सत्यमेव जयते

साइबर सुरक्षा पर किशोरों/छात्रों के लिए पुस्तिका

गृह मंत्रालय
भारत सरकार

सत्यमेव जयते

साइबर सुरक्षा पर किशोरों / छात्रों के लिए पुस्तिका

गृह मंत्रालय

भारत सरकार

यह पुस्तिका साइबर सुरक्षा विशेषज्ञों के परामर्श से तैयार की गई है।

गृह मंत्रालय
भारत सरकार
नॉर्थ ब्लॉक,
नई दिल्ली - 110001
द्वारा प्रकाशित

डिस्क्लेमर :

इस पुस्तिका में प्रदान की गई जानकारी का आशय नागरिकों विशेषकर छात्रों के बीच उन्हें प्रभावित करने वाले विभिन्न प्रकार के साइबर खतरों और साइबर अपराध से स्वयं को सुरक्षित रखने के बारे में जागरूकता पैदा करना है। पुस्तिका में दी गई सूचना, तकनीक और सुझाव केवल मार्गदर्शन हेतु हैं। यदि आप साइबर अपराध के शिकार हो जाते हैं तो अपने स्थानीय पुलिस स्टेशन अथवा राज्य साइबर अपराध सेल से संपर्क करें।

विषय सूची

पुस्तिका के बारे में पृष्ठ-(i)

साइबर सुरक्षा चिंता का विषय क्यों है ? पृष्ठ-1

साइबर खतरे जो किसी को भी प्रभावित कर सकते हैं पृष्ठ-3

साइबर बुलिंग पृष्ठ-5

साइबर ग्रूमिंग पृष्ठ-9

ऑनलाइन गेमिंग पृष्ठ-13

ई-मेल धोखाधड़ी पृष्ठ-18

ऑनलाइन लेनदेन में धोखाधड़ी पृष्ठ-23

आपकी सोशल नेटवर्किंग प्रोफाईल्स की सुरक्षा के उपाय पृष्ठ-28

पुस्तिका के बारे में

सूचना एवं संचार प्रौद्योगिकी हमारे दैनिक जीवन का अभिन्न हिस्सा बन गई है। इसने हमारे बातचीत करने, मित्र बनाने, अद्यतन जानकारी को साझा करने, गेम्स खेलने, खरीददारी करने इत्यादि के तरीके को बदल दिया है। प्रौद्योगिकी का हमारे दैनिक जीवन के अधिकांश पहलुओं पर प्रभाव पड़ा है।

हमारी नई पीढ़ी बहुत ही युवा अवस्था में साइबर स्पेस से रूबरू हो रही है। ज्यादा–से–ज्यादा बच्चे ऑनलाइन गेम्स़ खेलने, मित्र बनाने के लिए तथा सोशल नेटवर्किंग साइट का प्रयोग करने में अपना अधिकांश समय व्यतीत कर रहे हैं। वास्तव में स्मार्ट फोन से सोशल नेटवर्किंग, ऑनलाइन गेम्स्, शॉपिंग इत्यादि तक पहुंच काफी व्यापक हो गई है। साइबर स्पेस हमें वास्तव में विश्व भर के करोड़ों ऑनलाइन उपयोगकर्ता से जोड़ता है। साइबर स्पेस के बढ़ते उपयोग के साथ–साथ साइबर अपराधों में भी अत्यंत तीव्र गति से वृद्धि हुई है।

बच्चों को इससे से बहुत अधिक खतरा है क्योंकि वे साइबर स्पेस से जुड़े खतरों एवं सुरक्षा उपायों की सीमित समझ के साथ साइबर स्पेस का उपयोग कर रहे हैं। बच्चे अभी प्रयोगागिक आयु वर्ग में है। वे प्रयोग करना चाहते हैं, नई चीजों को सीखना चाहते हैं तथा नई–नई प्रौद्योगिकियों का प्रयोग करना चाहते हैं। हालांकि प्रयोग करना सीखने का एक अच्छा तरीका है किंतु बच्चों को उपयुक्त मार्गदर्शन प्रदान किया जाना भी उतना ही महत्वपूर्ण है ताकि वे स्वयं को साइबर तकनीक के प्रतिकूल प्रभाव से बचा सकें।

यह पुस्तिका 13 वर्ष से अधिक आयु के बच्चों के लिए है। इसका उपयोग युवा विद्यार्थियों द्वारा साइबर वर्ल्ड को बेहतर ढंग से समझने तथा स्वयं को भावी उत्तरदायी एवं सजग

साइबर सिटीजन के रूप में तैयार करने के लिए किया जा सकता है। इस पुस्तिका का उद्देश्य ऐसे विभिन्न साइबर खतरों, जो बच्चों को प्रभावित कर सकते हैं, की जानकारी बच्चों को मुहैया करवाना तथा साइबर अपराध को रोकने में सहायक सुरक्षा उपायों के बारे में विचार–विमर्श करना है।

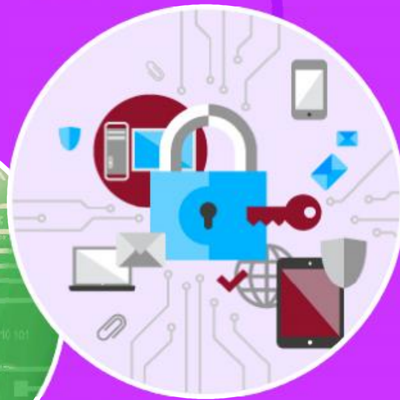
पुस्तिका का प्रथम एवं द्वितीय अध्याय बच्चों को इस बात की जानकारी प्रदान करता है कि साइबर सुरक्षा चिंता का विषय क्यों है तथा ऐसे विभिन्न प्रकार के साइबर अपराध कौन से हैं जो हमें प्रभावित कर सकते हैं। पुस्तिका का तृतीय अध्याय साइबर बुलिंग तथा इससे बच्चे किस प्रकार प्रभावित होते हैं, के संबंध में जानकारी प्रदान करता है। इस अध्याय में उन महत्वपूर्ण सुरक्षोपायों के बारे में विस्तृत जानकारी प्रदान की गई है जिनका प्रयोग बच्चें स्वयं को साइबर बुलिंग से बचाने के लिए कर सकते हैं तथा इसके साथ–साथ साइबर बुलिंग से निपटने से तरीकों के बारे में भी बताया गया है।

पुस्तिका का चौथा अध्याय साइबर ग्रूमिंग तथा बच्चों पर इसके प्रभाव की जानकारी प्रदान करता है। इस अध्याय में उन विभिन्न सुरक्षा उपायों की विस्तृत जानकारी प्रदान की गई है जिन्हें अपनाकर बच्चे स्वयं को साइबर ग्रूमिंग से बचा सकते हैं।

पुस्तिका का पांचवा अध्याय ऑनलाइन गेमिंग तथा ऐसी सुरक्षा जानकारी को कवर करता है जो बच्चों के लिए स्वंयं को ऐसे साइबर खतरों से बचाने में सहायक सिद्ध हो सकती है। साइबर अपराधियों द्वारा सामान्तया ई–मेल का प्रयोग किया जाता है। छठा अध्याय यह जानकारी प्रदान करता है कि किस प्रकार साइबर अपराधी ई–मेल का उपयोग करके साइबर अपराधों को अंजाम देते हैं और किस प्रकार बच्चे सुरक्षित ढंग से ई–मेल का उपयोग कर सकते हैं।

साइबर तकनीक ने हमारे वित्तीय लेन–देन के तरीकों को भी पूरी तरह बदल दिया है। अधिक से अधिक लोग खरीददारी, धन हंस्तातरण तथा अन्य वित्तीय लेन–देनों के ऑनलाइन प्लेटफॉर्मों का उपयोग कर रहे हैं। इसके अलावा बच्चों को भविष्य के लिए तैयार करने के उद्देश्यो से विद्यालय में वित्तीय शिक्षा को प्रदान किए जाने के तरीके को सुविधाजनक बनाने के लिए भी प्रयास किए जा रहे हैं। वित्तीय जालसाजी से संबंधित बढ़ते साइबर अपराधों को ध्यान में रखते हुए पुस्तिका का सातवां अध्याय बच्चों को ऑनलाइन वित्तीय लेन–देन से संबंधित खतरों तथा ऐसे खतरों से स्वयं को बचाने के तरीकों की जानकारी प्रदान करता है। पुस्तिका का अंतिम अध्याय सोशल नेटवर्किंग से जुड़े साइबर खतरों तथा ऐसे खतरों से किस प्रकार बचा जाए, से संबंधित जानकारी पर प्रकाश डालता है।

यह पुस्तिका साइबर खतरों तथा उनसे स्वयं को बचाने के तरीकों के बारे में समझने में बच्चों के लिए मददगार सिद्ध होगी। परिवर्तन के वाहक के रूप में विद्यार्थियों से यह आशा की जाती है कि वे अपनी इस जानकारी को अपने साथियों तथा माता–पिता के साथ साझा करें और साइबर स्पेस को और सुरक्षित बनाने में अपना योगदान दें।



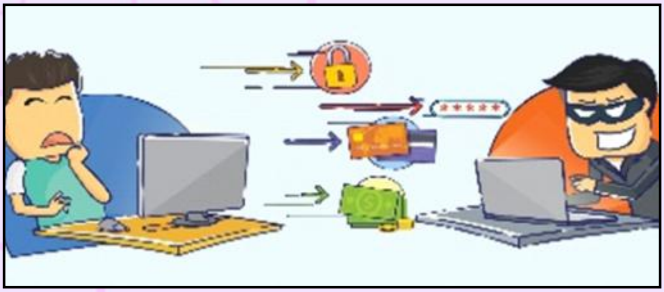
साइबर सुरक्षा चिंता का विषय क्यों है ?

आज इंटरनेट, कंप्यूटर, स्मार्ट फोन तथा संचार प्रौद्योगिकी के अन्य उपकरण हमारे जीवन का अभिन्न हिस्सा बन गए हैं। कल्पना कीजिए कि हम अपने प्रत्येक दिन का कितना समय इन स्मार्ट उपकरणों का उपयोग करने पर खर्च करते हैं। हम ने Google, emails, WhatsApp, Twitter, Facebook इत्यादि जैसे इंटरनेट संचार माध्यमों को अपनी दैनिक गतिविधियों का एक अभिन्न हिस्सा बना लिया है किंतु हम में से अधिकांश लोग साइबर सुरक्षा एवं स्वयं को साइबर अपराधों से बचाने के लिए आवश्यक सुरक्षा उपायों के प्रति अनभिज्ञ हैं।

क्या आप जानते हैं कि जो भी सूचना या व्यक्तिगत जानकारी इंटरनेट पर साझा की जाती है वह हमेशा के लिए वहां मौजूद रहती है क्योंकि सूचना को पूरी तरह डिलीट करना अत्यंत कठिन है?

साइबर अपराध क्या हैं?

साइबर अपराध ऐसे अपराध होते हैं जो कम्प्यूटर, इंटरनेट या मोबाइल टेक्नोलॉजी का उपयोग करके व्यक्तियों, कंपनियों या संस्थानों के प्रति किए जाते हैं। साइबर अपराधी सोशल नेटवर्किंग साइटों, ईमेल, चैट रूम, नकली सॉफ्टवेयर, वेबसाइटों इत्यादि जैसे प्लेटफॉर्मों का उपयोग पीड़ितों पर हमला करने के लिए करते हैं। बच्चे भी विभिन्न प्रकार के साइबर अपराधों के शिकार हो सकते हैं।



"भारतीय कम्प्यूटर आपातकालीन कार्रवाई दल (सीईआरटी–इन), के अनुसार वर्ष 2017 के दौरान भारत में 53000 से अधिक साइबर सुरक्षा संबंधी घटनाओं की सूचना प्राप्त हुई।"

क्या आप जानते हैं साइबर हमले और अधिक जटिल तथा परिष्कृत होते जा रहे हैं तथा इनका लक्ष्य फोन नं., पता, फोटोग्राफ, बैंक संबंधी विवरण इत्यादि जैसी व्यक्तिगत जानकारी को चुराना है। साइबर अपराधियों द्वारा आपकी इस व्यक्तिगत जानकारी का उपयोग आपके खिलाफ कई तरीकों से किया जा सकता है जैसे कि जाली प्रोफाइल बनाकर, साइबर खतरा देकर।

मित्रों, चिंता न करें, एहतियात बरतकर तथा सजग रहकर आप स्वयं को साइबर अपराधों से बचा सकते हैं। मैं हूं आपका साइबर दोस्त और मैं आपकी विभिन्न प्रकार के साइबर अपराध को समझने तथा उन सावधानियों को अपनाने में मदद करूंगा जो साइबर अपराध के शिकार बनने के खतरे को कम करने के लिए आपको अपनानी चाहिए।

साइबर खतरे जो किसी को भी प्रभावित कर सकते हैं

साइबर खतरे वे ऐसे विभिन्न तरीके हैं जिनका उपयोग इंटरनेट या मोबाइल टैक्नोलॉजी का उपयोग करके हमें हानि पहुंचाने के लिए किया जा सकता है।

क्या आप जानते हैं हैकर ऐसा कोई भी व्यक्ति हो सकता है जो अनपेक्षित उपयोग के लिए प्रौद्योगिकी का उपयोग / दुरुपयोग करके व्यक्तियों को वित्तीय हानि/उनकी प्रतिष्ठा को क्षति पहुंचाने के लिए करता है। हैकर्स आपके कम्प्यूटर को क्षति पहुंचाने तथा आपके डाटा तक पहुंच बनाने के लिए मालवेयर्स, वायरस या ट्रोजंश का उपयोग कर सकते हैं।

साइबर अपराधी हमारी संवेदनशील सूचना तक अनधिकृत पहुंच बनाना चाहते हैं। अधिकांश मामलों में साइबर अपराधी स्पष्ट उद्देश्य के लिए अटैक करते हैं जिसकी लिए वे सबसे प्रभावी तरीकों को उपयोग करते हैं ।

साइबर अपराधियों द्वारा प्रयोग किए जाने वाले कुछ सामान्य तरीके निम्नलिखित हैं:

☞ **ई–मेल स्पूफिंग** – आपको ऐसे ई–मेल भेजकर जो वास्तविक लगे तथा विश्वसनीय ई–मेल आई डी से भेजा गया लगे किंतु वास्तव में ऐसा नहीं होता।

☞ **द्वेषपूर्ण फाइल एप्लीकेशन** : आपके स्मार्टफोन तथा व्यक्तिगत डाटा तक पहुंच बनाने के लिए सीधे मैसेज भेजना, गेमिंग, ई–मेल और वेबसाइट के द्वारा आपको द्वेषपूर्ण तथा बुरे एप्लीकेशन और फाइल भेजना।

☞ **सामाजिक इंजीनियरिंग** : सामाजिक इंजीनियरिंग एक ऐसी तकनीक है जिसका प्रयोग साइबर अपराधियों द्वारा आपसे जानकारी प्राप्त करने के लिए आपका विश्वास जीतने के लिए किया जाता है। आपकी जानकारी प्राप्त करने तथा/अथवा आपको कुछ नुकसान पहुंचाने के लिए साइबर अपराधी आपसे सम्प्रेषण स्थापित करने का प्रयास करने के लिए इस बात का प्रयोग करता है कि आपको सबसे अधिक क्या पसंद है। मान लीजिए आपको ऑनलाइन गेम खेलना पसंद है, बहरूपिया एक अन्य बच्चे की तरह व्यवहार करेगा तथा आपको बातचीत तथा जानकारी साझा करने के लिए आमंत्रित करेगा।

☞ **साइबर बुलिंग:** इलेक्ट्रोनिक तथा संचार माध्यमों जैसे कंप्यूटर, मोबाइल फोन, लैपटॉप इत्यादि का प्रयोग करके किसी को प्रताड़ित या बुली करने का एक प्रकार है।

☞ **पहचान चुराना:** वित्तीय लाभ के लिए अथवा किसी अन्य व्यक्ति के नाम पर/सहयोगियों के नाम पर ऋण लेने या अन्य लाभ प्राप्त करने के लिए किसी व्यक्ति की पहचान को जान–बूझकर क्षति पहुंचाना।

☞ **(जॉब फ्रॉड) नौकरी से संबंधित जालसाजी:** किसी कर्मचारी अथवा भावी कर्मचारी द्वारा अपने नियोक्ता के प्रति धोखाधड़ी या कपटपूर्ण निरूपण करना।

☞ **बैंकिंग फ्रॉड** : स्वयं को बैंक या अन्य वित्तीय संस्थान के रूप में प्रस्तुत करके जमाकर्ता के खाते से धोखाधड़ी करके धन प्राप्त करना।

साइबर बुलिंग

साइबर बुलिंग उन साइबर खतरों में से एक है जिनका सामना बच्चों और युवाओं द्वारा किया जा रहा है। यद्यपि साइबर बुलिंग से कोई भी प्रभावित हो सकता है परन्तु साइबर खतरों के बारे में सीमित समझ होने के कारण बच्चे आसानी से साइबर बुलिंग का शिकार हो जाते हैं।

साइबर बुलिंग से तात्पर्य इंटरनेट या मोबाइल टेकनोलॉजी का प्रयोग करके असभ्य, घटिया या तकलीफदेह संदेश, टिप्पणियां और इमेज/वीडियो भेजकर किसी को जानबूझकर तंग करना या डराना धमकाना है। किसी साइबर बुली द्वारा दूसरों को डराने धमकाने के लिए टेक्स्ट मेसेज, ई–मेल, सोशल मीडिया प्लेटफार्म, वेब पेज, चैट रूम आदि का प्रयोग किया जाता है।

क्या आप जानते हो कि शुरू में तो हमें इस बात का एहसास भी नहीं होता है कि कोई हमें ऑनलाइन बुली कर रहा है? साइबर बुली कोई जानकार व्यक्ति, दोस्त, रिश्तेदार या ऐसा अनजान व्यक्ति भी हो सकता है जिससे हम सोशल मीडिया प्लेटफार्म या चैट रूम, गेमिंग पोर्टल आदि पर ऑनलाइन मिले हों।

बच्चों के प्रति साइबर बुलिंग के परिणाम कई प्रकार के होते है। ये शारीरिक, भावनात्मक और मनोवैज्ञानिक परिणामों के रूप में हो सकते है जिससे न केवल विद्यार्थियों का शैक्षणिक निष्पादन बल्कि काफी हद तक उनका दैनिक जीवन भी प्रभावित होता है।

साइबर बुलिंग से चिंतित है? चिंता न करें ---- जागरूकता और सावधानी से आप बिना किसी डर के इंटरनेट और मोबाइल टेक्नोलॉजी का प्रयोग कर सकते है। आपको सतर्क होने और स्वयं को और अपने दोस्तों को साइबर बुलिंग से बचाने के लिए सुरक्षोपायों का अनुपालन करने की जरूरत है।

आओ चर्चा करे कि आप साइबर बुलिंग का शिकार होने से अपने आपको कैसे बचा सकते है:–

- सोशल मीडिया प्लेटफार्म पर अनजान व्यक्तियों की फ्रेंड रिक्वेस्ट स्वीकार न करें। साइबर बुली अपने शिकार से दोस्ती करने के लिए जाली एकाउंट भी बना सकता है। अनुभव सिद्ध ढंग से उन्हीं लोगों को ऑनलाइन जोड़े जिन्हें आप ऑफ लाइन जानते हैं।

- सोशल मीडिया या अन्य ऑनलाइन प्लेटफार्म पर अपनी निजी सूचना जैसे जन्म, तिथि, पता और फोन नम्बर साझा न करें। आपकी आनलाइन पोस्ट तक कौन पहुंच सकता है इसके लिए आप सोशल मीडिया प्लेटफार्म पर प्राइवेसी सेटिंग में जाए। अपनी प्रोफाइल तक केवल आपके दोस्तों की पहुंच को ही सीमित करने का प्रयास करें। (किंतु याद रखें सभी पोस्टों के लिए प्राइवेसी का विकल्प सभी सोशल मीडिया प्लेटफार्म प्रदान नहीं करते हैं।) उदाहरण के लिए किसी एक प्लेटफार्म पर पिक्चर स्टोरीज बाए–डीफाल्ट ही पब्लिक होती हैं।

- याद रखें कि आप जो भी आनलाइन पोस्ट करते है, वह वहीं रहता है इसलिए, महत्वपूर्ण है कि सतर्क रहें और सोशल मीडिया प्लेटफार्म पर कमेंट्स या पोस्ट में अपना फोन नम्बर और अन्य निजी ब्योरे साझा न करें।

- कभी भी अनजान स्रोतों से अनावश्यक साफ्टवेयर और एप्स जैसे डेटिंग एप, आनलाइन गेम, आदि को इंस्टाल न करें। चैट रूम में चैटिंग करते समय आपको विशेष रूप से सतर्क होना चाहिए। चैट रूम में अपने निजी ब्योरे कभी साझा न करें और अपनी पहचान को सीमित करें।

- यदि किसी दोस्त या अनजान व्यक्ति की पोस्ट पढ़कर आप दुःखी महसूस करे तो उस पर आक्रामक उत्तर न दें। इससे बुली इस प्रकार के मेसेज पोस्ट करने

के लिए प्रोत्साहित होगा। यदि पीड़ाकर पोस्ट/मेसेज आपके दोस्त का हो तो दोबारा ऐसा न करने का अनुरोध उससे कर सकते हैं। यदि आप बार–बार इस प्रकार के मेसेज/पोस्ट प्राप्त करते हैं, तो कृपया तत्काल अपने माता–पिता या बड़ों को इसकी जानकारी दें जिससे वे आपकी सहायता कर सकें।

☞ कृपया यह भी याद रखें कि एक अच्छा इंटरनेट उपयोगकर्ता होने के नाते आपको घटिया कमेंट या दुःखदायी मेसेज या परेशान करने वाली पिक्चर्स / वीडियोज आनलाइन शेयर नहीं करनी चाहिए। कृपया सतर्क रहें और यह जांच करें कि आपकी पोस्ट/कमेंट/वीडियो आपके दोस्त या किसी अन्य व्यक्ति के लिए भी परेशान करने वाली न हों। यदि ऐसा है तो कृपया पोस्ट न करें। आपको भी साइबर बुली नहीं बनना चाहिए क्योंकि ऐसा करना दण्डनीय अपराध है। यह पीड़ित को प्रतिकूल रूप से प्रभावित करता है।

यदि आप साइबर बुलिंग के पीड़ित हैं तो आपको क्या करना चाहिए?

यदि आपको महसूस होता है कि आप साइबर बुलिंग के पीड़ित हैं, तो कृपया अपने बड़ों को सूचित करें ताकि वे हस्तक्षेप कर सके और आपकी सहायता कर सकें। निम्नलिखित सुझाव स्थिति से निपटने में सहायक हो सकते है।

☞ **तत्काल अपने माता–पिता/बड़ों को सूचित करें**: यदि कोई आपको डरा धमका रहा है तो तत्काल अपने माता–पिता/बड़ों को सूचित करें। यह न सोचे कि आपके माता–पिता आपके आनलाइन कार्यकलापों को प्रतिबंधित कर देंगे या आपसे कंप्यूटर/स्मार्टफोन का उपयोग न करने के लिए कहेंगे। उन्हें सूचित करना महत्वपूर्ण है ताकि वे आपकी सहायता व मार्गदर्शन करें। पूरी बात स्पष्ट रूप से आपने माता–पिता/बड़ों को बताएं।

☞ **बुली की पहचान करना**: बुली की पहचान करने की कोशिश करें कि वह जानकार है या अनजान व्यक्ति आपको यह पता लगाने कि कोशिश करनी चाहिए कि बुली आपको क्यों परेशान कर रहा है। बुली आपका दोस्त या कोई परिचित व्यक्ति हो सकता है। आप बुली तक पहुंचने में अपने माता–पिता/अध्यापकों की मदद ले सकते है और आपको बुली करने से उसे रोक सकते है।

☞ **बुली को ब्लॉक करें:** यदि बुली आपको डराने धमकाने के लिए सोशल मीडिया प्लेटफार्म का उपयोग कर रहा है तो आप उसे ब्लॉक कर सकते है। सभी सोशल मीडिया एप या सेवाओं में यूजर को ब्लॉक करने का विकल्प है।

☞ **पोस्ट/मेसेज को क्लेक्ट और सेव करें:** आपके विरूद्ध प्रयोग किए गए पोस्ट/मेसेज सेव करें। कानूनी कार्रवाई किए जाने के मामले में, इस प्रकार के मेसेज/पोस्ट का उपयोग साक्ष्य के रूप में किया जा सकता है।

☞ **बुली को कभी भी आक्रामक उत्तर न दें:** बुली चाहता है कि आप आक्रामक हो जाए और आपकी उससे बहस हो। इससे अनावश्यक रूप से सूचना में फायदा होता है। इसलिए बेहतर तरीका यह है कि आप विनम्रतापूर्वक व्यक्ति को इसे बंद करने के लिए कहें और यदि वह नाराज हो जाता है तो उसके साथ चैट बंद कर दें और उसे ब्लॉक कर दें।

☞ यदि आपके माता–पिता/बड़ों को जरूरत महसूस हो तो, वे बुली के खिलाफ शिकायत करने के लिए पुलिस स्टेशन से संपर्क कर सकते हैं।

क्या आप जानते हैं कि किसी को ऑनलाइन धमकाना गैर–कानूनी तथा अनैतिक है? यहां तक कि यदि आप उन्हें आपत्तिजनक संदेश भेजते हैं, उन्हें भद्दे नामों से बुलाते हैं, वे कैसे लगते हैं इस पर टिप्पणी करते हैं, इत्यादि तो आप मुसीबत में पड़ सकते हैं ?

साइबर ग्रूमिंग

साइबर ग्रूमिंग एक ऐसा बढ़ता हुआ साइबर थ्रेट है जिसका सामना बच्चों और किशोरों द्वारा किया जा रहा है। यह एक ऐसी प्रक्रिया है जहां कोई यौन उत्पीड़न अथवा शोषण करने के लिए बच्चों का विश्वास प्राप्त करने के उद्देश्य से सोशल मीडिया अथवा मेसेजिंग प्लेटफार्म के माध्यम से बच्चों के साथ भावनात्मक संबंध स्थापित करता है।

साइबर ग्रूमर जाली एकाउंट बनाकर बच्चे जैसा ही व्यवहार करता है अथवा बच्चे के जैसे ही शौक रखकर गेमिंग वेबसाइट, सोशल मीडिया, ई–मेल, चैट–रूम, इंस्टेंट मेसेजिंग इत्यादि का प्रयोग कर सकता है।

क्या आप जानते हैं कि हममें से बहुत से लोगों को यह एहसास भी नहीं होता है कि कोई हमें ऑनलाइन ग्रूम कर रहा है? ऑनलाइन ग्रूमर कोई परिचित व्यक्ति, रिश्तेदार अथवा ऐसा कोई अनजान व्यक्ति भी हो सकता है जिससे हम सोशल मीडिया प्लेटफार्म, चैट रूम अथवा गेमिंग पोर्टल इत्यादि पर ऑनलाइन मिले हों।

प्रारंभ में साइबर ग्रूमर आपकी प्रशंसा कर सकता है, उपहार, मॉडलिंग जॉब का प्रस्ताव दे सकता है बाद में वो भद्दे मैसेज, फोटोग्राफ अथवा वीडियो भेजना शुरू कर सकता है और आपसे आपकी अश्लील तस्वीरें अथवा वीडियो उनसे साझा करने को कह सकता है।

ऑनलाइन ग्रूमर अधिकतर किशोर वर्ग को लक्षित करते हैं क्योंकि किशोरावस्था में उनमें कई शारीरिक, व्यक्तिगत तथा सामाजिक परिवर्तन होते हैं। किशोरों की आवेगशील तथा जिज्ञासु प्रवृत्ति उन्हें ऑनलाइन गतिविधियों में लगे रहने की ओर प्रोत्साहित करती है जिससे वे ऑनलाइन ग्रूमिंग के शिकार हो जाते हैं।

साइबर ग्रूमिंग का बच्चे की शारीरिक, भावनात्मक तथा मनोवैज्ञानिक दशा पर गहरा प्रभाव पड़ता है। यह न केवल उनकी शैक्षिक उपलब्धियों को प्रभावित करता है अपितु उनकी रोजमर्रा की जिंदगी को भी काफी हद तक प्रभावित करता है। ऑनलाइन ग्रूमिंग के हानिकारक प्रभाव कई बार दीर्घावधि तक रहते हैं और पीड़ित को उनकी युवावस्था में भी परेशान करते हैं।

साइबर ग्रूमिंग से चिंतित हैं? चिंता न करें जागरूकता और सावधानी से आप बिना किसी डर के इंटरनेट और मोबाइल टेक्नॉलाजी का प्रयोग कर सकते हैं। आपको सतर्क रहने और स्वयं को और अपने दोस्तों को साइबर ग्रूमिंग से बचाने के लिए सुरक्षा उपायों का अनुपालन करने की जरूरत है।

आइए चर्चा करें कि आप साइबर ग्रूमिंग का शिकार होने से अपने आपको कैसे बचा सकते हैं।

- सोशल मीडिया प्लेटफार्म पर अनजान व्यक्तियों की फ्रेंड रिक्वेस्ट स्वीकार न करें। साइबर ग्रूमर अपने शिकार से दोस्ती करने के लिए जाली एकाउंट भी बना सकता है।
- सोशल मीडिया अथवा अन्य ऑनलाइन प्लेटफार्मों पर अपनी व्यक्तिगत जानकारी जैसे जन्म तिथि, पता, फोन नंबर और स्कूल का नाम साझा न करें। आपकी ऑनलाइन पोस्ट तक कौन पहुंच सकता है इसके लिए आप सोशल मीडिया प्लेटफार्म पर प्राइवेसी सेटिंग में जाए। अपने प्रोफाइल तक केवल अपने दोस्तों की पहुंच को ही सीमित रखने का प्रयास करें।
- सावधान हो जाएं जब जान पहचान की छोटी सी अवधि में ही आपका चैट पार्टनर आपके रंग रूप की ज्यादा प्रशंसा करे।
- ऐसे लोगों से बात न करें जो आपके शारिरिक और यौन अनुभवों के बारे में आपसे प्रश्न पूछे। आप उस व्यक्ति से ऐसे प्रश्न नहीं पूछने को कह सकते है क्योंकि आप असहज महसूस करते हैं। यदि वे फिर भी ऐसा ही करते हैं तो तुरंत अपने माता–पिता को सूचित करें।

☞ ऐसे लोगों से बात न करें जो आपसे आपकी अश्लील फोटोग्राफ और वीडियो साझा करने को कहे। यदि आप अपनी अश्लील फोटोग्राफ अथवा वीडियो किसी के साथ साझा करते हैं तो वह व्यक्ति उन्हें किसी और के साथ साझा कर सकता है अथवा उन्हें सोशल मीडिया पर पोस्ट कर सकता है। वो आपको ब्लैकमेल भी कर सकते हैं।

☞ जब आपका चैट पार्टनर वेबकैम से कनेक्ट न हो तो अपने वेबकैम को कभी भी ऑन न करें।

☞ यदि आपका चैट पार्टनर उसके साथ आपकी बातचीत को गोपनीय रखने को कहे तो अपने बड़ो अथवा माता–पिता से बात करें।

☞ उस व्यक्ति से मिलने अकेले न जाएं जिससे आप ऑनलाइन मिले हों। हमेशा अपने साथ अपने किसी मित्र अथवा किसी बुजुर्ग को लेकर जाएं।

☞ कभी भी अनजान स्त्रोतों से अनावश्यक सॉफ्टवेयर और एप्स जैसे डेटिंग एप, ऑनलाइन गेम इत्यादि को इंस्टाल ने करें। चैट रूम में चैटिंग करते समय विशेष रूप से सतर्क रहना चाहिए। चैट रूम में अपनी व्यक्तिगत जानकारी कभी साझा न करें और अपनी पहचान को सीमित करें।

यदि आप साइबर ग्रूमिंग के शिकार हैं तो आपको क्या करना चाहिए ?

यदि आपको यह महसूस होता है कि आप साइबर ग्रूमिंग के शिकार हैं तो कृपया अपने बड़ो को सूचित करें ताकि वे हस्तक्षेप करके आपकी सहायता कर सकें। निम्नलिखित सुझाव स्थिति से निपटने में सहायक हो सकते हैं।

☞ **तत्काल अपने माता–पिता/बड़ों को सूचित करें**:– यदि कोई ऑनलाइन आपको असहज महसूस करा रहा है तो तत्काल अपने माता–पिता/बड़ों को सूचित करें। यह न सोचे कि आपके माता–पिता आपके ऑनलाइन कार्यकलापों को प्रतिबंधित कर देंगें या आपसे कंप्यूटर/स्मार्टफोन का उपयोग न करने के लिए कहेंगें। उन्हें सूचित करना महत्वपूर्ण है ताकि वे आपकी सहायता व मार्गदर्शन करें। अपने माता–पिता/बड़ों को पूरी बात स्पष्ट रूप से बताएं।

- **ग्रूमर को ब्लॉक करें**:– यदि ग्रूमर आपको ग्रूम करने के लिए सोशल मीडिया अथवा मैसेजिंग प्लेटफार्म का प्रयोग कर रहा है तो आप उसे ब्लॉक कर सकते हैं। सभी सोशल मीडिया ऐप अथवा सेवाओं में यूजर को ब्लॉक करने का विकल्प होता है।
- **मैसेज को कलेक्ट और सेव करें**:– ग्रूमर द्वारा आपके साथ साझा किए गए मैसेज, फोटो अथवा वीडियों को सेव करें। ऐसे मैसेज, फोटो अथवा वीडियो का प्रयोग उनके विरूद्ध कानूनी कार्यवाही किए जाने पर साक्ष्य के रूप में किया जा सकता है।
- आपके माता–पिता/बड़े, ग्रूमर के खिलाफ शिकायत करने के लिए स्थानीय पुलिस स्टेशन से संपर्क कर सकते हैं।

क्या आप जानते हैं कि इलैक्ट्रानिक रूप में अश्लील सामग्री अथवा बाल यौन शोषण सामग्री (सी एस ए एम) को तैयार करना, प्रदर्शित करना और उसका प्रचार करना भारत के सूचना प्रौद्योगिकी अधिनियम 2000 के अंतर्गत दंडनीय अपराध हैं ?

ऑनलाइन गेमिंग

हैरानी की बात है कि ऑनलाइन गेमिंग साइबर सुरक्षा से कैसे संबंधित है? मैं आपको बताता हूँ कि अधिक से अधिक बच्चे और युवा ऑनलाइन गेम खेल रहे हैं और भविष्य में यह संख्या बढ़कर कई गुना होने वाली है। जहां कहीं भी इंटरनेट यूजर्स की संख्या ज्यादा है, साइबर अपराधी उनको शिकार बनाने का रास्ता ढूंढ लेते हैं। यह धोखाधड़ी, साइबर बुलिंग, अनुचित विषयों को साझा करने आदि के रूप में हो सकता है।

गेमिंग एक अन्य क्षेत्र है जिसे सूचना प्रौद्योगिकी के पदार्पण से रूपान्तरित किया गया है। अधिक से अधिक बच्चे ऑनलाइन गेमिंग कम्युनिटी में शामिल हो रहे हैं। आसान पहुंच और प्लेटफार्म की विभिन्नता जिसका प्रयोग ऑनलाइन गेम खेलने में किया जा सकता है, उससे भारत में ऑनलाइन गेमिंग में वृद्धि हुई है। बच्चे मोबाइलों, कन्सोलों, कम्प्यूटरों, पोर्टेबल गेमिंग यंत्रों और सोशल नेटवर्कों पर ऑनलाइन गेम खेल सकते हैं। गेमिंग कन्सोल्स कम्प्यूटर की तरह कार्य करते हैं जिसमें आपको एकाउंट बनाना होता है। लॉग–इन करके हैडसेट लगाकर, वेब कैम या अन्य यंत्रों का उपयोग करना होता है। आप केवल करोड़ों यूजर्स के साथ ऑनलाइन गेम ही नहीं खेलते बल्कि उनसे बातचीत भी करते हैं, अपने विचार साझा करते हैं, दोस्त बनते हैं, ग्रुप में शामिल होते हैं इत्यादि। एक समय में करोड़ों प्लेयर्स ऑनलाइन गेम खेलते हैं। ऑनलाइन गेम्स मनोरंजक हो सकते हैं, परंतु इनके साथ जुड़े हुए जोखिम भी हैं।

क्या आप जानते हैं कि ऑनलाइन गेम्स के साथ स्पैम, वाइरस, द्वेषपूर्ण सॉफ्टवेयर भी डाउनलोड हो जाएंगे जो आपके कम्प्यूटर या मोबाइल फोन या गेमिंग कन्सोल को प्रतिकूल रूप से प्रभावित कर सकते हैं? प्रख्यात साइट्स से गेम डाउनलोड करना ही सही है। कभी भी अवैध गेम्स और सॉफ्टवेयर डाउनलोड/इंस्टाल न करें।

यह चिन्ता का विषय है कि कम्प्यूटर और स्मार्ट फोन से प्रेम करने वाले बच्चों के आउटडोर कार्यकलाप और शारीरिक खेल छूट रहे हैं। यह उपयुक्त होगा कि ऑनलाइन गेम्स के अतिरिक्त आउटडोर गेम्स को भी शामिल किया जाए जो आपके समग्र शारीरिक, मानसिक और सामाजिक विकास में सहायता करते हैं।

उपलब्ध ऑनलाइन गेम्स की रेंज और विश्व भर में करोड़ों प्लेयर्स के साथ खेलने की सुगमता को ध्यान में रखते हुए कहा जा सकता है कि ऑनलाइन गेमिंग दूसरों से जुड़ने में आपके लिए मनोरंजक हो सकता है, परन्तु वास्तव में आपके लिए इससे जुड़े जोखिमों को समझना और कतिपय परिस्थितियों से निपटने की जानकारी होना महत्वपूर्ण है। ऑनलाइन गेमिंग अनुभव का आनंद लीजिए और मजे कीजिए, परन्तु यह सुनिश्चित कर लीजिए कि आप सुरक्षित खेल रहे हैं।

क्या आप जानते हैं कि ऑनलाइन गेमिंग से जुड़े हुए जोखिम कौन–कौन से हैं?

- ऑनलाइन आक्रामक खिलाडियों की संख्या अधिक है जो आपको डरा–धमका सकते हैं। कुछ खिलाड़ी दूसरों को डराने–धमकाने या परेशान करने के लिए ही खेलते हैं। वे अशोभनीय भाषा का प्रयोग कर सकते हैं या दूसरों को धोखा दे सकते हैं। आपके लिए सतर्क रहना महत्वपूर्ण है।
- बहुत से वयस्क और साइबर अपराधी भी ऑनलाइन गेम खेलते हैं और बालक होने का बहाना करते हैं। वे आपको गेमों के बारे में टिप्स देकर, आपके साथ प्वाइंट साझा करके आपके साथ दोस्ती करने का प्रयास करते हैं और आपका विश्वास जीतने का प्रयास करते हैं। इस अवसर का प्रयोग करके वे आपकी व्यक्तिगत

सूचना प्राप्त करके अथवा आपसे अकेले में मिलकर आपको कोई घोटाला करने के लिए प्रोत्साहित कर सकते हैं।

- बहुत से ऑनलाइन गेम से जुड़ी वेबसाइटें हैं। इस के अतिरिक्त, कोई रूचिकर ऑनलाइन गेम डाउनलोड करने के लिए आपको ई–मेल अथवा टेक्स्ट मैसेज के माध्यम से लिंक्स भेज सकता हैं। कई गेमों में कोई खाता खोलने से पहले खेलने वाले के बारे में बहुत–सी व्यक्तिगत जानकारी मांगी जाती हैं। यह आपकी व्यक्तिगत जानकारी जैसे आपका नाम, आयु, मोबाइल नम्बर आदि के साथ समझौता हो सकता है जिसका बाद में दुरूपयोग किया जा सकता है। असुरक्षित साइटों से डाउनलोड किए गए निःशुल्क ऑनलाइन गेम के साथ वायरस और मॉलवेयर आदि भी डाउनलोड हो सकता है जो आप के कम्प्यूटर, स्मार्टफोन अथवा अन्य गेम वाले यंत्रों पर बुरा प्रभाव डाल सकता है।

- बहुत से ऑनलाइन गेमों में आपको प्वाइंट/सिक्के आदि खरीदने के लिए कहा जाता है जिन्हें खेल में सुधार के लिए अथवा समय या साधनों के अनुसार आप को फायदा देने के लिए उपयोग किया जाता है। आप से भुगतान के लिए क्रेडिट कार्ड का विवरण साझा करने के लिए कहा जाता है। इसे खरीदने के लिए आप अपने माता–पिता से सहायता मांगते हैं। हालांकि कुछ संक्रमित ऑनलाइन गेम्स आप के क्रेडिट कार्ड का ब्यौरा प्राप्त कर सकते हैं और इसका दुरूपयोग कर सकते हैं।

क्या– आप ऑनलाइन गेमिंग के बारे में चिंतित हैं? चिंता न करें...... जानकारी और सावधानी के साथ आप सुरक्षित ढ़ग से ऑनलाइन गेम खेल सकते हैं। आपको सतर्क रहने और स्वयं को तथा अपने मित्रों को ऑनलाइन गेमिंग से जुड़े गहरे जोखिमों से बचाने के लिए सुरक्षा उपाय अपनाने की आवश्यकता है।

आओ अब इस बात पर चर्चा करते हैं कि आप स्वयं को कैसे सुरक्षित रख सकते हैं।

- ऑनलाइन गेम खेलते समय दूसरे खिलाड़ियों के साथ अपनी व्यक्तिगत सूचना जैसे नाम, जन्म तिथि, पता और दूरभाष संख्या साझा न करें क्योंकि आपको पता नहीं होता है कि वे खिलाड़ी कौन हैं और उनकी मंशा क्या है? हो सकता है आप अपनी जानकारी घोटाले बाजों या साइबर बुलिज़ के साथ साझा कर दें।

- जब आप ऑनलाइन गेम खेल रहे हों तो अपने अथवा अपने माता–पिता के क्रेडिट

कार्ड/डेबिट कार्ड का ब्यौरा किसी के भी साथ साझा नहीं करें। कुछ साइबर अपराधी गेम जीतने या प्वाइंट्स साझा करने में सहायता प्रदान करके बच्चों के साथ मित्रता कर लेते हैं। वे आपका विश्वास जीत सकते हैं और बाद में सिक्के /प्वाइंट आदि खरीदने के लिए आपकी सहायता मांग सकते हैं। वे आपके क्रेडिट अथवा डेबिट कार्ड का ब्यौरा मांग सकते हैं। यह ब्यौरा किसी के साथ भी साझा नहीं करें।

- अप्रतिष्ठित निःशुल्क ऑनलाइन गेमिंग वेबसाइट से डाउनलोड किए गए गेमों को कभी भी इंस्टाल नहीं करें। मेल अथवा टेक्स्ट मैसेज अथवा पोप अप के माध्यम से प्राप्त लिंक पर क्लिक करके कभी भी गेम डाउनलोड नहीं करें। हो सकता है आप वायरस और मालवेयर डाउनलोड कर लें जो आपके कम्प्यूटर अथवा स्मार्ट फोन की सुरक्षा के लिए खतरा बन सकते हैं।

- अपने कम्प्यूटर, स्मार्ट फोन या हाथ में रखे जाने वाले किसी अन्य यंत्र पर हमेशा अच्छे वाला एंटीवायरस इंस्टाल करें। एंटीवायरस और अन्य एप्लिकेशनों को नियमित रूप से अपडेट करते रहें।

- अपना पासवर्ड किसी को नहीं बताएं। आपको अपने ऑनलाइन गेमिंग एकाउंट और अन्य ऑनलाइन एकाउंट के लिए जटिल पासवर्ड रखना चाहिए। अच्छा हो कि आप नियमित अंतराल पर अपना पासवर्ड बदलते रहें।

- ऑनलाइन गेम खेलते समय कभी भी वाइस चैट अथवा वेब कैम का उपयोग नहीं करें। इससे आपकी पहचान दूसरे खिलाड़ियों के साथ साझा हो सकती है और यह साइबर बुलिज़ और अन्य साइबर अपराधियों को आकर्षित कर सकती है।

- आपके ऑनलाइन गेमिंग वर्ल्ड से जुड़े किसी भी व्यक्ति से कभी भी न मिलें। वास्तविक जीवन में वह बहुत अलग हो सकते हैं। साइबर अपराधी आपके मित्र बन सकते हैं तथा आपसे मिलने का या आपकी व्यक्तिगत जानकारी प्राप्त करने का प्रयास कर सकते हैं। उनकी गलत मंशा हो सकती है।

- ऑनलाइन गेमिंग वर्ल्ड में यदि आप किसी चुनौती का सामना करते हैं तो तुरन्त अपने माता–पिता अथवा बुजुर्गों को बताएं ताकि वो आपकी सहायता और मार्गदर्शन कर सकें।

आउटडोर गेम खेलने की आदत डालें। आप आउटडोर क्रियाकलापों का आनन्द उठाएंगे और आप सही और सच्चे मित्र बना सकते हैं। जहां तक संभव हो ऑनलाइन गेम एक सीमा तक ही खेलें।

आपको पता है आउटडोर गेम खेलने से आपको पर्यावरण के बारे में जानकारी प्राप्त करने, मांसपेशियों को मजबूत बनाने, आत्मविश्वास प्राप्त करने, नये सच्चे मित्र बनाने तथा समग्र रूप से आपके व्यक्तित्व का विकास करने में मदद मिलती है?

ई-मेल धोखाधड़ी

अधिकतर लोगों के पास व्यक्तिगत ई–मेल एकाउंट होते हैं। हमें ई–मेल एकाउंट की जरूरत अपने दोस्तों और परिवार के सदस्यों को केवल ई–मेल भेजने के लिए ही नहीं होती है बल्कि सोशल मीडिया एकाउंट, ऑनलाइन गेमिंग एकाउंट खोलने और अन्य ऑनलाइन एकाउंट खोलने के लिए भी इसकी जरूरत होती है। हमारा ई–मेल एकाउंट हमारे जीवन का एक अभिन्न अंग बन गया है। जैसे–जैसे आप बड़े होंगे आपके ई–मेल एकाउंट की उपयोगिता बढ़ेगी। आप अपने ई–मेल एकाउंट का प्रयोग बैंक, मोबाइल सेवा प्रदान करने वाले से जोड़ने के लिए और अपने महाविद्यालय आदि से पत्र व्यवहार करने के लिए करेंगे। यह बहुत जरूरी है कि आप यह सीखें कि अपने ई–मेल एकाउंट को कैसे सुरक्षित रखा जाए।

क्या आपको पता है की हम सभी को नियमित रूप से अनावश्यक मेल प्राप्त होते हैं? क्या आपने अपने ई–मेल एकाउंट में स्पैम ई–मेल बॉक्स पर ध्यान दिया है? लगभग सभी ई–मेल प्रदाता स्पैम बॉक्स की सुविधा प्रदान करते हैं जिसमें अनावश्यक मेल को अंतरित किया जाता है। ई–मेल धोखाधड़ी एक आम बात है और व्यक्तिगत लाभ अथवा किसी व्यक्ति को नुकसान पहुंचाने हेतु अन्य ई–मेल एकाउंट को खतरे में डालने के लिए साइबर अपराधियों द्वारा इसे न्यूनतम व्यय पर उपयोग किया जाता है।

यह कैसे काम करता है?

ऐसे बहुत से तरीके हैं जिन्हें साइबर अपराधी ई–मेल का उपयोग करके आपके सिस्टम को नुकसान पहुंचा सकता है अथवा आपकी महत्वपूर्ण व्यक्तिगत जानकारी संग्रहित कर सकता है। आपने फिशिंग, विशिंग आदि के बारे में सुना होगा। आप इनके बारे में ऑनलाइन पढ़ सकते हैं लेकिन अब हम यहां बहुत साधारण तरीके से यह समझने का प्रयास करेंगे कि ई–मेल धोखाधड़ी किस प्रकार हो सकती है।

☞ विश्व में कहीं भी बैठा हुआ साइबर अपराधी एक सही लगने वाले जाली एकाउंट से आपको ई–मेल भेज सकता है। उदाहरण के लिए आपको अपने गेमिंग पोर्टल या सोशल मीडिया प्लेटफॉम से ई–मेल प्राप्त हो सकती है जिसमें सर्विस प्रदाता की वर्तनी अथवा ई–मेल आईडी थोड़ी परिवर्तित होगी जैसे – customersupport@gammingportal.com. क्या आपने यह नोट किया कि "गेमिंग" की वर्तनी सही नहीं है? इस प्रकार की ई–मेल में ऐसे लिंक होते हैं जो आपको किसी दूसरे पेज पर भेज देंगे जहां आपको टेक्नोलोजिकल अपग्रेड, अनुपालन या अन्य जाली कारणों हेतु (जो आपको सही प्रतीत होंगे) पासवर्ड/अन्य विवरण भरने के लिए कहा जाएगा और इस प्रकार अंत में आप अपने ब्यौरे साइबर अपराधियों को दे देंगे।

☞ साइबर अपराधियों द्वारा उपयोग में लाया जाने वाला एक और आम तरीका एक मालवेयर (एक खतरनाक प्रोग्राम जो आपके कम्प्यूटर को प्रभावित कर सकता है) वाला दस्तावेज़ (वर्ड या एक्सेल फाइल) संलग्न करके आपको ई–मेल भेज देना है। इस ई–मेल अथवा दस्तावेज का शीर्षक आपके लिए बहुत लुभावना हो सकता है जैसे प्रसिद्ध ऑनलाइन गेम जीतने के संबंध में टिप्स या किसी प्रसिद्ध ऑनलाइन गेम के लिए निःशुल्क सिक्के प्राप्त करने के बारे में टिप्स अथवा इसका कोई दूसरा लुभावना शीर्षक हो सकता है। यदि आप ऐसे किसी दस्तावेज़ को खोलते हैं तो यह मालवेयर आपके कम्प्यूटर अथवा मोबाइल में इंस्टोल हो सकता है। यह मालवेयर आपके कम्प्यूटर से महत्वपूर्ण विवरण जैसे पासवर्ड, लॉगइन आईडी आदि साइबर अपराधियों को भेज सकता है।

☞ अन्य सामान्य ई–मेल धोखाधड़ी यह भी है कि कोई साइबर अपराधी आपको यह सूचना देने वाला ई–मेल भेजता है कि आपने एक लॉटरी अथवा एक अनोखा उपहार जीता है अथवा विदेश में रह रहे आपका कोई दूर का रिश्तेदार आपके लिए धन छोड़कर गया है। यह प्रस्ताव इतना लुभावना होता है कि आप ई–मेल खोल लेत हैं और इसका जवाब दे देते है। साइबर अपराधी जीती गई राशि भेजने के लिए आपसे

आपका व्यक्तिगत ब्यौरा और बैंक का ब्यौरा मांगता है। वे आपसे प्रक्रिया शुल्क जमा करने के लिए भी कह सकते हैं ताकि वे जीती गई राशि भेज सकें। ऐसी सभी ई–मेल प्रायः जाली होती हैं और इनकी मंशा आपसे आपका व्यक्तिगत विवरण या आपसे पैसा ले लेना है। बालक होने के कारण हो सकता है आपका बैंक खाता नहीं हो किन्तु फिर भी आपको ऐसे ई–मेल प्राप्त हो सकते हैं। आपको चाहिए कि आप अपने माता–पिता को ऐसे ई–मेलों की जानकारी दें ताकि वे अपना बचाव कर सके।

- साइबर अपराधी द्वारा किए जाने वाला एक आम अपराध ईमेल एकाउंट को हैक करना है। आपकी ईमेल आईडी और पासवर्ड प्राप्त करने के लिए malware अथवा अन्य चालबाजियों को इस्तेमाल कर सकते हैं। आपका ईमेल एकाउंट हैक हो जाने पर साइबर अपराधी इस का इस्तेमाल सोशल मीडिया एकाउंट, बैंक एकाउंट आदि जैसी आपकी महत्वपूर्ण जानकारी प्राप्त कर सकते हैं। वे आपके सभी contacts को offensive ईमेल भी भेज सकते हैं।

- आपकी ईमेल हैक करना साइबर अपराधियों द्वारा की जाने वाली एक और सामान्य चालबाजी है जिसके जरिये वे आपके नाम से आपके परिवार और आपकी ईमेल address book में दर्ज आपके मित्रों से वित्तीय सहायता मांग सकते हैं। क्या आपको अपने किसी जानकार व्यक्ति से वित्तीय सहायता मांग की ईमेल प्राप्त हुई है कि वह आपात स्थिति में हैं और उसके पास टेलीफोन अथवा उसके बैंक एकांउट तक सीमित पहुँच है।

क्या आप ईमल पर होने वाली धोखाधड़ी को लेकर चिंतित है? आपको चिंता नहीं करनी चाहिए, आप एहतियात बरतकर बिना किसी भय के ईमेल का इस्तेमाल कर सकते हैं। आपको सावधान होकर और एहतियात बरतकर ईमेल पर होने वाली चालबाजियों से स्वयं अपना और अपने मित्रों का बचाव करना है।

आइये यह सुनिश्चित करें कि आप ईमेल पर होने वाली चालबाजियों से अपना बचाव कैसे कर सकते हैं। आपको इन सुझावों की जानकारी अपने परिवार और अपने मित्रों को अवश्य देनी चाहिए।

- पहला महत्वपूर्ण कदम अपनी ईमेल आईडी की रक्षा करना है ताकि यह हैक नहीं हो सके। इसके लिए आपको एक जटिल पासवर्ड का प्रयोग करना चाहिए और समय–समय पर इसे बदलते रहना चाहिए। साइबर अपराधियों के लिए साधारण पासवर्ड जैसे password 123, आपका नाम अथवा आपकी जन्म तारीख का अनुमान लगाना बहुत आसान होता है। मुशिकल पासवर्ड का उपयोग करें जिसके लिए आप उसमें अक्षरो और अंको का इस्तेमाल कर सकते है।

- login के लिए two factor authentication का इस्तेमाल कर सकते हैं। अधिकतर ईमेल सेवा प्रदाताओं द्वारा इस विशेषता की व्यवस्था की जाती है। Two factor authentication की सहायता से पासवर्ड के साथ–साथ अपने मोबाइल फोन पर प्राप्त OTP के जरिये आप अपने एकांउट में login कर सकते हैं। सुरक्षा की दृष्टि से यह एक अच्छा तरीका है और इससे आप अपने एकांउट को सुरक्षित रख सकते हैं।

- अपने ईमेल एकाउंट का पासवर्ड कभी भी किसी को न बताएं। पासवर्ड बताने से आपका ईमेल एकाउंट खतरे में पड़ सकता है। अपरिचित व्यक्ति से प्राप्त लिंक अथवा अटैचमेंट को click नहीं करें।

- यदि आप अपने ईमेल एकांउट को access करने के लिए अपने मित्र का कम्प्यूटर अथवा किसी साइबर कैफे में कोई कम्प्यूटर इस्तेमाल कर रह हैं तो इस बात का अवश्य ख्याल रखें कि आप "remember password popup" पर yes click नहीं करें । ये संदेश आमतौर पर उस समय आते हैं जब आप किसी नए कम्प्यूटर पर login करते हैं। आपको यह सुनिश्चित करना है कि कोई भी कम्प्यूटर आपका पासवर्ड याद न रख पाए (इसका मतलब यह है कि उस कम्प्यूटर पर अपने एकाउंट को login करने के लिए पासवर्ड की आवश्यकता नहीं होगी)। इसका उपयोग करने के बाद अपने ईमेल एकाउंट को sign-off करना हमेशा याद रखें। साइबर कैफे में रखे कम्प्यूटर जैसे पब्लिक कम्प्यूटर से access किए गए अपने पासवर्ड को हमेशा बदल दें।

- यदि आप अपने मोबाइल फोन पर ईमेल access कर रहे हैं, तो अपने फोन के इस्तेमाल के लिए एक मुश्किल पासवर्ड रखें।

- अपना ईमेल हैक / compromised हो जाने पर अपने contacts को इस बारे में ईमेल अथवा संदेश के माध्यम से जानकारी दे दें और उन्हें सावधान करें कि वे आपकी ईमले आईडी से लिंक /अटैचमेंट नहीं खोलें। Help page के जरिए अपने ईमेल सेवा प्रदाता से तत्काल संपर्क करें और उनसे कहें कि वे आपके ईमेल को अस्थायी रूप से block कर दें। अपने पासवर्ड को फिर से प्राप्त करने का प्रयास करें और अपने पासवर्ड को तत्काल बदल दें।

- अज्ञात स्रोतों से अवांछित सॉफ़्टवेयर और ऐप्स इंस्टॉल ना करें। अज्ञात व्यक्ति से प्राप्त ईमेल या संदेश पर प्राप्त लिंक या फ़ाइलों पर कभी भी क्लिक न करें। यह आपके कंप्यूटर / फोन को मैलवेयर से infect करने का प्रयास हो सकता है।

- यदि आपको कोई लॉटरी जीतने अथवा अन्य कई प्रलोभन के बारे में ईमेल प्राप्त होता है तो कृपया उसका उत्तर न दें अथवा नाम पता, बैंक एकाउंट ब्यौरा आदि जैसी

व्यक्तिगत जानकारी न दें। यदि आपको किसी अपडेट अथवा किसी अन्य वास्तविक कारण के बारे में अपने सेवा प्रदाता से ईमेल प्राप्त होता है तो ईमेल भेजने वाले की आईडी की ध्यान पूर्वक जांच करें। यह भी जांच करें कि क्या कोई स्पेलिंग की गलती तो नहीं है। ऐसी ईमेल में प्राप्त लिंक्स पर क्लिक न करें। यह जानने के लिए क्या ईमेल की वास्तविक है या नहीं अपने सेवा प्रदाता से संपर्क साधने का प्रयास करें।

- यदि आपको अपने मित्र अथवा रिश्तेदार से वित्तीय सहायता के लिए कोई इमरजेंसी ईमेल प्राप्त होता है तो उस व्यक्ति से फोन पर अथवा अन्य जानकार व्यक्तियों से संपर्क कर के ईमेल की वास्तविकता का पता लगाएं। यह भी संभव हो सकता है कि उसका एकाउंट हैक हो गया है और ऐसे ईमेल भेजने में प्रयोग किया जा रहा हैं।

- चौकन्ना रहे और समय–समय पर अपना पासवर्ड बदलते रहने की आदत डालें, अज्ञात श्रोतों से प्राप्त होने वाले ईमेल्स पर ध्यान न दें और ईमेल पर अपने व्यक्तिगत ब्यौरे की जानकारी न दें तथा अज्ञात श्रोतों से प्राप्त लिंक/दस्तावेजों को क्लिक न करें।

क्या आप यह जानते हैं कि संचार उपकरणों अथवा अन्य उपकरणों का उपयोग करके लोगों को धोखा देना एक दंडनीय अपराध है।

ऑनलाइन लेनदेन में धोखाधड़ी

हालांकि यह संभव है कि आप में से अधिकतर लोग इस समय डेबिट कार्ड, क्रेडिट कार्ड, नेटबैंकिंग आदि जैसी बैंकिंग सेवाओं का उपयोग नहीं कर रहे हैं, लेकिन समय के साथ आप इन सेवाओं का उपयोग करने लगेंगे। इसके अतिरिक्त एक जागरूक नागरिक के रूप में आपको इस बात की जानकारी अवश्य होनी चाहिए कि ऑनलाईन लेनदेन में धोखाधड़ी किस प्रकार होती है ताकि आप अपने परिवार अपने मित्रों को इसकी जानकारी दे सकें।

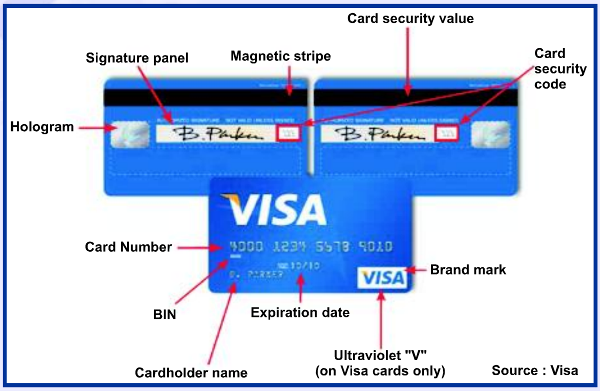
ऑनलाईन लेनदेन में धोखाधड़ी का मतलब किसी साइबर अपराधी द्वारा आपके बैंक एकाउंट से गैर कानूनी रूप से पैसा निकालना अथवा उसे अन्य बैंक एकाउंट में अंतरित करना है। ऑनलाईन लेनदेन में धोखाधड़ी उस समय हो सकती है जब आपका login अथवा बैंक एकाउंट ब्यौरा अथवा क्रेडिट कार्ड ब्यौरा किसी साइबर अपराधी द्वारा चुरा लिया गया हो।

यह कैसे होता है?

साइबर अपराधियों द्वारा लोगों से ऑनलाईन धोखाधड़ी करने के लिए कई तरीके अपनाए जाते हैं।

साइबर अपराधी किसी फर्जी एकाउंट से आपको ईमेल भेज सकते हैं जिससे यह प्रतीत होता है कि वह या तो बैंक अथवा क्रेडिट कार्ड सेवा प्रदाता से प्राप्त हुई है। जब आप

ईमेल दिए गए लिंक पर क्लिक करते हैं तो वह आपको ऐसे पेज पर ले जाता है जिसमें आपके बैंक एकांउट, क्रेडिट कार्ड, Card Verification Value (CVV), expiry date आदि जैसी संवेदनशील सूचना मांगी गयी होती है। यह सूचना देने पर आपका एकाउंट compromised हो सकता है।



साइबर अपराधी अपनी फर्जी पहचान से अपने को बैंक कर्मचारी बताकर आपको कॉल कर सकते हैं और आपसे क्रेडिट कार्ड अथवा बैंक ब्यौरा अर्थात् एकाउंट नंबर, Personal Identification Number (PIN), CVV, expiry date, जन्म तारीख पूछने का प्रयास कर सकते हैं। ऐसा ब्यौरा देने पर आपका एकाउंट compromised हो सकता है।

क्या आप जानते हैं कि आपका डेबिट/क्रेडिट कार्ड PIN यूनीक नंबर है जिसकी आवश्यकता एटीएम पर अथवा अन्य ऑनलाइन लेनदेन के लिए आपके कार्ड को access करने के लिए होती है। आप अपना पिन नंबर आसानी से बदल सकते हैं। समय–समय पर अपना पिन नंबर बदलते रहना अच्छी आदत है।

आमतौर पर हमारा मोबाइल नंबर हमारे बैंक एकाउंट से लिंक्ड होता है। साइबर अपराधी अपने को मोबाइल सर्विस प्रदाता का कर्मचारी बताकर आपको कॉल भी कर सकते हैं और आपको यह सूचित कर सकते हैं कि यदि आप अपना Subscriber Identification Module अर्थात् सिम को अपडेट नहीं करेंगे तो आपका मोबाइल बंद हो जाएगा। सिम को अपडेट करने के लिए ये लोग आपको लिंक भेजेंगे अथवा आपसे कहेंगे कि आप अपने

नंबर से सेवा प्रदाता को SMS भेजें। वास्तव में वे आपसे मोबाइल प्रदाता को SMS इसलिए भिजवाने का प्रयास कर रहे हैं कि आपका मौजूदा सिम block हो जाए और आपका duplicate SIM जारी हो जाए। वे सेवा प्रदाता से duplicate SIM प्राप्त करके आपके मोबाइल नंबर और banking app का इस्तेमाल करके ऑनलाइन लेनदेन करने के लिए उसका इस्तेमाल करते हैं।

क्या आप जानते हैं कि बैंक, बैंकिंग धोखाधड़ी की हानि की भरपाई तभी करता है जब लापरवाही अथवा सुरक्षा में कमी बैंक की ओर से हुई हो?

साल 2017 में क्रेडिट / डेबिट कार्ड और इंटरनेट बैंकिंग धोखाधड़ी से संबंधित कुल 1785 मामलें दर्ज कराए गए थे। इससे कुल 71.48 करोड़ रूपये का नुकसान हुआ।

क्या आप ऑनलाइन लेन–देन की धोखाधड़ी को लेकर चिंतित हैं, चिंता मत कीजिए जानकारी और सावधानी से आप स्वयं को ऑनलाइन लेन–देन की धोखाधड़ी से बचा सकते हैं। कृपया याद रखें यदि आप अपने बैंक तथा कार्ड का ब्योरा जैसे कार्ड नंबर,PIN, CVV, वैद्यता समाप्ति तिथि, बैंक खाता पासवर्ड इत्यादि, किसी के साथ साझा न करें इससे आप स्वयं को ऑनलाइन लेन–देन की धोखाधड़ी से बचा सकते हैं। आपको सतर्क रहने और स्वयं को तथा अपने मित्रों को ऐसी धोखाघड़ी से बचाने के लिए सुरक्षा उपायों को अपनाना होगा।

आइए इस बात पर चर्चा करें कि कैसे आप स्वयं को ऑनलाइन लेन–देन की धोखाधड़ी का शिकार होने से बचा सकते हैं। इन सुझावों को अपने परिवार तथा मित्रों से साझा करना न भूलें।

☞ अपने बैंक तथा कार्ड का ब्योरा जैसे कि ऑनलाइन एकाउंट पासवर्ड, कार्ड नंबर, CVV, वैद्यता समाप्ति तिथि, PIN, OTP इत्यादि किसी के साथ साझा न करें। इन ब्योरों को साझा करने से आपके खाते को खतरा हो सकता है जिससे अवैध ऑनलाइन वित्तीय लेन–देन किया जा सकता है।

☞ अपने बैंक खाते के ऑनलाइन पासवर्ड तथा अपने डेबिट/क्रेडिट कार्ड के PIN को नियमित रूप से अपडेट करने की आदत बनाए।

☞ जब भी अपने बैंक खाते में लॉग–इन करें तो बैंक की वेबसाइट स्वयं टाइप करने की आदत बनाए। ई–मेल, मैसेज अथवा पॉप–अप पर आने वाले बैंक वेबसाइट के लिंक पर कभी क्लिक न करें। ये जाली लिंक हो सकते हैं और आपको जाली साइट पर ले जा सकते हैं। एक बार जब आप जाली साइट से अपने बैंक खाते पर लॉग–इन करते हैं आपकी गोपनीय जानकारी जैसे खाता संख्या तथा पासवर्ड चोरी हो सकते हैं।

☞ यह सुनिश्चित करने के लिए कि आप सुरक्षित बैंक वेबसाइट पर पहुंचे हैं, बैंक के सुरक्षा प्रमाणपत्र ब्यौरें तथा विभिन्न साइनों जैसे ग्रीन एड्रेस लाइन, एड्रेस बार पर लॉक साइन तथा HTTPS की जांच करें।

☞ हमेशा ध्यान दे कि वेबसाइट URL HTTPS से शुरू हो रहा हो। HTTPS वाले वेबसाइट URL आपके डाटा को वेबसाइट पर encrypt करके प्रदान करता है तथा उसे किसी प्रकार की हानि से सुरक्षित रखता है। जो वेबसाइट HTTPS से आरंभ नहीं होती है उस पर अपनी गोपनीय सूचना जैसे कि ऑनलाइन एकाउंट पासवर्ड, कार्ड नंबर, CVV वैद्यता समाप्ति तिथि, PIN, OTP इत्यादि साझा न करें।

☞ अपने मोबाइल फोन को भी सुरक्षित रखना आवश्यक है क्योंकि आपका मोबाइल नबंर आपके बैंक खाते के साथ जुड़ा होता है। अपने मोबाइल फोन को खोलने के लिए हमेशा एक जटिल पासवर्ड प्रयोग करें तथा एक अच्छा ऐंटीवायरस साफ्टवेयर इन्स्टाल करें। अगर आपको आपके मोबाइल सर्विस प्रदाता से कॉल प्राप्त होती

है कि यदि आप अपना नंबर अपडेट नहीं करेंगें तो आपका नंबर निष्क्रिय कर दिया जाएगा या ऐसा कोई अन्य संदेश प्राप्त होता है, तो सावधान हो जाएं। फोन को काट दे और अपने मोबाइल सेवा प्रदाता के कस्टमर केयर नंबर पर कॉल करके पता करें कि वह काल वास्तविक थी या नहीं।

☞ अपने मोबाइल अथवा कम्प्यूटर में कभी भी चोरी का सॉफ्टवेयर इंस्टाल न करें। यह न केवल गैरकानूनी है बल्कि यह आपके उपकरण की सुरक्षा को नुकसान भी पहुंचा सकता है। हमेशा अपने कम्प्यूटर तथा मोबाइल फोन में अच्छा एंटीवायरस इंस्टाल करें। यह आवश्यक है कि आप अपने कम्प्यूटर सॉफ्टवेयर तथा एंटीवायरस को up-to-date रखें।

☞ कभी भी किसी सार्वजनिक वाय–फाई या साइबर कैफे के कम्प्यूटर का प्रयोग ऑनलाइन लेनदेन के लिए न करे क्योंकि हो सकता है कि साइबर कैफे के कम्प्यूटर में अपडेटिड एंटीवायरस न हो या मैलवेयर से इंफैक्टिड हो जो आपके बैंक विवरण और अन्य महत्वपूर्ण गोपनीय जानकारी प्राप्त कर सकता है जैसे कार्ड नं., कार्ड समाप्ति की तारीख, सी वी वी आदि।

☞ अपने बैंक खाते और क्रेडिट कार्डों के मासिक विवरण को नियमित रूप से जांचने की आदत डालें। यह देखें कि कोई अप्राधिकृत लेनदेन तो नहीं हुआ है।

☞ यदि आपको यह पता चले कि आपके बैंक खाते या कार्ड के विवरण किसी के द्वारा प्राप्त कर लिए गए हैं/चुरा लिए गए हैं या आपका डेबिट या क्रेडिट कार्ड गुम हो गया है तो तुरंत बैंक को फोन करे और अपना कार्ड/खाता तुरंत ब्लॉक कर दें। यदि आपके खाते से कोई अप्राधिकृत लेनदेन हुए हैं तो अपने निकटतम पुलिस स्टेशन पर औपचारिक शिकायत दर्ज करवाएं।

आपकी सोशल नेटवर्किंग प्रोफाईल्स की सुरक्षा के उपाय

आजकल हम सभी फेसबुक, ट्विटर, इंस्टाग्राम स्नैपचैट आदि जैसी सोशल नेटवर्किंग साइटों का अधिकाधिक प्रयोग कर रहे हैं। हम अपने मित्रों और रिश्तेंदारों से अपना अपडेट या सेल्फी या तस्वीरें शेयर करना पसंद करते हैं। हम यह भी चाहते कि हमारी पोस्ट/तस्वीरों और अपडेट्स पर लाइक्स और कमेंट भी मिलें। हालांकि, सोशल नेटवर्किंग साइटों ने हमें अपने मित्रों और रिश्तेदारों से आसानी से जुड़ने में हमारी मदद की लेकिन यदि हम सावधान न रहे तो गंभीर साइबर खतरे भी हो सकते हैं जो हमें नुकसान पहुंचा सकते हैं।

यह कैसे काम करते हैं?

साइबर क्रिमिनल्स और साइबर बुलीज हमें नुकसान पहुंचाने के लिए सोशल नेटवर्किंग प्लेटफार्मों का प्रयोग करते हैं। आओ हम यह जानें कि सोशल नेटवर्किंग साइटों से जुड़े ऐसे कौन से कॉमन साइबर खतरे हैं जो हमें नुकसान पहुंचा सकते हैं।

☞ साइबर क्रिमिनल आपकी छवि को नुकसान पहुंचाने के लिए या अन्य अवैध प्रयोजनों के लिए सोशल मीडिया पर आपका फेक एकाउंट बनाकर नेगेटिव बातें और अनुचित जानकारी शेयर कर सकते हैं। यह एक गंभीर खतरा है जो किसी को भी नुकसान पहुंचा सकता हैं। किसी भी ई मेल आई डी का इस्तेमाल करके सोशल मीडिया एकाउंट आसानी से बनाया जा सकता है। आजकल हमारी तस्वीरें, ई मेल आई डी, जन्मतिथि और अन्य जानकारी ऑनलाइन पर आसानी से मिल जाती है। साइबर अपराधी हमारा फेक एकाउंट खोलने के लिए इन विवरणों का प्रयोग कर सकते हैं।

☞ सोशल मीडिया प्लेटफार्मों पर आज–कल साइबर बुलिंग बहुत अधिक होने लगी है। साइबर बुलीज़ आपको दुख पहुंचाने या अपमानित करने के लिए अभद्र या अशोभनीय संदेश भेजने के लिए सोशल मीडिया का प्रयोग कर सकते हैं।

☞ सोशल नेटवर्किंग साइटों पर शेयर किए गए लिंकों के जरिए ऑनलाइन धोखाधड़ी की जा सकती है। साइबर अपराधी मैलिसियस लिंक या मेलवेयर से युक्त कोई पोस्ट शेयर कर सकते हैं। यदि आपने उस लिंक पर क्लिक कर दिया तो आपका कम्प्यूटर या मोबाइल इंफैक्टिड हो सकता है या जोखिम ग्रस्त हो सकता है।

सोशल नेटवर्किंग प्लेटफॉर्मों पर साइबर खतरों से चिंतित हैं? परेशान न हों:–

थोड़ा सतर्क रह कर और एहतियात बरतकर आप अपने आपको इन खतरों से बचा सकते हैं और आसानी से सोशल नेटवर्किंग साइटों का प्रयोग कर सकते हैं। ऐसी धोखाधड़ियों से स्वयं को और अपने मित्रों को बचाने के लिए आपको सतर्क रहना होगा और कुछ सुरक्षा उपाय करने होंगे।

आइए चर्चा करें कि आप खुद को और अपने सोशल मीडिया एकाउंटों को कैसे सुरक्षित रख सकते हैं। आप इन सुझावों को अपने परिवार और मित्रों को भी शेयर करें।

☞ अपने सोशल नेटवर्किंग एकाउंट को सुरक्षित रखने के लिए पहला जरूरी कदम यह है कि यह हैक न होने पाए या खतरे में न पड़े। इसके लिए आपको एक मुश्किल पासवर्ड का प्रयोग करना चाहिए और समय–समय पर इसे बदलते रहें।

क्या आप जानते हैं कि अधिकांश सोशल मीडिया साइटें और ई मेल सर्विस प्रोवाइडर आपको आपके खाते को लॉग इन करने के लिए टू फैक्टर ऑथेंटिकेशन का विकल्प देते हैं। आप 'सेटिंग्स' पर जाएं और टू फैक्टकर ऑथेंटिकेशन को एक्टिवेट करें। इसका अर्थ यह है कि आपको अपना एकाउंट लॉग इन करने के लिए अपना पासवर्ड और आपके मोबाइल पर प्राप्त हुआ वन टाइम पासवर्ड (ओटीपी) टाइप करना होगा। यह एक अच्छा सुरक्षा फीचर है और इसका प्रयोग आपके सभी एकाउंट खोलने के लिए किया जाना चाहिए।

☞ अपने सोशल मीडिया एकाउंट का पासवर्ड किसी से शेयर न करें। पासवर्ड शेयर करने से आपके एकाउंट का दुरुपयोग किया जा सकता है।

☞ आप जो कुछ भी सोशल नेटवर्किंग साइट्स पर पोस्ट करते हैं, वह हर किसी को दिखाई देगा जब तक आप अपनी पोस्ट की एक्सेस को अपने मित्रों/फोलोअर्स

तक सीमित नहीं करेंगे। आपको अपने सोशल मीडिया एकाउंट की प्राइवेसी सेटिंग्स बदलनी चाहिए और यह सुनिश्चित कर लें कि आपके अपडेट्स/पोस्ट केवल आपके मित्र/फोलोअर्स ही देख सकें।

☞ अनजान लोगों की फ्रेंड रिक्वेस्ट एक्सेप्ट न करें। कोई भी फ्रेंड रिक्वेस्ट एक्सेप्ट करने से पहले यह देख ले कि रिक्वेस्टर को और कितने लोग फौलो कर रहे हैं या उसकी फ्रेंड लिस्ट में कितने लोग हैं। साइबर अपराधी आपके जानकार व्यक्ति का फेक एकाउंट बना सकते हैं। इसलिए, सतर्क रहें।

☞ आप सोशल मीडिया पर जो भी पोस्ट करते हैं आमतौर पर वह वहीं पर रहता है। अतः सोशल मीडिया पर कुछ भी पोस्ट करने से पहले सावधानी बरतें। ध्यान रखें कि यह जानकारी किसी के साथ भी शेयर हो सकती है। अपने निजी विवरण जैसे कि पता, फोन नं., जन्मातिथि आदि सोशल मीडिया साइट पर शेयर न करें।

☞ यदि आप सोशल मीडिया एकाउंटस को access करने के लिए अपने मित्र का कम्प्यूटर या साइबर कैफे में कोई कम्प्यूटर इस्तेमाल कर रहे हैं तो इस बात का अवश्य ख्याल रखें कि आप remember password pop up पर यस क्लिक नहीं करें। ये संदेश आमतौर पर उस समय आते हैं जब आप किसी नए कम्प्यूटर पर लॉगइन करते हैं आपको यह ध्यान रखना है कि कोई भी कम्प्यूटर आपका पासवर्ड याद न रख पाए (इसका मतलब यह है कि उस कम्प्यूटर पर अपने एकाउंट को लॉगइन करने के लिए पासवर्ड की आवश्यकता नहीं होगी)। हमेशा याद रखें कि इसका उपयोग करने के बाद अपने एकाउंट से साइन–ऑफ कर दें।

☞ यदि आप अपने मोबाइल फोन पर सोशल मीडिया एकाउंटस एक्सेस कर रहे हैं तो अपने फोन को एक्सेस करने के लिए एक मुश्किल पासवर्ड बनाएं।

☞ अपना सोशल मीडिया एकाउंट हैक हो जाने/खतरे में पड़ जाने पर अपने कांटैक्टस को अलर्ट ई मेल या मैसेज भेज दें। अपने सोशल मीडिया सर्विस प्रोवाइडर को तत्काल अस्थायी रूप से अपना एकाउंट बंद करने के लिए कहें। अपने पासवर्ड को रिट्रीव करने का प्रयास करें और अपना पासवर्ड तुरंत बदल दें।

☞ यदि आपको पता चले कि आपका जाली एकाउंट बनाया गया है, आप सोशल मीडिया प्रोवाइडर को तुरंत सूचित करे ताकि आपका एकाउंट ब्लॉक किया जा सके। यदि आपको कोई bully कर रहा है, अशोभनीय कमेंट्स या इमेजिस पोस्ट कर रहा है या आपकी छवि बिगाड़ने के लिए आपका फेक एकाउंट बना रहा है तो तुरंत अपने माता–पिता या बड़े लोगों को बताएं ताकि वे आपको सपोर्ट करें और गाइड करें। आप अपने माता–पिता की सहायता से अपने निकटतम पुलिस स्टेशन पर शिकायत भी दर्ज करवा सकते हैं।

- अज्ञात स्रोतों से अवांछित सॉफ्टवेयर और ऐप्स इंस्टॉल न करें। अज्ञात व्यक्ति से सोशल मीडिया पर प्राप्त लिंक या फाइल पर कभी भी क्लिक न करे। यह आपके कम्प्यूटर को मैलवेयर से इन्फेक्ट करने का प्रयास हो सकता है।
- जाली खबरें अथवा झांसा देने वाले संदेश सोशल मीडिया पर आग की तरह फैलते हैं। इससे कानून और व्यवस्था की समस्या उत्पन्न हो सकती है तथा कुछ मामलों में जान की हानि भी हो सकती है। सोशल मीडिया अथवा मैसेजिंग एप पर कोई भी संदेश आगे भेजने अथवा साझा करने से पहले अन्य स्रोतों से उसकी प्रमाणिकता की पुष्टि कर लें।
- कॉपीराइटेड विषयवस्तु जैसे कविता, निबंध, वीडियो, संगीत, चित्र, संगीत, संगीत की रचना, साफ्टवेयर इत्यादि को लेखक की अनुमति के बिना कभी भी डाउनलोड अथवा अपलोड न करें। किसी और की कॉपीराइटेड विषयवस्तु को डाउनलोड तथा अपलोड करना एक अपराध है।

आशा है कि आपको यह पुस्तिका अच्छी लगी होगी। ये सुझाव आपको साइबर अपराधों से सुरक्षित करने में मदद करेंगे। जैसा कि आप जानते हैं कि साइबर अपराधी लोगों को धोखा देने के लिए नित नए तरीके ढूंढता है। अतः, यह बहुत जरूरी है कि हम अपने आपको सुरक्षित रखने के लिए नए खतरों और धोखाधड़ी से बचने के नए तरीकों की जानकारी रखें।

साइबर दोस्त के कुछ सुझाव

- साइबर सुरक्षा, नए खतरों और साइबर अपराधों से बचने के उपायों के बारे में अधिकाधिक जानकारी प्राप्त करें।
- अच्छे साइबर सिटिजन बने। साइबर सुरक्षा के लिए एहतियात बरतें और अपने मित्रों और परिवार को भी बताएं।
- सुरक्षित साइबर पद्धतियों पर नियमित रूप से अपडेट्स के लिए **twitter handle @CyberDost** पर फोलो करें।
- आपसे अनुरोध है कि आप अपना फीडबैक **dircis2-mha@nic.in or pmuiec.cis-mha@nic.in** पर हमारे साथ साझा करें।

आपका साइबर दोस्त

CYBER DOST

@CyberDost

सत्यमेव जयते

गृह मंत्रालय
भारत सरकार