

★★★ कम्प्युनिटी पोलीसिंग अंतर्गत ★★★

बुलडाणा जिल्हा पोलीस दल

सायबर गुन्ह्यांपासून बचाव कसा करावा
यासंबंधी मार्गदर्शन करणारी पुस्तिका
(अल्पवयीन विद्यार्थ्यांसाठी)



अरविंद चावरिया भा.पो.से.
पोलीस अधीक्षक, बुलडाणा





सायबर गुन्ह्यांपासून बचाव कसा करावा यासंबंधी मार्गदर्शन करणारी पुस्तिका

(अल्पवयीन विद्यार्थ्यांसाठी)



संकल्पना

अरविंद चावरीया भा.पो.से.
पोलीस अधीक्षक, बुलडाणा

बुलडाणा जिल्हा पोलीस दल

गृह मंत्रालय भारत सरकार

ही 'सायबर सुरक्षा पुस्तिका' सायबर सुरक्षा तज्ज्ञांकडून तयार केली गेली आहे.

● प्रकाशक
पोलीस अधीक्षक
बुलडाणा जिल्हा

© गृह मंत्रालय
भारत सरकार
नॉर्थ ब्लॉक, नवी दिल्ली - ११०००१
द्वारा प्रकाशित

● मुद्रणस्थळ
ओंकार शास्त्री
मयुरेश क्रिएशन
जालना मो. ९८२२०७५०२६

● प्रकाशन : दि.
मराठी अनुवाद

अस्वीकृती :

या पुस्तिकेत सायबर गुन्ह्यांशी संबंधित माहिती अभ्यासकांना व नागरिकांना जागरूक करण्यासाठी देण्यात आली आहे. ज्यायोगे अशा गुन्ह्यांची पध्दत माहित झाल्यास सावधगिरी बाळगता येईल व आपले होणारे नुकसान टाळेल. तसेच गुन्हा घडण्यापासून अटकाव करता येईल. यातील माहिती व सल्ले फक्त सर्वसाधारण मार्गदर्शन आहे. जर आपणास असा गुन्हा निदर्शनास आला तर जवळच्या पोलीस स्टेशनमधील सायबर गुन्हे शाखेशी त्वरीत संपर्क करा.

अरविंद चावरीया भा.पो.से.
पोलीस अधीक्षक, बुलडाणा



सध्या लोक कॉम्प्युटर, लॅपटॉप, मोबाईलचा सर्रास वापर करीत आहेत. सर्व आर्थिक व्यवहार ऑनलाईन होत आहेत. भारतात ही क्रांती वेगाने होत आहे. याचबरोबर सायबर गुन्हेगारीही वेगाने वाढत आहे. याचे मुख्य कारण आहे, लोकांमध्ये सायबर-सुरक्षेच्या बाबतीत आवश्यक असणारी माहितीचा अभाव. या गुन्ह्यांपासून बचाव करण्यासाठी सायबर सुरक्षेची माहिती सर्वश्रुत व्हावी हा हेतू ही पुस्तिका प्रकाशित करण्यामागे आहे.

विशेषकरून अल्पवयीन मुले व विद्यार्थी यांना आपल्या जाळ्यात सहजपणे ओढणाऱ्या अनेक प्रकारची संकटे व सायबर गुन्ह्यांपासून स्वतःचा बचाव करण्यासाठी व सुरक्षित ठेवण्यासाठी जागरूकता निर्माण व्हावी यासाठी उपाय योजना जाणून घेणे हाच या पुस्तिकेचा मुख्य हेतू आहे. या पुस्तिकेत दिलेल्या सूचना आणि सल्ले फक्त मार्गदर्शनासाठी आहेत जर अल्पवयीन मुले व विद्यार्थी या गुन्ह्यांचे शिकार होतात तर घाबरू नका. आपल्या अभिभावकांशी यासंबंधी मोकळेपणाने चर्चा करा. त्यांच्या साह्याने स्थानिक पोलीस स्टेशन अथवा राज्य सायबर अपराध सेलशी संपर्क करा.

मनोगत

आज भारत इंटरनेट वापरात दुसऱ्या क्रमांकावर आहे मात्र सायबर सुरक्षेच्या बाबतीत पिछाडीवर आहे. सायबर गुन्हे हा एक प्रकारचा आर्थिक दहशतवादच आहे. नुकतेच एका बातमीने १३ लाख भारतीयांना संकटात टाकले आहे. त्यांच्या डेबिट व क्रेडिट कार्डचा तपशील 'डार्कवेब' वर विक्रीसाठी उपलब्ध असल्याची ही बातमी होती. यामुळे सायबर गुन्हेगार आता ही माहिती खरेदी करतील व तिचा वापर फसवणूक व सायबर दरोड्यासाठी करतील हे कटू सत्य आहे. जर सुज्ञ, ज्ञानी, बुद्धिमान लोक या सायबर गुन्द्यांना बळी पडतात तर अल्पवयीन मुले व विद्यार्थी हे या संकटापासून कसे बचाव करणार हा यक्ष प्रश्नच आहे.

या सायबर गुन्द्यांचा आवाका वाढतच आहे. केवळ भारतच नव्हे तर सर्व जगापुढे सायबर सुरक्षेचे आव्हान उभे आहे. किमान अल्पवयीन मुलांचा लैंगिक शोषण व फसवणूक यापासून बचाव करण्यासाठी कोणती खबरदारी घ्यावी यासाठी ही पुस्तिका प्रकाशित करित आहोत. त्याचा फायदा अल्पवयीन मुले, विद्यार्थी, पालक, शिक्षक यांनी घ्यावा, ही सदिच्छा!



अनुक्रमणिका

पुरतिकेविषयी

पान क्र.07

वाढत्या सायबर
गुन्ह्यांची चिंता

पान क्र.0९

सायबर गुन्ह्याचे संकट
कोणावरही येऊ शकते.

पान क्र.११

सायबर
बुलिंग

पान क्र.१३

ऑनलाईन गेमिंग

पान क्र.२१

सायबर
गुमिंग

पान क्र.१७

ई-मेल
द्वारे फसवणूक

पान क्र.२६

ऑनलाईन
व्यवहार घोटाळे

पान क्र.३१

अनुक्रमणिका

सोशल प्रोफाईल
सुरक्षित कसे ठेवावे

पान क्र.३६

सायबर
मित्राचे सल्ले

पान क्र.४०

ऑनलाईन गेम्स
मुलांसाठी सूचना

पान क्र.४१

ऑनलाईन गेम्स :
काय करू नये

पान क्र.४२

इंटरनेटचा वापर :
नैतिक सूचना

पान क्र.४३

दूरध्वनी सूची

पान क्र.४७



पुस्तिकेच्या संदर्भात

माहिती आणि प्रसारण क्षेत्र आमच्या दैनंदिन जीवनाचा अभिन्न भाग बनला आहे. यामध्ये आमचे बोलणे, मित्र बनविणे, अद्ययावत माहितीचा समावेश करणे, गेम्स खेळणे, खरेदी करणे इत्यादी बाबींना बदलून टाकले आहे. प्रसारणाचा आमच्या दैनंदिन जीवनाच्या बहुतांश गोष्टींवर प्रभाव पडला आहे.

आमची नवी पिढी तारुण्याच्या उंबरठ्यावरच सायबर स्पेसशी परिचित झाली आहे. जास्तीत जास्त मुले ऑनलाईन गेम्स खेळणे, मित्र बनवण्यासाठी सोशल नेटवर्किंग साईटचा उपयोग करण्यामध्ये आपला जास्तीत जास्त वेळ घालवित आहेत. लहानपणापासूनच स्मार्ट फोन द्वारे सोशल नेटवर्किंग, ऑनलाईन गेम्स, शॉपिंग इ. पर्यंत पोहचून खूप व्यापक झाले आहे. सायबर स्पेस आम्हाला वास्तवात विश्व जिंकून कोट्यवधी ऑनलाईन फायद्यांना जोडतो. इंटरनेटमुळे फायद्याशिवाय सायबर गुन्हांमध्ये ही अत्यंत जलद गतीने वाढ झाली आहे.

लहान मुलांना या संकटांपासून फार धोका आहे. कारण इंटरनेटचा वापर करताना त्याबरोबर येणाऱ्या संकटांची आणि त्यापासून बचाव करावयाच्या उपायांची त्यांना खूप कमी माहिती असते. मुले अजून प्रायोगिक वयाच्या वर्गात आहेत ते प्रयोग करू इच्छितात. नवीन गोष्टी शिकू इच्छितात व नवनविन गोष्टींचा प्रयोग करू इच्छितात. वास्तविक प्रयोग करत शिकणे हा चांगला मार्ग आहे. परंतु मुलांना योग्य मार्गदर्शन केले जाणे अत्यंत आवश्यक आहे. म्हणजे ते स्वतःला सायबर तंत्रज्ञानाच्या वाईट प्रभावापासून सुरक्षित ठेवू शकतील.

ही पुस्तिका अल्पवयीन मुले व मोठ्या मुलांसाठीही आहे. याचा उपयोग तरुण विद्यार्थी जे सायबर वर्ल्डला चांगल्या प्रकारे जाणतात व स्वतःला भावी पिढीचे पार्सक व सजग सायबर नागरिक समजतात यांचेसाठी आहे. पुस्तिकेच्या पहिल्या व दुसऱ्या प्रकरणात मुलांना ही माहिती देण्यात आली आहे की, 'सायबर सुरक्षा' हा चिंतेचा

विषय का आहे? असे अनेक प्रकारचे सायबर गुन्हे कोणते आहेत? जे आम्हाला जाळ्यात अडकवू शकतात. पुस्तिकेच्या तिसऱ्या प्रकरणात 'सायबर बुर्लींग' व तेरा वर्षावरील मुले कसे प्रभावित होतात यासंबंधी माहिती दिली आहे. या प्रकरणात त्या सर्व महत्त्वाच्या सुरक्षेच्या उपायांबद्दल विस्ताराने माहिती देण्यात आली आहे. यामुळे मुले स्वतःला सायबर बुर्लींग पासून सुरक्षित ठेवण्यासाठी योग्य ती सावधगिरी बाळगू शकतात. सायबर बुर्लींग कशा प्रकारे केली जाते, याबाबत सांगण्यात आले आहे.

पुस्तिकेचे चौथे प्रकरण 'सायबर ग्रुमिंग' व त्याचा मुलांवर पडणारा प्रभाव याची माहिती देणारे आहे. या प्रकरणामध्ये त्या निरनिराळ्या प्रकारच्या सुरक्षेच्या उपायांची सखोल-विस्तृत माहिती देण्यात आली आहे; ज्याला अभ्यासून, जाणून मुले सायबर ग्रुमिंगपासून आपला बचाव करू शकतात.

पुस्तिकेचे पाचवे प्रकरण 'ऑनलाईन गेर्मींग' व याबाबत सुरक्षेची माहिती देणारे आहे ज्यामुळे मुले स्वतःला अशा सायबर संकटापासून वाचवू शकतात. सायबर गन्हेगारांद्वारे सामान्यतः ई-मेलचा उपयोग केला जातो.

सहाव्या प्रकरणामध्ये सायबर गुन्हेगार ई-मेलचा वापर करून कसा गुन्हा करतात. तसेच मुलांनी ई-मेलचा वापर सुरक्षितपणे कसा करावा यासंबंधी माहिती देण्यात आली आहे.

सायबर तंत्रज्ञानाने आमच्या देवाण-घेवाणाच्या पध्दतीला पार बदलून टाकले आहे. बरेच लोक खरेदी करणे, पैसे पाठविणे व इतर आर्थिक देवाण-घेवाणीसाठी इंटरनेटचा उपयोग करतात. याशिवाय मुलांना भविष्यात आर्थिक प्रशिक्षण मिळावे म्हणून शाळांमध्ये प्रयत्न केले जात आहेत. व्यवहार सरळ व उपयोगी व्हावेत म्हणून प्रयत्न करीत आहेत. आर्थिक फसवणुकीच्या सायबर गुन्हांना समोर ठेऊन सातवे प्रकरण आले आहे.

सातव्या प्रकरणामध्ये मुलांना ऑनलाईन आर्थिक देवाण-घेवाणीच्या संदर्भात धोके व अशा धोक्यांपासून स्वतःचा बचाव करण्यासाठी कशी दक्षता घ्यावी यासंबंधी माहिती देण्यात आली आहे.

पुस्तिकेचे शेवटचे प्रकरण म्हणजे आठवे प्रकरण सोशल नेटवर्किंगशी जोडलेल्या सायबर धोक्यांचा व अशा धोक्यांपासून बचाव करण्यासाठीची माहिती देण्यात आली आहे. ही पुस्तिका सायबर धोके व त्यापासून बचाव करण्यासाठी कोणते उपाय करावेत हे समजावण्यासाठी प्रयत्न केले गेले आहेत. जे मुलांसाठी उपयुक्त ठरणार आहेत. परिवर्तन घडवू शकणाराच्या रूपामध्ये विद्यार्थ्यांकडून ही अपेक्षा आहे की त्यांनी आपली माहिती आपल्या मित्रांना, आई-वडिलांना द्यावी व त्यांनाही या धोक्यांपासून बचाव करण्यास शिकवावे आणि सायबर स्पेसला आणखी सुरक्षित बनविण्यासाठी आपणे योगदान द्यावे.



वाढत्या सायबर गुन्हांची चिंता

आजच्या युगात इंटरनेट, कॉम्प्युटर, स्मार्टफोन व इतर अनेक संवाद माध्यमे व उपकरणे जीवनाचा अभिन्न भाग बनले आहेत. कल्पना करा की, आमचा प्रत्येक दिवसाचा किती भाग या स्मार्ट उपकरणांचा वापर करण्यामध्ये खर्च करतो. आम्ही गुगल, ई-मेल्स, व्हॉट्सॲप, ट्वीटर, फेसबुक इत्यादी माध्यमांना आपल्या दैनंदिन जीवनाचा एक अभिन्न भाग बनविला आहे. परंतु आमच्यापैकी अनेकांना सायबर सुरक्षा आणि स्वतःला सायबर गुन्हांपासून सुरक्षित आवश्यक असणाऱ्या उपाययोजनांची माहिती नाही ते पूर्णतः अनभिज्ञ आहेत.



काय आपण हे जाणता का ज्या काही सूचना वा व्यक्तिगत माहिती इंटरनेटवर टाकली जाते ती नेहमी करीता तेथेच राहते? कारण सूचना वा व्यक्तिगत माहिती 'डिलीट' करणे फार अवघड आहे.

सायबर गुन्हा म्हणजे काय?

सायबर गुन्हे असे गुन्हे असतात की जे संगणक, इंटरनेट वा मोबाईल तंत्रज्ञानाचा उपयोग करून माणसे, कंपन्या, संस्था, ग्रुप, समुह यांच्याद्वारे

केले जातात. सायबर गुन्हेगार सोशल नेटवर्किंग साईट्स, ईमेल, चॅटरूम, बनावट सॉफ्टवेअर, वेबसाईट अशा माध्यमांचा उपयोग करून सावजावर हल्ला करण्यासाठी या गोष्टींचा उपयोग करतात.



‘भारतीय कॉम्प्युटर आपातकालीन कारवाई दल’ (सीईआरटी-इन) प्रमाणे सन २०१७ या वर्षात भारतामध्ये ५३००० हून अधिक सायबर सुरक्षा गुन्हांच्या घटना घटल्याची माहिती मिळाली आहे.



काय आपण जाणता की सायबर हल्ले अधिक गुंतागुंतीचे व बळकट होत आहेत. यांचे लक्ष्य फोन नंबर, पत्ता, फोटोग्राफ, बँकासंबंधी माहिती इत्यादी. वैयक्तिक माहितीची चोरी करून सायबर गुन्हेगार आपले बनावट प्रोफाईल तयार करून आपल्याला संकटात टाकण्यासारख्या अनेक गोष्टींसाठी आपल्याविरुद्ध तिचा वापर करतात.



‘मित्रांनो, काळजी करू नका. सावध व दक्ष राहून स्वतःला सायबर गुन्हांपासून वाचवू शकता. मी आहे आपला सायबर मित्र आणि मी आपली वेगवेगळ्या प्रकारच्या सायबर गुन्हांना जाणण्यास व त्या दक्षतेना जाणून मदत करीन जे सायबर गुन्हांना बळी ठरण्याच्या धोक्याला कमी करण्यासाठी आपल्याला माहिती करून घ्यायला हवीच!’



सायबर संकट कोणावरही येऊ शकते

सायबर संकटाचे विविध प्रकार आहेत. इंटरनेट वा मोबाईल तंत्रज्ञानाच्या साहाय्याने तुम्हाला संकटात टाकू शकतात, तुमचे नुकसान करू शकतात.



काय आपण हे जाणता की हॅकर ही अशी व्यक्ती असते जी अनपेक्षित फायद्यासाठी संचार माध्यमांची उपयोग / दुरुपयोग करून अनेकांचे आर्थिक नुकसान करू शकते, ज्यांच्या प्रतिष्ठेला धक्का पोहचवू शकते. हॅकर्स तुमच्या कॉम्प्युटरचे नुकसान करणे व तुमच्या डाटा पर्यंत पोहचवणे यासाठी मालवेअर्स वायरस वा ट्रोजन्स चा उपयोग करू शकतात.

सायबर गुन्हेगारांकडून आपल्या संवेदनशील माहितीपर्यंत अनधिकृतपणे जाऊ पाहतात. बहुतांश घटनांमध्ये सायबर गुन्हेगार स्पष्टपणे त्यांच्या उद्देशासाठी आक्रमण करतात. यासाठी ते सर्वात जास्त प्रभावशाली पद्धतीचा उपयोग करतात. सायबर गुन्हेगारांकडून वापरण्यात येणारी काही सामान्य पद्धती खालीलप्रमाणे आहेत.



ई-मेल स्फुफिंग :- तुम्हाला असे ई-मेल पाठविले जातात जे तुम्हाला खरे वाटावेत. ज्यावर तुमचा विश्वास बसावा. असे ई-मेल आयडी ने पाठविला आहे असे वाटावे. परंतु हे खरे नसते. ही फसवणूक असते.

 **द्वेषपूर्ण फाईल अप्लिकेशन :-** तुमच्या स्मार्टफोन व व्यक्तीगत डाटा पर्यंत पोहचण्यासाठी मॅसेज पाठविणे, गेमिंग, ई-मेल आणि वेबसाईटच्या मार्फत तुम्हाला द्वेषपूर्ण व घाणेरडे एप्लिकेशन आणि फाईल पाठविणे.

 **सामाजिक संबंधांचे व्यवस्थापन :-** सामाजिक संबंधांचे व्यवस्थापन असे तंत्रज्ञान आहे ज्याचा उपयोग सायबर गुन्हेगार तुमची माहिती मिळविण्यासाठी, आपला विश्वास संपादन करण्यासाठी केला जातो. तुमची माहिती मिळविणे व तुमचे काही नुकसान करण्यासाठी सायबर गुन्हेगार आपल्याशी संपर्क साधण्याचा प्रयत्न करण्यासाठी या गोष्टींचा प्रयत्न करतात की तुम्हाला जास्तीत-जास्त काय आवडते. उदा. तुम्हाला ऑनलाईन गेम खेळणे फार आवडते तर हा ठग अन्य लहान मुलांसारखा वागेल व तुमच्याशी संवाद साधेल व तुमची माहिती तुमच्याकडून काढून घेईल.

 **सायबर बुलिंग :-** इलेक्ट्रॉनिक व संचार माध्यमे जसे संगणक, मोबाईल फोन, लॅपटॉप इत्यादींचा वापर करून कोणाला मनस्ताप देणे (त्रासदेणे) एक प्रकार आहे.

 **ओळख चोरणे :-** आर्थिक लाभासाठी कोणादुसऱ्या व्यक्तीच्या नावावर, बनावट अथवा आपल्या सहकाऱ्याच्या नावावर कर्ज घेणे वा दुसरा फायदा मिळविण्यासाठी एखाद्या व्यक्तीची ओळख चोरणे (वापरणे) वा नुकसान पोहचविणे.

 **नोकरीसंबंधी फसवणूक (जॉब फ्रॉड) :-** नोकरी करणारा वा नोकरीला लागणार आहे अशांच्या मदतीने आपल्या नियुक्तीसाठी फसवणूक वा कपटी नियोजन करणे.

 **बँकिंग फ्रॉड :-** स्वतः बँकेचा वा अन्य वित्तीय संस्थेचा प्रतिनिधी असल्याचे दाखवून दुसऱ्याच्या बँकेच्या खात्यावरून फसवून पैसे काढणे.



सायबर बुलिंग

सायबर बुलिंग हे सायबर संकटापैकी एक आहे. ज्यांचा सामना मुले व तरुणांना करावा लागत आहे. वास्तविक सायबर बुलिंगने कोणीही प्रभावित होऊ शकतो. याचे कारण सायबर संकटाची माहिती नसणे हेच आहे. यामुळे अल्पवयीन मुले सहज जाळ्यात अडकतात.

सायबर बुलिंग म्हणजे इंटरनेट अथवा मोबाईल तंत्रज्ञानाचा उपयोग करून घाणेरडे वा अश्लील वा त्रासदायक संदेश, प्रतिमा/व्हिडिओ पाठवून कोणाला जाणून-बुजून त्रास देणे, भीती दाखविणे, धमकी देणे आहे. सायबर बुलिंगने दुसऱ्यांना भीती दाखविण्यासाठी संदेश, ई-मेल, सोशल मीडिया प्लेटफॉर्म वेबपेज, चॅटरूम इत्यादींचा उपयोग केला जातो.



काय तुम्ही जाणता की सुरुवातीला आपल्याला ही जाणीव नसते की कोणी आपल्याला ऑनलाईन बुलिंग करीत आहे? सायबर बुलिंग कोणी ओळखूया, मित्र, नातेवाईक अशी अनोळखी व्यक्तीही असू शकतात. ज्याच्याशी आम्ही सोशल मीडिया प्लेटफॉर्म, वा चॅटरूम, गेमिंग पोर्टलवर ऑनलाईन भेटले असतील?

अल्पवयीन मुलांवर सायबर बुलिंगचे परिणाम अनेक प्रकारचे होऊ शकतात. ते शारीरिक, भावनात्मक आणि मानसिक स्वरूपात होऊ शकतात. यामुळे विद्यार्थ्यांच्या शैक्षणिक प्रगतीवर मोठा परिणाम होऊ शकतो. इतकेच नाही तर त्यांचे दैनंदिन जीवनही प्रभावित होऊ शकते.



काय आपण सायबर बुलिंगने काळजीत आहात? पण काळजी करू नका. दक्ष व सावध राहून तुम्ही न भीता निर्धास्तपणे इंटरनेट व मोबाईल तंत्रज्ञानाचा वापर करू शकता. तुम्हाला सावधपणे स्वतःला, मित्रांना सायबर बुलिंगपासून बचाव करण्यासाठी सुरक्षा उपायांचे पालन करण्याची गरज आहे.

आता आपण सायबर बुलिंगपासून आपला बचाव कसा करू शकू यावर चर्चा करूया!

-  सोशल मीडिया प्लॅटफॉर्मवरती अनोळखी व्यक्तींची फ्रेंड रिक्वेस्ट स्विकारू नका. सायबर बुकी आपल्या अकाउंटशी साधर्म्य साधण्यासाठी नकली अकाउंटही बनवू शकतो. अनुभवी व जाणकार मोठ्या हुशारीने त्याच लोकांना ऑनलाईन जोडतात ज्यांना ते ऑफलाईन जाणतात.
-  सोशल मीडिया वा अन्य ऑनलाईन प्लेटफॉर्मवर आपली गुप्त (खाजगी) माहिती जसे - जन्मतारीख, घरचा पत्ता, फोन नंबर कोणाला देऊ नये. तुमच्या ऑनलाईन पोस्टपर्यंत कोण पोहोचू शकतो हे जाणण्यासाठी सोशल मीडिया प्लॅटफॉर्मपर्यंत प्रायव्हसी सेटिंगमध्ये जा. तुमच्या प्रोफाइलपर्यंत फक्त आपले मित्रच पोहोचू शकतील अशी मर्यादा घालण्याचा प्रयत्न करा. (परंतु लक्षात ठेवा सर्व पोस्टसाठी प्रायव्हसीचा पर्याय सर्व सोशल मीडिया प्लॅटफॉर्म देऊ शकत नाही) उदा. कोणत्याही एका प्लॅटफॉर्मवर पिक्चर स्टोरीज बाय डिफॉल्टच पब्लिक होते.
-  लक्षात ठेवा की तुम्ही जे काही ऑनलाईन पोस्ट करता ते तेथेच राहते. म्हणून महत्त्वपूर्ण हे आहे की, सतर्क रहा आणि सोशल मीडिया प्लेटफॉर्मवर कमेंट्स किंवा पोस्टमध्ये आपला फोन नंबर आपल्या खाजगी माहितीत टाकू नका.
-  लक्षात ठेवा कोणत्याही अनोळख्या स्रोताकडून अनावश्यक सॉफ्टवेअर किंवा ॲप्ससारख्या डेटिंग आणि ऑनलाईन गेम, इत्यादींचा इन्स्टॉल करू नका. चॅटरूम मध्ये चॅटिंग करतेवेळी तुम्हाला विशेष करून सावध राहायला हवे. चॅट रूम मध्ये तुमच्या खासगी गोष्टी कधी शेअर करू नका आणि आपली ओळख मर्यादित करा.

👉 जर कोणी मित्र वा अनोळखी व्यक्तीची पोस्ट वाचून तुमचे मन दुखावले तर त्यावर तीव्र प्रतिक्रिया देऊ नका.

यामुळे बुली या प्रकारचे मेसेज पोस्ट करण्यासाठी प्रोत्साहित होईल. जर त्रासदायक पोस्ट/ मेसेज आपल्या मित्राचा असेल तर तुम्ही असे न करण्याविषयी त्याला विनंती करू शकता. जर तुम्हाला अशा प्रकारचे पोस्ट/ मेसेज वारंवार मिळत असतील तर तुम्हाला विनंती आहे की तुम्ही तात्काळ आपल्या आई-वडिलांना वा घरातील वडिलधाऱ्यांना याविषयी सांगा. म्हणजे ते तुम्हाला यासाठी मदत करतील.

👉 कृपया हे नेहमी लक्षात ठेवा की एक चांगला इंटरनेट वापरणारे असल्यामुळे तुम्ही घाणेरडे कॉमेंट्स, दुःखी करणारे मेसेज वा त्रास देणारे पिक्चर्स, व्हिडिओज ऑनलाईन पाठवू नयेत. कृपया सावध रहा आणि तपासून घ्या की तुमची पोस्ट/कॉमेंट, व्हिडिओ तुमचे मित्र वा अनोळखी व्यक्तीला त्रास देणारे नसावेत. जर असे करण्याची इच्छा झाली तरी कृपया पोस्ट करू नका. कारण तुम्हाला सायबर बुली बनावचे नाही आहे कारण असे करणे कायद्याने गुन्हा आहे. यासाठी तुम्हाला शिक्षा व दंड होऊ शकतो. या प्रकारामुळे (सायबर बुलिंगमुळे) पीडितावर प्रतिकूल प्रभाव पडू शकतो.

जर तुम्ही सायबर बुलिंगमुळे हैराण झाला आहात तर तुम्हाला हे करायला हवे.

जर तुम्ही सायबर बुलिंगने पीडित आहात तर ताबडतोब आपल्या पालकांना या स्थितीची स्पष्ट कल्पना द्या. म्हणजे ते योग्य ती कारवाई करतील. तुमची मदत करतील. खालील उपाययोजना तुम्हाला सहायक ठरतील.

👉 ताबडतोब आपल्या आई/वडिलांना, वडिलधाऱ्यांना सर्व काही स्पष्ट सांगा. जर तुम्हाला कोणी भीती दाखवत असेल, धमकी देत असेल तर ताबडतोब आपले आई-वडील, घरातील वडिलधाऱ्यांना सर्व काही खरेखरे सांगून टाका. हा विचार करू नका की आपले आई-वडील, वडिलधारे आपल्या ऑनलाईन कामावर प्रतिबंध लावतील, वा तुम्हाला कॉम्प्युटर/मोबाईलचा वापर करू देणार नाहीत. त्यांना तुम्हाला होणाऱ्या बुलिंगच्या त्रासाबद्दल ताबडतोब सांगा. यामुळे तुम्हाला त्यांचे सहकार्य मिळेल व तुम्हाला मदत होईल, मार्गदर्शन मिळेल.



👉 **बुलींग करणाऱ्याला ओळखणे** - बुलीला ओळखण्याचा प्रयत्न करा की कोणी ओळखीचा माणूस करतोय की अनोळखी माणसाचे काम आहे हे जाणणे फार गरजेचे आहे. हे जाणणे गरजेचे आहे की, कोणी असे बुलींग का करीत आहे? का त्रास देत आहे? हा बुली तुमचा मित्र वा परिचित व्यक्तीही असू शकतो. तुम्ही तुमच्या आई/वडिल, वडिलधाऱ्यांच्या मदतीने त्याला थांबवू शकता.

👉 **बुलींग करणाऱ्याला ब्लॉक करा** - जर तुम्हाला भीती दाखवत असेल वा धमक्या देत असेल यासाठी तो सोशल मीडिया प्लेटफॉर्मचा उपयोग करीत असेल तर तुम्ही त्याला ब्लॉक करू शकता. सर्व सोशल मीडिया ॲप वा सेवांमध्ये युजरकडे ब्लॉक करण्याचा पर्याय आहे.



👉 **पोस्ट मेसेजला सिलेक्ट आणि सेव्ह करा** - तुमच्या विरुद्ध केल्या गेलेल्या पोस्ट/ मेसेज सेव्ह करा. कायदेशीर कारवाई केल्यावर अशी पोस्ट/ मेसेज पुराव्यासाठी कामाला येतात.

👉 **बुलींग करणाऱ्याला कधीही आक्रमकपणे उत्तर देऊ नका** - बुलीची नेहमी हीच इच्छा असते की, तुम्ही आक्रमक व्हावे, चिडावे, तुमचा त्याचा वादविवाद व्हावा. यामुळे अनावश्यक माहिती दिल्याने फायदा होतो. यासाठी फायदेशीर हेच आहे की, नम्रपणे समोरच्या व्यक्तीला हे बंद करण्यास सांगावे आणि जर तो नाराज होत असेल तर त्याच्याबरोबर चॅट बंद करा वा त्याला ब्लॉक करा.

👉 जर तुमच्या आई/वडील, वडिलधाऱ्यांना आवश्यक वाटत असेल तर ते बुलीच्या विरोधात तक्रार करण्यासाठी पोलीस स्टेशनमध्ये जाऊ शकतात वा पोलिसांशी संपर्क साधू शकतात.



काय तुम्ही जाणता की कोणालाही ऑनलाईन धमकी देणे बेकायदेशीर व अनैतिक आहे. इतकेच नाही तर जर तुम्ही त्यांना आक्षेपार्ह संदेश पाठविता, घाणेरड्या नावांनी हाक मारता, ते कसे दिसतात यावर टीका-टिप्पणी करता तर तुम्ही संकटात सापडू शकता. असे काहीही करू नका. शांत राहा.



सायबर ग्रूमिंग

सायबर ग्रूमिंग एक वाढता सायबर गुन्हा आहे, ज्याचा सामना अल्पवयीन मुले करत आहेत. ही एक अशी प्रक्रिया आहे जेथे कोणीतरी लैंगिकशोषण करण्यासाठी मुलांचा विश्वास जिंकण्यासाठी सोशल मीडिया अथवा मेसेजिंग प्लॅटफॉर्मवरून मुलांबरोबर भावनिक संबंध जोडतो.

सायबर ग्रूमर नकली अकाऊंट बनवून मुलांसारखाच वागतो किंवा लहान मुलांसारखाच छंद दाखवून आवड दाखवून गेमिंग वेबसाईट, सोशल मीडिया, ई-मेल, चॅट-रूम इंस्टंट मेसेजिंग इत्यादींचा उपयोग करू शकतो.



काय तुम्ही जाणता की तुमच्यापैकी कितीतरी लोकांना हे माहीतच नसते की कोणी त्यांना ऑनलाईन ग्रूमिंग करीत आहे? ऑनलाईन ग्रूमर कोणी ओळखीची व्यक्ती, नातेवाईक अथवा अशी कोणी अपरिचित अनोळखी व्यक्तीही असू शकतो. ज्याच्याशी तुम्ही सोशल मीडिया प्लेटफॉर्म, चॅटरूम, गेमिंग पोर्टल इत्यादी सायबरवर ऑनलाईन भेटला असाल.

प्रारंभी सायबर ग्रूमिंग तुमची प्रशंसा करू शकते. बक्षीसे, मॉडर्न जॉब असे प्रस्ताव ठेवू शकतो. नंतर घाणेरडे मेसेज, फोटोग्राफ अथवा व्हिडिओ पाठविणे सुरू करू शकतो आणि तुमच्याकडून तुमचे अश्लील फोटो अथवा व्हिडिओ त्यांना पाठविण्यास सांगू शकतो. ऑनलाईन ग्रूमर जास्त करून किशोरवयीन मुलांना

लक्ष्य करतात. कारण की किशोरवयात त्यांच्यामध्ये अनेक शारीरिक, वैयक्तिक व सामाजिक बदल होतात. किशोरांचा उत्साह व जिज्ञासू प्रवृत्ती त्यांना ऑनलाईन कार्यक्रमांकडे आकर्षित करतात. प्रोत्साहित करतात. यामुळे ते ऑनलाईन बुकिंगला बळी पडतात.

ऑनलाईन ग्रुमिंग किशोरवयीन मुलांच्या शारीरिक, भावनात्मक व मानसिक दशेवर खोलवर प्रभाव पडतो. याचा परिणाम फक्त त्यांच्या शैक्षणिक कार्याला प्रभावित करीत नाही तर त्यांच्या दैनंदिन जीवनावरही प्रभाव पडतो. ऑनलाईन ब्रूमरचा हा हानिकारक प्रभाव पुष्कळ वेळा दीर्घकाळ राहू शकतो आणि पीडिताला



त्यांच्या तारुण्यामध्येही त्रासदायक ठरतो.

सायबर ग्रुमिंगने काळजीत आहात? तर काळजी करू नका. दक्ष आणि सावध राहून न भीता इंटरनेट आणि मोबाईल तंत्रज्ञानाचा वापर करू शकता. फक्त तुम्ही सावध राहून स्वतःला व आपल्या मित्रांना सायबर ग्रुमिंगपासून वाचविण्यासाठी सुरक्षा उपायांचे पालन करायला पाहिजे.

आपण आता ही चर्चा करू या की तुम्ही स्वतःला सायबर ग्रुमिंगच्या हल्ल्यापासून वाचविण्यासाठी काय करू शकता?

- 👉 सोशल मीडिया प्लेटफॉर्मवर अनोळखी व्यक्तींची फ्रेंड रिक्वेस्ट मान्य करू नका. सायबर ग्रूमर आपल्या सावज्याशी मैत्री करण्यासाठी नकली अकाऊंटही बनवू शकतात.
- 👉 सोशल मीडिया अथवा अन्य ऑनलाईन प्लॅटफॉर्मवर वैयक्तिक माहिती जसे जन्मतारीख, पत्ता, फोन नंबर, शाळेचे नाव देऊ नका. तुमची ऑनलाईन पोस्टपर्यंत कोण पोहचू शकतो यासाठी तुम्ही सोशल मीडिया प्लेटफॉर्मवर प्रायवेसी सेटिंगमध्ये जा आपला प्रोफाईलसुद्धा फक्त आपल्या मित्रांपर्यंतच सिमीत ठेवा. नाही तसाच प्रयत्न करा.
- 👉 सावध व्हा. जेव्हा जुजबी ओळख झालेली व्यक्ती अल्पावधीतच आपला चॅट पार्टनर तुमच्या सौंदर्याची, गुणांची स्तुती करू लागतो.
- 👉 अशा मित्रांशी संबंध ठेवू नका. जे शारीरिक आणि लैंगिक अनुभवांबद्दल तुम्हाला प्रश्न विचारतात. तुम्ही त्यांना असे प्रश्न न विचारण्याबद्दल स्पष्ट शब्दात सांगा की त्यांना असे प्रश्न विचारलेले आवडत नाहीत असे सांगितल्यावरही ते ऐकत नसतील परत तसेच घाणेरडे प्रश्न विचारत असतील तर हे प्रकरण आपल्या आई-वडिलांच्या, वडीलधाऱ्यांच्या कानावर घाला.

- 👉 अशा लोकांशी बोलू नका जे लोक तुम्हाला तुमचे अश्लील फोटोग्राफ आणि व्हिडिओ शेअर करायला सांगतात. जर तुम्ही असे अश्लील फोटोग्राफ आणि व्हिडिओ एखाद्याशी शेअर केले असतील तर ते अन्य कोणाशी शेअर करू शकतात. तो अन्य व्यक्ती दुसऱ्याशी शेअर करू शकते किंवा सोशल मीडियावर पोस्ट करू शकतो व तुम्हाला ब्लॅकमेलही करू शकतो.
- 👉 जेव्हा तुमचा चॅट पार्टनर वेबकॅमशी कनेक्ट नसेल तर तुमच्या वेबकॅमला कधीही ऑन करू नका.
- 👉 जर तुमचा चॅट पार्टनर त्याच्याशी केलेल्या संभाषणाला गुप्त ठेवण्यास सांगत असल्यास तुमच्या आई-वडीलांशी, वडिलधाऱ्यांशी याबाबत बोलून सर्व सांगा.
- 👉 ज्या व्यक्तीला तुम्ही ऑनलाईन भेटला आहात त्याला प्रत्यक्ष भेटायला एकटे जाऊ नका. नेहमी आपल्या मित्राला वा वडिलधाऱ्यांना बरोबर घेऊन जा.
- 👉 कधीही माहीत नसलेल्या स्रोतांकडून अनावश्यक सॉफ्टवेअर आणि ॲप्स जसे डेटिंग ॲप, ऑनलाईन गेम इत्यादी इस्टॉलमेंटने घेऊ नका. चॅट रूम मध्ये चॅटिंग करताना विशेष करून अत्यंत सतर्क राहावे. चॅट रूम मध्ये आपली व्यक्तिगत माहिती कधीही देऊ नका. आपली ओळख मर्यादित ठेवा.

जर तुम्ही सायबर ब्रूमिंगचे शिकार बनला आहात तर तुम्ही काय कराल ?

जर तुम्हाला असे वाटले की, तुम्ही सायबर ब्रूमिंगचे शिकार बनला आहात तर कृपा करून आपल्या वडिलधाऱ्यांना त्याविषयी स्पष्टपणे कल्पना द्या म्हणजे ते या प्रकरणात हस्तक्षेप करून तुमची मदत करू शकतील. खालील उपायांपासून तुम्हाला वाचविण्यासाठी मदत करतील.

- 👉 आई-वडील-वडीलधाऱ्यांना सर्व काही स्पष्टपणे सांगा.

जर कोणी ऑनलाईन तुम्हाला त्रास देत असेल तर तात्काळ आई-वडील, वडिलधाऱ्यांना याबाबतीत स्पष्टपणे सांगा, चर्चा करा, हा विचार करू नका की, तुमचे आई-वडील तुम्हाला ऑनलाईन वापरण्यास प्रतिबंध घालतील किंवा तुमचा कॉम्प्युटर/स्मार्टफोन

काढून घेतील. वापरू देणार नाहीत. त्यांना याबाबतीत स्पष्ट कल्पना देणे अत्यावश्यक आहे, महत्त्वाचे आहे. म्हणजे ते तुम्हाला या चक्रव्यूहामधून सोडविण्यासाठी मदत करू शकतील. मार्गदर्शन करतील.



-  **ग्रूमरला ब्लॉक करा** - जर ग्रूमर तुम्हाला ग्रूम करण्यासाठी सोशल मीडिया अथवा मेसेजिंग प्लेटफॉर्मचा वापर करीत असेल तर तुम्ही त्याला ब्लॉक करू शकता. सर्व सोशल मीडिया ॲप अथवा सेवांमध्ये यूजरला ब्लॉक करण्याचा विकल्प असतो.
-  **मेसेजला कलेक्ट आणि सेव्ह करा** - ग्रुमद्वारे तुमच्या बरोबर शेअर केले गेलेले मॅसेज, फोटो किंवा व्हिडिओला सेव्ह करा. असे मॅसेज, फोटो किंवा व्हिडिओचा उपयोग त्यांच्याविरुद्ध कायदेशीर कारवाई केल्यानंतर साक्षीच्या रूपात केला जाऊ शकतो.
-  **तुमचे आई/वडील/वडीलधारे ग्रूमरच्या विरोधात तक्रार करण्यासाठी स्थानिक पोलीस स्टेशनशी संपर्क साधू शकतात.**



काय आपण जाणता की इलेक्ट्रॉनिक रूपामध्ये अश्लील साहित्य किंवा बालशोषण साहित्य (सीएसएएम) ला तयार करणे, प्रदर्शन मांडणे आणि त्याचा प्रचार करणे भारताच्या माहिती अधिनियम २००० च्या अंतर्गत शिक्षापात्र अपराध आहे ?



ऑनलाईन गेमिंग

ऑनलाईन गेमिंगचा सायबर सुरक्षेशी कसा संबंध आहे ही एक आश्चर्याचीच गोष्ट आहे. याविषयी खुलासा असा की, जास्तीत जास्त लहान मुले व युवा वर्ग ऑनलाईन गेम खेळत आहेत. युजर्सही आवड दिवसेंदिवस वाढतच आहे. भविष्यात ही कित्येक पटीने वाढणारच आहे. जेथे कोठेही इंटरनेट युजर्सची संख्या अधिक आहे तेथे सायबर गुन्हेगार, त्यांची शिकार करण्यासाठी टपून बसले आहेत. ऑनलाईन गेम खेळणाऱ्यांना जाळ्यात ओढण्यासाठी नवेनवे मार्ग शोधित आहेत. ही फसवणूक, सायबर बुलिंगमध्ये सामील करणे इत्यादीच्या रूपात असू शकते.

गेमिंग एक वेगळे क्षेत्र आहे. ज्या माहिती तंत्रज्ञानाच्या सुरुवातीपासून रूपांतरीत केले गेले आहे. जास्तीत-जास्त लहान मुले ऑनलाईन गेमिंग कॅम्प्युनिटीमध्ये सहभागी होत आहेत. हे गेम खेळण्यास सोपे व वैविध्यपूर्ण असल्यामुळे याचा उपयोग ऑनलाईन गेम खेळण्यामध्ये केला जाऊ शकतो. यामुळे भारतात ऑनलाईन गेमिंग लोकप्रिय होत आहे. युजर्सची संख्या वाढत आहे. लहान मुले मोबाईल, कन्सोलो, कॅम्प्युटर, पोर्टेबल गेमिंग यंत्रे आणि स्पेशल नेटवर्कींगवर ऑनलाईन गेम खेळता येऊ शकतात. गेमिंग कन्सोल्स कॅम्प्युटरसारखे कार्य करतात. ज्यासाठी तुम्हाला अकाउंट बनवावा लागतो. लॉग-इन करून हॅण्डसेट लावून वेब कॅम वा अन्य यंत्राचा उपयोग करावा

लागतो. तुम्ही फक्त कोट्यवधी युजर्सबरोबर गेमच खेळत नाही तर त्यांच्याशी शेअर करता. दोस्त बनतात. ब्रुपमध्ये सामील होतात दगैरे दगैरे. एकाचवेळी कोट्यवधी प्लेअर्स ऑनलाईन गेम खेळतात. ऑनलाईन गेम्स मनोरंजक होऊ शकतात पण यांच्याबरोबर अनेक जोखमीही येतात.



काय तुम्हाला माहीत आहे का? ऑनलाईन गेम्सबरोबर स्पॅम, व्हायरस, कारण सॉफ्टवेअर्स डाऊनलोड होऊन जातील जे तुमच्या कॉम्प्युटर किंवा मोबाईल, फोन वा गेमिंग कन्सोलला प्रतिकूल रूपाने प्रभावित करू शकतात. प्रसिद्ध साइट्सकडूनच गेम डाऊनलोड करणे योग्य आहे. कधीही अवैध गेम्स आणि सॉफ्टवेअर डाऊनलोड / इस्टॉल करू नयेत.

हा चिंतेचा विषय आहे की, कॉम्प्युटर व स्मार्टफोनवर वेळ घालवणारी मुले बाह्य जगाशी आणि शारीरिक खेळांपासून दूर जात आहेत. त्यांच्यासाठी हेच फायदेशीर ठरेल की ऑनलाईन गेमशिवाय मैदानी खेळांकडेही मुलांचा ओढा असायला हवा. यासाठी पालकांनी प्रयत्न करायला हवेत. जे मुलांच्या समग्र शारीरिक आणि मानसिक विकासासाठी अत्यंत आवश्यक आहेत. उपलब्ध ऑनलाईन गेम्सची रेंज आणि सर्व जगातील प्लेअर्सबरोबर खेळण्यातील सोपेपणा लक्षात घेऊन असे म्हणणे योग्य होईल की ऑनलाईन गेमिंग दुसऱ्यांबरोबर जोडले जाण्यासाठी मनोरंजन करणारे ठरू शकते. परंतु वस्तुस्थिती अशी आहे की, तुमच्यासाठी असणारे धोके जाणून घेणे व त्यापासून बचाव कसा करता येईल याची माहिती असणे अत्यंत गरजेचे आहे. ऑनलाईन गेमिंगचा आस्वाद अवश्य घ्या. मौज करा, परंतु निश्चित करा की, तुम्ही सुरक्षितपणे खेळत आहात.

काय तुम्ही हे जाणता का?
ऑनलाईन गेमिंग बरोबर असणारे
धोके कोणकोणते आहेत?



👉 ऑनलाईन आक्रमकपणे खेळणाऱ्या खेळाडूंची संख्या अधिक आहे. जे तुम्हाला धमकावू शकतात, भीती दाखवू शकतात. काही खेळाडू तर दुसऱ्यांना भीती दाखविणे,

धमकाविणे वा हैराण करण्यासाठीच खेळतात. ते असभ्य भाषेत बोलू शकतात. दुसऱ्याला धोका देऊ शकतात. म्हणून तुम्हाला सावध राहणे अत्यावश्यक आहे.

👉 अनेक प्रौढ व सायबर गुन्हेगारही ऑनलाइन गेम्स खेळतात आणि समोरच्या खेळाडूसाठी लहान असल्याचा बहाणा करून तुम्हाला गेमसंबंधी टीप्स देतात व तुमच्याबरोबर पॉईंट्स शेअर करून तुमच्याशी मैत्री करण्याचा प्रयत्न करतात. त्यांचा हेतू तुमच्याशी मैत्री करून तुमचा विश्वास संपादन करण्याचा असतो. मैत्री व विश्वासाचा फायदा घेऊन ते तुमची व्यक्तीगत माहिती काढून घेतात किंवा तुम्हाला एकट्याला भेटून तुम्हाला गैरप्रकार करण्यासाठी उत्तेजन देऊ शकतात.

👉 अनेक ऑनलाईन गेमशी जोडले गेलेल्या वेबसाईट आहेत. याशिवाय एखादी मनोरंजक ऑनलाईन गेम डाऊनलोड करण्यासाठी तुम्हाला ई-मेल किंवा मॅसेजचा माध्यमातून लिंक्स पाठवू शकतो. कित्येक गेममध्ये एखादे खाते उघडण्यासाठी खेळणाऱ्याच्या बाबतीत अनेक प्रकारची व्यक्तीगत माहिती जसे - तुमचे नाव, वय, वैयक्तिक मोबाइल नंबर इत्यादी माहिती घावी लागते. ज्याचा नंतर दुरुपयोग होऊ शकतो. असुरक्षित साईटांशी डाऊनलोड वायरस आणि सॉफ्टवेअर इत्यादी ही डाऊनलोड होऊ शकतात. जो तुमचा कॉम्प्युटर, स्मार्टफोन अथवा अन्य गेमवाल्या यंत्रांवर वाईट प्रभाव टाकू शकतो.

👉 कित्येक ऑनलाईन गेममध्ये तुम्हाला पार्सट / नाणी इत्यादी विकत घेण्यासाठी सांगितले जाते. जे खेळामध्ये सुधारणा करण्यासाठी किंवा वेळवा साधनांच्याप्रमाणे तुमचा फायदा करून देण्यासाठी उपयोग केला जातो. तुमच्याशी पेमेंट करण्यासाठी क्रेडिट कार्डचे विवरण देण्यास सांगितले जाते. ते विकत घेण्यासाठी तुम्ही आपल्या आई व वडिलांची मदत मागता. वारतविक काही संक्रमित ऑनलाईन गेम्स तुमच्या क्रेडिट कार्डसंबंधीची सर्व माहिती गोळा करू शकतात व या माहितीचा दुरुपयोग करू शकतात. काय आपण ऑनलाईन गेमिंगच्या बाबतीत चिंतेत आहात? तर काळजी करू नका. माहिती व सावधगिरी बाळगून त्याच बरोबर तुम्ही सुरक्षितपणे ऑनलाईन गेम खेळू शकता, फक्त तुम्हाला सतर्क राहण्याची आणि स्वतःला आपल्या मित्रांना ऑनलाईन गेमिंगच्या धोक्यापासून वाचविण्यासाठी सुरक्षेच्या उपायांना आत्मसात करण्याची गरज आहे!