तथा लिंकलाई नखोलौं।

७. प्रयोगमा नरहेको वा प्रयोग नभएको समयमा Computer System लाई बन्द गरेर राखौं । साथै प्रयोगमा नरहेको बेला WiFi Connection, Bluetooth Connection लाई OFF गरेर राखौं।

८. Https भएको सुरक्षित वेबसाइटको मात्र Visit गरौं।

९. आफ्नो Router मा रहेको Security संग सम्बन्धित Setting हरुलाई Enable गरौं।

१०. Public WiFi बाट संवेदनशील डाटा, Personally Identifiable Information (PII) share नगरौं। साथै अनलाइन बैंकिंग जस्ता कारोवार Public WiFi बाट नगरौं ।

११. संवेदनशील Data Transfer तथा Transaction को लागि Secure VPN को प्रयोग गरौं।

१२. आफ्नो Computer को Performance बेला बेलामा निगरानी गरौ। प्रयोग नहुने अनावश्यक Software हरुलाई हटाऔ।

१३. आफ्नो Computer System Infected भएको शंका लागेमा System लाई Scan गरौ, Password परिवर्तन गरौ, साथै सम्बन्धित विज्ञसगं परामर्श लिऔ।

१४. Pirated/Freeware Software को प्रयोग नगरौ।

१५. आफ्नो महत्वपूर्ण Data हरुको Backup राखौ।

२९ साइबर सूरक्षाका लागि अपनाउनु पर्ने दश असल बानीहरु (Ten Good Habits for Cyber Security) सँग सम्बन्धित

१. आफ्नो उपकरणहरु जस्तै मोवाइल, ट्याब्लेट, ल्यापटप/डेस्कटप कम्प्युटरलाई सकेसम्म वेवारिसे (Unattended) नछोडौं, छोड्नै परेमा Lock गरेर राखौं।

२. बलियो पासवर्ड (अंक, अक्षर, Lower & Upper case, चिन्ह सहितको १० अक्षरहरुभन्दा बढी भएको) राखौं र पासवर्डलाई नियमित परिवर्तन गरौं।

३. आफ्नो Password, OTP, Pin Code कसैसंग Share नगरौ। साथै Password, OTP, Pin Code लाई सुरक्षित साथ राखौ।

४. आफ्नो खाता (Email Account, Social Media, Facebook, Mobile Banking App आदि) हरुमा पासवर्डका अतिरिक्त कम्तिमा थप एउटा Authentication गर्ने माध्यम जस्तै मोबाइल नम्बर, आफ्नो इमेल, Fingerprint जस्ता Multi–Factor Authentication को प्रयोग गरौ।

५. शंकास्पद लिंकहरुमा Click नगरौं। साथै असुरक्षित वेबसाइटहरुको Visit नगरौं र Freeware/Pirated Contents/Software हरु Download तथा Install नगरौं।

६. Operating System/Application Software/Antivirus हरुलाई नियमित अद्यावधिक (Update) गरौं। साथै, आफ्नो उपकरणहरुलाई नियमित Scan गरौ।

७. Public WiFi तथा सार्वजनिक Computer को प्रयोग गरी आर्थिक कारोबार आदि नगरौ।

८. आफ्ना महत्वपूर्ण तथा सम्वेदनशील डाटाहरुको नियमित Backup राखौं।

९. वेवारिस रुपमा भेटिएको USB Drive/Pendrive आदिलाई Scan नगरिकन आफ्नो कम्प्युटरमा प्रयोग नगरौ।

१०. आफ्नो पुरानो Computer, Mobile, Pendrive आदिवाट आफ्नो डाटा मेटिएको सुनिश्चित गरेर मात्र विसर्जन (Dispose) गरौ।

नेपाल दूरसञ्चार प्राधिकरण
कान्तिपथ, जमल, काठमाण्डौ
फोन नं.: ९७७-१-५३५५४७१
इमेल: info(at)nta.gov.np
URL: https://www.nta.gov.np