चला आला आपण ही चर्चा करुया की तुम्ही स्वत:ला कसे सुरक्षित ठेऊ शकता!

- ऑनलाइन गेम खेळतेवेळी दुसऱ्या खेळाडूंबरोबर आपली व्यक्तिगत माहिती जसे नाव, जन्मतारीख, पत्ता, दूरध्वनी क्रमांक शेअर करू नका. कारण तुम्हाला हे माहित नसते की ते खेळाडू कोण आहेत आणि त्यांच्या मनात कोणती योजना आहे आणि काय होऊ शकते, की तूम्ही आपली व्यक्तीगत माहिती ठग किंवा साइबर बुलिज बरोबर शेअर करून टाकाल.

- जेंव्हा तुम्ही ऑनलाईन गेम खेळत आहात तर आपल्या किंवा आपल्या आई-वडीलांच्या क्रेडिट कार्ड/ डेबिट कार्डची माहिती कोणाबरोबर शेअर तर करीत नाहित ना? काही सायबर गुन्हेगार गेम जिंकणे वा पाईंट्स शेअर करण्यासाठी मदत करुन मुलांबरोबर मैत्री करतात. ते आपल्या विश्वास संपादन करु शकतात. आणि यानंतर नाणी / पाईंटस इत्यादी विकत घेण्यासाठी तुमची मदत मागु शकतात. ते तुमच्या क्रेडिट अथवा डेबीट कार्डची माहिती मागु शकतात. म्हणुन तुम्हाला सावधानतेचा इशारा आहे की आपली ही माहिती कोणा बरोबरही शेअर करु नका.

- आपल्या कॉम्प्युटर, स्मार्टफोन व अन्य यंत्रावर नेहमी चांगला अँटिव्हायरस इंस्टॉल करा. अँटिव्हायरस आणि अन्य अॅप्लिकेशनला नियमितपणे अपडेट करीत राहा.

- तुम्ही आपला पासवर्ड कोणालाही सांगु नका. तुम्हाला आपल्या ऑनलाईन गेमिंग अकाऊंट आणि दुसरे अकाऊंटसाठी अवघड पासवर्ड ठेवायला हवा. तुम्ही नियमितपणे ठराविक अंतराने आपला पासवर्ड बदलत राहणे सुरक्षित उपाय आहे.

- ऑनलाईन गेम खेळतांना कधीही व्हाईस चॅट किंवा वेब कॅमचा उपयोग करु नका. याने तुमची ओळख दुसऱ्या खेळाडूंबरोबर शेअर होऊ शकते. ही गोष्ट सायबर बुलिंग आणि दुसऱ्या सायबर गुन्हेगारांना आकर्षित करु शकते.

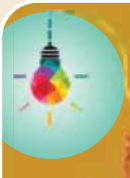
- तुमच्या ऑनलाईन गेमिंग वर्ल्डशी जोडल्या गेलेल्या कोणत्याही व्यक्तिशी कधीही प्रत्यक्ष भेटु नका. वास्तविक जीवनामध्ये तो खूप वेगळा असु शकतो. सायबर गुन्हेगार तुमचे मित्र बनु शकतात व तुम्हाला भेटण्यासाठी वा तुमची वैयक्तिक (व्यक्तिगत) माहिती काढून घेण्याचा प्रयत्न करु शकतात. त्यांचा हेतू वाईट असू शकतो.

- ऑनलाईन गेमिंग वर्ल्डमध्ये जर तुम्ही एखाद्या संकटांचा सामना करता अशावेळेस ताबडतोब आपल्या आई/वडील वा वडिलधाऱ्यांना सांगा म्हणजे ते तुमची मदत करु शकतील. ऑनलाइन गेम एका विशिष्ट मर्यादेतच खेळा. ऑनलाईन गेम खेळण्याऐवजी मैदानी खेळांची सवय लावा. मैदानी खेळांचा आनंद घ्या याद्वारे तुम्ही अत्तम व खरे मित्र बनु शकता.

तुम्हाला माहित आहे का? मैदानी खेळ खेळण्यामुळे स्नायूंना बळकट करणे, आत्मविश्वास प्राप्त करणे, नवे चांगली मित्र बनविणे, व सर्वांगीण व्यक्तिमत्वाचा विकास करण्यास मदत करतात.

ई-मेलद्वारे फसवणूक

बहुतेक लोकांकडे व्यक्तिगत ई-मेल अकाउंट असतात. तुम्हाला ई-मेल अकाउंटची गरज आपल्या मित्रांना, कुटुंबियांना फक्त ई-मेल पाठविण्यासाठी नसते. तर सोशल मिडीया अकाउंट, ऑनलाइन अकाउंट, गेमिंग अकाउंट उघडणे आणि इतर ऑनलाइन अकाउंट उघडण्यासाठी याची गरज असते. तुमचा ई-मेल अकाउंट तुमच्या जीवनाचा अभिन्न भाग बनला आहे. जसे जसे तुम्ही मोठे व्हाल तुमचा ई-मेल अकाउंटची उपयोगिता वाढेल. तुम्ही तुमच्या ई-मेल अकाउंट चा उपयोग बँक, मोबाईल सेवा देणाऱ्यासाठी जोडण्यासाठी आणि तुमच्या महाविद्यालय इत्यादीशी पत्रव्यवहार करण्यासाठी कराल. हे शिकणे फार गरजेचे आहे की, आपल्या ई-मेल अकाउंटला कसे सुरक्षित ठेवता येईल.



तुम्ही हे जाणता का? आपण सर्वांना नियमितपणे अनावश्यक मेल येत असतात? काय तुम्ही आपल्या ई-मेल अकाउंटमध्ये स्पैम ई-मेल बॉक्सवर लक्ष दिल आहे? सर्व ई-मेल सेवा देणारे स्पैम बॉक्सची सुविधा देतात. ज्यामध्ये अनावश्यक मेलला काढुन टाकता येते. ज्यामध्ये अनावश्यक सामान्य गोष्ट आहे आणि व्यक्तिगत फायदा अथवा कोणा व्यक्तिगत हानी पोहोचविण्यासाठी दुसऱ्या ई-मेल अकाउंटवरचा संकटात टाकण्यासाठी साईबर गुन्हेगारांद्वारे याला कमी खर्चात उपयोग केला जातो.

हे कसे कार्य करतात?

अशा अनेक प्रकारे साइबर गुन्हेगार ई-मेलचा उपयोग करून तुमच्या सिस्टमला नुकसान पोहचवू शकतात किंवा तुमची महत्वाची व्यक्तिगत माहिती गोळा करु शकतो. तुम्ही फिशींग, विसिंग इत्यादींच्या बाबतीत ऐकले असेल तुम्ही याबाबतीत ऑनलाईन माहिती घेऊ शकता परत आता आम्ही इथे सामान्यपणे हे समजा

☞ की तुम्ही एक लॉटेरी अथवा एक आकर्षक भेटवस्तू जिंकलेला आहे किंवा विदेशामध्ये राहण्यास तुमचा कोणी दूरचा नातेवाईक तुमच्यासाठी संपत्ती सोडुन गेला आहे. हा प्रस्ताव इतका आकर्षक असतो, की तुम्ही ई-मेल उघडता आणि या प्रस्वावाचे उत्तर देऊन टाकाता. साइबर गुन्हेगार जिंकलेली रक्कम पाठविण्यासाठी तुमच्याकडून तुमची माहिती मागतात. ते तुमच्या कडून प्रक्रियेसाठी काही रक्कम जमा करण्यास ही सांगू शकतात. म्हणजे तुम्ही जिंकलेली रक्कम तुमच्यापर्यंत पाठवू शकतील. परंतु तुम्हाला जे ई-मेल पाठवितात ते नकली असतात. त्यांना तुमचा पैसा घ्यायचा असतो. जो तुमच्या व्यक्तिगत माहितीच्या आधारे ते घेऊन टाकतात. तुमचे खाते नसेल. तरी ही तुम्हाला असे ई-मेल प्राप्त होऊ शकतात. तुम्ही ताबडतोब अशा ई-मेलची माहिती आपल्या आई-वडिलांना द्या. म्हणजे ते अशा फसवणुकीपासून तुम्हाला वाचवु शकतील.

☞ साइबर गुन्हेगारांकडुन केला जाणारा एक सामान्य गुन्हा आहे, म्हणजे ई-मेल अकाउंटला हैक करणे. तुमची ई-मेल आईडी आणि पासवर्ड मिळवण्यासाठी Malware किंवा अन्य उपायांनी चलाखीने वापरू शकतात. तुमचा ई-मेल अकाउंट हैक झाल्यामुळे ई-मेल गुन्हेगार याचा अपयोग सोशल मिडीया अकाउंट, बॅंक अकाउंट इत्यादीसारखी तुमची महत्वाची माहिती जाणुस घेऊ शकतात. ते तुमच्या सर्व Contacts ला आक्षेपार्ह ई-मेलही पाठवू शकतात.

☞ तुमचा ई-मेल हॅक करणे साइबर गुन्हेगारांकडुन केली जाणारी एक सामान्य चलाखी आहे. ज्याद्वारे ते तुमचे नावाने तुमच्या कुटुंबियांकडुन तुमच्या ई-मेल Address book मध्ये समाविष्ट तुमच्या मित्रांकडून आर्थिक मदत मागू

शकतात. काय तुम्हाला आपल्या कोण्या माहितीच्या व्यक्तीकडुन आर्थिक मदतीची मागणीची ई-मेल मिळाली आहे की आर्थिक संकटात आहे व त्याच्या जवळ टेलिफोन व बँक अकाउंटपर्यंत जाण्यासाठी वेळ नाही.काय तुम्ही ई-मेल वर होणाऱ्या फसवणुकीच्या बाबतीत चिंतेत आहात? तर काळजीचे कारण नाही फक्त सावधगिरी बाळगायला हवी. तुम्ही निर्धास्तपणे ई-मेल वापरु शकता. तुम्ही सावध राहुन काळजी घेऊन ई-मेलवर होणाऱ्या फसवणुकींबाबत स्वतःचा व आपल्या मित्रांचा बचाव करायला हवा. चला निश्चित करा की ई-मेलवर होण्याऱ्या फसवणुकीपासुन स्वतःसाठी बचाव कसा करायचा आहे. तुम्हाला जे अपाय सापडतील ते तुमच्या कुटुंब व मित्रांना अवश्य सांगा.

- पाहिले महत्वपूर्ण पाऊल आपली ई-मेल आईडी सुरक्षित करायचे. म्हणजे ती हॅक होणार नाही. यासाठी तुम्हाला एक अवघड व गुगलचा पासवर्ड बनवायला हवा. व वेळोवेळी हा पासवर्ड बदलत राहायला हवा. सायबर गुन्हेगारांसाठी सामान्य पासवर्ड जसे Password123, तुमचे नाव अथवा तुमची जन्म तारीख असा अंदाज बांधणे सोपे असते. कठीण (अवघड) पासवर्डचा उपयोग करा ज्यासाठी तुम्ही त्याच्यामध्ये अक्षरांचा व अंकाचा अपयोग करु शकता.
- Login साठी Two factor authentication चा उपयोग करु शकता . जास्त करुन ई-मेल सेवा देणाऱ्याकडुन या वैशिष्ट्याची व्यवस्था केली जाते. Two factor authentication च्या मदतीने पासवर्ड बरोबर तुमच्या मोबाईल फोनवर मिळणारा OTP च्या द्वारे तुम्ही आपल्या अकाउंट मध्ये Login करु शकता. सुरक्षीच्या दृष्टीने हा एक चांगला पर्याय आहे. आणि यामुळे आपल्या अकाउंटला सुरक्षित ठेऊ शकता.
- तुमच्या ई-मेलचा पासवर्ड कधीही कोणाला सांगू नका. पासवर्ड सांगितल्यामुळे तुमचा ई-मेलचे अकाउंट संकटात सापडु शकते. अनोळख्या व्यक्तिकडुन मिळालेली लिंक किंवा अटेंचमेंटला Click करु नका.

- जर तुम्ही तुमच्या ई-मेल अकाउंटला Acccess करण्यासाठी आपल्या मित्राचा कम्युटर अथवा एखाद्या साइबर कॅफे मध्ये एखाद्या कॉम्प्युटरचा उपयोग करीत असाल तर ही गोष्ट निश्चित लक्षात ठेवा की तुम्ही

remember password popup वर yes click करु नका. असे संदेश सामान्यतः अशा वेळी येतात जेंव्हा तुम्ही नव्या कॉम्प्युटरवर Login करतात तुम्हाला हे निश्चित ठरवायचे आहे की कोणताही कॉम्प्युटर तुमचा पासवर्ड आठवणीत ठेऊ शकणार नाही. (याचा अर्थ असा आहे की त्या कम्युटर तुमच्या अकाउंटला Login करण्यासाठी पासवर्डची आवश्यकता असणार नाही.) याचा उपयोग झाल्यानंतर तुमच्या ई-मेल अकाउंटला Sign-off करणे नेहमी लक्षात ठेवा. साइबर कॅफे मध्ये ठेवलेले कॉम्प्युटर सारख्या पब्लिक कॉम्प्युटरने access केलेले तुमचे पासवर्ड नेहमी बदलत राहा.

☞ जर तुम्ही आपल्या मोबाईलवर ई-मेल Acccess करत असाल, तर आपल्या फोनचा वापर करण्यासाठी एक अवघड पासवर्ड ठेवा.

☞ तुमचा ई-मेल हॅक/ Compromised झाल्यावर आपल्या Contacts ला याबाबतीत ई-मेल अथवा संदेशाच्याद्वारे माहिती द्या आणि त्यांना सावध करा की त्यांनी आपल्या ई-मेल आईडीने लिंक / अॅटेचमेंट उघडु नयेत. Help page च्या द्वारे आपल्या ई-मेल सेवा देणाऱ्यांसाठी ताबडतोब संपर्क साधावा व त्यांना सांगा की त्यांनी तुमच्या ई-मेलला तात्पुरते Block करावे. आपल्या पासवर्डला परत मिळविण्यासाठी प्रयत्न करा आणि आपल्या पासवर्डला ताबडतोब बदलून टाका.

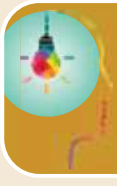
☞ माहित नसलेल्या स्त्रोतांकडून नको असलेले सॉफ्टवेअर आणि अॅप्स इन्स्टॉल करु नका. अज्ञात व्यक्ती कडून मिळालेले ई-मेल व संदेशवर मिळालेली लिंक व फाईलवर कधीही क्लिक करु नका. हे तुमच्या कॉम्प्युटर / फोनला मालवेअरने Infect करण्याचा प्रयत्न होऊ शकतो.

☞ जर तुम्हाला कोणी लॉटरी जिंकण्याचा वा अन्य अनेक प्रलोभनाचा बाबतीत ई-मेल प्राप्त होतो तर कृपा करुन त्याचे उत्तर देऊ नका. अथवा तुमचे नाव, पत्ता, बँक अकाउंटची माहिती इत्यादी सारखी व्यक्तिगत माहिती अजिबात देऊ नका. जर तुम्हाला एखादा अपडेट अथवा कोण्या अन्य खऱ्या कारणाच्या बाबतीत आपल्या सेवा देणाऱ्याकडून ई-मेल येतो जर ई-मेल पाठविणाऱ्यासाठी आईडी काळजीपुर्वक तपासून घ्या. हे

पण तपासुन घ्या की काही स्पेलिंगची चूक तर नाही ना. अशा ई-मेल मध्ये प्राप्त लिंक्सवर क्लिक करु नका. हे जाणण्यासाठी की आलेला ई-मेल खरा आहे की नाही हे पडताळून पाहण्यासाठी आपल्याला सेवा देणाऱ्यांसाठी संपर्क साधण्याचा प्रयत्न करा.

☞ जर तुम्हाला तुमच्या मित्र अथवा नातेवाईकांशी आर्थिक मदतीसाठी इमरजेंशी ई-मेल प्राप्त होतो तर त्या व्यक्तीशी फोनवर वा अन्य ओळखीच्या व्यक्तीशी संपर्क करुन ई-मेलच्या खरेपणाची माहिती मिळवा. कारण अशी संभावना असू शकते की आर्थिक मदत मागणाऱ्याचा अकाउंट हॅक झाला असेल आणि या प्रकारचा ई-मेल पाठविण्याचा प्रयोग केला जात असेल.

☞ सावध राहा आणि वेळोवेळी आपल्या पासवर्ड बदलण्याची सवय लावून घ्या. अनोळखी स्त्रोतांकडून प्राप्त होणारे ई-मेल्स वर लक्ष देऊ नका आणि ई-मेलवर आपली व्यक्तिगत बाबींबद्दल कोणालाही माहिती देऊ नका. व अनोळखी स्त्रोतांकडुन प्राप्त झालेल्या लिंक/ documents वर क्लिक करु नका.



काय आपण हे जाणता का संचाराची साधने व अन्य उपकरणांचा उपयोग करुन लोकांना फसविणे हा एक शिक्षापात्र गुन्हा आहे.

देवाण-घेवाणीत ऑनलाईन फसवणूक

वास्तविक पाहता हे शक्य आहे की जास्तीत जास्त लोक सध्या डेबिट कार्ड, क्रेडिट कार्ड, नेटबँकिंग इत्यादीसारख्या बँकिंग सेवेचा उपयोग करीत नाहीत. परंतु काळानुसार ते या सेवेचा उपयोग करू लागतील. याशिवाय एक जागरूक नागरिकाच्या रूपात तुम्हाला ही गोष्ट माहित असायला हवी की ऑनलाईन देवाण-घेवाणीच्या बाबतीत फसवणूक कशाप्रकारे होत असते, म्हणजे तुम्ही ही माहिती आपल्या मित्रांना, कुटुंबाला देऊ शकाल.

ऑनलाईन देवाण-घेवाणीमध्ये फसवणूक म्हणजे कोणा सायबर गुन्हेगाराकडून तुमच्या बँक अकाउंटमधून बेकायदेशिरपणे पैसे काढणे अथवा त्याला दुसऱ्या बँक अकाउंटमध्ये जमा करणे, ऑनलाईन देण्या-घेण्याबाबत फसवणूक त्याचवेळी होऊ शकते जेव्हा तुमचे Login अथवा बँक अकाऊंटची माहिती अथवा क्रेडिट कार्डची माहिती कोणासायबर गुन्हेगाराकडून चोरला जाणे.

हे कसे होते?

सायबर गुन्हेगारांकडून लोकांची ऑनलाईन फसवणूक करण्यासाठी अनेक प्रकार केले जातात. सायबर गुन्हेगार एखाद्या नकली (खोट्या) अकाउंटने तुम्हाला ई-मेल पाठवू शकतात. ज्याने असे जाणवते की तो बँक अथवा क्रेडिट सेवा देणाऱ्याकडून प्राप्त झाला आहे. जेव्हा तुम्ही ई-मेल दिल्या गेलेल्या लिंकवर क्लिक करता तर तो तुम्हाला अशा पेजवर

घेऊन जातो. ज्यामध्ये तुमच्या बँक अकाउंट, क्रेडिट कार्ड Card Varification Value (CVV), Expiry date इत्यादी सारखी संवेदनशील सूचना मागितलेली असते. ही माहिती दिल्यावर तुमच्या बँक खात्याला धोका निर्माण होऊ शकतो.

सायबर गुन्हेगार आपली खोटी ओळख दाखवून स्वतःला बँक कर्मचारी आहे असे सांगत तुम्हाला कॉल करू शकतो आणि तुमच्याकडून क्रेडिट कार्ड अथवा बँक अकाउंटची माहिती, नंबर, Personol Identification Number (Pin) CVV, expiry date, जन्मतारीख, विचारण्याचा प्रयत्न करू शकतात. अशा प्रकारची माहिती दिल्यावर तुमच्या बँक खात्याला धोका निर्माण होऊ शकतो.

काय आपण हे जाणता का डेबिट / क्रेडिट कार्ड पीन, युनिक नंबर आहेत ज्याची गरज एटीएम वर अथवा दुसऱ्या ऑनलाईन देवाण-घेवाणीसाठी तुमच्या कार्डाला Access करण्यासाठी असतात. तुम्ही आपल पीन नंबर सहजतेने बदलू शकता. वेळोवेळी आपला पीन नंबर बदलत राहणे चांगली सवय आहे.

साधारणतः तुमचा मोबाईल नंबर तुमचा बँक अकाउंटशी लिंक होतो. सायबर गुन्हेगार स्वतःला मोबाईल सेवा देणाऱ्या कंपनीचा कर्मचारी आहे, अशी बतावणी करून तुम्हाला कॉलही करू शकतात आणि तुम्हाला हे सांगू शकतात की जर तुम्ही तुमचा Subscriber Identification Module म्हणजे सिमला अपडेट करीत नाहीत करण्यासाठी हे गुन्हेगार तुम्हाला लिंक पाठवतील अथवा तुम्हाला सांगतील की तुम्ही तुमच्या मोबाईलनंबरवरून सेवा देणाऱ्याला SMS पाठवा. वास्तवात ते तुमच्याकडून मोबाईल सेवा देणाऱ्याला एसएमएस यासाठी पाठविण्याचा प्रयत्न

करीत आहेत की तुमचा सध्या चालू असलेला सिम ब्लॉक होऊन जावा आणि तुमचा डुप्लिकेट सीम सुरू व्हावा. सायबर गुन्हेगार सेवा देणाऱ्याकडून डुप्लिकेट सिम मिळवून तुमचा मोबाईल नंबर आणि बँकिंग ॲपला वापरून ऑनलाईन देवाण-घेवाणासाठी याचा वापर करू शकतात.

काय आपण हे जाणता का बँक, बँकिंग फसवणुकीची नुकसान भरपाई तेंव्हाच करतात. जेंव्हा बेपर्वाई अथवा सुरक्षेत कमतरता बँकेकडून झाली असेल.

सन २०१७ मध्ये क्रेडिट/डेबिट कार्ड आली इंटरनेट बँकिंग फसवणुकीचे संबंधी एकुण १७८५ केस फाईल करण्यात आले. यामुळे एकुण ७१.४८ कोटी रूपयांचे नुकसान झाले.

काय तुम्ही ऑनलाइन देवाण- घेवाणाची फसवणुकी संबंधी काळजीत आहात तर तुम्ही काळजी करु नका. माहिती आणि सावधगिरी बाळगून तुम्ही स्वतःला ऑनलाइन फसवणुकींपासुन वाचवू शकता. कृपा करुन लक्षात ठेवा की जर तुम्ही तुमच्या बँक व कार्डची माहिती जसे कार्ड नंबर PIN, CVV वैधता समाप्तीची तारीख, बँक खात्याला पासवर्ड इत्यादी कोणती ही माहिती कोणालाही सांगु नका. यामुळे तुम्ही ऑनलाइन देवाण- घेवाणीच्या फसवणुकीपासुन स्वतःला वाचवू शकता तुम्ही स्वतः सावध राह आणि आपल्या मित्रांना अशा फसवणुकीसंबंधी वाचाविण्यासाठी जे सुरक्षा उपाय असतात ते अंमलात आणण्यास सांगा. चला आपण या गोष्टीवर चर्चा करू या की कसे आपण स्वतःला ऑनलाइन देवाण-घेवाणसंबधी फ सवणुकाचे बळी ठरण्यासापासून वाचू शकतो. या सुरक्षेततेच्या उपायांना आपल्या मित्रांना व कुंटुंबियांना अवगत करण्यास विसरु नका.

- आपल्या बँक व कार्डची माहिती विसरू जसे ऑनलाइन ॲकाउंट, पासवर्ड, कार्ड नंबर, CVV, समाप्तीची तारीख, PIN, OTP इत्यादी संबंधी कोणालाही काही सांगू नका. ही माहिती दुसऱ्यांना सांगितल्यामुळे तुमच्या बँक खात्याला धोका होऊ शकतो. ज्यामुळे अवैध ऑनलाइन देवाण-घेवाण होऊ शकते.
- जेंव्हा तुमच्या बँक खात्याच्या ऑनलाईन पासवर्ड व तुमच्या डेबिट /क्रेडिट कार्डच्या PIN ला नियमित अपडेट करण्याची सवय लावा.

☞ जेंव्हाची तुमच्या बँक खात्यामध्ये लॉग इन कराल तर बॅक ची वेबसाईट स्वतः टाईप करण्याची सवय लावा. ई-मेल मॅसेज अथवा पॉप-अॅपवर येणारे बँक वेब साईटवरच्या लिंकवर कधीही लिंक करू नका. ही खोटी लिंक असु शकते. आणि तुम्हाला खोट्या साईटवर घेऊन जाऊ शकतात. तुम्ही जेंव्हा खोट्या साईटने आपल्या बँक खात्यावर लॉगइन कराल तेव्हा तुमची गुप्त माहिती जसे खाते क्रमांक व पासवर्डची चोरी होऊ शकते.

☞ हे निश्चित करण्यसाठी की तुम्ही सुरक्षित बँक वेबसाइट वर पोहोचला आहात, बँकेच्या सुरक्षा प्रमाणपत्राची माहिती व विभिन्न साईन-ईन क्रमांक जसे ग्रीन अॅड्रेस लाइन, अॅक्सेसबार वर लॉनइन व HTTPS ची तपासणी करा.

☞ नेहमी लक्षात ठेवा की वेबसाईट URL / HTTPS ने सुरु होत आहे. HTTPS वाले वेबसाईट URL तुमच्या डेटाला वेबसाईटवर Enscript करून पाठवतो व त्याला कोणतेही नुकसान होऊन बदल सुरक्षित ठेवतो. जी वेबसाईट HTTPS ने सुरू होत नाही. तिच्यावर आपली गुप्त माहिती जसे की ऑनलाइन अॅकाउंट, पासवर्ड, कार्ड नंबर CVV वैधता समाप्तीची तारीख PIN, OTP इत्यादी बद्दल सांगू नका.

☞ आपल्या मोबाईल फोनलाही सुरक्षित ठेवणे आवश्यक आहे. कारण की तुमचा मोबाईल नंबर तुमच्या बँक खात्याशी जोडलेला असतो. तुमच्या मोबाईल फोनला उघडण्यासाठी नेहमी एक अवघड, गुंतागुंतीचा पासवर्डचा वापर करा व एक चांगला अँटिव्हायरस सॉफ्टवेअर इन्स्टॉल करा. जर तुम्हाला तुमच्या मोबाईल सर्विस देण्याऱ्या कंपनीकडून कॉल आला असेल की जर

तुम्ही तुमचा नंबर अपडेट करणार नसाल किंवा रिचार्ज करणार नसाल तर तुमचा नंबर निष्क्रिय करण्यात येईल किंवा अशा आशयाचा दुसरा एखादा संदेश येतो तर, सावध व्हा. आपल्या फोनवरून आपल्या मोबाईल सेवा देणाऱ्या कंपनीच्या ग्राहक सेवा केंद्राला कॉल करुन विचारा की तुम्हाला आलेला त्यांचा कॉल खरा आहे की खोटा आहे.

☞ तुमच्या मोबाईल अथवा कॉम्प्युटर मध्ये कधीही चोरीचा सॉफ्टवेअर इन्स्टॉल करू नका. हे फ क्त बेकायदेशीर नाही तर हे तुमच्या उपकरणाच्या सुरक्षेलाही नुकसान पोहचवू शकते, नेहमी तुमच्या कम्युटर व मोबाईल फोनमध्ये उत्तम दर्जाचा ॲन्टीवायरस इन्स्टॉल करा. हे आवश्यक आहे की तुम्ही आपल्या सॉफ्टवेअर व ॲन्टीवायरस ला Up to date ठेवा.

☞ कधीही कोणा सार्वजनिक वाय-फाय व सायबर कॅफेचा कॉम्प्युटरचा उपयोग ऑनलाईन देवाण-घेवाणीसाठी करू नका. कारण की सायबर कॅफेच्या कॉम्प्युटरमध्ये अपडेट ॲन्टीवायरस नसेल वा मेलवेयरने प्रभावित झाला असेल जे तुमच्या बँक विवरण आणि अन्य महत्वाची माहिती मिळवू शकतो. जसे ; कार्ड नंबर, कार्ड समाप्तीची तारीख, सी.वी.वी. इत्यादी

☞ तुमचे बँक खाते आणि क्रेडिट कार्डांच्या मासिक विवरणाला नियमितपणे तपासण्यासाठी सवय लावा. हे तपासा की अनधिकृत घेवाण-देवाण झाली का.

☞ जर तुम्हाला हे माहित झाले की तुमचे बँक खाते व कार्डच्या माहितीला कोणी काढुन घेतले आहे, चोरले आहे वा तुमचे डेबिट/ क्रेडिट कार्ड हरवले आहे. तर ताबडतोब बँकेला फोन करा व आपले कार्ड/ खाते तातडीने ब्लॉक करुन टाका. जर तुमच्या खात्यावरुन एखादी अनधिकृत देवाण-घेवाण झाली असेल तर आपल्या जवळच्या पोलीस स्टेशनमध्ये औपचारिक तक्रार नोंदवा.

तुमच्या सोशल नेटवर्किंग प्रोफाईलच्या सुरक्षेचे उपाय

आजकाल आम्ही सर्व फेसबुक, ट्विटर, इँस्टाग्राम, स्नॅपचॅट इत्यादी सारख्या सोशल नेटवर्किंग साईटचा जास्तीत-जास्त वापर करीत आहेत. आम्ही आमच्या मित्रांशी वा नातेवाईकांशी आपला अपडेट वा सेल्फी व फोटो शेअर करणे पसंत करतो. आमची ही पण इच्छा असते की आमची पोस्ट/फोटो आणि अपडेटवर लाइक्स आणि कमेंट ही मिळावेत वास्तविक सोशल नेटवर्किंग साईटस्शी सहजगत्या जोडले जाण्यासाठी मदत मिळाली. पण जर आम्ही सावध राहिलो नाही तर गंभीर सायबर धोकेही होऊ शकतात . जे आमचे नुकसान ही करु शकतात.

हे सायबर गुन्हेगार कसे काम करतात ?

सायबर क्रिमिनल आणि साईबर बुलींग आमचे नुकसान करण्यासाठी सोशल नेटवर्किंग प्लॅटफार्मचा उपयोग करतात. या आपण हे जाणुन घेऊ की सोशल नेटवर्किंग साईटस्शी जोडले गेलेले असे कोणते सर्वसाधारण सायबर धोके आहेत. जे आम्हाला नुकसान पोहचवू

☞ सायबर क्रिमिनल तुमच्या प्रतिक्रियेला नुकसान पोहचविण्यासाठी वा अन्य अवैध प्रयोजनासाठी सोशल मिडीयावर तुमचा बनावट अॅकाउंट बनवुन निगेटिव्ह गोष्टी आणि अनुचित माहिती शेअर करु शकतात. हा एक गंभीर धोका आहे जो कोणतेही नुकसान करू शकतो. कोणत्याही ई-मेल आईडीचा उपयोग करुन सोशल मिडीया अॅकाउंट बनविला जाणे सहज शक्य आहे. आजकाल आमचे फोटो, ई-मेल आईडी, जन्मतारीख आणि इतर माहिती ऑनलाइनवर सहज मिळु शकते. साइबर गुन्हेगार तुमचा बनावट अॅकाउंट उघडण्यासाठी या माहितीचा उपयोग करु शकतात.

- सोशल मिडिया प्लॅटफार्मांवर आज-काल सायबर बुलिंग फार होऊ लागले आहेत. गुन्हेगार असभ्य व अश्लील संदेश पाठविण्यसाठी सोशल मिडियाचा उपयोग करतात.
- सोशल नेटवर्किंग साईटवर शेअर केल्या गेलेल्या लिंकच्या मार्फत ऑनलाइन फसवणुक केली जाऊ शकते. जर साइबर अपराधी मॅसेजेस लिंक वा मालवेअर ने युक्त एखादी पोस्ट शेअर करु शकतात. जर तुम्ही त्या लिंकवर क्लिक केले तर तुमचा कॅम्युटर वा मोबाईल इफेक्टेड होऊ शकतो अथवा धोकादायक बनू शकतो.

सोशल नेटवर्किंग प्लॅटफार्मवरील धोक्यांमुळे तुम्ही काळजीत आहात का? घाबरु नका.

सावध राहून आणि काळजी घेऊन तुम्ही स्वतःला या धोक्यांपासुन सुरक्षित होऊ शकता आणि सहजपणे सोशल नेटवर्किंग साईटस् उपयोग करू शकता. अशा फसवणुकीपासुन वाचविण्यासाठी तुम्हाला सावध राहावे लागेल आणि काही सुरक्षेचे उपाय करावे लागतील. या आपण चर्चा करु या की तुम्ही स्वतःला आणि आपल्या सोशल मिडीया अकाउंटस्ना कसे ठेऊ शकता यावरील उपायोजनांना (मार्गदर्शनाचा) आपल्या कुंटुबियांना व मित्रांना सांगा.

- आपल्या सोशल नेटवर्किंग अॅकाउंटला सुरक्षित ठेवण्यासाठी गरज पाहिजे आहे. ते अकाउंट हैक होता कामा नये आणि धोक्यात येऊ नये. यासाठी तुम्हाला एक अवघड पासवर्ड ठेवायला हवा आणि वेळोवेळी याला बदलत रहा.

काय आपण जाणता की बहुतांश सोशल मिडीया साईट आणि ई-मेल सर्व्हिस प्रोवाइडर तुम्हाला तुमच्या खात्यांना लॉग इन करण्यासाठी ते सांगतात की तुम्ही सेटिग्सवर जा आणि टु फॅक्टर अॅप्लिकेशनशला एक्टिवेट करा. याला लॉग-इन करण्यासाठी आपल्या पासवर्ड आणि तुमच्या मोबाईलवर प्राप्त झालेल्या वनटाईम पासवर्ड (ओ टि पी) टाईप करावा लागेल. हा एक चांगला सुरक्षित मार्ग आहे. याचा उपयोग तुमची सर्व अॅकाउंट उघडण्यासाठी केला जाऊ शकतो.

- तुमच्या सोशल मिडिया अकाऊंटचा पासवर्ड कोणालाही सांगू नका. पासवर्ड सांगितल्यामुळे तुमच्या अॅकाउंटचा दुरपयोग होऊ शकतो.
- तुम्ही जे काहीही सोशल नेटवर्किंग साइट्स वर पोस्ट करता ते प्रत्येकाला दिसेल जोपर्यंत तुम्ही तुमच्या पोस्ट एक्सेसला आपल्या मित्रांना/ फॉलोअर्स पर्यंत सिमित करणार नाहित. तूम्हा तूमच्या सोशल मिडीया अॅकाउंटच्या प्रायव्हेसी सेंटिग्स बदलायला हवी आणि हे निश्चित करा की तुमचे अपडेट्स /पोस्ट फक्त तुमचे मित्र /फॉलोअर्सच पाहू शकतील.
- अनोळखी लोकांच्या फ्रेंड रिक्वेस्ट स्विकारू नका. कोणतेही फ्रेंड रिक्वेस्ट एक्सेप्ट करण्यापुर्वी हे जाणुन घ्या की रिक्वेस्टला आणखी किती लोक फॉलो करीत आहेत.

किंवा त्याच्या फ्रेंड लिस्टमध्ये किती लोक आहेत. गुन्हेगार तुम्हाला ओळखणाऱ्या व्यक्तीचा बनावट अकाऊंट बनवू शकतात. म्हणून सावध राहा.

- तुम्ही सोशल मिडियावर जी पोस्ट करता ती सामान्यतः तिथेच राहते. म्हणून सोशल मिडियावर काहीही पोस्ट करण्याआधी सावधगिरी बाळगा. लक्षात ठेवा की ही माहिती कोणाबरोबरही शेअर होऊ शकते. आपले खाजगी विवरणाला (माहिती) जसे की, पत्ता, फोन नंबर, जन्म तारीख इत्यादी सोशल मिडिया साईटवर शेअरकरू नका.
- जर तुम्ही सोशल मिडीया अॅकाउंटला Access करण्यासाठी आपल्या मित्राचा कम्प्युटर किंवा साइबर कॅफेमधील एखादा कॉम्प्युटर वापरणार आहात तर ही गोष्ट अवश्य लक्षात ठेवा की तुम्ही Remeber Password pop-up वर एस क्लीक करु नका. हे संदेश सामान्यतः त्यावेळी येतात जेंव्हा तूम्ही एखाद्या नव्या कॉम्प्युटर वर लॉगइन करता तेंव्हा तुम्हाला हे लक्षात ठेवायला हवे की कोणताही कॉम्प्युटर तुमचा पासवर्ड लक्षात ठेऊ शकणार नाही. (याचा अर्थ असा आहे की त्या कॉम्प्युटर वर आपला अकाऊंटला लॉगइन करण्यासाठी पासवर्डची आवश्यकता असणार नाही.) नेहमी लक्षात ठेवा की याचा उपयोग केल्यावर आपल्या अॅकाऊंटमधून साईन–ऑफ करुन टाका.
- जर तुम्ही आपल्या मोबाईल फोनवरुन सोशल मिडीया अकाऊंट एक्सेस करीत आहात जर आपल्या फोनला एक्सेस करण्यासाठी एक अवघड पासवर्ड बनवा.

तुमचा सोशल मिडीया अॅकाऊंट हॅक झाल्यावर/ संकटात पडल्यावर आापल्या कॉन्टॅक्टस्ना अर्जंट ई-मेल वा मेसेज पाठवुन द्या. आपल्या सोशल मीडिया सर्व्हिस प्रदात्याला (प्रोव्हाइडरला) ताबडतोब कळवा. की तात्पुरता तुमचा अॅकान्ट बंद करायला सांगा. आपल्या पासवर्डला रिट्रीव करण्यसाचा प्रयत्न करा. आणि आपल्या पासवर्ड ताबडतोब बदला.

- जर तुम्हाला माहित झाले की तुमचा नकली अकाऊंट बनविला गेला आहे, तुम्ही सोशल मिडिया प्रदात्याला (प्रोवायडरला) ताबडतोब कळवा. म्हणजे कोणी तुम्हाला bully करीत आहे. अश्लील कॅमेन्ट्स व इमेजेस (फोटो) पोस्ट करीत आहे किंवा तुमची प्रतिमा डागाळण्यासाठी तुमचा फेक अॅकाउंट बनवित आहे. तर तात्काळ आपल्या आई-वडिलांना / वडिलधा-यांना सांगा व त्यांच्या मदतीने, मार्गदर्शने तुम्हाला मानसिक धैर्य मिळेल नंतर त्यांनतर त्यांच्या मदतीने नजिकच्या पोलिस स्टेशनमध्ये जाऊन तक्रार (F.I.R.) दाखल करा.

- अनोळखी स्त्रोतांकडून नको असलेले सॉफ्टवेअर आणि अॅप्स इस्टॉल करु नका. अनोळखी व्यक्तिकडून सोशल मिडियावर मिळालेल्या लिंक वा फाईलवर कधीही क्लीक करु नका. हे तुमच्या कॅम्युटरला मेलवेअर इन्फेक्ट करण्याचा प्रयत्न असु शकतो.

- खोट्या बातम्या पसरवणारे अथवा फसविणारे /भ्रमित करणारे संदेश सोशल मिडियावर रोगासारखे पसरतात. यामुळे कायदाव व्यवस्थेच्या समस्या उत्पन्न होऊ शकतात. व काही प्रकरणात तर जिवीत हानीही होऊ शकते. सोशल कोणताही संदेश पुढे पाठविणे किंवा शेअर करण्यासाठी अन्य स्त्रोतांकडून त्याचा खरेपणाची खात्री करुन घ्या.

- कॉपीराइटेड विषय जसे कविता, निबंध, व्हिडिओ, संगीत, चित्र, संगीत, संगीताची रचना करणारे, सॉफ्टवेअर इत्यादींना लेखकाच्या परवानगी शिवाय कधीही डाऊनलोड अथवा अपलोड करु नका. दुसऱ्यांना कॉपीराइटेड वस्तु वा विषयांना डाऊनलोड व अपलोड करावी हा एक अपराध आहे. आपल्या पूर्ण खात्री आहे की तुम्हाला ही पुस्तक निश्चित आवडली असेल. आम्ही सुचविलेले उपाय तुम्हाला साईटवर अपराधांपासुन सुरक्षित राहण्यासाठी मदत करतील. तुम्ही हे जाणता की साइबर गुन्हेगार लोकांना धोकादेण्यसाठी नेकमी नवनविन उपाय शोधत असतात. म्हणुन आम्ही स्वतःला सुरक्षित ठेवण्यासाठी नवीन नवीन संकटापासून फसवणुकीपासून बचाव करण्यासाठी नवीन प्रकारची अद्ययावत महिती असणे फार गरजेचे आहे.

सायबर मित्राचे काही सल्ले

- नवीन सायबर संकटांपासून आणि सायबर गुन्हांपासून बचाव करण्यासाठी ज्या उपाययोजना आहेत त्यांची जास्तीत जास्त माहिती करुन घ्या.
- जागृत व सजग सायबर नागरिक व्हा. सायबर सुरक्षेसाठी सावधगिरी बाळगा आणि आपल्या मित्रांना व नातेवाईकांनाही याबाबत सांगा.
- सुरक्षित सायबर पद्धतींवर नियमीतपणे अपड्रेससाठी Twitter handle@cyber Dost फॉलो करा.
- तुम्हाला ही विनंती आहे की तुम्ही आपला प्रतिसाद dircis2-mha@nic.in किंवा pmuiec.cismha@nic.in या मेलवर आमच्याशी शेअर करा.

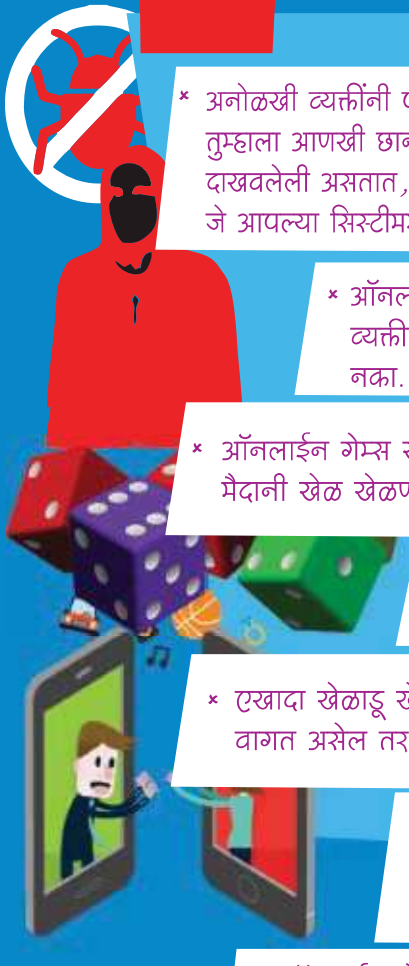
ऑनलाईन गेम्स खेळणाऱ्या मुलांसाठी सुरक्षेच्या काही सूचना

करमणूक करत वेळ घालवण्यासाठी खेळले जाणारे ऑनलाईन गेम्स संघभावना वाढवतात आणि कौशल्यांचा विकास करतात. एक आभासी क्रीडांगण मुलांना खूप आवडते आणि ते त्यात रममाण होऊन जातात. ते लवकरच इतके तयार होतात की ऑनलाईन लॉग इन करतात, वेब कॅम सुरू करतात आणि जगभरातील अगणित अनोळखी लोकांशी संपर्क साधला जाताच त्यांच्याशी बोलत खेळायला सुरूवात करतात. इतके सगळे त्यांच्या अंगवळणी पडते.

ऑनलाईन गेम्स खेळताना काय करावे?

- ✓ मालवेअर, धोकादायक सॉफ्टवेअर किंवा व्हायरसपासून आपले संगणक आणि अन्य सिस्टीम सुरक्षित ठेवण्यासाठी वैध ॲन्टीव्हायरस वापरून सिस्टीम अद्ययावत ठेवा.
- ✓ आपल्याला लक्षात ठेवण्यात सोपा मात्र दुसऱ्यांना अंदाज लावणे खूप अवघड असा १२ आकडी पासवर्ड अंक, अक्षरे, चिन्हे वापरून तयार करा.
- ✓ तुमचे नाव, पत्ता, वय, लिंग, दूरध्वनी क्रमांक किंवा अन्य कोणतीही वैयक्तिक, कौटुंबिक माहिती उघड करू नका.
- ✓ आपल्या वयाला अनुसरून योग्य असणारे, ज्ञान आणि कौशल्य वाढवणारे अथवा शैक्षणिक किंवा निखळ करमणूक करणारे गेम्स खेळावेत.
- ✓ सायबर हल्लेखोर आणि धोकादायक गोष्टींपासून सावधगिरी बाळगा.
- ✓ खेळ खेळण्यापूर्वी कुटुंबातील वडिलधाऱ्या व्यक्तींचे मार्गदर्शन घ्या.
- ✓ ऑनलाईन गेम्स खेळताना निर्माण होणारे धोके ओळखा आणि योग्य अंदाज लावण्याचा सराव करावा. घरातील वडिलधाऱ्या व्यक्तींचे मार्गदर्शन घ्या.

ऑनलाईन गेम्स खेळताना काय करू नये?



× अनोळखी व्यक्तींनी पाठवलेले फोटो, व्हिडिओ डाऊनलोड करू नका. तुम्हाला आणखी छान खेळता येईल, बक्षीस मिळेल अशी प्रलोभने त्यात दाखवलेली असतात, मात्र त्यात खरे तर मालवेअर वगैरे लपवलेले असतात जे आपल्या सिस्टीममध्ये शिरतात आणि आपली माहिती चोरतात.

× ऑनलाईन गेम्स खेळताना माहित झालेल्या एखाद्या अनोळखी व्यक्तीला अजिबात भेटायला जाऊ नका अथवा तिला बोलावू नका. लोक जे आहेत असे सांगतात तसे ते नसतात.

× ऑनलाईन गेम्स खेळताना वेळेची मर्यादा पाळा. मैदानी खेळ खेळण्यास प्राधान्य द्या.

× आपली वैयक्तिक किंवा कौटुंबिक माहिती, तशा माहितीची लिंक सहकारी खेळाडूला पाठवू नका.

× एखादा खेळाडू खेळताना विचित्र किंवा अयोग्य वागत असेल तर त्याला प्रतिसाद देऊ नका.

× ऑनलाईन गेम्स खेळताना व्हॉईस किंवा व्हिडिओ चॅट करू नका. अनोळखी लोक ते रेकॉर्ड करून त्याचा गैरवापर करू शकतात.

× ऑनलाईन गेम्स खेळताना अनोळखी लोकांशी खेळले जातात यामुळे ओळखी वाढतात असे सांगितले जात असले तरी वास्तवात त्याचा फायदा होण्याऐवजी तोटाच जास्त होतो.

× ऑनलाईन गेम्स खेळताना काय काय धोके आणि जोखमी असतात याची मुलांना स्पष्ट जाणीव करून द्या.

इंटरनेट वापरणाऱ्या मुलांसाठी काही नैतिक सूचना

एक जबाबदार व्यक्ती म्हणून इंटरनेट वापरताना काही नियम पाळणे आपले कर्तव्य आहे. मुलांनी इंटरनेट वापरताना कसे वागावे आणि प्रामाणिक राहून आपल्या हक्क व कर्तव्याची जाणीव ठेवावी.

स्विकारणे :-

इंटरनेट हे असे जग आहे जिथे माहितीची देवाण-घेवाण करताना आणि संवाद साधताना काही मूल्ये जपणे आवश्यक असते. इंटरनेट हे जगाच्या संस्कृतीपेक्षा वेगळे नसून त्याचाच एक भाग आहे.

स्थानिक आणि राष्ट्रीय संस्कृतीबद्दल संवेदनशिलता :-

इंटरनेटचे जग सर्वांसाठी आहे आणि त्याला स्थानिक किंवा एखाद्या देशाच्या मर्यादा नाहीत. स्थानिक वर्तमानपत्र, एखादी करमणूक किंवा वृत्त वाहिनीसारखी त्याची एकच एक साचेबद्ध मूल्य व्यवस्था नाही. जगातील सर्व प्रकारच्या लोकांना तिथे सामावून घेतले असल्याचे ध्यानात ठेवले पाहिजे.

शाळेचे काम करताना :-

ज्ञान मिळवण्यासाठी, शैक्षणिक उपयोगासाठी, माहिती संकलित करण्यासाठी, काही चांगल्या गोष्टी शिकण्यासाठी त्याचा जरूर वापर करावा.

ई-मेल आणि चाट वापरताना :-

कुटुंबिय मित्रमंडळी आणि हितचिंतक किंवा सहकाऱ्यांशी संपर्क ठेवणे, संवाद साधणे याकरिता ई-मेल आणि चॅटचा वापर करावा.

मात्र अनोळखी लोकांशी बोलण्यासाठी किंवा संपर्क करण्यासाठी तसेच अज्ञात व्यक्तीकडून आलेले मेल्स अथवा मेसेजेस फॉरवर्ड करण्यासाठी ते वापरू नये.

ओळख लपवून वावरण्यासाठी :-

आपण जे नाही ते भासवून आपण कोणी वेगळीच व्यक्ती आहोत असे ढोंग करत किंवा आपली ओळख लपवत आपण इंटरनेट वापरू नये. दुसऱ्यानेही खोटे वागू नये ही आपली अपेक्षा असते ना, त्यामुळे आपण तसे वागू नये.

असभ्य भाषेचा वापर :-

असभ्य, गर्विष्ठ, उध्दट किंवा अश्लील भाषा वापरू नये. ई-मेल्स, चॅट, ब्लॉगिंग वगैरे ठिकाणी सभ्य सुसंस्कृत भाषेचा वापर करावा. इंटरनेनटवर कधीही कोणावर टीका करू नये.

खासगी माहिती उघड न करणे :-

आपला पत्ता, दूरध्वनी क्रमांक, आवडी, छंद, छायाचित्र घराचे फोटो, कौटुंबिक माहिती अनोळखी लोकांना पाठवू नये, सांगू नये. त्यांना भेटायला जाऊ नये किंवा आपल्याकडे बोलावू नये.

डाऊनलोड करताना :-

इंटरनेटचा उपयोग काही चांगले शिकण्यासाठी, दर्जेदार करमणुकीसाठी आणि आपल्या जवळच्या लोकांशी संवाद साधण्यासाठी करावा. आक्षेपार्ह फोटो, व्हिडिओ किंवा बौद्धिक संपदा अधिकार (कॉपीराईट) प्राप्त साहित्य डाऊनलोड करण्यासाठी इंटरनेट वापरू नये.

विद्यार्थी मित्रांनो आज आपण माहिती तंत्रज्ञानाच्या युगात जगत आहोत. तंत्रज्ञानाने आपले जीवन सुखकर केलेले आहे. परंतु सायबर तंत्रज्ञानाचा वापर कशा पध्दतीने होतो. यावर आपल्या समाजाचा, देशाचा विकास अवलंबून आहे. यासाठी सदर सायबर तंत्रज्ञान हाताळताना, वापरतांना आपण नैतिक मुल्य अंगी बाळगली तरी त्याचा उपयोग स्वतःसाठी व समाजासाठी होऊ शकतो.

सायबर तंत्रज्ञानाकडे ज्ञानकोष किंवा ज्ञानभांडार म्हणून पाहणे.

आपल्याला कोणतेही ज्ञान किंवा एखाद्या गोष्टीबाबतची माहिती गुगलवर सहज उपलब्ध होते अशी कोणतीही बाब नाही की, ती गुगलला माहिती नाही. जेव्हा आपल्याला एखाद्या गोष्टीबद्दल माहिती घ्यावयाची असेल, तर सायबर तंत्रज्ञानाचा विशेषतः गुगलचा वापर करू शकता व आपल्या ज्ञानामध्ये भर घालू शकता.

खोटी माहिती पसरवू नये.

इंटरनेटने सर्व व्यक्तींना अतिशय जवळ आणले आहे. त्यामुळे आपण जर एखादी माहिती पसरवत असेल तर ती अतिशय कमी कालावधीत जास्तीत जास्त लोकांपर्यंत पोहचते. यासाठी कोणतीही खोटी माहिती पसरवून लोकांची दिशाभूल करू नये. खरी व समाजउपयोगी माहिती प्रसारीत करणे ही आपली नैतिक जबाबदारी आहे.

अतिवापर (Addict) करू नये.

आजकाल बऱ्याच कंपन्यांकडून स्वस्तात व सहजरित्या इंटरनेट उपलब्ध होतो. त्यामुळे तो आपल्या आयुष्याचा भाग बनणे हे स्वाभाविक आहे, परंतु त्यास अविभाज्य भाग बनवू नका. तसेच त्याच्या अतिवापरामुळे काही मानसिक व शारिरीक रोग झाल्याचे संशोधनातून सिध्द झाले आहे.

तंत्रज्ञान जेव्हा
आपण मनोरंजनाचे साधन
म्हणून वापरता
तेव्हा
दुसऱ्याचे नुकसान
होणार नाही
याकडे लक्ष द्या.

बुलडाणा जिल्हा पोलीस - दूरध्वनी सूची

वरिष्ठ अधिकारी कार्यालय	दूरध्वनी क्रमांक
पोलीस अधीक्षक, बुलडाणा	ऑफिस - ०७२६२-२४२३९५ नि.स्थान - ०७२६२-४२३०३
अप्पर पोलीस अधीक्षक, बुलडाणा	ऑफिस - ०७२६२-२४४९२५ नि.स्थान - २४२४६६ ऑफिस - २०२
अप्पर पोलीस अधीक्षक, खामगाव	०७२६३ -२५२०४८
पो.उपअधिक्षक (गृह)	०७२६२ -२४२१०१
उपविभागीय पोलीस अधिकारी, मलकापूर	०७२६७ - २२२३६८
उपविभागीय पोलीस अधिकारी, बुलडाणा	०७२६२ - २४२३२६
पो.उपअधिक्षक, अर्थिक गुन्हे शाखा, चिखली	०७२६२ - २४२७३८
उपविभागीय पोलीस अधिकारी देउळगावराजा, सिंदखेडराजा	०७२६१ - २३१६५०
उपविभागीय पोलीस अधिकारी, मेहकर	०७२६८ - २२५९७५
उपविभागीय पोलीस अधिकारी, खामगांव	०७२६३ - २५२१६७
उपविभागीय पोलीस अधिकारी, जळगांव जा.	०७२४ - २४३४१११
पोलीस उपअधिक्षक, लाचलुचपत प्रतिबंध शाखा, बुलडाणा	०७२६२ - २४२५४८

बुलडाणा जिल्हा पोलीस संपर्क क्रमांक

अ.क्र	कार्यालय	एसटीडी कोड	दूरध्वनी
उपविभाग बुलडाणा			
१.	बुलडाणा शहर	०७२६२	२४२३२७
२.	बुलडाणा ग्रामीण	०७२६२	२४१२५५
३.	बोराखेडी	०७२६७	२४५२२६
४.	धामणगाव बढे	०७२६७	२४१५४१
५.	चिखली	०७२६४	२४२०६७
६.	अमडापूर	०७२६४	२६४०३४
७.	धाड	०७२६२	२६५१३२
८.	रायपूर	०७२६२	२७००३०
उपविभाग मेहकर			
१.	मेहकर	०७२६८	२२४५३६
२.	डोणगांव	०७२६८	२६६२४०
३.	जानेफळ	०७२६८	२६२५३३
४.	साखरखेर्डा	०७२६४	२६६०३८
५.	लोणार	०७२६०	२२१३२१
६.	बिबी	०७२६०	२७१२५०
उपविभाग देउळगांव राजा			
१.	देउळगांव राजा	०७२६१	२३२००२
२.	सिंदखेड राजा	०७२६९	२३४२४४
३.	किनगांव राजा	०७२६९	२६४४३३
४.	अंढेरा	०७२६१	२६५०३३

उपविभाग खामगांव			
१.	खामगांव शहर	०७२६३	२५२०३८
२.	शिवाजी नगर	०७२६३	२५२१४२
३.	खामगांव ग्रामीण	०७२६३	२५२२९५
४.	पिंपळगांव राजा	०७२६३	२७१२३४
५.	हिवरखेड	०७२६३	२६६६३६
६.	शेगांव शहर	०७२६५	२५२०१०
७.	शेगांव ग्रामीण	०७२६५	२५३०१०
८.	जलंब	०७२६५	२७७५४२
उपविभाग मलकापुर			
१.	मलकापूर शहर	०७२६७	२२२०१८
२.	मलकापूर ग्रामीण	०७२६७	२२२२५८
३.	एमआयडीसी दसरखेड	०७२६७	२६२४००
४.	नांदुरा	०७२६५	२२१०२८
५.	जळगांव जा.	०७२६६	२२१५३०
६.	तामगांव	०७२६६	२३२२३२
७.	सोनाळा	०७२६६	२३८५३८
स्थानिक शाखा			
१.	आर्थिक गुन्हे शाखा	०७२६२	२४२७३८
२.	स्थानिक गुन्हे शाखा	०७२६२	२४२७३८
३.	जिल्हा विशेष शाखा	०७२६२	२४१०४०
४.	कल्याण शाखा/ सायबर सेल	०७२६२	२४७७६७
५.	FRO/पासपोर्ट	०७२६२	२४१०४०
६.	नियंत्रण कक्ष बुलडाणा	०७२६२	२४२४००