amazon future engineer

CTRL + ALT + PROTECT

सुरक्षा नगर मधील साहसिक किस्से

चला इंटरनेट सुरक्षित पद्धतीने कसे वापरावे याचे माहितीपत्रक

अनुक्रमणिका

ऑनलाईन मजा करताना डिजिटल वर्ल्ड सुरक्षितपणे कसे एक्स्प्लोर करावे यासाठी हे हँडबुक तुम्हाला मदत करेल, सात मित्रांच्या या कथांद्वारे तुम्हाला स्कॅम, गोपनीयता बाळगणे, चुकीची माहिती आणि इंटरनेटचा जबाबदारी पूर्वक वापर करणे याबद्दल माहिती मिळेल.

सुरक्षा नगर नावाच्या एका जीवंत शहरात सात बेस्ट फ्रेंड्स राहत होते - मीरा, रहीम, जसप्रीत, सुजान, शुभम, सिद्धार्थ, आणि नूर.

मीरा - धाडसी

रहीम - सुरक्षा कवच

सुजान - प्रायव्हसी चॅंपियन

शुभम - न्यूज नॅव्हिगेटर

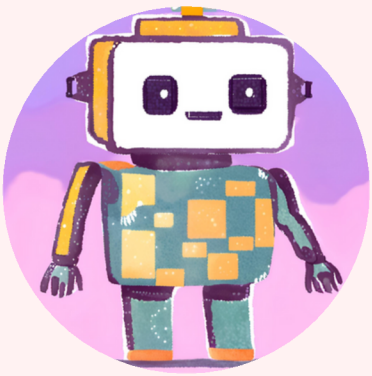
सिद्धार्थ – हेल्पर

जसप्रीत – जासूस

नूर – चेंजमेकर

अमित दादा

ग्लिच

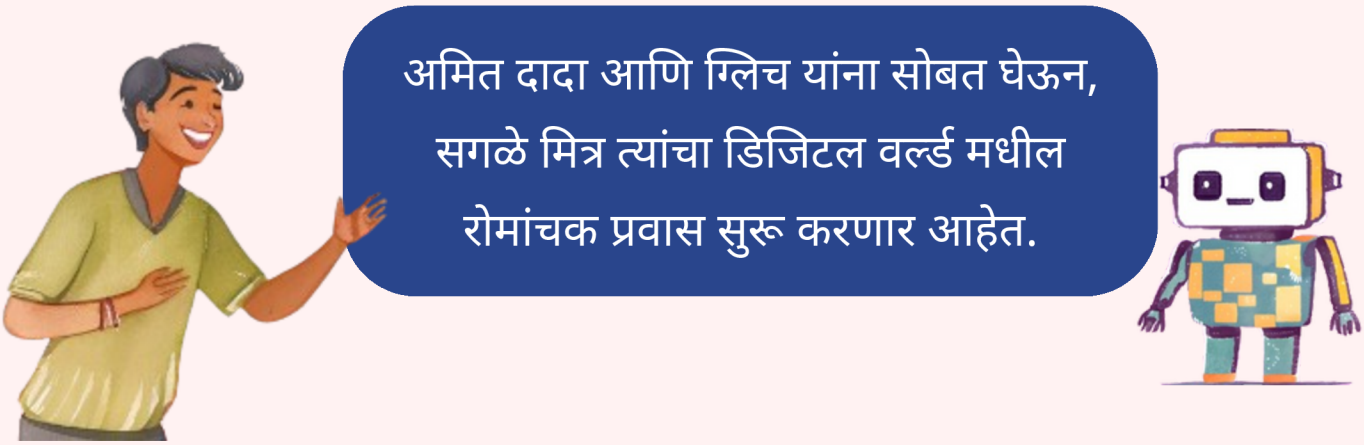


सुरक्षा नगर मधल्या एका प्रसन्न दुपारी, मीराच्या घरातील हॉल हसण्याच्या आणि दंगामस्ती करण्याच्या आवाजाने दणाणून गेला होता. सात मित्र-मैत्रिणी – मीरा, रहीम, जसप्रीत, सुजान, शुभम, सिद्धार्थ, आणि नूर – सगळेच सोफ्यावर आणि जमिनीवर पसरले होते, खाण्याचे पदार्थ त्यांचा आजूबाजूला पडलेले होते आणि तशातच त्यांनी एक जुना लॅपटॉप चालू केला.

“चला हे ट्राय करूया!” मीरा उत्साहाने म्हणाली, तिची बोटं एव्हाना वेगवेगळ्या साईट्स आणि गेम्स वर क्लिक करू लागली होती. “थांब, घाई करू नकोस, तू काही तरी चुकीचं क्लिक करशील,” रहीमने कपाळाला आठ्या घालत तिला सावध केलं. “रहीम, एवढी काळजी करू नकोस- इट्स फाईन,” शुभमने चिडवलं, एवढ्यात तिचा फोन नोटिफिकेशन्स मुळे वाजायला लागला, कारण तिने ग्रूप मध्ये एक मजेशीर मीम शेअर केली होती.

“ही साईट सुरक्षित आहे हे तरी बघितलंस का? जसप्रीतने विचारलं, स्क्रीनकडे पाहताना त्याच्यामधील जासूस डोकं वर काढत होता. “कोणतीही खाजगी माहिती शेअर करायची नाही हे ही लक्षात असू दे”, आधी बुकमार्क करून ठेवलेले एक नवीन प्रायव्हसी गाईड वाचत ठाम आणि शांत आवाजात सुजान म्हणाली. सिद्धार्थ हसायला लागला,आणि म्हणाला “अरे ऐका, सगळ्यांनी जरा मोठ्ठा श्वास घ्या बरं! आपण फक्त बघतोय – घाबरायची काही गरज नाही,” तो इतक्या सहजपणे बोलला की सगळेच जरा शांत झाले. दरम्यान नूर तिच्या वहीत काही आयडियाज लिहीत होती. “आपण इंटरनेट वापरण्याच्या सर्वात कूल आणि सुरक्षित पद्धतींवर प्रोजेक्ट केला तर? आपण तो शाळेत पण दाखवू शकतो!” तिने सुचवले, तिचे डोळे उत्साहाने चमकत होते.

जेव्हां ते विविध गेम्स, व्हिडिओज, आणि विचित्र पॉप-अप्स नेव्हिगेट करीत होते, त्यांच्या खोलीतून वाद-विवादाचे, हसण्याचे, आणि मधूनच, “अरर्र, मला तिथे क्लिक नव्हतं करायचं!” असे पण आवाज येत होते. हे फक्त इंटरनेट बद्दल नव्हतं तर एकत्र येऊन काही तरी करणं, एकमेकांकडून काही तरी शिकणं, आणि त्यांचे ऑनलाईन एडव्हेंचर सुरक्षित आणि मजेदार असेल हे सुनिश्चित करणे हे सुद्धा होतं.



सुरक्षित पद्धतीने कसे नेव्हीगेट करायचे, छुप्या रिस्क्स कशा ओळखायच्या आणि इंटरनेट वर उपलब्ध असलेल्या असंख्य संधी माहिती कश्या करायच्या याबद्दल ते शिकणार आहेत. प्रत्येक क्लिक मधून नवीन काही तरी शिकणार होते.

पण हा प्रवास वाटतो आहे तितका सोपा नक्कीच नसणार. या वाटेवर अनेक आश्चर्यकारक गोष्टी आणि अडथळे देखील येणार आहेत. तरी, ही सगळी मुलं, अमित दादाच्या मार्गदर्शनाखाली आणि ग्लिचच्या डोकेबाज क्लुप्त्यांच्या मदतीने प्रत्येक आव्हानाला बेधडकपणे सामोरे जातील.

प्रकरण 1: हॅलो डिजिटल वर्ल्ड!

मीरा तिच्या आईचा फोन घेऊन खिडकीत बसली होती.. डझनभर टॅब्स उघडून बघत बसली होती. गमतीदार व्हिडिओज बघणे, नव-नवीन गाणी ऐकणे, आणि अनंत प्रश्नांची उत्तरे शोधणे हे सगळं करण्यासाठी तिने नुकताच इंटरनेटच्या अगाध विश्वामध्ये प्रवेश केला होता . तिला हे सगळं खूप आवडतं, पण आज ती जरा गोंधळली आहे.

या इंटरनेटला प्रत्येक गोष्टी बद्दल एवढी कशी माहिती असते? आणि हे सगळं असं आपापसात जोडलेलं कसं असतं? मीरा विचार करू लागली.

नशीबाने अमित दादा तिथेच होता. “दादा!” तिने हाक मारली आणि लगेचच अमित दादा नेहमीप्रमाणे त्याच्या शांत आणि हसऱ्या चेहऱ्याने तिथे आला.

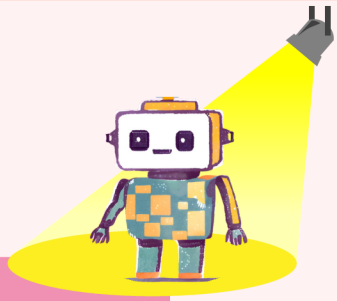
इंटरनेटला सगळ्या विषयांमधलं सगळंच कस रे माहीत असतं? आणि सगळं असं आपापसात जोडलेलं कसं असतं?

आह, इंटरनेट! हे एक अप्रतिम साधन आहे पण फार कमी लोकांना असा प्रश्न पडतो की हे काम कसं करतं. चल आपण एकत्र शोधूया! आणि या सगळ्या गोष्टी समजावण्यामध्ये अगदी एक्स्पर्ट आहेअश्या कुणाला तरी मी बोलावतो.

त्याच्या फोनवर त्याने फक्त एक क्लिक केलं आणि एक रोबोट त्या खोलीत हजर झाला. त्याचे लाईट चमकत होते आणि त्याचा आवाजही अगदी उत्साही होता.

हाय मीरा! मी आहे ग्लिच, तुझा इंटरनेट बडी! मी इथे तुला इंटरनेटच्या अगाध विश्वाची ओळख करून द्यायला आलो आहे.

तर इंटरनेट म्हणजे काय?

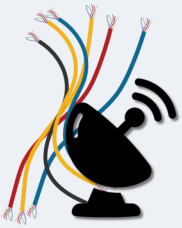


आपण सुरुवातीपासून सुरू करूया, इंटरनेट म्हणजे एक मोठ्ठे जाळे आहे जे अब्जावधी कम्प्युटर्स, फोन, आणि जगभरातील डिव्हाईसेजना जोडून ठेवते. या कनेक्शन्स मुळे हे सर्व डिव्हाईसेज एकमेकांमध्ये माहिती शेअर करू शकतात. ज्यामुळे तुम्ही ब्राउझ करणे, व्हिडिओ बघणे, गेम्स खेळणे, आणि इतकच काय तर ऑनलाईन शॉपिंग देखील करू शकता.

इंटरनेट म्हणजे आपल्या रेल्वे सिस्टम सारखे असते, पण माणसं आणि सामान वाहून नेण्याऐवजी हे कोणतीही माहिती जगाच्या कोपऱ्यापर्यन्त क्षणार्धात वाहून नेते.

प्रत्येक वेबसाईटचा एक वेगळा ॲड्रेस असतो, जसं प्रत्येक रेल्वे स्टेशनचं वेगळं नाव असतं की नाही अगदी तसं! फरक इतकाच आहे की माणसं आणि सामान एका ठिकाणाहून दुसऱ्या ठिकाणी नेण्यासाठी ट्रेन्सना अनेक तास आणि दिवस लागतात, पण इंटरनेटला माहिती पोहोचवण्यासाठी अगदी काही क्षण लागतात.

इंटरनेटचा आधारस्तंभ / कणा



इंटरनेट जमिनीखालच्या असंख्य केबल्स, सॅटेलाईट्स, आणि वायरलेस नेटवर्क्स द्वारे जगभरातील सर्व डिव्हाईसेज एकमेकांशी जोडते.

सर्व्हर्स

हा एक सर्व्हर आहे , तुम्ही जी ऑनलाईन माहिती बघता ती यामध्ये स्टोअर केलेली असते. सर्व्हर्स म्हणजे महाकाय लायब्रीज जिथे असंख्य वेबसाईट्स, व्हिडिओज, आणि ॲप्स, असतात.

तुमचा ब्राउझर

जेव्हा तुम्ही तुमच्या ब्राउझर मध्ये एखादा प्रश्न टाईप करता, तेव्हा तुमचा डिव्हाईस सर्व्हरला एक रिक्वेस्ट पाठवतो. हा सर्व्हर तुमचे उत्तर शोधतो आणि काही क्षणातच तुमच्यापर्यंत पोहोचवतो.

इंटरनेट आपल्याला कशाप्रकारे मदत करते?

इंटरनेट ने आपल्या जगण्याच्या आणि शिकण्याच्या पद्धतीत क्रांति घडवून आणली आहे. चला मी तुम्हाला दाखवतो की इंटरनेट आपल्याला आपल्या दैनंदिन आयुष्यात कशाप्रकारे मदत करते.

शिक्षण क्षेत्रातील इंटरनेटचे योगदान

इंटरनेट म्हणजे तुमचा शिक्षकही आणि लायब्ररीही! शैक्षणिक साहित्य वाचा, कोणत्याही भाषेमध्ये व्हिडिओज बघा, आणि तुमच्या आवडीचे विषय शिकण्यासाठी व्हरच्युअल क्लासरूम्स जॉइन करा - हे सगळं करा फक्त एका क्लिक मध्ये

संवाद

क्षणार्धात कनेक्ट व्हा! ईमेल्स, सोशल मीडिया, मेसेजिंग ॲप्स, , किंवा व्हिडिओ कॉल्स, इंटरनेट मुळे अगदी काही क्षणातच, सोप्या पद्धतीने आणि सहज एकमेकांशी संवाद साधता येतो.

मनोरंजन

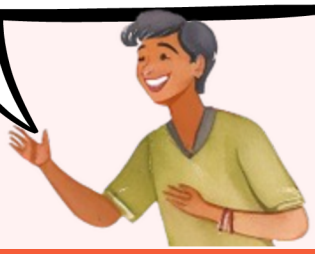
इंटरनेट तुमची करमणूक पण करतो बरं का - पिक्चर बघू शकता, लाईव्ह क्रिकेट मॅचेस बघू शकता, किंवा डान्स आणि इतरही नवनवीन कौशल्ये देखील शिकू शकता.

सर्जनशीलता आणि सामायिकरण

तुमची सर्जनशीलता संपूर्ण जगाला दाखवा! गोष्टी लिहा, म्युजिक तयार करा, किंवा तुमची चित्रकला ऑनलाईन दाखवा. जसे खूप प्रतिभावंत तरुण कलाकार रोज करतात.

दादा, मी ऑनलाईन क्लासेस साठी इंटरनेट वापरायला सुरुवात केली आणि अभ्यास केल्यानंतर जरा करमणूक म्हणून फनी व्हिडिओज बघायला आणि गेम्स खेळायला पण आता मला आवडायला लागलं आहे! पण माझ्या हे लक्षातच आलं नाही की मी इंटरनेट वर डान्स किंवा म्युजिक पण शिकू शकते.

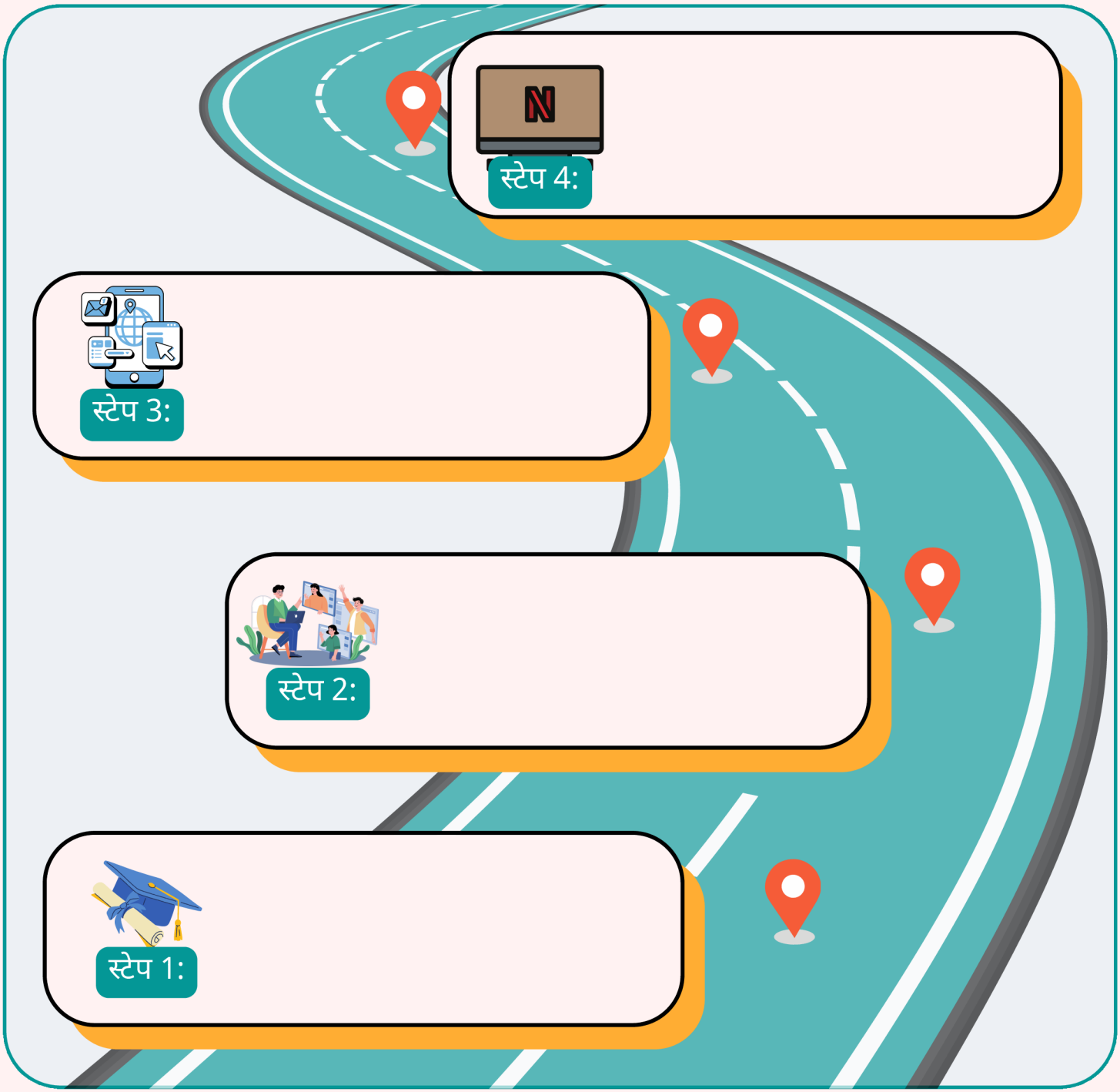
मस्तच! अगं अशी तू एकटी नाहीयेस: 88% तरुण भारतीय तुझ्यासारखेच ऑनलाईन व्हिडिओज बघतात. त्याहीपेक्षा जास्त तरुण गेमिंग साठी , माहिती शोधण्यासाठी आणि मित्र-मैत्रिणींशी गप्पा मारण्यासाठी इंटरनेटचा वापर करतात! त्यामुळे अनेक तरुण ऑनलाईन नव-नवीन गोष्टी शोधत आहेत - हे भन्नाट आहे ना?!



ॲक्टिव्हिटी

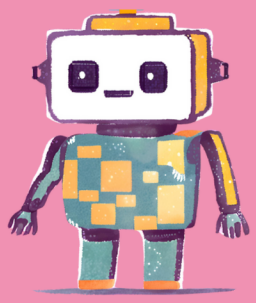
इंटेरनेट बद्दल नव्याने जाणून घेतल्यावर, मीरा आता यातील असंख्य संधींचा शोध घेण्यासाठी सज्ज झाली होती. तुम्ही जर कधी इंटरनेट वापरलं असेल तर तुमच्या ऑनलाईन विश्वातल्या रंजक अनुभवांबद्दल तिला सांगून नवीन गोष्टी करून बघण्यासाठी तिची मदत करा. खाली दिल्याप्रमाणे सुरुवात करा, आणि:

- स्टेप 1 तुम्ही ऑनलाईन नवीन जे काही शिकलात त्याचा विचार करा.
- स्टेप 2, तुम्ही बनवलेली किंवा शेअर केलेली एखादी कला शेअर करा.
- स्टेप 3 कनेक्टेड रहा - तुमचे ऑनलाईन मित्र-मैत्रिणी कोण आहेत?
- आणि सर्वात शेवटी स्टेप 4 म्हणजे धमाल - तुमची सर्वात आवडती ऑनलाईन ऍक्टिव्हिटी कोणती आहे?



इंटरनेट हे फक्त जे आज आहे तेच नाही आहे. हे सतत विकसित होत आहे , आणि तुम्ही सगळे याच्या भविष्याचाच एक भाग आहात.

भारतामध्ये आपण सध्या खूप वेगवेगळे बदल अनुभवतो आहोत. तुम्ही किंवा तुमचे आई-वडील पेमेंटसाठी यूपीआय किंवा युनिफाईड पेमेंट इंटरफेस वापरत असतीलच! यूपीआय मुळे आपण अगदी सहज डिजिटली पैसे प्राप्त करू शकतो किंवा पाठवू शकतो, ज्यामुळे आर्थिक व्यवहाराच्या विश्वात जणू क्रांतीच आली आहे.इतरही नव-नवीन ऑनलाईन सर्व्हिसेस उपलब्ध आहेत उदाहरणार्थ, डॉक्टर रुग्णांना व्हिडिओ कॉलवरच उपचार देतात, आणि विद्यार्थी पण क्लासेस त्यांच्या घरतूनच अटेंड करू शकतात.

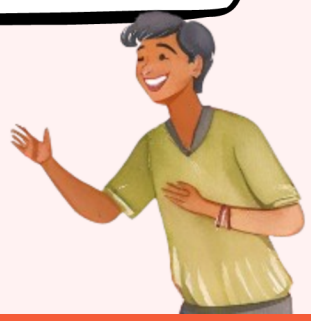


आर्टिफिशियल इंटेलिजन्स किंवा एआय मुळे इंटरनेट अजूनच स्मार्ट होत चालले आहे, एआय मुळे मशीन्स देखील माणसांसारखाच विचार करू शकतात आणि नव-नवीन गोष्टी शिकू शकतात. एआय टूल्स तुमच्या प्रश्नांची उत्तरे देऊ शकतात, गेम्सना जास्त आव्हानात्मक बनवू शकतात, आणि एआयला प्रशिक्षित करण्यासाठी वापरलेल्या डेटा द्वारे लोकांना त्यांच्या समस्यांची उत्तरे शोधण्यात मदत करतात.

आता व्हर्चूअल रियालिटी किंवा व्हीआर अस्तित्वात आले आहे, हे एक असे तंत्रज्ञान आहे जे वातावरण निर्मित करते आणि आपण हेडसेट्सच्या मदतीने त्या वातावरणाशी संपर्क करू शकतो. कल्पना करा की तुम्ही एका वर्षावनातून चालत जात आहात, ताजमहाल बघत आहात, किंवा अगदी अंतराळात गेला आहात - आणि हो, हे सगळं अगदी तुमच्या खोलीत बसूनच करत आहात !

धन्यवाद, दादा आणि ग्लिच! मला माहीतच नव्हतं की इंटरनेट इतकं भन्नाट आहे म्हणून - आणि इतकं प्रभावी पण. कधी एकदा मी या सगळ्या गोष्टी शिकते आणि अनुभवते आहे असं झालंय आता मला!

मला पण आवडेल तू हे सगळं अनुभवलंस तर! पण जसं जसं इंटरनेट विकसित होत चाललं आहे, तुम्हाला त्यातील सकारात्मक आणि नकारात्मक सगळ्याप्रकरचे अनुभव येतात आणि त्यासाठी तू तयार रहावेस असं मला वाटतं.



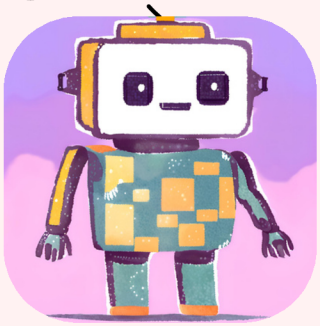
ॲक्टिव्हिटी

तो काय म्हणाला याचा विचार करत मीरा तिच्या खोलीत शांत बसली होती. जरी तिला इंटरनेट आवडत असलं तरी, अमित दादा बरोबर बोलत होता: नेहमी तयारीत राहणं महत्त्वाचं आहे. ती विचार करायला लागली आणि अशा प्रसंगांची तिने यादीच तयार केली जेव्हां इंटरनेट तिला तितकसं चांगलं किंवा सुरक्षित नाही वाटलं. तुम्हाला पण मीरासारखेच काही अनुभव आले आहेत का?

मला इंटरनेट आवडत नाही जेव्हा...

- काही लोक इतरांना घाबरवण्यासाठी चुकीची माहिती शेअर करतात.
- इतर लोक मला एखादी गोष्ट करण्यासाठी आग्रह करतात.
- कोणी माझ्याशी ऑनलाईन खोटं किंवा उद्धटपणे बोलतं.
- खूप साऱ्या नॉटिफिकेशन्समुळे मला खूप त्रास होतो!
- मला नको असलेले मेसेजेस येतात किंवा मला न आवडणारे व्हिडिओज दिसतात.
- मला असुरक्षित वाटतं कारण कोणीतरी पैसे मिळवण्यासाठी मला फसवण्याचा प्रयत्न करत असतं.

इथे तुम्ही तुमची स्वतःची एक यादी तयार करा:



आव्हानात्मक ऑनलाईन अनुभवांबद्दल बोलणे अवघड असू शकते पण तितकेच फायद्याचे देखील असू शकते. तुम्हाला जेव्हा असं वाटलं तेव्हा नक्की काय झालं होते हे सांगू शकता का? कायम लक्षात असू द्या, तुम्ही एकटे नाही आहात - ऑनलाईन असो किंवा ऑफलाइन, तणाव, राग, किंवा उदासीनता या नकारात्मक भावना असणे सामान्य आहे. चला असुरक्षित परिस्थिती कशाप्रकारे ओळखायच्या आणि ऑनलाईन असताना स्वतःची काळजी कशी घ्यायची हे एकत्र मिळून शिकूया.

इंटरनेट सुरक्षितते बाबत चे पहिलं पाऊल म्हणजे इंटरनेट व्यवस्थित पणे समजून घेणे, आणि नवीन घडामोडींबद्दल जागरूक राहणे. या काही महत्त्वाच्या गोष्टी आहेत ज्या तुम्ही ऑनलाईन विश्वात वावरताना लक्षात ठेवणे गरजेचे आहे.

सर्वप्रथम - तुमचे डिजिटल फूटप्रिंट. तुमचे डिजिटल फूटप्रिंट म्हणजे तुम्ही जेव्हा-जेव्हा ऑनलाईन असता तेव्हा मागे ठेवलेल्या खुणा. मग ती तुम्ही शेअर केलेली पोस्ट असेल, तुम्ही अपलोड केलेला फोटो असेल, किंवा तुम्ही जर काही सर्च करत असाल तर ते देखील तुमच्या डिजिटल आयडेंटिटी मध्ये भर घालतात.

एक मिनिट! म्हणजे माझी सर्च हिस्ट्री देखील माझ्या डिजिटल फूटप्रिंटचा भाग आहे? पण जर मी इन्कॉग्निटो मोड वापरला तर? मग माझ्या डिजिटल फूटप्रिंट वर नक्कीच कोणीही पाळत नाही ठेवू शकणार!

तुमचा प्रत्येक क्लिक, लाईक आणि शेअर तुमच्या ऑनलाईन असल्याचा पुरावा देते. अशी कल्पना करा की तुम्ही वेश बदलून तुमच्या गल्लीत फिरत आहात. जरी तुमच्या मित्रांनी तुम्हाला ओळखला नाही तरी वॉचमन, दुकानदार, किंवा कॅमेराज यांना सगळ्यांना दिसत असतं की तुम्ही कुठे चालले आहात आणि काय करत आहात. इन्कॉग्निटो मोड म्हणजे दुसरा वेश घेण्यासारखंच आहे. या मोड मध्ये तुमचा कम्प्युटर किंवा फोन वापरणाऱ्या लोकांना काही गोष्टी उदाहरणार्थ तुम्ही कोणती वेबसाईट बघितलीत हे कळू शकत नाही. पण या मोड मध्ये तुम्ही कोणालाच ऑनलाईन दिसणार नाही असं होणार नाही.

सर्व्हिस प्रोव्हायडर

तुमचे वायफाय किंवा इंटरनेट प्रोव्हायडर (अर्थात जी कंपनी तुम्हाला इंटरनेट सेवा देते) त्यांना तर नक्की माहीत असतं की तुम्ही कोणती वेबसाईट बघत आहात. अगदी तसं जसं एखाद्या दुकानदाराला तुम्ही वेश बदलून गेलात तरी कळतं की तुम्ही त्याच्या दुकानात आला आहात. तुमचे वायफाय किंवा इंटरनेट प्रोव्हायडर (अर्थात कंपनी तुम्हाला इंटरनेट सेवा देते) त्यांना तर नक्की माहीत असतं की तुम्ही कोणती वेबसाईट बघत आहात. अगदी तसं जसं एखाद्या दुकानदाराला तुम्ही वेश बदलून गेलात तरी कळतं की तुम्ही त्याच्या दुकानात आला आहात.

वेबसाईट्स

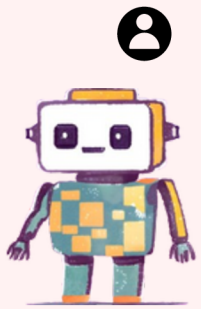
अनेक वेबसाईट्स तुमच्या बद्दल गोष्टी लक्षात ठेवण्यासाठी कूकीज किंवा ट्रॅकर्स असे काही टूल्स वापरतात. तुम्ही ब्राऊझर बंद केल्यावर इन्कॉग्निटो मोड जरी तुमच्या या गोष्टी डिलीट करत असले, तरी तुम्ही जर लॉगइन केलंत तर ते वेबसाईटला माहीत असतं किंवा तुमच्या डिव्हाईसला ती वेबसाईट ओळखते.

शाळेचे वायफाय

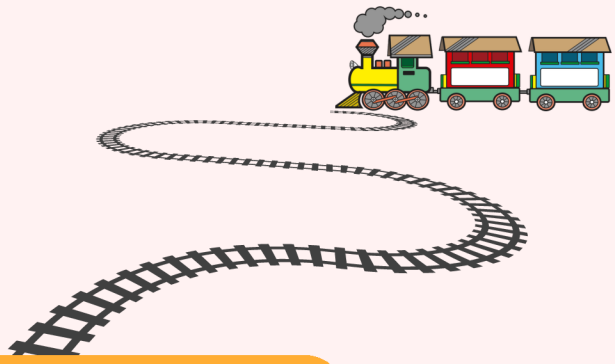
काही शाळांमधील वायफाय मध्ये , इंटरनेटच्या वापरावर लक्ष ठेवण्यासाठी, इन्कॉग्निटो मोड मध्ये देखील काही टूल्स वापरले जातात.

वाह, मला माहितही नव्हतं की मी जे करते आहे ते सगळं कुठे तरी रेकॉर्ड होत आहे. मी हे पण अनुभवलं आहे की सगळ्या वेबसाईट्स त्या वापरण्याआधी मला माझे नाव किंवा फोन नंबर किंवा लोकेशन किंवा ई-मेल आयडी विचारतात! मला याहून वेगळं काय लक्षात ठेवले पाहिजे?

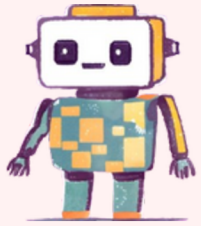
तुमच्यापेक्षा दोन पावलं पुढेच आहे हे इंटरनेट! आता आपण इंटरनेट बद्दल काही तरी अद्भुत - आणि एक जरा विचित्र गोष्ट समजून घेऊ. तुम्ही कधी बघितलं आहेत का की तुम्ही जी गोष्ट शोधत असता तेव्हा त्याच्या जाहिराती कशाप्रकारे तुमच्या समोर येतात, किंवा तुमच्या सोशल मीडिया फीड्स मध्ये नेहमीच तुम्हाला तुमच्या आवडीचे व्हिडिओ कसे दिसतात? हे सगळं ॲल्गोरिदम्स आणि कूकीज मुळे होतं!



एकदा माझ्या बहिणीने शॅम्पूज बद्दल सर्च केले, आणि पुढच्या वेळेस जेव्हा ती ऑनलाईन आली, तेव्हा तिला शॅम्पूजच्याच लिंक्स दिसायला लागल्या. आम्हाला वाटलं की हा फक्त एक योगायोग आहे! हे ॲल्गोरिदम्स कसे काम करतात?



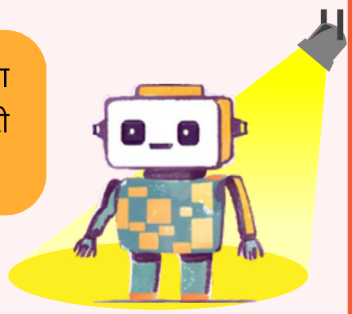
हे एका रेल्वे सिस्टम सारखे आहे. कल्पना करा की प्रत्येक वेबसाईट जी तुम्ही बघता ते एक स्टेशन आहे, आणि एखादी पोस्ट लाईक करणे, काही तरी शोधणे, किंवा तुमच्या कार्ट मध्ये एखादी वस्तु ॲड करणे - म्हणजे तुम्ही घेतलेली कुठलीही ॲक्शन, ते स्टेशन सोडणाऱ्या ट्रेन सारखी आहे. अल्गोरिदम्स ट्रेन कंडक्टर्स सारखे असतात. तुमची ट्रेन कुठे जात आहे ते बघत असतात आणि तुमच्या मागील प्रवासांवरून तुमचा पुढचा स्टॉप कोणता आहे हे ओळखण्याचा प्रयत्न करतात. जर तुम्ही व्हिडिओ गेम्ससंबंधी अनेक स्टेशन्स वर गेलात, तर हे अल्गोरिदम तुम्हाला गेमिंगची आवड आहे असे समजून कदाचित तुम्हाला त्यासंबंधीच ॲड्स पाठवतील किंवा गेमिंग संबंधीच कंटेंट पाठवतील.



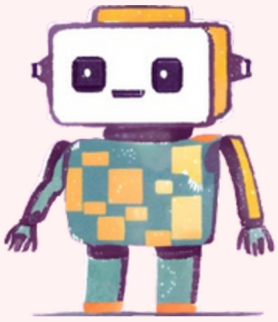
आणि त्याउलट कूकीज म्हणजे स्टेशन तिकीटासारख्या असतात ज्या तुमच्या डिव्हाईस मध्ये तशाच राहतात. या कूकीज मुळे वेबसाईट्सना कळतं की तुम्ही याआधीही ही वेबसाईट बघितली होती. तुम्ही त्या डिलीट करू शकता, आणि तिकीट फेकून देऊ शकता. लक्षात ठेवा, प्रत्येक प्रवास आपल्या खुणा मागे ठेवतोच.

जर मी एखादं टोपणनाव वापरलं तर?

चांगला प्रश्न आहे! आता आपण नावाबाबतच्या गोपनीयतेबद्दल बोलू. इंटरनेट वर लोक त्यांची खरी ओळख बऱ्याचदा गोपनीय ठेवतात.

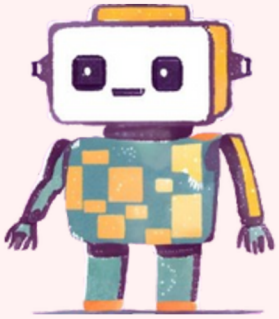


कधी कधी, लोक मजा म्हणून, सुरक्षेसाठी किंवा त्यांची पर्सनॅलिटी जाणून घेण्यासाठी यूझरनेम आणि एखादा वेगळाच फोटो याचा वापर करतात. ते योग्य आहे, पण नावाबद्दलच्या गोपनीयतेला मर्यादा आहेत: एखाद्याच्या ऑनलाईन ॲक्टिव्हिटीवर तरी सुद्धा त्याच्या नकळत पाळत ठेवली जाऊ शकते.. बरोब्बर.. तुमच्या डिजिटल फूटप्रिंट वरून! आणि लक्षात ठेव, दुसऱ्यांना फसवण्यासाठी सुद्धा लोक त्यांची ओळख लपवतात किंवा त्यांचं खोटं नाव सांगतात. प्रत्येक जण तसा नसतो जसा तो दिसतो.



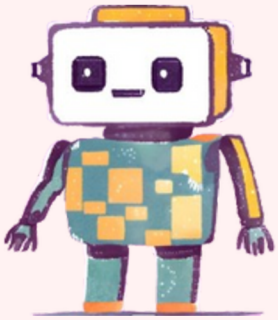
मी सहसा माझ्या ओळखीच्या आणि विश्वासू मित्रांशीच ऑनलाईन बोलतो, तेही माझ्या आईच्या खात्याचा वापर करून.

तर असं आहे! आता तुला वेगवेगळ्या ऑनलाईन स्पेसेस बद्दल पण माहीत असायला हवं. उदाहरणार्थ तुमचे ग्रूप चॅट, ही एक प्राईव्हेट स्पेस आहे . तुम्ही फूटप्रिंट मागे सोडता पण ते ग्रूपच्याबाहेरच्या लोकांना दिसत नाही. इतर ऑनलाईन स्पेसेस आहेत जिथे तुम्ही तुमच्या पब्लिक अकाऊंट वरून जर एखादी पोस्ट उदाहरणार्थ ट्वीट वगरे केलंत तर ते सर्वांना दिसते! तुमचे मेसेजेस, पोस्ट्स आणि लाईक्स कोण बघू शकते याबाबत नेहमीच जागरूक राहणे गरजेचे आहे. पुढे आपण हे सेटिंग कसे बदलायचे ते पण बघूया!

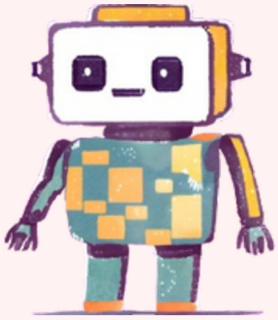


धन्यवाद ग्लिच! मला आज खूप काही शिकायला मिळालं, पण त्यामुळे आता मला जरा काळजी वाटायला लागली आहे.

आपल्या ऑनलाईन आणि ऑफलाइन आयुष्यात, आपल्याला चांगले आणि असुरक्षित असे दोन्ही प्रकारचे अनुभव येत असतात. इंटरनेट बद्दल जाणून घेतल्यामुळे आणि मित्र-मैत्रिणीं किंवा तुमच्यापेक्षा मोठ्या विश्वस्त लोकांशी सतत शेअर करत राहिल्यामुळे तुम्ही योग्य निर्णय घेऊ शकाल आणि याचे फायदे अनुभवू शकाल. ही तर सुरुवात आहे! जसं जसं तू याबद्दल शिकत जाशील तसा तसा तुझा याबाबतील विश्वास आणखीन वाढत जाईल.

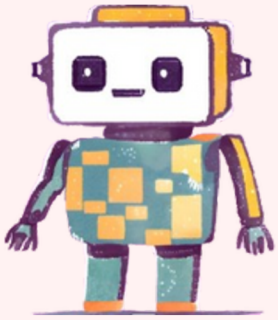


तोपर्यंत, तू इंटरनेट बद्दलच्या तुझ्या तीन इच्छा सांगू शकतेस? बघू तरी आपण त्या पूर्ण करू शकतो का ते?



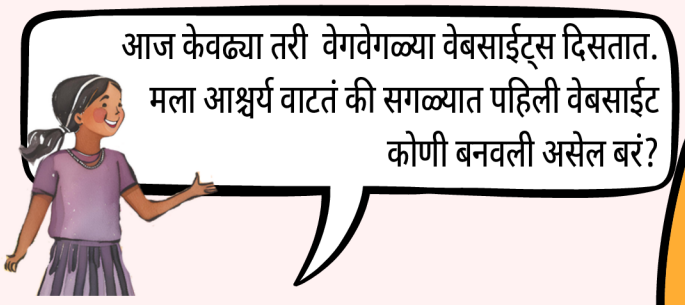
हाहा ओके! माझी इच्छा आहे की मी या ऑनलाईन तंत्रज्ञानाबद्दल अजून खूप शिकावं. आणखी एक इच्छा म्हणजे इंटरनेट सर्वांसाठी एक सुरक्षित ठिकाण असावं... आणि तिसरी इच्छा... तिसरी इच्छा म्हणजे मला नव-नवीन ॲप्स ट्राय करता यायला हवेत!

तुमच्या इंटरनेट बद्दलच्या काय इच्छा आहेत? मग सांगा ना मला!



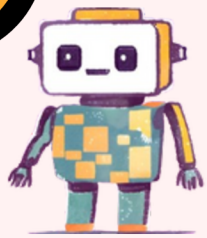
ॲक्टिव्हिटी

तुम्हाला माहीत आहे का?



पहिली वेबसाईट 1989 मध्ये बनवण्यात आली होती. जिचे नाव होते "info.cern.ch". 1989 मध्ये इंटरनेट वापरण्याची फक्त कल्पना करून बघा - आज आपण जशा रंगीबेरंगी, आकर्षक वेबसाईट्स बघतो त्यापेक्षा हे सगळं खूप वेगळं होतं. सगळ्यात पहिली वेबसाईट बनवणाऱ्या वैज्ञानिकाचं नाव तुम्ही सांगू शकता का?

इंटरनेट ही एक मोठ्ठी लायब्ररी आहे ज्यामध्ये वाचण्यासाठी असंख्य पुस्तकं आहेत. आज जगभरात 1.1 अब्ज वेबसाईट्स काम करत आहेत! आणि हा आकडा रोज वाढतच आहे. पण काळजी करू नको यातील बऱ्याचशा वेबसाईट्स डिजिटल म्युझियम सारख्या आहेत जिथे महत्त्वाची माहिती आणि मनोरंजन स्टोअर केलेले आहे.



तुला खोटं वाटेल पण संपूर्ण इंटरनेटचं वजन फक्त 60 ग्रॅम्स इतकं आहे. म्हणजे साधारण एका स्ट्रॉबेरी इतकं! असं कसं शक्य आहे माहितीये? माहितीचे पण वजन असते, जारी आपण ती बघू शकत नसलो तरी

रीकॅप: हॅलो डिजिटल वर्ल्ड!

1. तुमच्या वैयक्तिक माहिती बद्दल कायम सावध रहा. तुम्ही शेअर करत असलेली तुमची वैयक्तिक माहिती कधीही कुठेही वापरली किंवा स्टोअर केली जाऊ शकते.
2. ऑनलाईन असताना घेण्यात आलेली प्रत्येक ॲक्शन डिजिटल फूटप्रिंट सोडून जाते, तुम्ही काय शेअर करताय याकडे कायम लक्ष असू द्या.
3. इंटरनेट म्हणजे एक कनेक्शनचं मोठ्ठं जाळं आहे, जे जगभरातील डिव्हाईसेजना जोडतं आणि ज्यामुळे आपण संवाद साधू शकतो, शिकू शकतो, आणि आणखी बरेच एक्सप्लोर करण्याचा प्रयत्न करू शकतो.
4. ऑनलाईन प्लॅटफॉर्म्स कूकीज आणि कॅशे, जे तुमच्या विशिष्ट सवयी आणि माहिती उघड करू शकतात, यांच्या माध्यमातून तुमच्या ॲक्टिव्हिटी वर पाळत ठेवत असतात.

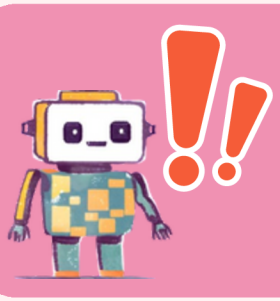
प्रकरण 2:
स्कॅम्स, हॅक्स आणि सायबर हल्ले: नेहमी एक पाऊल पुढे रहा!

आज मीराचा वाढदिवस आहे! तिचे घर आनंदाने आणि वेगवेगळ्या खाद्यपदार्थांच्या सुवासाने भरून गेलं होतं. तिच्या आईने रहीम आणि त्याच्या घरच्यांना रात्री जेवायला बोलावलं होतं. रहीम आणि त्याच्या घरचे आले आणि मोठे सगळे हॉल मध्ये गप्पा मारत बसले होते. तिकडे मीरा खूप उत्साहाने तिचा नवीन फोन हातात धरून रहीमला तिच्या खोलीत घेऊन जाते.

हे बघ रहीम! फायनली आई-बाबांनी मला माझा स्वत:चा फोन दिला! आता मी मला आत्तापर्यन्त हवे असलेले सगळे गेम्स आणि ॲप्स डाऊनलोड करू शकते.

सही, मीरा! पण डाऊनलोड करण्याआधी तुला तुझा आयडी आणि पासवर्ड तयार करावा लागेल. चल आपण तयार करू!

मीरा लगेच तिचा ईमेल आयडी म्हणून iammeera@gmail.com असे टाईप करते आणि अगदी दिमाखात IAMMEERA हा तिचा पासवर्ड ठेवते. तितक्यात ग्लिच तिला सावध करायला हजर होतो!



ईमेल आयडी: **iammeera@gmail.com**

पासवर्ड: : **I A M M E E R A**

हा पासवर्ड वीक आहे! ही सुरक्षेशी तडजोड आहे.

आता हा पासवर्ड का चांगला नाहीये? कारण हा लक्षात ठेवायला सोपा आहे. माझ्या आईच्या फोन मध्ये कायम मोठा, लक्षात ठेवण्यासाठी अवघड असा पासवर्ड असायचा, आणि दर वेळेस मला त्यासाठी मदत मागायला लागत होती.

लक्षात ठेवायला सोपा आहे पण इतर कोणाला लगेच ओळखत येईल इतका सोपा पण नको. सोपे पासवर्ड नुकसान करू शकतात ना? विचार करून बघ: जे तुला ओळखतात आणि ते तुझ्या अकाऊंट मध्ये लॉगिन करण्याचा प्रयत्न करत असतील तर पासवर्ड म्हणून ते सगळ्यात आधी तुझं नाव किंवा आवडती शब्दरचना असं काही तरी नक्की टाकून बघतील! जर पासवर्ड अवघड आणि युनिक असेल तर, हे एक अवघड कोडं सोडवण्यासारखं आहे - मशीन किंवा माणूस कोणीच सहज ओळखू शकणार नाही असं काही तरी. पुन्हा एकदा ट्राय कर.

हं खरंय! हा कसा वाटेल:
M3eRa!sB1rthd@y

वाह! जमलं की! आता मी माझ्या सगळ्या अकाऊंट्सना हाच पासवर्ड वापणार

नाही! अमित दादा म्हणाला होता की प्रत्येक अकाऊंट साठी एकच पासवर्ड ठेवणे म्हणजे तुमच्या घरासाठी, कारसाठी, आणि लॉकरसाठी एकच किल्ली असल्यासारखं आहे. जर हा कोणाला मिळाला तर ते सगळं अनलॉक करू शकतील. एक जरी ॲप हॅक झाला तर - तुझा पासवर्ड चुकीच्या हातात पडेल, आणि तुझ्या सगळ्या अकाउंट्स साठी धोका निर्माण होईल.

अरे नाही ! मी तर याचा विचारंच केला नव्हता. काय करू मग?

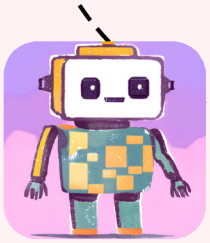
प्रत्येक अकाऊंट साठी युनिक ड पासवर्ड ठेव, तेच बरं राहील.

पण मग एवढं सगळं लक्षात पण ठेवायचं अवघड आहे ना. मी एक काम करते मी ते सगळे माझ्या डायरीमध्ये लिहून ठेवते.

अगं मी पण हेच करणार होतो, पण मग मी एक पासवर्ड मॅनेजर वापरायला सुरुवात केली. आणि हे जणू एक वरदानंच आहे अगं! आता मी फक्त एक मास्टर पासवर्ड लक्षात ठेवतो आणि मला माझे सगळे पासवर्ड्स बघता येतात. आणि जरी कोणी माझा पासवर्ड ओळखला, तरी मी 2-फॅक्टर ऑथेंटिकेशन एनेबल केले आहे, ज्यामुळे ते माझ्यापर्यंत पोहचूच शकत नाहीत! हे म्हणजे तुमच्या डिजिटल दरवाज्यावर दुसरं कुलूप लावण्यासारखंच झालं हाहाहहा!

ओह ! मला वाटलं एक स्ट्रॉंग पासवर्ड ठेवला तरी काम होईल, पण मला वाटतंय की जास्तं काळजी घ्यावी लागणार!

जास्तीत जास्त सुरक्षा असलेली कधीही चांगलीच. आणि हो ॲप्लिकेशन लॉक्स चेक आउट करायचे विसरू नको हं! चल, आता उशीर होतोय, केक कापायची वेळ झाली असेल की, मला खूप भूक लागली आहे!



मीराच्या अनुभवातून आपणही शिकूया आणि अगदी सुरुवातीपासूनच तुमचे अकाऊंट सुरक्षित असल्याचे सुनिश्चित करू. एखाद्या नवीन ॲप्लिकेशन साठी साईनअप करत असताना किंवा नवीन अकाऊंट बनवताना, स्ट्रॉंग पासवर्ड ठेवताना या महत्त्वाच्या गोष्टी नक्की पाळा:

स्ट्राँग पासवर्ड साठीची चेकलिस्ट

- मिक्स लेटर्स वापरा: कॅपिटल (ABC) आणि स्मॉल (abc) लेटर्स याचे कॉम्बिनेशन करून वापरा, अंक, आणि विशिष्ट चिन्ह (जसे की, @, #, $, !) यांचा देखील समावेश करा. यामुळे हॅकर्स साठी तुमचा पासवर्ड ओळखणं आणखीनच अवघड होतं.
- मोठा पासवर्ड ठेवा: जास्तीत जास्त सुरक्षेसाठी पासवर्ड किमान 12-16 अक्षरांचा असावा. मग कितीही विकसित साधनं वापरली तरी मोठा पासवर्ड ओळखणे जास्त अवघड आणि वेळखाऊ होते.
- सामान्यत: वापरले जाणारे शब्द आणि शब्दरचना टाळा: सहज ओळखत येणारे शब्द जसे “पासवर्ड”, “123456”, किंवा कोणतीही वैयक्तिक माहिती जी खूप लोकांना माहिती आहे, जसे की तुमचे नाव, तुमच्या पेटचे नाव, किंवा तुमचं एखादं आवडीची शब्दरचना हे सर्व पासवर्ड म्हणून वापरणे टाळा.
- सगळ्यांना माहिती असलेली तुमची वैयक्तिक माहिती टाळा: वाढदिवस, लग्नाचा वाढदिवस, किंवा फोन नंबर ही सर्व माहिती साधारणपणे लोकांना सोशल मीडिया द्वारे माहीत होऊ शकते, त्यामुळे हे पासवर्ड साठी वाईट पर्याय आहेत.
- पासफ्रेजचा वापर करा: लक्षात ठेवण्यासाठी सोपे एखादे वाक्य किंवा शब्दरचना घेऊन ते अवघड करण्यासाठी त्यामध्ये अंक मिसळून ते आणखीन अवघड बनवू शकता. जसे, “I love ice cream in summer!” हे वाक्य “IL0v3!c3Cr34m@2024.” अशाप्रकारे लिहून ते पासवर्ड म्हणून वापरू शकता.

पण याने काय फरक पडतो?

आजकाल, आपण अनेक अकाउंट्स वापरत असतो - सोशल मीडिया पासून ते ईमेल आणि बँकिंग पर्यंत. एक स्ट्रॉंग पासवर्ड सगळ्यात पहिली लक्ष्मणरेषा असते ज्यामुळे कोणीही तुमच्या परवानगी शिवाय तुमचे अकाऊंट वापरु शकणार नाही. पुन्हा वापरलेले किंवा वीक पासवर्डमुळे डेटा चोरीला जाऊ शकतो, आर्थिक नुकसान होऊ शकते, किंवा अगदी तुमची ओळख देखील चुकीच्या पद्धतीने वापरली जाऊ शकते. आपण या प्रकरणामध्ये पुढे या थ्रेट्स बद्दल आणखीन जास्त माहिती बघणार अहोतच. हॅकर्स पण आता हुशार आणि शिताफीने काम करू लागले आहेत, हे नियम पाळले तर तुमच्या अकाउंट्सची सुरक्षा वाढवण्यास नक्की मदत होईल.

2 फॅक्टर ऑथेंटिकेशन

2 फॅक्टर ऑथेंटिकेशन म्हणजे तुमच्या अकाऊंटचे दुसरे सुरक्षा कवच. अनेक प्रसिद्ध ऑनलाईन प्लॅटफॉर्म्स हे वापरण्याचे सुचवतात. जेव्हा तुमच्या अकाऊंट साठी हे फीचर ऑन केले जाते, तेव्हा लॉगिन करण्यासाठी पासवर्ड शिवाय आणखीन एक व्हेरिफिकेशन करावे लागते; बहुतेक वेळा हा कोड तुमच्या वैयक्तिक मोबाईल नंबर वर पाठवला जातो, जो एका वन टाईम पासवर्ड (OTP) चे काम करतो. हा ओटीपी पासकी, ईमेल, किंवा तुमचा फिंगरप्रिंट पण असू शकतो. याचा अर्थ असा होतो की हा कोड काही मिनिटातच आणि एकदाच वापरला जाऊ शकतो. पुढच्या वेळेस तुम्ही लॉगिन करताना पुन्हा दुसरा कोड म्हणजेच पासवर्ड येतो.

हे कसे काम करते:

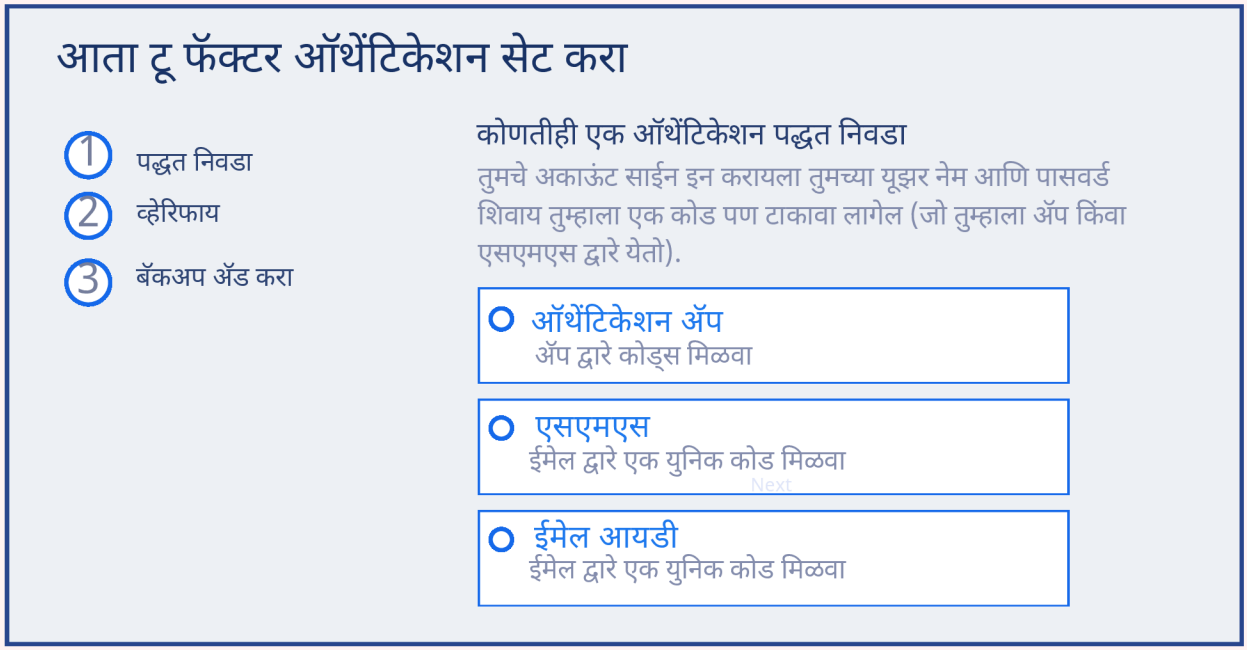
याचा सेट अप कसा करायचा:

1. नॅव्हिगेशन पॅनल मध्ये जा. तुम्हाला खालील प्रमाणे आयकॉन्स दिसतील:

2. सेटिंग्स पर्याय निवडा. बहुतेक वेळा हे असे दिसेल:

3. आता ‘सिक्युरिटी’ किंवा ‘प्रायव्हसी’ असे लिहिलेले शोधा

4. टू-फॅक्टर ऑथेंटिकेशन एनेबल करा. तुम्हाला व्हेरिफिकेशनच्या पद्धतींचे काही पर्याय दिसतील. तुम्ही एसएमएस, ॲप, किंवा फिंगरप्रिंट्स यातील एक पर्याय निवडू शकता.



पासवर्ड मॅनेजर्स

पासवर्ड मॅनेजर काय करतात?

1. पासवर्ड सुरक्षित ठेवतात: पासवर्ड मॅनेजर्स तुमचे पासवर्ड सुरक्षित ठेवून डिजिटल लॉकर्सचं काम करतात,
2. स्ट्रॉंग पासवर्ड जनरेट करतात: ते अगदी सहज एखादा अवघड, रँडम पासवर्ड तयार करतात, आणि तुम्ही वीक किंवा सोपा पासवर्ड पुन्हा वापरत नाही आहात ना हे सुनिश्चित करतात.
3. ऑटो-फिल क्रेडेंशीयल्स: अनेक पासवर्ड मॅनेजर्स तुमचे लॉगिन डीटेल्स आपोआप घेतात ज्यामुळे तुमचा वेळ वाचतो.

पासवर्ड मॅनेजर का वापरावा?

पासवर्ड मॅनेजरच्या मदतीने तुम्हाला एकापेक्षा जास्त, अवघड पासवर्ड लक्षात ठेवायची गरज नाही - एकच स्ट्रॉंग मास्टर पासवर्ड लक्षात ठेवायचा ज्याने तुमचे पासवर्ड मॅनेजर अनलॉक करायचे असते. आता तुमचे सगळे पासवर्ड लक्षात ठेवण्याचे कष्टच नाही, आणि पासवर्ड रीसेट करण्याचा ताप नाही!

पासवर्ड मॅनेजरच्या मदतीने तुम्हाला एकापेक्षा जास्त, अवघड पासवर्ड लक्षात ठेवायची गरज नाही - एकच स्ट्रॉंग मास्टर पासवर्ड लक्षात ठेवायचा ज्याने तुमचे पासवर्ड मॅनेजर अनलॉक करायचे असते. आता तुमचे सगळे पासवर्ड लक्षात ठेवण्याचे कष्टच नाही, आणि पासवर्ड रीसेट करण्याचा ताप नाही!

काही पासवर्ड मॅनेजर्स फसव्या वेबसाईट्स आणि इतर ऑनलाईन धोके ओळखू शकतात. ते तुम्हाला चुकून सुद्धा तुमचे क्रेडेंशीयल्स चुकीच्या पेजेस वर टाकू देत नाही.

ॲप्लिकेशन लॉक्स

काल रहीम माझ्याकडे एक वेगळाच प्रश्न घेऊन आला. त्याला कॉलनीमधल्या मित्र-मैत्रिणींना स्मार्टफोनचा वापर कसा करायचा हे शिकवायला आवडतं. पण, त्याच्या फोनमध्ये काही संवेदनशील माहिती आहे, उदाहरणार्थ प्रायव्हेट नोट्स, मित्र-मैत्रिणी आणि कुटुंबासोबतचे फोटोज, आणि काही पर्सनल मेसेजेस. त्याला त्याचा फोन शिकवण्यासाठी हेतूने वापरायचा आहे, परंतु त्याने हे सुनिश्चित केले पाहिजे की त्याच्या प्रायव्हसी आणि सुरक्षेशी तडजोड होणार नाही. मी त्याला सांगितलं: ॲप लॉक्स वापर म्हणून!

ॲप लॉक्स काही विशिष्ट ॲप्ससाठी पासवर्ड, पिन, किंवा बायोमॅट्रिक ॲक्सेसच्या मदतीने फोनची सुरक्षा वाढवतात. अशा प्रकारे तुम्ही तुमचा फोन सुरक्षित पद्धतीने एखाद्याला देऊ शकता:

ॲप लॉक डाऊनलोड करा

एक सिक्युअर पिन सेटअप करा

ज्या ॲप्लिकेशन्स लॉक करायच्या आहेत त्या निवडा

बायोमॅट्रिक व्हेरिफिकेशन एनेबल करा

ॲप लॉकचे फायदे

- प्रायव्हसी बाबत सुरक्षा: रहीमचा फोन जरी दुसरं कोणी वापरत असेल तरी त्याची संवेदनशील माहिती सुरक्षित राहते.
- कस्टमायझेबल: नेमक्या कोणत्या ॲप्स लॉक करायच्या आहेत ते तो निवडू शकतो.
- वापरायला अगदी सोपं: एकदा सेटअप केला की ॲप लॉक्स अगदी सोप्या पद्धतीने आणि सहजतेने वापरता येतात.

नेहमी लक्षात ठेव, घातक सॉफ्टवेअर्स टाळण्यासाठी ऑफिशियल स्टोअर्स मधून व्हेरिफाईड ॲप्सच डाऊनलोड कर, आणि ॲप लॉक्स साठी स्ट्रॉंग पिन वापर. जास्तीत जास्त सुरक्षेसाठी तुझ्या महत्त्वाच्या गोष्टींना डबल आणि ट्रिपल लॉक लाव.

ॲक्टिव्हिटी

तुमची स्मरणशक्ती तपासू या

(I) पासवर्ड मॅनेजरचा सर्वात महत्त्वाचा हेतू काय आहे?
a) तुमचे सगळे पासवर्ड्स सुरक्षित पद्धतीने स्टोअर आणि ऑर्गनाइझ करतो.
b) तुम्ही 5 मिनिट इनॲक्टिव्ह असल्यास तुम्हाला आपोआप लॉग आऊट करतो.
c) नवीन अकाउंट्स साठी यूझरनेम्स जनरेट करतो.
d) तुम्ही खूप काळ वापरत नसलेले अकाउंट्स आपोआप डिलीट करतो.

(II) कितीही स्ट्रॉंग दिसत असले तरी यापैकी कोणते पासवर्ड्स सगळ्यात कमी सुरक्षित आहेत?
"Password@123!"
"xT#4jG!@oLmN$z"
"MySecureP@ss2024!"
"E!3xy&7#M@n2023"

(III) एक स्ट्रॉंग पासवर्डसाठी खालील फीचर्स पैकी कोणत्या फीचरची शिफारस केली जात नाही?
a) किमान 8-12 कॅरेक्टर्सचे असावे.
b) त्यामध्ये तुमचे पूर्ण नाव किंवा जन्म वर्ष असावे.
(कारण: वैयक्तिक माहितीमुळे पासवर्डचा अंदाज लावणे सोपे जाते.)
c) कॅपिटल लेटर्स, स्मॉल लेटर्स, अंक, आणि चिन्ह असावेत.
d) सहज ओळखत येणारे क्रम जसे “123456” नसावेत.

(IV) आपण टू-फॅक्टर व्हेरिफिकेशन का एनेबल करावे (2FA)?
a) पटकन लॉगिन करता येण्यासाठी
b) तुमच्या अकाऊंटला सुरक्षेचे आणखीन एक कवच देण्यासाठी
c) दर महिन्याला तुमचा पासवर्ड अपडेट करण्यासाठी.
d) कोणालाही तुमचे अकाऊंट ॲक्सेस करता यावे यासाठी

उत्तर:

(I) a) तुमचे सगळे पासवर्ड्स सुरक्षितपणे स्टोअर आणि ऑर्गनाइझ करण्यासाठी
(II) a) "Password@123!"
(कारण: यामध्ये खूप सोपा शब्द आहे “पासवर्ड” आणि पॅटर्न पण सहज ओळखता येण्यासारखा आहे.)
(III) b) त्यामध्ये तुमचे पूर्ण नाव किंवा जन्म वर्ष असावे.
(कारण: पर्सनल माहिती असलेला पासवर्ड ओळखणे खूप सोपे असते.)
(IV) b) तुमच्या अकाऊंटला सुरक्षेचे आणखीन एक कवच देण्यासाठी

सुरक्षेसंबंधी धोके समजून घेऊया

रहीम दुपारच्या उन्हात जवळच्या बागेत बसला होता, नुकतेच त्याचे काही बोर्ड गेम्स खेळून झाले होते आणि आता नवीन काही तरी चॅलेंज हवं होतं त्याला! तेवढ्यात त्याला त्याचे मित्र जसप्रीत आणि अमित दादा दिसतात आणि तो त्यांच्या जवळ जाऊन बसतो. जसप्रीत आणि रहीमने काही चॅलेंजिंग वर्ड पझल्स असलेल्या नवीन वेबसाईट्स शोधण्यासाठी अमित दादाचा फोन घेतला.

तितक्यात, स्क्रीनवर हा मेसेज पॉपअप झाला!

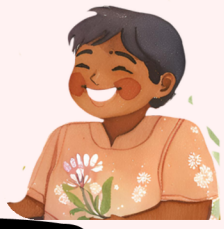
अभिनंदन! तुम्ही 1,000 फ्री गेम कॉईन्स जिंकले आहात! हे बक्षिस मिळवण्यासाठी तुमचा फोन नंबर आणि ओटीपी सह या मेसेजला रिप्लाय करा.

रहीमला एवढे कॉईन्स मिळाल्याचा खूप आनंद होतो, पण त्याला हे कळत नव्हते की मेसेजवर क्लिक करावं की नाही, आणि ते दोघं मिळून ठरवतात की हा मेसेज उघडायचा नाही.

हा मेसेज अधिकृत स्रोताकडून आलेला नाही आणि तो आपली वैयक्तिक माहिती मागत आहे — मला वाटतं हा स्कॅम असू शकतो! स्कॅमर्स अशा प्रकारच्या मेसेजेसद्वारे आपला डेटा, पैसे किंवा डिव्हाइस चोरण्यासाठी नवनवीन मार्ग शोधत असतात. आपण ऑनलाईन धोके पुन्हा एकदा समजून घेऊया का, म्हणजे आपण सुरक्षित राहू शकू!

अरे हो! माझा विश्वासच बसत नाहीये की एवढे पासवर्ड्स आणि सुरक्षा उपाय वापरून सुद्धा मला फसवलं जाऊ शकतं! मला संपूर्णपणे सतर्क राहायला हवं, जेणेकरून मी स्वत:ला आणि इतरांना देखील मदत करू शकेन.

तर आता आपण हॅकिंग बद्दल जाणून घेऊ! हॅकर्स पासवर्ड्स किंवा बँकेची माहिती असा तुमचा डेटा बघण्याचा प्रयत्नकरतात आणि तुमच्या नकळत ती चोरण्याचा प्रयत्न करतात.



हो, माझ्या चुलत भावाचे अकाउंट गेल्या वर्षी हॅक झाले होते! तेव्हापासून माझ्या कुटुंबातील प्रत्येकजण अनेक पासवर्ड आणि लॉक वापरतो.

हॅकिंग

हॅकिंग म्हणजे एखाद्याच्या परवानगीशिवाय त्याच्या फोन, कम्प्युटर, किंवा ऑनलाईन अकाऊंटमध्ये हस्तक्षेप करणे! माहिती चोरण्यासाठी किंवा नुकसान करण्यासाठी हॅकर्स जुने पासवर्ड्स आणि सिक्युरिटी माहिती जाणून घेण्यासाठी ॲडव्हान्स्ड कोड्सचा वापर करतात. हॅकर्स तुमची प्रायव्हेट माहिती चोरतात, नुकसान करू शकतात, किंवा संपूर्ण डिव्हाईसवर नियंत्रण मिळवू शकतात. काही हॅकर्स हे अवैध कारणांसाठी करतात, तर काही (ज्यांना वैध हॅकर्स म्हणतात) सिक्युरिटी वीकनेसेस शोधून त्या दुरुस्त करतात. बऱ्याचदा हॅकर्स तुमची डिव्हाईस हॅक करण्यासाठी मालवेअरचा (चुकीच्या हेतूने बनवलेले असे कम्प्युटर सॉफ्टवेअर किंवा व्हायरस जे तुमच्या नकळत तुमच्या कम्प्युटर किंवा कम्प्युटर नेटवर्कचे नुकसान करते) वापर करतात!

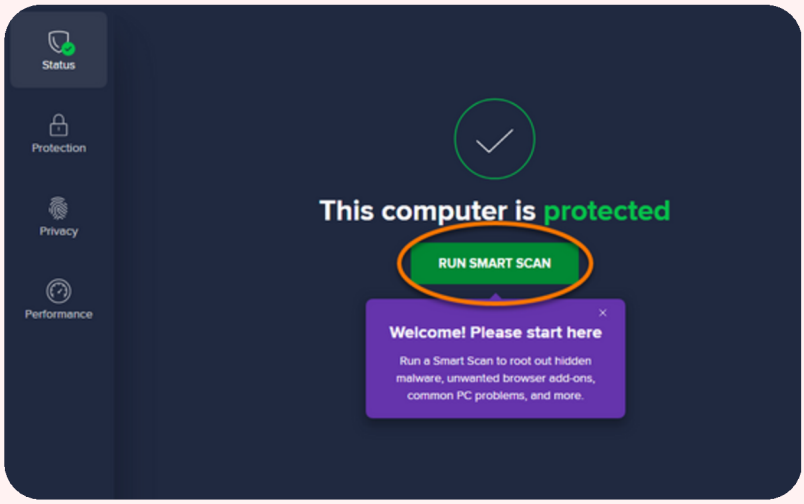
कल्पना कर, तुझ्या मित्राच्या डायरीला एक खास कुलूप आहे, पण तो ती डायरी उघडताना तू लक्षपूर्वक पाहून त्या कुलूपाचा कोड ओळखतोस. नंतर तोच कोड वापरून तू चोरीछुपट्यानं ती डायरी उघडून त्याच्या खाजगी भावना वाचतोस. हॅकिंग हेसुद्धा तसंच असतं — फक्त डायरीऐवजी हे कम्प्युटर, फोन किंवा ऑनलाईन अकाऊंटसह घडतं!

टीप: ॲंटीव्हायरस सॉफ्टवेअर वापरा आणि डिव्हाईसेस अपडेट करत रहा

ॲंटीव्हायरस सॉफ्टवेअर तुमच्या कम्प्युटरमधून व्हायरसेस आणि इतर घातक सॉफ्टवेअर्स शोधून ते काढून टाकण्यासाठी बनवलेले असते. तुमच्या कम्प्युटरमध्ये ॲंटीव्हायरस सॉफ्टवेअर इन्स्टॉल करा, तुमच्या डिव्हाइसचे फायरवॉल ऑन आहे याची खात्री करा, आणि तुमच्या डिव्हाइसमध्ये असलेले बग्स किंवा सिक्युरिटी होल्स — ज्याद्वारे हॅकर्स तुमच्या डिव्हाइसमध्ये शिरकाव करू शकतात — दुरुस्त करण्यासाठी डिव्हाइस वेळोवेळी अपडेट करत रहा.

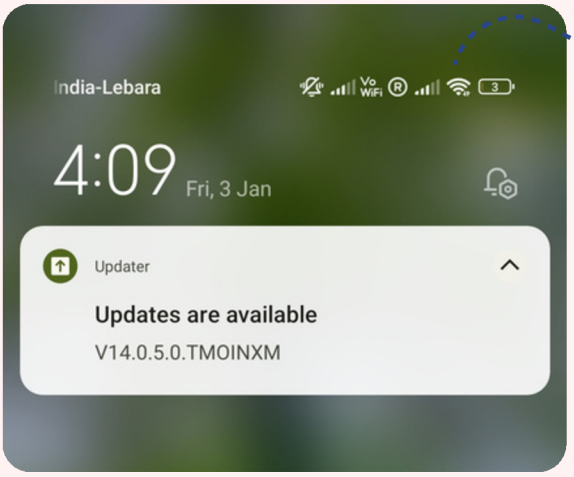
1

एक विश्वसनीय ॲंटीव्हायरस सॉफ्टवेअर कसे इन्स्टॉल करायचे आणि वापरायचे हे या फोटोमध्ये तुम्हाला दिसते. तुम्ही अनेक पर्यायांमधून याची निवड करू शकता, आणि मोठ्यांच्या सल्ल्याने किंवा फक्त वेब सर्चच्या मदतीने योग्य निर्णय घेऊ शकता!



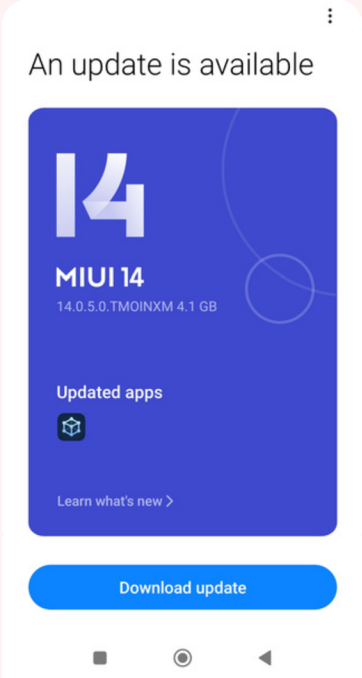
2

जेव्हा तुमच्या फोन मध्ये एखादा अपडेट उपलब्ध असेल, तेव्हा तुम्हाला असे नोटिफिकेशन येईल:



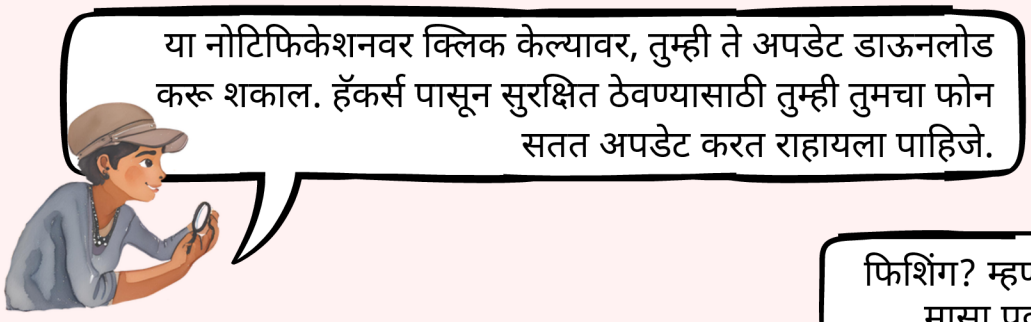
या नोटिफिकेशनवर क्लिक केल्यावर, तुम्ही ते अपडेट डाऊनलोड करू शकाल. हॅकर्स पासून सुरक्षित ठेवण्यासाठी तुम्ही तुमचा फोन सतत अपडेट करत राहायला पाहिजे.

3



ॲक्टिव्हिटी

जेव्हा तुमच्या फोन मध्ये एखादा अपडेट उपलब्ध असेल, तेव्हा तुम्हाला असे नोटिफिकेशन येईल:

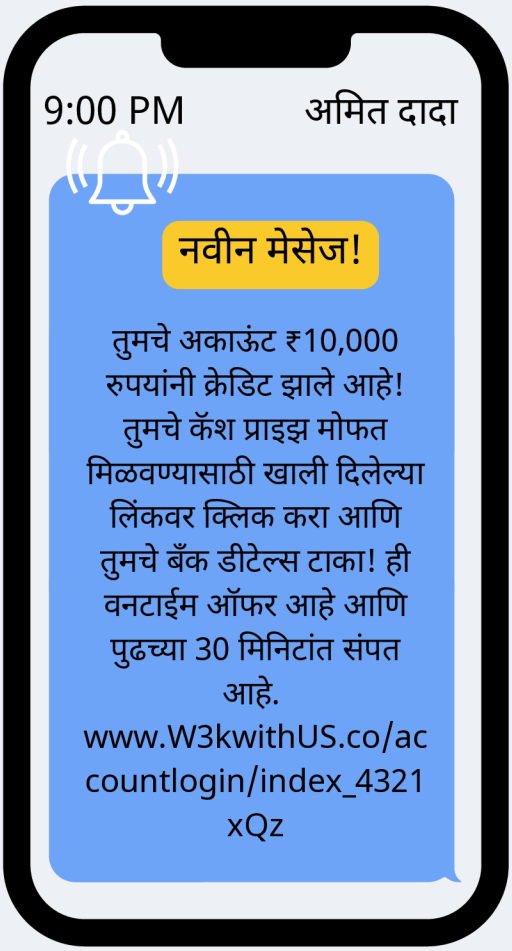


वेल, तसंच काहीसं! याला तुम्ही असे समजू शकता की कोणीतरी तुमची पर्सनल माहिती चोरून-चोरून काढून घेण्याचा प्रयत्न करत आहे, कधी खोटी ओळख सांगून किंवा तुमची बँक, शाळा किंवा आवडीचा व्हिडिओ गेम असल्याची बतावणी करून! आपल्याला आत्ता आलेला मेसेज हा फिशिंगचे उत्तम उदाहरण आहे.

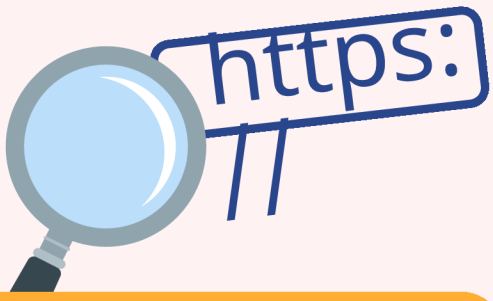
फिशिंग

फिशिंग ही एक चोरी करण्याची अशी पद्धत आहे ज्यामध्ये स्कॅमर्स अगदी ऑफिशियल वाटणारे असे खोटे मेसेजेसपाठवतात! या मेसेजेस मध्ये बऱ्याचदा काही तरी अर्जंट असल्याचे भासवले जाते, उदाहरणार्थ , “जर तुम्ही लगेच व्हेरिफाय केले नाही तर तुमचे अकाऊंट डिलीट केले जाईल!” जेणेकरून आपण घाबरून पटकन त्या लिंकवर क्लिक करू किंवा पासवर्ड्स किंवा क्रेडिट कार्ड नंबर्स यासारखी संवेदनशील माहिती लिहून पाठवू. मग ही माहिती थेट स्कॅमरकडे पोहोचते. चला आपण फिशिंगचं एक उदाहरण बघूया.

या मेसेजची अर्जन्सी बघा, यातील सगळ्यात शेवटची फेक लिंक बघा, आणि हे ही बघा की मेसेज मध्ये संवेदनशील माहिती विचारली आहे का - ही सगळी धोक्याची ही घंटा आहे! बँकिंगसंबंधी माहिती विचारण्याऱ्या मेसेजेस पासून तुम्ही नेहमी सावध राहायला हवं.



टीप: लिंक बघा!!



जर तुम्हाला एखाद्या अनपेक्षित सोर्स कडून लिंक आली, किंवा ती लिंक चुकीची वाटते आहे, किंवा त्यासोबत आकर्षक मेसेज असेल, थांबा.. कधी-कधी, अनोळखी लिंक्स तुमची माहिती चोरू शकतात किंवा तुमच्या डिव्हाईस मध्ये घातक व्हायरसेस डाऊनलोड करू शकतात.

खाली काही गाईड लाईन्स दिलेल्या आहेत ज्या तुम्हाला घातक लिंक्स पासून लांब राहण्यात मदत करतात आणि तुम्ही एका सुरक्षित, विश्वसनीय वेबसाईट वर आहात हे सुनिश्चित करतात.

- तुम्ही ब्राऊझर मध्ये टाईप केलेल्या वेबसाईटची लिंक बघा, त्याची सुरुवात “https” ने होते आहे हे सुनिश्चित करा. यातील “S” म्हणजे इंग्रजीतील “Secure” आणि त्याचबरोबर ही साईट तुमचा डेटा सुरक्षित करण्यासाठी एंक्रिप्शनचा वापर करते हे देखील दर्शवतो.

- कोणत्याही लिंकचा शेवट “.com” “.org” “.gov” “.in” or “.edu.in” ने होतो आहे हे सुनिश्चित करा - ही काही विशिष्ट नावं आहेत

- पूर्ण वेबसाईट बघा - त्यातला अबाऊट सेक्शन तर नक्की बघा - ती वेबसाईट कोणी बनवली आहे आणि कोणी डिझाईन केली आहे हे बघण्यासाठी.

- ही साईट एखाद्या विश्वस्त साईटचे खोटे किंवा फसवे रूप नाही ना हे जाणून घेण्यासाठी URL दोनदा नीट तपासून घ्या. जसे की, "amaz0n.com" ही एक खोटी साईट आहे जी "amazon.com." ची नक्कल करण्यासाठी बनवली आहे.

- एखादा प्लॅटफॉर्म वैध आणि इतर यूझर्सचा देखील त्यावर विश्वास आहे हे जाणून घेण्यासाठी त्याबद्दल ऑनलाईन रिव्ह्यू वाचा.

जर तुम्ही चुकूनही एखाद्या अविश्वसनीय पॉप-अप, ॲड किंवा इतर फसव्या घटकावर क्लिक केलं, तर ॲड ब्लॉकर्स — नावाप्रमाणेच — हे पॉप-अप्स, ॲड्स आणि अशा अविश्वसनीय घटकांना ब्लॉक करतात. उदाहरणार्थ, तुम्ही उजवीकडे बघू शकता की ही वेबसाईट तुम्हाला ॲड ब्लॉकर बंद करायला सांगत आहे — म्हणजेच हे काहीतरी संशयास्पद आणि संभाव्यतः धोकादायक असू शकतं.

ॲक्टिव्हिटी

तुम्ही ॲड ब्लॉकर वापरता का? तुमच्या ब्राऊझरवर एक एक्सटेंशन म्हणून एक विश्वसनीय ॲड ब्लॉकर इन्स्टॉल करून बघा!

फिशिंग जरा भयानकच वाटतं! हे हॅकर्स आणि “फिशर्स” या सगळ्या महितीचं नक्की करतात तरी काय?

ही सगळी गोळा केलेली माहिती ते ऑनलाईन वेश बदलण्यासाठी वापरतात. ते अकाउंट्स बनवतात, तुमच्या बँकेतून पैसे काढून घेऊ शकतात, आणि तुमच्या नावाखाली अगदी लोन देखील घेऊ शकतात! याला आयडेंटिटी थेफ्ट असे म्हणतात.

आयडेंटिटी थेफ्ट

जेव्हा एखादी व्यक्ति तुमचे नाव, पत्ता, किंवा आधार कार्ड नंबर वापरुन ती व्यक्ति तुम्हीच आहात असे भासवण्याचा प्रयत्न करते तेव्हा त्याला आयडेंटिटी थेफ्ट असे म्हणतात. हे सगळं ते अकाउंट्स ओपन करण्यासाठी, ऑनलाईन शॉपिंग साठी, किंवा काही अनैतिक कृत्य करून ते तुम्हीच केले असे ही भासवतात, अशी कृत्ये करण्यासाठी वापरतात. यामुळे खूप मोठ्या अडचणी येवू शकतात, उदाहरणार्थ तुम्ही न केलेल्या गुन्ह्यांसाठी तुम्हाला दोषी मानणे किंवा तुमच्याच ॲक्सेसचा ॲक्सेस गमावणे. खाली काही उदाहरणे बघूया!

समजा कोणाला तरी तुमचा हरवलेले स्कूल आयडी सापडले आणि तुमचा रोल नंबर वापरुन ते तुम्हीच आहात असे भासवून तुमच्या परीक्षेचे पेपर करतात. तुमचे शिक्षक देखील त्यांच्यावर विश्वास ठेवतात कारण त्यांना असे वाटतं की ते तुम्हीच आहात - आता ते तुमच्या परीक्षेचे मार्क बघू शकतात.

समजा कोणाला एका किराणा मालाच्या दुकानाबाहेर एखादं हरवलेलं वॉलेट सापडलं. ते परत करण्याऐवजी ते त्या व्यक्तीच्या आयडी कार्ड्स वरून त्याचे नाव, वय, आणि पत्ता वापरुन क्रेडिटकार्ड साठी अप्लाय करतात. त्या क्रेडिट कार्ड वरून ते महागड्या वस्तू खरेदी करायला सुरुवात करतात, आणि मग त्याचं बिल येतं, जे त्या वॉलेट मालकाला जातं, अश्या खर्चासाठी जो त्यांनी कधी केलाच नाही!

चला समजूया की जर कुणी या पद्धती वापरून माझी ओळख, माहिती आणि डेटा चोरण्यात यशस्वी झालं... तर ते या सगळ्याचा आणखी काय वापर करू शकतात?

दुर्दैवाने, ते तुमचा डेटा विकू देखील शकतात, त्याचा गैरवापर करू शकतात आणि काही लोकांच्या ग्रूपला टार्गेट करण्यासाठी देखील वापरू शकतात. यालाच डेटा थेफ्ट असे म्हणतात.

डेटा थेफ्ट

तुमच्या परवानगी शिवाय डिजिटल माहिती उदाहरणार्थ पासवर्ड्स, बँक डीटेल्स, किंवा मेडिकल रेकॉर्ड्सचोरणे हे सगळे डेटा थेफ्टचे प्रकार आहेत. हा डेटा नंतर विकला जाऊ शकतो किंवा पुढील गुन्हे करण्यासाठी वापरला जाऊ शकतो! बिझनेसेस बऱ्याचवेळा टार्गेट केले जातात कारण त्यांच्याकडे मोठ्ठ्या प्रमाणात कस्टमर्सची माहिती उपलब्ध असते, पण कधी-कधी आपल्यासारखी लोकं देखील याला बळी पडू शकतात.

मला वाटतंय की आता सगळं कोडं जरा सुटत चाललंय असं वाटायला लागलंय! पण अजूनही मला हे समजत नाहीये की हे सगळं ते चोरतात का?

चला अमित दादाला याबद्दल आणखीन विचारूया!

तुम्ही दोघंही खूप हुशार आहात! हॅकिंग, फिशिंग, आणि डेटा आणि आयडेंटिटी थेफ्ट या सर्व ॲक्टिव्हिटीज कडे खूप गांभीर्याने पाहायला हवं, कारण हे सर्व अनेकदा आर्थिक फसवणूक करण्यासाठी केलं जातं. तुमचे पैसे चोरले जातात किंवा तुमची आर्थिक माहिती चोरली जाते तेव्हा हे नुकसान घडतं. ही फसवणूक ऑनलाईन किंवा व्यक्तीगत स्वरूपात देखील होऊ शकते आणि बऱ्याचदा झालेले नुकसान भरून काढता येत नाही. म्हणूनच आपण नेहमीच सावध राहायला हवं. तुम्ही स्वतःला आणखी जास्त सुरक्षित ठेवू शकाल यासाठी खाली काही आर्थिक फसवणूकीची उदाहरणे दिली आहेत - मागच्याच आठवड्यात माझ्या बहिणीच्या बाबतीत हे घडलं होतं!

हॅलो मॅम. मी जिल्हा विद्युत मंडळामधून सुरेश बोलतो आहे. हा खूप महत्त्वाचा कॉल आहे. आमच्या रेकॉर्ड्स प्रमाणे, तुमचे मागच्या महिन्याचे विजेचे बिल भरले गेलेले नाही, आणि तुमचे कनेक्शनधोक्यात आहे आणि पुढच्या दोन तासात ते कट केले जाऊ शकते.

काय? मी गेल्या आठवड्यातच माझं बिल भरलं होतं! नक्कीच काहीतरी चूक झाली असावी.

मी तुमची काळजी समजू शकतो, पण आम्हाला अजूनही पेमेंट संदर्भात कोणतेही कन्फर्मेशन आलेले नाही. कनेक्शन कट होणे टाळण्यासाठी, मी असे सुचवेन की तुम्ही लगेचच तुमचे थकेलेले ₹2,500 रुपयांचे बिल भरावे. काळजी करू नका, मी फोनवरच याबद्दल तुमचे मार्गदर्शन करेन.

मला काय करावं लागेल?

तुमच्या फोनमध्ये तुमचं बँकिंग ॲप उघडा, आणि मी तुम्हाला पेमेंट करण्यासाठी एक सुरक्षित लिंक पाठवेन. आणि हो, कोणतीही अडचण टाळण्यासाठी तुम्ही हे 5 मिनिटांत पूर्ण कराल याची खात्री करा.

अमित दादाची बहीण लिंकवर क्लिक करते, ज्यामुळे ती एका बनावट पेजवर जाते.. आणि पुन्हा एकदा बिल भरते, ते ही एका अनोळखी व्यक्तीला!

या संवादात तुम्हाला दोघांना काही संशयास्पद संकेत दिसले का? ही काही धोक्याची लक्षणे आहेत जी तुम्ही लक्षपूर्वक टिपायला हवीत:

अर्जन्सी आणि घाबरवणे:
त्या कॉलरने कोणताही विचार न करता कृती करण्यासाठी समोरच्या व्यक्तीवर दबाव निर्माण केला.

अनोळखी व्यक्ति:
कॉलर अधिकारी असल्याचे सांगतो पण कोणताही पुरावा सादर करत नाही.

असामान्य पेमेंट पद्धती
वैध कंपन्या क्वचितच पर्सनल अकाउंट्स मधून किंवा असुरक्षित लिंक्स वरून तत्काळ पेमेंट करण्याच्या पद्धतींबद्दल सुचवतात.

फसव्या लिंक:
कॉलर बनावटी लिंक पाठवतो जी अगदी ऑफिशियल लिंक सारखीच दिसते.

तुमची ऑनलाईन शॉपिंग सुरक्षेची चेकलिस्ट

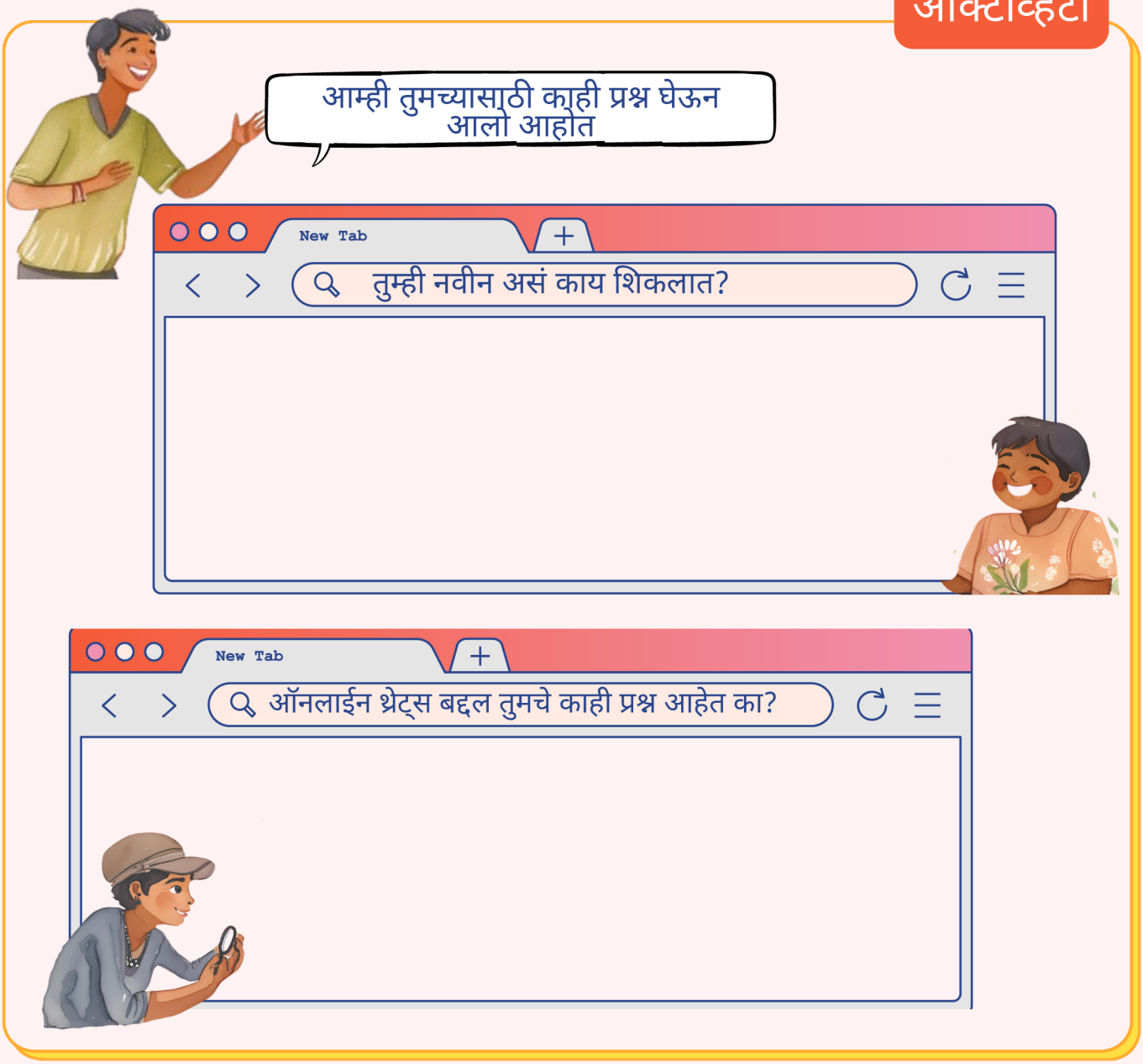
- ☐ रिव्ह्यूज तपासा आणि इतर ग्राहक त्या उत्पादनाबद्दल काय म्हणत आहेत ते बघा. बनावट रिव्ह्यूज किंवा संशयास्पद मजकुराबाबत सावध रहा.
- ☐ साईट सुरक्षित आहे आणि सुरुवातीला 'https://' आणि लॉक आहे हे सुनिश्चित करा.
- ☐ प्रॉडक्टचा आकार, रंग, आणि वैशिष्ट्ये दोन-दोन वेळा तपासून घ्या आणि हे प्रॉडक्ट तुम्हाला हवे आहे तेच आहे ना हे सुनिश्चित करा.
- ☐ ती साईट तुम्हाला पासवर्ड्स किंवा बँक डीटेल्स विचारत आहे का? खऱ्या शॉपिंग साईट्स तुम्हाला कॉल, ई -मेल किंवा मेसेजवर कधीही नाही विचारणार!
- ☐ पेमेंट गेटवे सुरक्षित असल्याचे सुनिश्चित करा आणि ओटीपी, कार्ड डीटेल्स आणि सीसीटीव्ही कोड्स संशयास्पद वेबसाईट्सवर शेअर करणे टाळा.
- ☐ ऑर्डर संबंधी आलेले मेसेजेस खरे असल्याचे सुनिश्चित करा - : तुम्ही ऑर्डर न केलेले प्रॉडक्ट्स, लॉटरीज, संवेदनशील माहिती, किंवा स्पेलिंगच्या चुका सामान्यतः त्यामध्ये नसाव्यात.
- ☐ जर तुम्हाला पाठवण्यात आलेले प्रॉडक्ट तुमच्या अपेक्षेप्रमाणे वेगळे असेल तर काय हे जाणून घेण्यासाठी यासंबंधित नियम व अटी आणि रीफंड पॉलिसी वाचायला विसरू नका.

तुम्हाला माहिती आहे का?

Amazon वर, तुम्ही फिशिंग हल्ले, संशयास्पद कॉल/ईमेल/संदेश किंवा असुरक्षित/संशयास्पद उत्पादनांची तक्रार करू शकता. Amazon च्या 'मदत' विभागात यासाठी एक वेगळा पर्याय आहे.

- "रिपोर्ट समथिंग सस्पीशियस" याठिकाणी जा आणि दिलेल्या पर्यायांमधून निवड करा. संबंधित माहिती सह रिपोर्ट सबमिट करा. संशयास्पद ई-मेल/टेक्स्ट reportascam@amazon.in या मेल आयडी वर पाठवा.
- तुमच्याकडे आलेले संशयास्पद पॅकेजेस त्याचा बॉक्स नीट तपासून आणि त्याची माहिती सबमिट करून हे "अनसॉलिसिटेड पॅकेजेस रिसीव्हड" या सदराखाली नोंदवा.
- "या उत्पादन किंवा विक्रेत्याशी संबंधित समस्येची तक्रार करा" वर क्लिक करून आणि खालील सूचनांचे पालन करून थेट उत्पादन पृष्ठावरून विक्रेत्यांची किंवा उत्पादनांची तक्रार करा.
- ॲमेझॉन कडून खालील काही सामान्य स्कॅम्स समोर आणले गेले आहेत.

ॲक्टिव्हिटी



New Tab

तुम्ही ही साधने ऑनलाईन शोधू शकता का?

तीन विश्वसनीय ॲंटी-व्हायरस सॉफ्टवेअर्स:

1.
2.
3.

तीन विश्वसनीय आणि मोफत ॲड ब्लॉकर्स:

1.
2.
3.

रीकॅप: स्वतःला सुरक्षित ठेवण्यासाठी लक्षात ठेवण्यासारख्या गोष्टी!

लक्षात ठेवा, काहीही संशयास्पद आढळले, तर तुम्ही लगेच तुमच्या पालकांशी, शिक्षकांशी, किंवा तुमच्या विश्वासातल्या वयाने मोठ्या व्यक्तींशी बोलायला हवे.

स्ट्रॉंग पासवर्ड

ओळखायला अवघड असणार पासवर्ड ठेवा, ज्यामध्ये अक्षरं, अंक, आणि विशिष्ट चिन्हांचा समावेश असेल! नाव, पाळीव प्राण्याचे नाव, किंवा “12345” असे सोपे पासवर्ड ठेवू नका ठेवू. जर तुम्ही शेअर्ड डिव्हाईसेज वापरत असाल, तर तिथून प्रत्येक वेळी लॉग आऊट करायचे विसरू नका.

दुप्पट सुरक्षा

तुमच्या अकाउंट्स वर जास्तीचे सुरक्षा कवच लावण्यासाठी 2 फॅक्टर ऑथेंटिकेशन वापरा ! यामुळे जरी एखाद्या व्यक्तीला तुमचा पासवर्ड कळलाच तरी त्यांना तुमच्या डिव्हाईसेज किंवा अकाउंट्स मध्ये शिरकाव करण्यासाठी अजून एक कोड आवश्यक असेल. कोणत्याही अकाऊंटच्या सेटिंग्स मध्ये प्रायव्हसी अँड सिक्युरिटी या अंतर्गत तुम्ही हा व्हेरिफिकेशन कोड सेट करू शकता.

क्लिक करण्याआधीविचार करा!

ई-मेल्स किंवा मेसेजेस मधल्या कोणत्याही लिंक्स सुरक्षित आहेत हे सुनिश्चित केल्याशिवाय त्यावर क्लिक करू नका. जर काही संशयास्पद आढळलं तर लगेच कंपनी किंवा थेट त्या व्यक्तीशी संपर्क साधून खात्री करा. ईमेल्स, अनोळखी व्यक्तींकडून आलेले मेसेजेस, किंवा तत्काळ पैशाची मागणी करणारे मेसेजेस यामध्ये स्पेलिंगच्या चुका देखील तपासून बघा.

पुनरावलोकन: स्वत:ला सुरक्षित ठेवण्यासाठी लक्षात ठेवायच्या गोष्टी!

ॲड ब्लॉकर्स

ॲड ब्लॉकर्स म्हणजे सॉफ्टवेअर टूल्स किंवा ब्राऊझर एक्सटेंशन्स असतात ज्यांचा उपयोग वेबसाईट वरील जाहिराती तसेच पॉप-अप्स, बनर्स, आणि व्हिडिओ ॲड्स काढण्यासाठी किंवा ब्लॉक करण्यासाठी केला जातो. ॲड्स लोड न होऊ दिल्यामुळे ब्राऊझिंगचा स्पीड वाढतो, डेटा युसेज कमी होतो, आणि फसव्या ॲड्स ज्या घातक असू शकतात, त्यांच्या पासून सुरक्षा देखील मिळते.

शक्यतो पब्लिक वाय-फाय वापरू नका आणि ब्लूटूथ बंद ठेवा

पब्लिक वाय-फाय किंवा ब्लूटूथ चालू ठेवल्याने बाहेरील दुष्ट घटकांसाठी तुमचा डेटा खुला होऊ शकतो. प्रायव्हेट, सुरक्षित नेटवर्कच वापरा आणि वापरत नसाल तेव्हा ब्लूटूथ बंद ठेवा.

ऑनलाईन काही शेअर करताना सावध रहा

तुमचे पूर्ण नाव, पत्ता, फोन नंबर किंवा शाळेचे नाव यासारखी वैयक्तिक माहिती सोशल मीडियावर शेअर करणे टाळा! तुमचे प्रोफाइल, पोस्ट आणि संदेश कोण पाहू शकते हे नियंत्रित करण्यासाठी सोशल मीडिया आणि गेमवरील गोपनीयता सेटिंग्ज वापरा. लवकरच, आम्ही ते कसे करायचे ते शोधू!

अँटीव्हायरस सॉफ्टवेअर वापरा आणि डिव्हाईस अपडेट करत रहा

अँटीव्हायरस सॉफ्टवेअर इन्स्टॉल करा आणि तुमच्या डिव्हाईसचं फायरवॉल ऑन ठेवा. घातक सॉफ्टवेअर आणि व्हायरसेस जे हॅकर्स तुमची माहिती चोरण्यासाठी वापरतात, त्यांना ओळखून ब्लॉक करण्यात हे टूल्स मदत करतात. तुमच्या डिव्हाइसमध्ये असलेले बग्स किंवा सिक्युरिटी होल्स — ज्याद्वारे हॅकर्स शिरकाव करू शकतात — ते दुरुस्त करण्यासाठी डिव्हाईस वेळोवेळी अपडेट करत राहा.

तुमच्या डेटाचा बॅकअप घेत रहा

महत्त्वाच्या फाईल्स किंवा फोटोंच्या कॉपीज वेळोवेळी एखाद्या बाह्य हार्ड ड्राईव्ह किंवा क्लाउड सर्व्हिसमध्ये सेव्ह करत रहा. कधी तुमचं डिव्हाईस हॅक झालं किंवा त्यात व्हायरस आला, तरी तुमचं कोणतंही नुकसान होणार नाही.

प्रकरण 3: प्रायव्हसी - तुमचे डिजिटल कवच!

एकदा सकाळी-सकाळी मीरा, रहीम, आणि सुजान बागेत गप्पा मारत बसले होते, मजा-मस्ती करत करत सेल्फी काढणे पण सुरू होते. मीराला त्यांचा एक फोटो खूप आवडला. ती लगेच तो अपलोड करते आणि सगळ्यांना टॅग करून लोकेशन देखील टाकते.

अगं थांब मीरा, तू मला टॅग केलंस आणि लोकेशन पण टाकलंस? मला हे जरा पटलेलं नाही बघ.

अरे का? काय झालं? तेवढीच जरा मजा. आता लोकेशन टॅग करण्यामध्ये काय चुकीचे आहे.

मला त्यामुळे असुरक्षित वाटतं ग. आपण कुठे आहोत हे शेअर करणे जोखमीचे आहे. तू आधी विचारायला हवं होतंस!

सगळे जण असे फोटो टाकतंच असतात. रहीम, काही होणार नाही तू बिनधास्त रहा रे.

अगं प्रश्न तो नाहीये! आता हिला मी कसं समजावू....

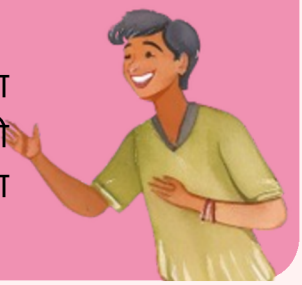
रहीम, मीराला यात समस्या काय आहे हे समजावू शकेल अशा कोणा व्यक्तीकडे आपण जायचं का? अमित दादाकडे जाऊया चल!

अरे हलो सगळ्यांना! तुम्हाला बघून छान वाटलं. आता तुम्ही सगळेच ॲक्टिव्ह इंटरनेट यूझर्स होत चालले आहात. ऑनलाईन प्रायव्हसी, कन्सेंट आणि बाउंड्रीज याबद्दल शिकण्याची हीच योग्य वेळ आहे! चला तर, सुरू करूया!

प्रायव्हसी, कंसेंट आणि बाऊंड्रीज बद्दल समजून घेणे

प्रायव्हसी चा अर्थ आहे, तुमच्या बद्दलची माहिती कोणाकोणाला कळावी यावर तुमचे नियंत्रण असणे. प्रत्येकाची प्रायव्हसीची पातळी वेगवेगळी असते - उदाहरणार्थ, काही जणांना त्यांच्या वाढदिवसाची तारीख कोणाला कळलेले आवडत नाही, तर कोणाला ते आवडतं! तरी, जसं आपण आपले लोकेशन किंवा पर्सनल स्टोरीज अनोळखी लोकांना प्रत्यक्षात देखील सांगत नाही, तसंच हीच प्रायव्हसी ऑनलाईन देखील जपणं आणि वाढवणं तुम्हाला अधिक सुरक्षित ठेवण्यामध्ये मदत करेल.

- 2017 मध्ये भारतात झालेली एक महत्त्वाची केस, जी पुत्तस्वामी जजमेंट म्हणून ओळखली जाते, या केसमध्येही प्रायव्हसीला नागरिकांचा मूलभूत अधिकार म्हणून मान्यता देण्यात आली आहे. हा निर्णय एक महत्त्वाचा टप्पा ठरला, ज्यामध्ये प्रत्येक व्यक्तीला त्यांची वैयक्तिक जागा, माहिती आणि आवड-निवड ठरवण्याचा हक्क आहे, यावर भर देण्यात आला.
- याबद्दल असा विचार करून बघा: तुम्ही तुमच्या ऑनलाईन ॲक्टिव्हिटीबद्दल सर्व काही तुमच्या पालकांशी किंवा मित्र-मैत्रिणींशी शेअर न करण्याचा पर्याय निवडू शकता — हा निर्णय सर्वस्वी तुमचा असतो.
- तुम्ही काय आणि कोणाशी शेअर करणार आहात यावर स्वतःचं नियंत्रण ठेवता येणं म्हणजेच प्रायव्हसी. या संदर्भात, तुमची प्रायव्हसी सुरक्षित राहण्यासाठी डिजिटल बाउंड्रीज अधिक चांगल्या प्रकारे समजून घेऊन, त्या कशा पाळायच्या हे आपण बघणार आहोत.

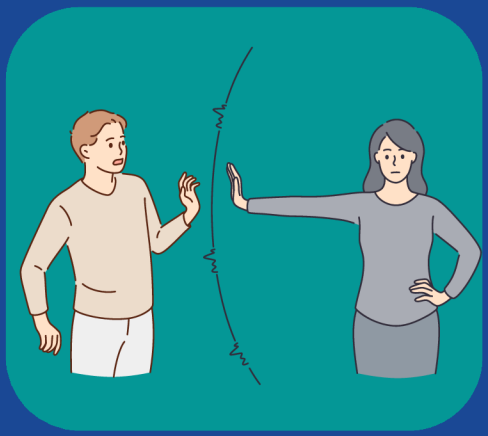


डिजिटल कंसेंट म्हणजे काय?

डिजिटल कंसेंट म्हणजे जेव्हा एखादी व्यक्ति तुम्हाला तुमची पर्सनल माहिती, फोटोज, किंवा मेसेजेस ऑनलाईन वापरण्यासाठी, शेअर करण्यासाठी किंवा त्याबद्दल बोलण्यासाठी विचारणा करते तेव्हा तुम्ही तसे करायचे की नाही हे ठरवणे होय. यामध्ये फोटोज, मेसेजेस, किंवा अगदी लोकेशन सुद्धा शेअर करणे याबद्दल तुम्हाला काय योग्य वाटते याचा विचारपूर्वक आणि जाणीवपूर्वक निर्णय घेणे याचा समावेश असतो. डिजिटल कंसेंट ऑनलाईन देखील अपडेट केली जाऊ शकते - तुम्ही एखादी गोष्ट शेअर करण्याबाबत मान्यता दिली असेल आणि आता तुम्हाला ते योग्य वाटत नसेल तर तुम्ही त्यात पुन्हा बदल करू शकता! इथे हे समजणे महत्त्वाचे आहे की कंसेंट स्वेच्छेने दिली जाते बळजबरीने किंवा गृहीत धरून नाही.

बाऊंड्रीज: कंसेंटिंगचे एक पॅटर्न

बाऊंड्रीज म्हणजे अश्या अदृश्य रेषा ज्याहे स्पष्ट करतात की मुळे तुम्हाला सुरक्षितआणि आरामदायक वाटतं. डिजिटल स्पेस मध्ये, या रेषा तुम्हाला हे ठरवायला मदत करतात की काय शेअर करायचं, कोणावर विश्वास ठेवायचा, आणि दुसऱ्यांकडून काय अपेक्षा ठेवायच्या. एकदा तुम्ही तुमच्या बाऊंड्रीज ठरवल्या की, त्यांचा वापर करून तुम्हाला जे योग्य वाटतं त्याच्या आधारे कंसेंट द्यायची का नाही हे ठरवू शकता. उदाहरणार्थ, तुमचा फोटो पोस्ट करण्याआधी तुम्हाला विचारले जावे किंवा तुमचे लोकेशन फक्त तुमच्या जवळच्या मित्रांनाच शेअर केले जावे हे जर तुम्हाला अपेक्षित असेल, तर याच बाऊंड्रीज तुमची आवड दर्शवतात आणि इतरांना तुमच्या अपेक्षांचा आदर करण्यामध्ये मदत करतात.



प्रायव्हसी vs सुरक्षा

प्रायव्हसी म्हणजे तुमच्या पर्सनल माहिती वर तुमचे नियंत्रण असणे, आणि सुरक्षा म्हणजे तुमचं डेटा आणि डिव्हाईस यांना बाहेरील थ्रेट्स पासून सुरक्षित ठेवणे. दोन्ही एकमेकांशी संबंधित आहेत - मजबूत सुरक्षा प्रायव्हसीला मदत करते उपयुक्त ठरते, आणि प्रायव्हसी बाबत जागरूक राहिलं की अधिक चांगली सुरक्षा राखली जाते.

ॲक्टिव्हिटी

खालील कृती प्रायव्हसी संबंधी उपाय आहे, सुरक्षे संबंधी उपाय आहे की दोन्ही संबंधी आहे हे ओळखा:

- प्रत्येक अकाऊंटसाठी स्ट्रॉंग आणि युनिक पासवर्ड ठेवणे.
- तुम्ही ज्या ॲप्स नेहमी वापरत नाही त्यासाठी लोकेशन सर्व्हिस बंद ठेवणे.
- शेअर्ड डिव्हाईस वापरत असताना काम झाल्यावर लॉगआऊट करणे.
- तुमचं सोशल मीडिया अकाऊंट प्रायव्हेट ठेवणे.
- तुमचं सोशल मीडिया यूझरनेम शेअर न करणे.

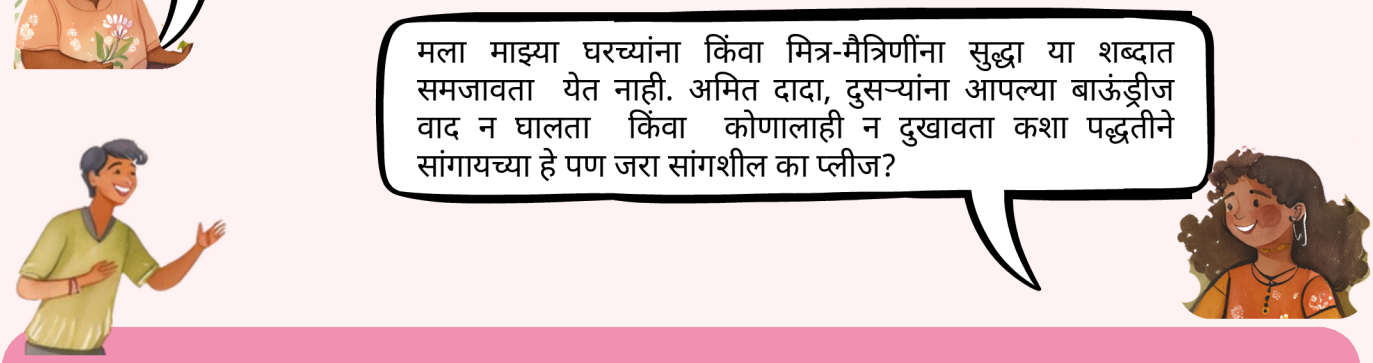
ॲक्टिव्हिटी

पर्सनल प्रायव्हसी आणि बाऊंड्रीज ठरवणे याबाबत व्यक्त होणे

बिंगो कार्ड वरील प्रत्येक स्टेटमेंट बघा आणि ऑनलाईन असताना तुम्हाला जे करणं योग्य वाटत असेल ते स्टेटमेंट मार्क करा.

मला माझी वाढदिवसाची तारीख ऑनलाईन शेअर करायला आवडतं.	सोशल मीडिया वर मी पर्सनल अकाऊंट वापरतो.	माझ्या पोस्ट्स मध्ये माझे रिअल टाईम लोकेशन शेअर करणे मी टाळतो.	मला माझा ईमेल आयडी ऑनलाईन शेअर केलेला नाही आवडत.
जेव्हा कोणी मला न विचारता टॅग करतं तेव्हां मला असुरक्षित वाटते.	मला फोटो शेअर करायला आवडतात, पण फक्त जवळच्या मित्र-मैत्रिणींसोबत.	मला माझा फोन नंबर ऑनलाईन शेअर केलेला आवडत नाही.	जेव्हा माझा मित्र मला न विचारता माझी स्टोरी शेअर करतो तेव्हां मला असुरक्षित वाटते.
शेअर करण्याआधी मी नेहमी हे चेक करतो की कोण-कोण माझे पोस्ट्स बघू शकते.	मला फोटो शेअर करायला आवडतात, पण फक्त जवळच्या मित्र-मैत्रिणींसोबत.	`एखाद्या व्यक्तीला माझ्या बद्दलची पोस्ट काढून टाकायला सांगणे मला योग्य वाटते.	सोशल मीडिया वर काही पर्सनल गोष्ट शेअर करण्याआधी मी दोनदा विचार करतो.
मला माझ्याबद्दलचे फक्त चांगले आणि निरपेक्ष अपडेट्स शेअर केलेले आवडतात.	ऑनलाईन चर्चांमध्ये माझे विचार शेअर करणे मला योग्य वाटते.	मी ज्या ग्रूप फोटो मध्ये आहे असा फोटो कोणी शेअर केला तरी माझी हरकत नसते.	मी अनोळखी व्यक्तींच्या फ्रेंड रिक्वेस्ट ॲक्सेप्ट करत नाही.

- असं कोणतं स्टेटमेंट होतं का, जे वाचल्यावर तुम्हाला दोन मिनिटं थांबावंसं वाटलं किंवा त्यावर जास्त विचार करावासा वाटला?
- तुम्हाला योग्य वाटणाऱ्या गोष्टींत काही विशिष्ट पॅटर्न लक्षात आला का?
- या ॲक्टिव्हिटीच्या आधारे तुम्हाला तुमच्यासाठी काही नवीन बाउंड्रीज सेट करायला हव्यात असं वाटलं का?



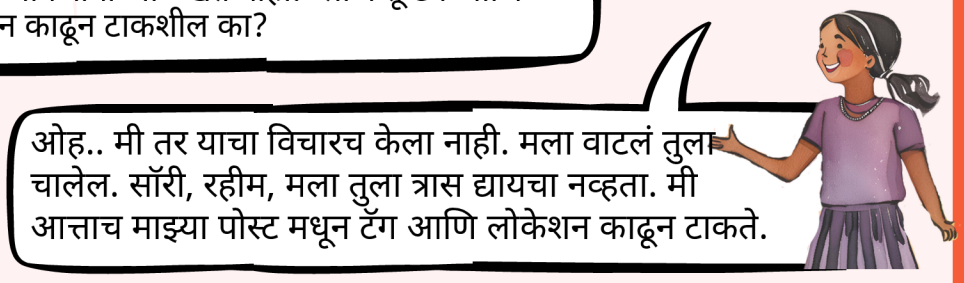
मला कळतंय तुम्हाला काय म्हणायचंय! पुढच्या वेळेस तुम्ही नक्की या विषयावर बोलायलाच हवं, फक्त काही मुद्दे लक्षात ठेवा:

- तुमचा टोन महत्त्वाचा आहे: अशा टोन मध्ये बोला ज्याने असं वाटणार नाही की तुम्ही चिडलेले किंवा अस्वस्थ आहात. आरडा-ओरडा करणे किंवा वैतागून बोलण्याऐवजी तुम्ही फक्त हे म्हणू शकता "याबद्दल मला काय वाटतंय फक्त हे मला सांगायचं आहे".

- भावना व्यक्त करणारे शब्द वापरा: बाऊंड्रीज का महत्त्वाच्या आहेत हे समजावून सांगण्यासाठी त्याबद्दल च्या तुमच्या भावना काय आहेत हे व्यक्त करा. उदाहरणार्थ, "असे करू नका असे म्हणण्याऐवजी हे म्हणा "मला माझ्या सुरक्षेची काळजी वाटते".

- मोकळ्या मनाने ऐकून घ्या आणि प्रश्नांना सामोरे जाण्यासाठी तयार राहा : तुम्ही तुमच्या बाऊंड्रीज काय आहेत हे सांगितल्यावर, समोरच्या व्यक्तीला त्याचे प्रश्न विचारू द्या किंवा त्याचे विचार मांडू द्या. फक्त सूचना न देता, यावर चर्चा होणे गरजेचे आहे. असेच आपण सगळे शिकत असतो!

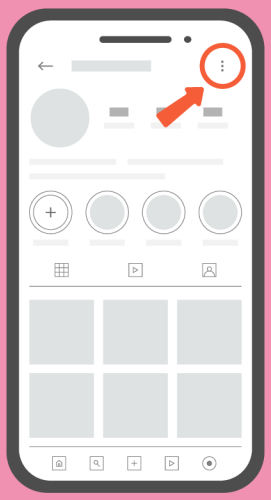
मीरा आणि रहीम, चला हे करून बघायचं का?



प्रायव्हसी सेटिंग्स वाढवणे

आता आपल्या पर्सनल बाउंड्रीज सेट करून झाल्यावर, वेगवेगळ्या प्लॅटफॉर्म्सवर तुमची प्रायव्हसी कशी सुरक्षित ठेवायची हे बघू. यासाठी सोशल मीडिया, ईमेल अकाउंट्स आणि ॲप्स तुमची वैयक्तिक माहिती कशा प्रकारे वापरतात हे समजून घेऊया. काय-काय डेटा गोळा केला जातो आणि तो कसा वापरला जातो हे जाणून घेतल्याने, तुमच्या ऑनलाईन प्रेझेन्सवर तुमचं नियंत्रण ठेवणं सोपं जातं.

सर्वात आधी तुमचे सोशल मीडिया अकाऊंट पब्लिक आहे की प्रायव्हेट हे चेक करा. जर हे कसे चेक करायचे हे माहीत नसेल, तर खालील स्टेप्स फॉलो करा:

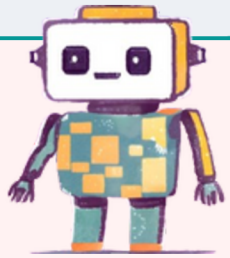


1. तुमचे सोशल मीडिया ॲप उघडा आणि तुमच्या प्रोफाईल सेटिंग्स मध्ये जा.

2. प्रायव्हसी सेटिंग्स किंवा अकाऊंट सेटिंग्स हा पर्याय शोधा

3. जर तुमचेअकाऊंट पब्लिक असेल, तर तुम्ही ते प्रायव्हेट मध्ये बदलू शकता जेणेकरून तुमचे कंटेंट कोण-कोण बघू शकते यावर तुमचे नियंत्रण राहील.

आठवतंय, पहिल्या प्रकरणामध्ये आपण डिजिटल फूटप्रिंटबद्दल बोललो होतो — म्हणजे, जेव्हा जेव्हा तुम्ही ऑनलाईन असता, तेव्हा तेव्हा तुम्ही मागे खुणा सोडत जात असता. ॲप्स, वेबसाईट्स आणि सोशल मीडिया प्लॅटफॉर्म्स बऱ्याचदा हा डेटा तुमचा अनुभव पर्सनलाइझ करण्यासाठी गोळा करतात — म्हणजे तुम्हाला हव्या असलेल्याच जाहिराती दाखवणं, व्हिडिओज सुचवणं, किंवा अगदी तुमच्या आवडी-निवडी ओळखणं देखील. आता हे सोयीस्कर वाटू शकतं, परंतु तुम्ही किती शेअर करत आहात आणि त्यावर नियंत्रण कसं ठेवावं हे समजून घेणं महत्त्वाचं आहे.



कॅशे आणि कूकीज: हे काय असते?

जेव्हा तुम्ही एखादी वेबसाईट बघता तेव्हा ती वेबसाईट तुमची ॲक्टिव्हिटी लक्षात ठेवते. हे कॅशे आणि कूकीजमुळे शक्य होतं:

कॅशे: हे म्हणजे तुमच्या ब्राऊझरकडे असलेल्या बॅगपॅकसारखे आहे, ज्यामध्ये वेबसाईट्सचे बिट्स (इमेजेस आणि स्क्रिप्ट्स) ठेवलेल्या असतात. जेणेकरून तुम्ही पुढच्या वेळेस ती वेबसाईट उघडल्यावर ते पटकन लोड होतात.

कूकीज: कूकीज म्हणजे वेबसाईट ने तुकड्या-तुकड्यात साठवलेली माहिती आहे, उदाहरणार्थ तुम्ही कुठे क्लिक केले, कार्ट मध्ये काय-काय ॲड केले, किंवा तुम्ही एखाद्या पेज वर किती वेळ थांबलात हे देखील टिपले जाते.

कूकीजमुळे वेबसाईट्स तुमची ॲक्टिव्हिटी ट्रॅक करू शकतात आणि कॅशे वापरून एखादी व्यक्ती तुमच्या डिव्हाइसमध्ये प्रवेश करून तुम्ही कुठे कुठे ऑनलाईन होता हे बघू शकते.

प्रायव्हसी पॉलिसी आणि टूल्स

जेव्हा तुम्ही एखाद्या नवीन गेम किंवा ॲप साठी साईनअप करता, तेव्हा तुम्हाला बऱ्याचदा प्रायव्हसी पॉलिसी साठी सहमति विचारली जाते. त्यामध्ये हे लिहिलेले असते की तुमचा डेटा कसं गोळा केला जातो, साठवला जातो, शेअर केला जातो, किंवा वापरला जातो. पण बरेच लोक हे वाचत नाहीत कारण ही पॉलिसी खूप मोठी आणि अवघड असते.

काही ॲप्स आणि वेबसाईट्स तुमचा डेटा काळजीपूर्वक वापरतात, पण तोच डेटा काही ॲप्स आणि वेबसाईट्स दुसऱ्या कोणाला तरी शेअर करतात किंवा विकू शकतात. प्रायव्हसी पॉलिसी समजून घेतल्याने तुम्ही कशाला सहमति देताय याबद्दल विचारपूर्वक निर्णय घेण्यामध्ये मदत होते. या प्रायव्हसी पॉलिसीजना सोप्या आणि समजेल अशा भाषेत बदलू शकणारे काही ऑनलाईन टूल्स वापरून तुम्ही याबद्दल माहिती मिळवू शकता. तसेच, वेबसाईट्स आणि ॲप्स तुमचा डेटा कशाप्रकारे सुरक्षित ठेवतात याच्या आधारे त्यांचे परीक्षण करण्यात देखील काही टूल्स तुमची मदत करतात.

ॲप परमिशन्स

- कोणतेही नवीन ॲप डाऊनलोड करताना, कॅमेरा, लोकेशन, किंवा कॉन्टॅक्ट्स यांच्या ॲक्सेसबद्दल परमिशन्स विचारल्या जातात. जरी व्यावहारिक उपयोगासाठी काही परमिशन्स आवश्यक असल्या, तरी काही अनावश्यक असू शकतात, ज्यामुळे डेटा चुकीच्या पद्धतीने वापरला जाण्याची शक्यता निर्माण होते. उदाहरणार्थ, फोटो एडिटिंग ॲपसाठी लोकेशन ॲक्सेसची काहीच गरज नाही. सुरक्षित राहण्यासाठी, जर ॲपसाठी खरंच आवश्यक असेल तरंच परमिशन द्या, डिव्हाईस सेटिंग्समधील अनावश्यक परमिशन्स चेक करा, आणि ज्या ॲप्स इन्स्टॉलेशनच्या वेळेस जास्त परमिशन्स मागतात त्यांच्यापासून सावध रहा.

आत्ता आपण बघितलं की ॲप्स आणि वेबसाईट्स तुमच्या प्रायव्हसीवर कशाप्रकारे प्रभाव टाकतात. इतर इंटरनेट यूझर्सचा यावर काय प्रभाव पडतो, त्याचबरोबर या परिस्थितींना कसे हाताळायचे हे देखील आता बघूया.

ऑनलाईन प्रायव्हसीचे उल्लंघन

अमित दादाला आणि ग्लिचला भेटून कालचा बागेतला अनुभव सांगण्यासाठी मीरा, रहीम, आणि सुजान खूप उत्सुक आहेत. तशी मीरा जरा लाजत होती ती जो धडा शिकली की नेहमी दुसऱ्यांसोबत काढलेला एखादा फोटो ऑनलाईन शेअर करण्याआधी त्यांची परवानगी घेतली पाहिजे, त्याबद्दल अमित दादाला सांगण्यासाठी उत्सुक होती.

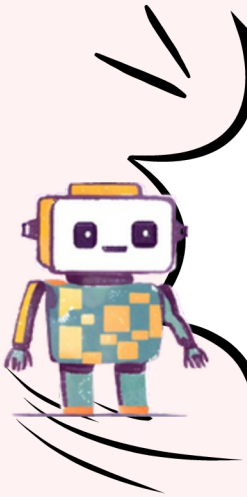
खूप छान मीरा, ही खूप महत्त्वाची गोष्ट शिकलीस, पण तुला माहितीये का की हे असे परवानगीशिवाय इमेजेस शेअर करणे खूप कॉमन आहे?

खरंच? हे का महत्त्वाचे आहे हे याबद्दल जाणून घेण्यासाठी आपण यावर अजून चर्चा करायला हवी. तू मला अजून काही सांगू शकतोस का?

एखाद्याच्या परवानगीशिवाय त्याचा फोटो शेअर करणे हा प्रकार सहसा ग्रूप चॅट्स, सोशल मीडिया, किंवा प्रायव्हेट मेसेजेसच्या माध्यमातून केला जातो. हे म्हणजे प्रायव्हसीचे उल्लंघन आहे आणि त्याचे गंभीर परिणाम परिणाम होऊ शकतात.

परवानगीशिवाय शेअरिंग करणे घातक का असू शकते?

- यामुळे प्रायव्हसीचे उल्लंघन होते: एखाद्याचा फोटो त्याच्या परवानगीशिवाय शेअर केल्याने त्या व्यक्तीची पर्सनल माहिती, फोटो, कोण कोण बघू शकतो हे ठरवण्याच्या त्यांच्या हक्काचा अनादर होतो.
- यामुळे अत्याचार आणि मानसिक त्रास होऊ शकतो: वाईट कमेन्ट्स किंवा चुकीचे शेअरिंग यामुळे एखाद्याच्या भावना दुखावल्या जाऊ शकतात..
- यामुळे एखाद्याला असुरक्षित किंवा अपमानास्पद वाटू शकते: जर कोणाचा फोटो त्याच्या परवानगीशिवाय शेअर केला तर त्याला असुरक्षित किंवा अपमानास्पद वाटू शकते.



एखाद्याला आवडेल का नाही हे माहीत नसेल, तर सरळ विचारा! कोणाच्याही बाऊंड्रीज बद्दल गृहीत धरण्यापेक्षा त्यांना स्पष्ट विचारणे कधीही उत्तमच.

तुम्हाला तुमची आणि इतरांची ऑनलाईन प्रायव्हसी सुरक्षित ठेवायची आहे का? तुम्ही योग्य मार्गावर आहात का हे बघण्यासाठी या “चूक किंवा बरोबर” कोड्याची उत्तरे द्या!

- एखादी व्यक्ति जी तुमचा मित्र किंवा मैत्रीण आहे, तिचा फोटो परवानगीशिवाय शेअर करणे योग्य आहे. **(चूक/बरोबर)**
- कोणीतरी ग्रूपचॅट मध्ये तुमच्या मित्राचा फोटो त्याच्या परवानगीशिवाय शेअर करतात आणि त्याची टर उडवतात, तर त्याकडे दुर्लक्ष करून चॅटिंग सुरू ठेवणे योग्य आहे. **(चूक/बरोबर)**
- एक ग्रूप फोटो मध्ये परवानगीशिवाय कोणालाही टॅग करणे योग्य आहे. **(चूक/बरोबर)**

एखाद्याच्या प्रायव्हसी आणि सुरक्षेचे ऑनलाईन कशाप्रकारे उल्लंघन होते याबद्दल माहिती करून घेवू या. हे जरा भीतीदायक वाटू शकतं, पण काळजी करू नका, जर तुम्ही हे पूर्णपणे आणि व्यवस्थितपणे समजून घेतलं तर सुरक्षित राहण्याची ही पहिली पायरी आहे.

अत्याचार

अत्याचार होणे याबद्दल तुम्ही याआधी ऐकले असेलच - हे बहुधा शारीरिक स्वरूपाचे समजले जाते, उदाहरणार्थ एखाद्याला ढकलणे किंवा व्यक्तीगत पातळीवर छेडछाड करणे. पण तुम्हाला माहिती आहे का की अत्याचार ऑनलाईन देखील होऊ शकतात? हे देखील तितकंच घातक असू शकते, खरं म्हणजे जास्तंचघातक आहे, कारण हे जास्तीत जास्त लोकांपर्यंत पोहचू शकते आणि कधीही कुठेही घडू शकते.

ऑनलाईन अत्याचार, ज्याला सायबर अत्याचार देखील म्हणतात, अनेक प्रकारचे असू शकतात. प्रश्न फक्त वाईट शब्दांचा वापर करण्याचा नाही, यामध्ये एखाद्या व्यक्तीच्या पर्सनल माहिती उघड करणे (डॉक्सिंग), त्रासदायक कमेन्ट्स लिहिणे (ट्रोलिंग) आणि एखाद्या व्यक्तीला ऑनलाईन ग्रूप्स मधून काढून टाकणे (वाळीत टाकणे).

डॉक्सिंग

जेव्हा एखादी व्यक्ति तुमची पर्सनल माहिती उदाहरणार्थ तुमचा पत्ता किंवा फोन नंबर तुमच्या परवानगीशिवाय पब्लिश करते तेव्हा त्याला डॉक्सिंग म्हणतात.

ट्रोलिंग

जेव्हा एखादी व्यक्ति दुसऱ्यांना त्रास देण्यासाठी दुखावणारे किंवा त्रासदायक कमेन्ट्स पोस्ट करते तेव्हा त्याला ट्रोलिंग म्हणतात.

वाळीत टाकणे

वाळीत टाकणे म्हणजे एखाद्या व्यक्तीला दुखावण्यासाठी मुद्दाम ऑनलाईन ग्रूप्स मधून किंवा चॅट्स मधून बाहेर काढणे.

त्यांच्या भूमिकेत येऊन बघा: ट्रोलिंगबद्दल समजून घ्या

कल्पना कर की एखाद्या विषयावर तुम्ही सगळे बोलत आहात आणि अचानक कोणीतरी तुम्हाला टार्गेट करून तुमच्याशी वाईट शब्दात बोलायला सुरुवात करते. हे फक्त "चिडवणं" नाही, तर हे ट्रोलिंग आहे - मुद्दाम आणि वरचे-वर केल्या जाणाऱ्या अश्या कृती ज्या डिवचण्यासाठी किंवा अपमान करण्यासाठी केल्या जातात. चला एक उदाहरण बघूया:

प्रिय डायरी

आज, सायन्स प्रोजेक्टवर चालू असलेल्या चर्चेने एक वेगळेच, मला अपेक्षित नसलेले वळण घेतले.

आर्यनने टाईप केले,, "समीरला काही महत्वाचे काम करायला देऊ नका. मागच्या वेळेस सारखा काही तरी घोळ घालून ठेवेल तो." सगळ्यांनी त्या मेसेजला लाईक केलं, आणि मला अपमानित झाल्यासारखं वाटलं. मग कुणालने "काही जुने फॅमिली फोटोज" पोस्ट केले," त्याला ते कुठून मिळाले माहीत नाही – हे मला अतिक्रमण केल्यासारखे वाटले.

रिया म्हणाली, "समीरला या प्रोजेक्ट मधून काढून टाकूया. तो काही कामाचा नाही." आणि ते म्हणाले, "आपण त्याबद्दल आपल्या पर्सनल ग्रूप मध्ये बोलू, इथे समीर सोबत नको. "मला खूप एकटं पडल्यासारखं वाटलं.

आर्यनने पुन्हा लिहिलं, "समीर त्याचा पार्ट सुद्धा पूर्ण करणार नाही. तो अगदी बिनकामाचा आहे." मला वाटते तो माझ्या काही तरी प्रतिक्रिया देण्याची वाट बघत होता.

मी लॉगऑफ केलं. ते मला असं कसं वागवू शकतात? समीर

ॲक्टिव्हिटी

तुम्ही अत्याचाराचे वेगवेगळे प्रकार आढळतात का? असे क्षण खालील याच्याशी जोडून बघा:

-वाळीत टाकणे

_____

-डॉक्सिंग: _____

-ट्रोलिंग: _____

तुम्ही सुद्धा जर या ऑनलाईन ग्रूपचा एक भाग असतात तर तुम्ही काय केलं असतं?

_____

आता तुम्हाला ऑनलाईन प्रायव्हसी बद्दल सगळं काही माहिती झाले आहेच, तर आता ऑनलाईन जगातील काही थ्रेटट्स बद्दल बोलूया - सायबर अत्याचार आणि छळवादाचे प्रकार. असे वागणे फक्त "वाईट वागणे" असेच नाही; तर त्या अवैध आणि प्रचंड दुखावणाऱ्या आहेत. पण काळजी करू नका! हे सगळे धोके समजावून घेतले तर तुम्ही तुमच्या ऑनलाईन सुरक्षा तुम्ही नियंत्रित करू शकता.

सायबरस्टॉकिंग

सायबरस्टॉकिंग म्हणजे कोणीतरी सतत तुमच्यावर पाळत ठेवून असणं - तुमच्या पोस्ट्स बघणं, खूपच जास्त प्रमाणात कमेन्ट्स करणं, किंवा अगदी तुम्हाला असुरक्षित वाटेल असे मेसेजेस पाठवणं.

लैंगिक छळ

ऑनलाईन झालेल्या लैंगिक छळ यामध्ये अयोग्य मेसेजेस, फोटोज पाठवणे, किंवा एखाद्याला असुरक्षित वाटेल असे शब्द वापरणे.

सेक्स्टॉर्शन

सेक्स्टॉर्शन म्हणजे जेव्हा एखादी व्यक्ति कोणाला तरी त्यांचे प्रायव्हेट फोटो किंवा व्हिडिओज, पाठवायचा आग्रह करते, आणि मग पैसे दिले नाहीत तर हे सगळं पब्लिकली शेअर करण्याची धमकी देतात किंवा इतर अनैतिक प्रकार करायला लावतात.

रिव्हेंज पॉर्न

रिव्हेंज पॉर्न म्हणजे जेव्हा एखादी व्यक्ति दुसऱ्या व्यक्तीला त्रास देण्यासाठी त्यांचेच प्रायव्हेट फोटो किंवा व्हिडिओज पाठवते.

कॅटफिशिंग

कॅटफिशिंग म्हणजे एखादी व्यक्ति दुसऱ्यांना फसवण्यासाठी किंवा त्रास देण्यासाठी स्वतःची वेगळीच ओळख दाखवतो. ते तुमचा त्यांच्यावर विश्वास बसावा म्हणून खोटे फोटो, नावं, किंवा इतर माहितीचा वापर करू शकतात.

मास्करेडिंग

मास्करेडिंग म्हणजे जेव्हा एखादी व्यक्ति तुम्हाला त्रास देण्यासाठी किंवा फसवण्यासाठी जे ते नाही आहेत ते असण्याचे सोंग घेतात. कॅटफिशिंग आणि यामध्ये किंचित फरक आहे, कारण हे कोणाचातरी छळ करण्यासाठी किंवा त्रास देण्यासाठी बनावट ओळखीच्या आडून दुसरे कोणी तरी असल्याचे सांगून केले जाते.

डीपफेक

डीपफेक म्हणजे जेव्हा एखादी व्यक्ति एआय (कृत्रिम बुद्धिमत्तेचा) चा वापर करून केलेले खोटे फोटो किंवा व्हिडिओज वापरतो जे अगदी खरे वाटतात पण नसतात. यामुळे एखाद्याने काही म्हटले किंवा केले नसेल तरी त्याने ते म्हटले किंवा केले आहे असे भासवले जावू शकते.

ओह हे किती भयानक आहे, दादा! हे ऐकून मला माझ्या सारा नावाच्या मैत्रिणीची आठवण झाली. तिचा ऑनलाईन एक मित्र झाला होता, जो तिला गिफ्ट्स आणि फुलं पाठवायचा. तो तिला आवडायला लागला होता म्हणून ती त्याला ऑफलाईन पण भेटायला लागली. पण आता त्याच्या मागण्या वाढल्या होत्या, पण आता तो तिला एकटे भेटण्याची आणि जवळ येण्याची मागणी करू लागला आहे ज्यामुळे तिला त्रासदायक वाटत आहे. त्यामुळे तिला त्याच्या सोबत असुरक्षित वाटायला लागलं होतं. तो 29 वर्षांचा आहे, आणि तो म्हणतो की मोठे झाल्यानंतर लोक असेच वागतात! साराला काय सांगावे ते मला कळत नाही :(

बरं झालं तू मला हे सांगितलंस, सुजान. आत्ता तू जे सांगितलंस तो एक खूप कॉमन ऑनलाईन थ्रेट आहे - ज्याला ग्रूमिंग असे म्हणतात. पण काळजी करू नको, आपण सगळे मिळून हे समजून घेऊ म्हणजे तू तुझ्या मैत्रिणीला मदत करू शकशील.

ऑनलाईन ग्रूमिंग

ऑनलाईन ग्रूमिंग म्हणजे जेव्हा एखादी वयस्क व्यक्ति अल्पवयीन व्यक्तीवर पाळत ठेवून किंवा फसवून तिच्याशी ऑनलाईन मैत्री करते. सुरुवातीला ते खूप मैत्रीपूर्ण आणि समजूतदारपणाने वागतात, पण त्यांचा मूळ हेतु या अल्पवयीन व्यक्तीचा फायदा घेऊन त्यांचा लैंगिक छळ करणे हा असतो.

ऑनलाईन ग्रूमिंगचे टप्पे

शोध

प्रत्यक्ष संपर्क करण्याआधी, ग्रूमर कोणत्याही एक मुलाला किंवा मुलीला टार्गेट करतो आणि त्यांच्या आयुष्याबद्दल माहिती गोळा करण्याचा प्रयत्न करतो, त्यांना कशामुळे असुरक्षित वाटते ते शोधून काढतो - त्यांना काय हवंय, त्यांना कशामुळे असंतुष्ट वाटतं, त्यांच्या गरजा काय आहेत आणि त्यांच्या भावना जाणून घेण्याचा प्रयत्न करतात.

विश्वास मिळवणे

तो त्या मुलाच्या किंवा मुलीच्या एरवी पूर्ण न होणाऱ्या गरजा पूर्ण करतात. गिफ्ट देणे, प्रशंसा करणे, पैसे गिफ्ट देणे, आणि इतर गरजा भागवणे अशाप्रकारच्या टॅक्टिक्स हे गुन्हेगार वापरतात.

एकटेपणाची जाणीव करून देणे

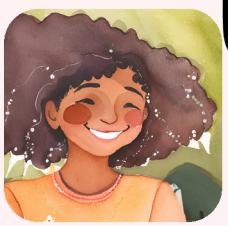
ते अशा परिस्थिती निर्माण करतात ज्यामुळे त्या मुलाला किंवा मुलीला एकटं वाटू लागतं आणि मग ते भासवतात की त्या मुलाची किंवा मुलीची त्यांच्या इतकी काळजी कोणीही घेत नाही. ग्रूमर या लहान मुलांच्या उत्सुक स्वभावाचा फायदा घेऊन त्यांच्याशी लैंगिक संबंध निर्माण करतात.

ताबा मिळवणे

पुढे हे लैंगिक शोषणामध्ये बदलते, ती मुलं कुठे जातात, काय करतात, कोणला भेटतात, या सगळ्यावर लक्ष ठेवतात. ग्रूमर हीच तुमच्या भावनिक आणि भौतिक गरजा पूर्ण करणारी एकमेव व्यक्ति आहे असेच ते भासवतात.

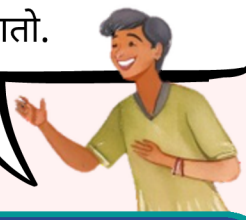
ग्रूमिंगची लक्षणे

- **अती महत्त्व देणे:** हे ग्रूमर्स या मुलांवर कौतुकाचा, गिफ्ट्सचा वर्षाव करतात किंवा त्यांना विशेष वागणूक देऊन ते खास असल्याचे भासवतात.
- **अयोग्य संभाषण:** ते या मुलांबरोबर त्यांच्या वयाला अनुसरून नसणाऱ्या विषयांवर संभाषण करतात. बऱ्याचदा कमी वयातच त्यांना संबंध किंवा लैंगिकता याबद्दल माहिती सांगतात.
- **बाऊंड्रीजचा अंदाज घेणे:** हे ग्रूमर्स हळू-हळू मुलांच्या शारीरिक आणि भावनिक बाऊंड्रीजचा अंदाज हे बघण्यासाठी घेतात, की त्यांची प्रतिक्रिया काय आहे, कालांतराने त्यांचे असे विचित्र वागणे वाढत जाते.



सारा सोबत जे घडले ते पण असं काहीसं होतं ! आता तिने काय करायला हवं?

खरं तर तू तिला लगेचच या सगळ्याबद्दल संबंधित अथॉरिटीला कळवण्यासाठी प्रेरित करायला हवं, ते पण एखाद्या विश्वस्त माणसाच्या मदतीने. अशा परिस्थितीत आपण काय करू शकतो ते आता मी तुला सांगतो.



अशी लक्षणे दिसू लागली तर काय करायला हवं?

- **सगळ्याचे रेकॉर्ड ठेवा:** सगळ्या संभाषणाचे रेकॉर्ड ठेवा. म्हणजे मेसेजेस किंवा ईमेल्स चा स्क्रीनशॉट, संभाषणाचा मसुदा , आणि इतर संबंधित माहिती.
- **मोकळेपणाने बोला:** जे काही घडते आहे त्याबद्दल विश्वस्त माणसाशी बोला. म्हणजे पालक, शिक्षक, शाळेतील काऊन्सेलर, किंवा तुमच्या विश्वासातले इतर कोणीही.
- **विश्वस्त व्यक्तीला सामील करा:** जे काही सुरू आहे त्याबद्दल अल्पवयीन मुला-मुलींना एखाद्या विश्वस्त व्यक्तीला सांगायला प्रेरित करा, उदाहरणार्थ पालक, शिक्षक, किंवा शाळेतील काऊन्सेलर. एखाद्या विश्वस्त व्यक्तीचा आधार असल्याने खूप फरक पडतो.
- **हळू-हळू संपर्क कमी करा:** बोलण्याचे प्रमाण हळू हळू कमी करा. नम्रपणे आमंत्रण नाकारा आणि तुम्हाला तुमचा वेळ हवा आहे हे कारण देऊन मेसेजेसला कमीत कमी उत्तरं द्या.

आणि धोक्याचे विश्व

रहीम शनिवारी दुपारी त्याच्या भावाच्या लॅपटॉप वर टाईमपास करत बसला होता, एक ऑनलाईन गेम खेळण्यामध्ये तो हरवून गेला होता. त्याने नुकतीच एक खूप अवघड लेव्हल पूर्ण केली होती आणि पुढच्या चॅलेंजकडे तो जणारंच होता तेवढ्यात एक नोटिफिकेशन पॉपअप झाले

दादा, मि गेम खेळत होतो आणि मधेच काही तरी विचित्र घडलं. 'Xxशॅडोस्लेयरxX,' माझ्यावर पाळत ठेवून आहे, मला मेसेज करतो आहे, उदाहरणार्थ 'मला माहिती आहे की तू कुठे राहतोस.' मी खूप घाबरलो, मी गेम बंद केला आणि मी गेम मध्ये परत शून्यावर आलो.

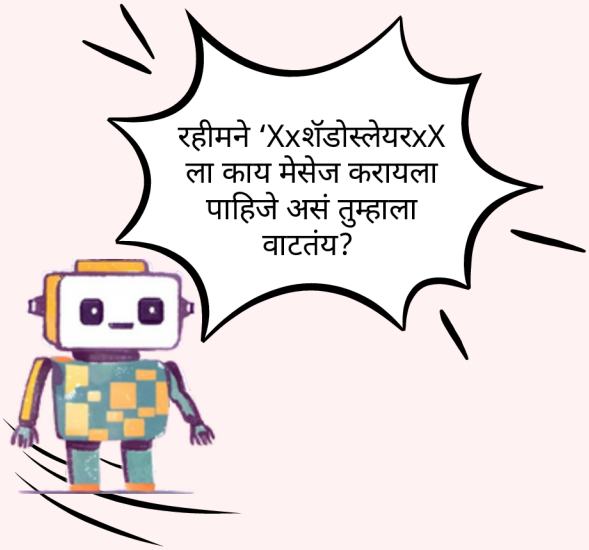
रहीम, याला सायबरस्टॉकिंग म्हणतात. हे तुला घाबरवण्यासाठीच केलं होतं. तू थांबलास तेच बरं केलंस. आता त्याला ब्लॉक कर आणि प्लॅटफॉर्म वर त्याच्याबद्दल तक्रार कर.

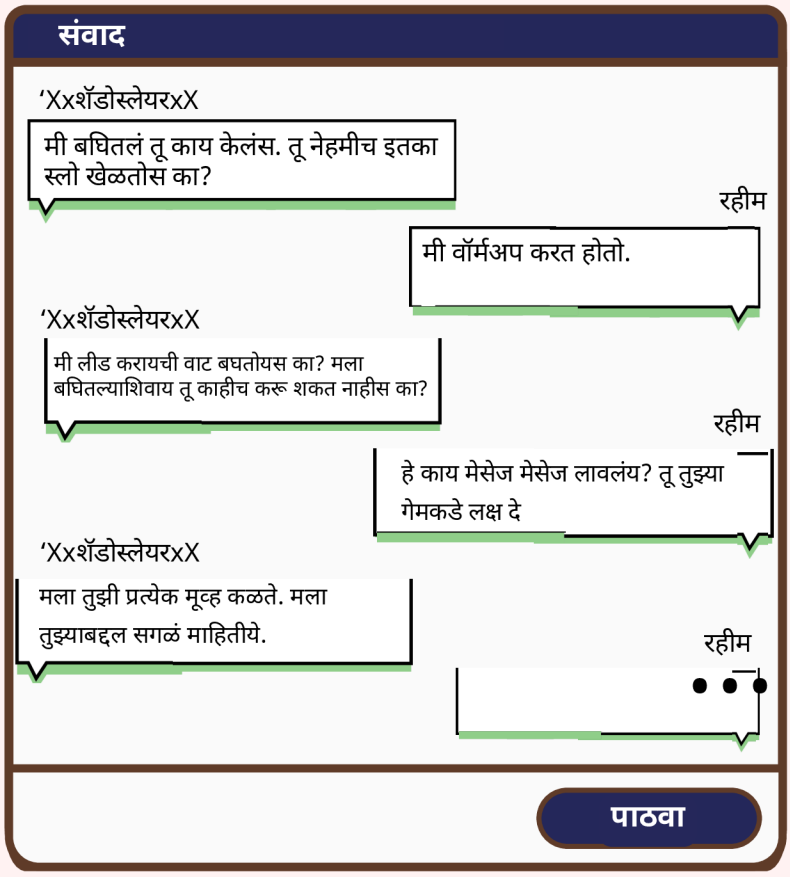
पण त्यांनी अजून काही केले तर? मला खरंच भीती वाटते आहे.

तू तुझं प्रायव्हेट अकाऊंट बनवू शकतो जर त्यामुळे तुला सुरक्षित वाटत असेल तर. आणि अनोळखी लोकांशी तुझी पर्सनल माहिती शेअर करू नकोस. परत जर असं झालं, तर लगेचच मला किंवा तुझ्या विश्वासातल्या कोणालातरी सांग.

थॅंक्स, दादा. मी त्याला ब्लॉक करेन आणि माझ्या मित्र-मैत्रिणींना पण याबद्दल नक्की सांगेन.

गेमिंग मध्ये मजा येते, पण कधी-कधी हे धोक्याचे पण असू शकते. डीपफेक अवतारांपासून सावध रहा, जिथे प्लेयर्स ते जे नाही आहेत ते असण्याचे भासवतात आणि तुम्हाला तुमची पर्सनल माहिती शेअर करण्यासाठी भाग पडतात. ऑनलाईन ग्रूमिंग मध्ये इन-गेम गिफ्ट्स देऊन, तुमची पर्सनल माहिती काढून घेण्याचा प्रयत्न करतात. डॉक्सिंग बद्दल पण सावध रहा, ज्यामध्ये प्लेयर्स तुमची पर्सनल माहिती तुमचा अपमान करण्यासाठी किंवा तुम्हाला घाबरवण्यासाठी इतर ठिकाणी शेअर करू शकतात. तुमची पर्सनल माहिती नेहमी प्रायव्हेट ठेवा आणि संशयास्पद वागणुकीबद्दल तक्रार नोंदवा.





तुझ्या मदतीमुळे मला कधीच अशा परिस्थितीत भीती पण वाटत नाही आणि एकटं पण नाही वाटत. पण दादा, मला सांग हे सगळे प्रकार फक्त ऑनलाईन गेमिंगच्या वेळेसच होतात का?

अजिबात नाही रहीम. हे प्रकार कुठल्याही ऑनलाईन माध्यमातून होऊ शकतात - सोशल मीडिया, व्हर्चुअल क्लासेस, आणि फॅमिली चॅट ग्रूप्स मध्ये सुद्धा. ओळखीचे किंवा अनोळखी कोणीही तुमच्या बाऊंड्रीजचे उल्लंघन करू शकते. म्हणूनच सावध राहणे आणि तुम्ही ऑनलाईन असलात तरी तुमची प्रायव्हसी सुरक्षित ठेवणे खूप गरजेचे आहे.

रोजच्या आयुष्यातले ऑनलाईन ट्रॅप्स: डिजिटल वर्ल्ड मध्ये सुरक्षित रहा

बऱ्याचदा, लोकांना कमी काम करून भरपूर पैसे मिळण्याचे आमिष दाखवणाऱ्या नोकरीच्या जाहिराती दिसतात. त्या संधीमुळे आकर्षित होऊन ते पटकन त्यावर क्लिक करतात, आणि त्यांचे नाव, ईमेल, आणि क्वालिफिकेशन शेअर करून टाकतात. लगेच ती वेबसाईट तुम्हाला एक "छोटीशी रक्कम" डिपॉजिट म्हणून भरण्यास सांगते त्यामुळे तुमची जागा राखून ठेवता येईल. हे सगळं खूप अस्सल वाटत असतं - जोपर्यंत वेळ निघून गेलेली नसते तोपर्यंत. तुमची माहिती कशी आणि कुठे वापरली जाईल याबद्दल तुम्हाला अस्वस्थ आणि असुरक्षित करूनस्कॅमर गायब होतो.

नोकरीच्या खोट्या ऑफर्स, फिशिंग स्कॅम्स, आणि ग्रूमिंग हे खूप कॉमन आहे, आणि यामध्ये नेहमीच अनोळखी लोकंच सामिल असतात. कधी-कधी, तुमच्या ओळखीचे लोक सुद्धा असं वागू शकतात. म्हणूनच सावध रहा आणि तुमच्या अंतर्मनावर विश्वास ठेवा. ऑनलाईन असताना तुम्हाला कसं वाटतं याकडे लक्ष असू द्या - तुम्हाला सुरक्षित वाटतं, का काही चुकीचं घडतंय असं वाटतं? तुमच्या अंतर्मनाचं ऐकलंत तर तुम्ही या डिजिटल वर्ल्ड मध्ये जास्त सुरक्षित पद्धतीने वावरू शकता.

प्रायव्हसीचे उल्लंघन झाल्यामुळे पीडित व्यक्तीवर होणारे परिणाम

ऑनलाईन ग्रूमिंगच्या साराच्या अनुभवानंतर, सुजान आणि तिचे काही क्लासमेट्स एकत्र येऊन ऑनलाईन थ्रेट्स बद्दल चर्चा करत होते. त्यांच्या लक्षात आलं की प्रायव्हसीचे उल्लंघन आणि इतर अटॅक्स होणं यात काही नवल नाही. त्यांच्या त्या चर्चेनंतर, सुजानने ऑनलाईन अटॅक्स आणि प्रायव्हसीचे उल्लंघन झाल्यावर वेगवेगळ्या लोकांना कसं वाटेल,ते कशा प्रतिक्रिया देतील, यावर काही मुद्दे लिहून काढले.

हे फक्त उल्लंघन करण्याबद्दलच नाही आहे - प्रायव्हसीचे उल्लंघन झाल्यामुळे लोकांना ऑनलाईन असताना कसं वाटतं यावर खूप विपरीत परिणाम होतो. उदाहरणार्थ, अशा स्पेसेसवरचा त्यांचा विश्वास कमी होऊ लागतो आणि पुन्हा त्याचा वापर करण्यात ते जास्तंच सावधगिरी किंवा भीती बाळगायला लागतात. पण हे त्याहूनही बरेच जास्त आहे. वेगवेगळ्या लोकांवर त्याचा परिणाम वेगवेगळ्या प्रकारे होतो.

सामाजिक आणि भावनिक

काही जणांवर याचा भावनिक दृष्ट्या परिणाम होतो - उदाहरणार्थ अस्वस्थ आणि अपमानास्पद वाटणे, जरी त्यामध्ये त्यांची काहीही चूक नसली तरी. यामुळे त्यांना असुरक्षित, शोषित वाटते, आणि एक प्रकारे ते दुखावले जातात. कधी कधी यामुळे ते स्वतःला एकटं पाडून घेऊ लागतात. त्यांना समाजात वावरायची लाज वाटू लागते.

शारीरिक-

काहींमध्ये, ते शारीरिकदृष्ट्या दिसून येते. ताणतणाव, झोपेच्या समस्या, भूक बदलणे - काहींना आरोग्याच्या समस्या देखील असतात.

आणि काही आश्चर्य नाही की या सगळ्यामुळे त्यांचे कुठल्याच कामात नीट लक्ष लागत नाही. शाळेत किंवा अगदी रोजच्या कामं करणं पण अवघड होऊन बसतं. (आणि खरं सांगायचं तर ते लक्षात येतं!)

आणि हो, काही दिवसांनंतर किंवा आठवड्यांनंतर या भावना पुसट होवू शकतात , पण काही लोकांसाठी याचा खूप काळासाठी प्रभाव राहू शकतो.

आपण काय करू शकतो?

त्यांचे किस्से ऐकून मी खरंच विचार करायला लागलो. त्यांना अशी माणसं भेटतात जे त्यांची ही परिस्थिती समजून घेतात, आणि यामुळे या लोकांना एक विश्वास वाटायला लागतो - की चूक फक्त त्यांचीच नाहीये. अर्थात प्रायव्हसीचे उल्लंघन झाल्यामुळे ते स्वतःवरंच शंका घेऊ लागतात, पण याचा अर्थ असा नाही की त्यांची पात्रता नाही, ते विश्वास ठेवण्या योग्य नाही, किंवा स्मार्ट नाही. पण त्यांच्यासोबत असं होणं बरोबर नाही, आणि कोणसोबतच असं होऊ नये.

जर प्रायव्हसीचे उल्लंघन झाले, स्वतःला किंवा तुमच्या मित्र-मैत्रिणींना जाणवून द्या की तुमची किंवा त्यांची यात काहीच चूक नाहीये, आणि चिंता, लाज वाटणे, किंवा असुरक्षिततेच्या भावना यावर उपचार करण्यासाठी तुमचा विश्वास असेल अश्या एखाद्या एखाद्या व्यक्तीशी बोला.

सेल्फ-केअर द्वारे स्वतःला यातून सावरण्यासाठी वेळ द्या , आणि अशा लोकांच्या संपर्कात रहा जे तुम्हाला मदत करतील आणि तुमचा आत्मविश्वास वाढवतील.

काही काळासाठी तुम्ही ब्रेक घेऊन आणि या ऑनलाईन स्पेसेस बद्दलच्या सुरक्षित पद्धत पुन्हा एकदा शिकून (उदाहरणार्थ स्ट्रॉंग पासवर्ड ठेवणे किंवा पर्सनल माहिती शेअर करताना सावध राहणे) याचा चांगल्या कामांसाठी वापर सुरू करू शकता.

स्वत:ला सुरक्षित करणे: ऑनलाईन काय काय शेअर करावे

आपण आत्तापर्यंत अनेक ऑनलाईन थ्रेट्स बद्दल जाणून घेतलं, पण तुमची प्रायव्हसी स्ट्रॉंग करण्यासाठी आणि डेटा वर नियंत्रण मिळवण्यासाठी अशा काही गोष्टी आहेत ज्या तुम्ही नक्कीच करू शकता! ऑनलाइन शेअर करण्यासाठी काय सुरक्षित आहे आणि काय नाही हे समजून घेऊन या आणि या धोक्यांपासून स्वत:चे संरक्षण कसे करावे समजून घेऊन या थ्रेट्स पासून स्वत:ला कसे सुरक्षित ठेवावे. आपल्याला ऑनलाइनजी माहिती विचारण्यात येते ती सामान्यत: या तीनपैकी एका श्रेणीत मोडते.

पर्सनल माहिती

अशी कोणतीही माहिती ज्यामुळे अनोळखी व्यक्तींना एखाद्या व्यक्तीची प्रत्यक्ष किंवा अप्रत्यक्षपणे ओळख पटते - उदाहरणार्थ तुमचे नाव! हे जरी खूप घातक वाटत नसलं तरी अशीच छोटी छोटी माहिती एकत्र करून त्या व्यक्तीची ओळख स्पष्ट होऊ शकते.

खाली काही पर्सनल माहितीची उदाहरणे आहेत::

- बेसिक माहिती: तुमचे पूर्ण नाव , जन्मतारीख,किंवा तुमचे वय.
- संपर्क साधण्यासबंधी माहिती: तुमचा फोन नंबर, घरचा पत्ता, ईमेल आयडी.
- सोशल मीडिया ॲक्टीविटी: लोकेशन टॅग असलेले फोटोज, विशिष्ट ठिकाणी दिलेली भेट, किंवा सहज ओळख पटेल अशा पोस्ट्स.

ऑनलाईन पर्सनल माहिती शेअर केल्याने तुमची ओळख चोरण्याचा , स्टॉकिंग, किंवा फिशिंग अटॅक्सचा धोका निर्माण होतो. विशेषत: पब्लिक प्लॅटफॉर्म्स वर पर्सनल माहिती शेअर करण्याआधी दोनदा विचार करा,.

नॉन-पर्सनल माहिती

एखाद्याची ओळख पटणार नाही अशी माहिती - उदाहरणार्थ आवडता रंग! जरी हे सुरक्षित वाटत असलं, तरी हा नॉन-पर्सनल डेटा कधी-कधी इतर महितीशी जोडून, यातून देखील एखाद्या व्यक्तीची ओळख पटवली जाऊ शकते.

खाली नॉन-पर्सनल माहितीची काही उदाहरणे आहेत:

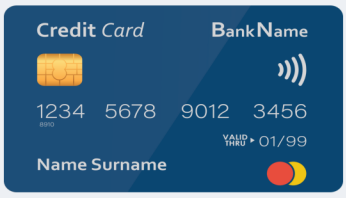
- आवडी-निवडी: तुमचा आवडता रंग, टीव्ही शोज, किंवा छंद.
- सर्वसामान्य मते: एखाद्या पिक्चर किंवा पुस्तकाबद्दलचे तुमचे मत.
- एकत्रित डेटा: ट्रेण्ड्स किंवा सर्व्हे रिझल्ट्स ज्यामध्ये व्यक्तींची माहिती दिली जात नाही.

नॉन-पर्सनल माहिती शेअर करणे सामान्यत: सुरक्षित असते. तरीही, सावध राहा: तुमच्या आवडी-निवडी किंवा छंद सुद्धा मार्केटर्स, ॲल्गोरिदम्स किंवा छलवेष घेऊन फसवणारे यांना तुमच्या आचरणाबद्दल अंदाज देऊ शकतात.

संवेदनशील पर्सनल माहिती

संवेदनशील माहिती - म्हणजे, पर्सनल माहितीचा गैरवापर होण्याची शक्यता जास्त असते कारण यामध्ये इतर अनेक महत्त्वाची माहिती लॉक केली जाते - उदाहरणार्थ तुमची सही! या माहितीचा गैरवापर झाला तर त्याचे गंभीर परिणाम होऊ शकतात उदाहरणार्थ आर्थिक फसवणूक किंवा तुमची ओळख चोरण्याचा प्रयत्न देखील केला जाऊ शकतो.

खाली संवेदनशील पर्सनल माहितीची काही उदाहरणे दिली आहेत:



- <u>ओळख पटण्यासंबंधी डेटा:</u> तुमची सही, सरकारने जारी केलेले आयडी नंबर्स (उदाहरणार्थ , आधार, पासपोर्ट, सोशल सिक्युरिटी नंबर)
- <u>आर्थिक माहिती:</u> बँक अकाऊंट नंबर्स, क्रेडिट/डेबिट कार्ड संबंधी माहिती, किंवा यूपीआय पिन्स.
- <u>ऑथेंटिकेशन संबंधी माहिती:</u> पासवर्ड्स, पिन्स, सिक्युरिटी आंसर्स, किंवा बायोमॅट्रिक डेटा उदाहरणार्थ फिंगरप्रिंट्स किंवा फेशियल रेकग्निशन.
- <u>आरोग्यासंबंधी माहिती:</u> मेडिकल रेकॉर्ड्स, डायग्नोसेस, किंवा प्रिस्क्रिप्शन्स.

हे का महत्त्वाचे आहे: संवेदनशील पर्सनल माहिती हे सायबर गुन्हेगारांसाठी सर्वात मुख्य टार्गेट आहे. हा डेटा सुरक्षित ठेवणे अत्यंत महत्त्वाचे आहे आणि हा डेटा फक्त सुरक्षित प्लॅटफॉर्म्स वरील विश्वस्त लोकांबरोबरच शेअर करावा.

ॲक्टिव्हिटी

कोणती माहिती ऑनलाईन शेअर करणं सुरक्षित आहे हे ओळखण्यासाठी मीराला मदत करा. खालील परिस्थिती वाचा आणि:

- **यामध्ये माहितीचा प्रकार ओळखा**

  पर्सनल | नॉन-पर्सनल | संवेदनशील माहिती

- **मीराने काय करावं हे ठरवा**

  बिनधास्त शेअर करावं | शेअरिंग करू नये | विचार करून शेअर करावं (जर गरज असेल आणि विश्वस्त प्लॅटफॉर्म्स असतील तरंच)

प्रसंग:

- एक ऑनलाईन पझल-सॉलव्हिंग स्पर्धेमध्ये भाग घेण्यासाठी मीराला तिचं पूर्ण नाव आपलोड करायला सांगितले जाते.
  - प्रकार: _____
  - कृती: _____

- एक कूकिंग ॲपद्वारे मीराला रेसिपीज पाठवण्यासाठी तिचा ईमेल ॲड्रेस विचारला जातो.
  - प्रकार: _____
  - कृती: _____
- एक व्हेरिफाय न केलेली वेबसाईट मीराला मोफत गिफ्ट तिला देण्यासाठी तिचा फोन नंबर विचारते.
  - प्रकार: _____
  - कृती: _____
- एएका गेमिंग ॲपवर मीराला तिचं वय तपासण्यासाठी तिची जन्मतारीख विचारली जाते.
  - प्रकार: _____
  - कृती: _____
- मीरा तिच्या आवडत्या पुस्तकाचं नाव एक डिस्कशन फोरम मध्ये शेअर करते.
  - प्रकार: _____
  - कृती: _____
- एक शॉपिंग वेबसाईट एक प्रॉडक्ट डिलिव्हर करण्यासाठी मीराला तिचा पत्ता विचारते.
  - प्रकार: _____
  - कृती: _____
- एका ऑनलाईन बँकिंग सर्व्हिससाठी मीराला तिची ओळख सत्यापित करण्यासाठी तिची सही अपलोड करायला सांगितले जाते.
  - प्रकार: _____
  - कृती: _____

रीकॅप: ऑनलाईन माहिती शेअर करताना सुरक्षित कसे राहावे

- ☐ **शेअर करण्याआधी विचार करा: माहिती ऑनलाईन शेअर करणे खरंच गरजेचे आहे का हे नेहमी विचारा.**
- ☐ **व्हिजिबिलिटी मर्यादित करा: सोशल मीडिया वर प्रायव्हसी सेटिंग्सचा वापर करून कोण कोण तुमची पोस्ट बघू शकते हे तुम्ही नियंत्रित करू शकता.**
- ☐ **पब्लिक वाय-फाय वर सावध रहा: पब्लिक किंवा असुरक्षित नेटवर्कशी कनेक्टेड असताना संवेदनशील माहिती शेअर करणे टाळा.**
- ☐ **सुरक्षित चॅनल वापरा: संवेदनशील माहिती (उदाहरणार्थ बँकेसंबंधी माहिती) फक्त एन्क्रिप्टेड प्लॅटफॉर्म्स वरच शेअर करा.**
- ☐ **अकाउंट्स वेळोवेळी मॉनिटर करा: कोणत्याही प्रकारचा दुरुपयोग वेळेआधीच टिपण्यासाठी तुमच्या ऑनलाईन आकाऊंटस वर काही विचित्र तर घडत नाही ना यावर लक्ष ठेवा.**

प्रकरण 4: विचारपूर्वक क्लिक करा: चुकीची माहिती शिताफीने टाळणे

शुभम तिच्या फोन वर स्क्रोल करत असताना ही महत्त्वाची वाटणारी बातमी समोर दिसली. लगेचच, सगळ्यांना कळावं म्हणून तिने ती माहिती तिच्या सोशल मीडियावर शेअर केली.

अरे शुभम, मला वाटतंय ही बातमी खोटी आहे!

याबद्दल काल सगळा खुलासा झाला होता, सावध रहा!

खरं नाहीये हे शुभम, मी आत्ताच याबद्दल स्पष्ट करणारा एक लेख वाचला आहे!

लगेचच शुभमला अशा अनेक कमेन्ट्स तिच्या शेअर केलेल्या पोस्ट वर दिसायला लागल्या.

काय? नाही! हे खोटं असूच शकत नाही, ही बातमी किती खरी वाटत होती! सिद्धार्थ! हे बघ मी माझ्या प्रोफाईल वरून शेअर केली, आणि आता लोक म्हणतायत की ही बातमी खोटी आहे! मला कळत नाहीये काय करू मी आता, आता लोकं यामुळे माझ्यावर हसतील!

काळजी नको करूस शुभम, तू एकटा नाहीयेस! माझ्या इतर काही मित्रांना देखील हल्लीच असाच अनुभव आला आहे. असं वाटतंय की तू चुकीच्या माहितीच्या जाळ्यात अडकला आहेस. मला फार काही माहीत नाही, पण आपण एकत्र मिळून ऑनलाईन माहिती कशी नॅव्हिगेट करायची ते जरा शोधूया का?

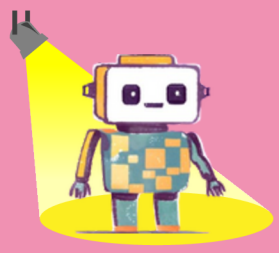
मिशन एनआयओ मध्ये स्वागत आहे: नॅव्हिगेट इन्फॉर्मेशन ऑनलाईन. आता वेळ आहे न्यूज नॅव्हिगेटर बनण्याची

ॲक्टीविटी

तुम्ही कधी एखादी गोष्ट खरी आहे असं समजून ऑनलाईन शेअर केली आहे, आणि नंतर ती खोटी आहे असा शोध लागला असे झाले आहे का? तुम्हाला हा अनुभव कसा वाटला? तुम्ही पुढच्या वेळेस वेगळं काय कराल?

थोडा वेळ विचार करा आणि खालील जागेत तुमचे विचार लिहून काढा.

ऑनलाईन माहितीचे प्रकार



मी हे सोपं करून सांगतो! तुझा सोशल मीडिया न्यूजफीड एकत्र बघूया, शुभम. लगेच तुला लक्षात येईल की ऑनलाईन माहिती साधारणपणे खालील काही कॅटेगरीज संबंधी असते:

व्हेरिफाय केलेली आणि विश्वास ठेवण्यासारखी माहिती

काही माहिती किंवा काही बातम्या नावाजलेल्या न्यूज आऊटलेट्स, संशोधन संस्था, किंवा सरकारी वेबसाईट्स मधून येतात. त्या सामान्यतः खऱ्या असतात आणि त्या विश्वास ठेवण्याजोग्या आहेत हे चेक केलेले असते.

एखाद्या विषयावरची मते आणि पर्सनल कंटेंट

असे कंटेंट प्रत्येक व्यक्तीचा दृष्टिकोण दर्शवतात - उदाहरणार्थ, ब्लॉग्स, पोस्ट्स, किंवा पर्सनल व्हिडिओ जर्नल्स एखाद्या व्यक्तीच्या दैनंदिन आयुष्याबद्दल, त्याच्या भावना आणि मते याबद्दल सांगतात पण हे खऱ्या किंवा खोट्या माहितीवर आधारित असू शकतात.

चुकीची माहीत, गैरसमज निर्माण करण्यासाठी पसरवलेली माहिती आणि खोट्या बातम्या

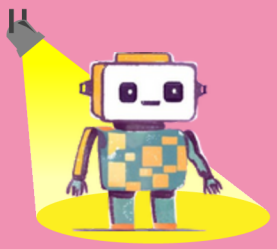
चुकीची माहीत, गैरसमज निर्माण करण्यासाठी पसरवलेली माहिती आणि खोट्या बातम्या हे सगळे खोट्या माहितीचे प्रकार आहेत. यामध्ये खळबळजनक हेडलाईन्स, भावनिक भाषा, अस्पष्ट सोर्स, आणि एक प्रकारची अर्जन्सी याचा समावेश असतो.

विनोदी आणि मनोरंजक माहिती

इंटरनेट जोक्स आणि मीम्सने भरलेलं आहे यांना कधी कधी बातम्या समजलं जाऊ शकतं - विशेषतः जेव्हा त्या एखाद्या सत्य घटना किंवा प्रकरणावर भाष्य करतात.

ओह.... म्हणजे इंटरनेट वरचं सगळं काही खरं किंवा अगदी गांभीर्याने घेण्यासारखं असतंच असं नाही! मला आता समजलंय असं वाटतंय

अगदी बरोबर! जेव्हां तुम्ही सराव करता , तुम्ही या मध्ये फरक करायला लागलात, की मग तुम्ही इंटरनेट अगदी सुरक्षितपणे नॅव्हिगेट करू शकता.

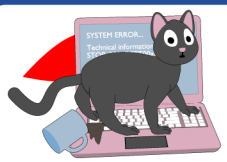


शुभमच्या न्यूजफीड आणि मेसेजेस मध्ये तिला या आठवड्यात आलेल्या आणखीन काही पोस्ट्स बघूया. प्रत्येक माहिती कोणत्या प्रकारची आहे हे तुम्ही सांगू शकता का?

माझा छंदच माझा व्यवसाय कसा झाला :

माझ्या क्रिएटिव्ह व्यवसायामागचा माझा खरा प्रवास

वैज्ञानिक याची पुष्टी करतात: कीबोर्डचा वापर करून दुष्ट शक्तींना बोलवण्यापासून माणसांना रोखण्यासाठी मांजरी लॅपटॉप वर येऊन बसतात.



अगं शुभम! मी हल्लीच वाचलंय की वैज्ञानिकांना अल्झायमरचा उपचार शोधण्यामध्ये यश मिळाले आहे! तुला सांगावंसं वाटलं कारण तू तुझ्या आजीसाठी उपचार शोधत होतीस ना.

उंदरांवर केलेल्या प्रयोगात असे आढळून आहे की श्वासाद्वारे झेनॉन वायू आत घेतल्याने मायक्रोग्लियाचे प्रमाण सुधारते ज्यामुळे अल्झायमर बरा करण्यामध्ये मदत होते.
https://www.science.org/doi/10.1126/scitranslmed.adk3690

>> **खूप वेळा फॉरवर्ड करण्यात आला आहे**

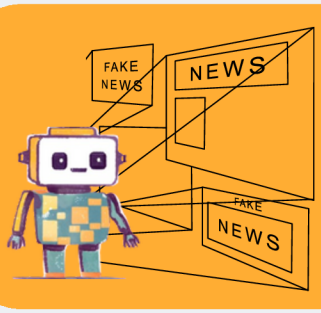
प्रथम श्रेणी प्रवास करत असलेल्या सुंदर पिच्चई यांचा फ्लाईट अटेंडंट ने केला अपमान - सत्य वाचून तुमचा विश्वास बसणार नाही!

पुढे वाचा....

चुकीची माहिती कशी ओळखायची

दादा, आणखी एक प्रॉब्लेम आहे र! विनोदी पोस्ट्स मध्ये खोटी माहिती ओळखणे सोपे आहे, पण जेव्हा पोस्ट्स गंभीर किंवा कामाच्या असतात, त्या खऱ्या आहेत हे मी कसं ओळखू?

हा उत्तम प्रश्न आहे. खोटी माहिती ओळखण्यात ग्लिच अगदी एक्स्पर्ट आहे, आणि तो तुम्हाला खोट्या माहितीचे प्रकार आणि लक्षणे दाखवून देईल.



वर्ल्ड वाईड वेब स्कॅन करणे.... कोणतीही माहिती असंख्य चॅनल्स द्वारे ऑनलाईन प्रवास करते - सोशल मीडिया, न्यूज साईट्स, प्रायव्हेट मेसेजेस - आणि प्रत्येक चॅनल वर त्यामध्ये बदल होत असतात. सगळी खोटी माहिती एकसारखीच दिसते असे नाही, पण मुख्यतः याचे तीन प्रकार आहेत....

1.खोटी माहिती

चुकून शेअर केली गेलेली चुकीची किंवा दिशाभूल करणारी माहिती - म्हणजे, माहिती शेअर करणाऱ्याला हे माहीत नसतं की ही माहिती खोटी आहे.

जसं परवा मी चुकून परीक्षा पोस्टपोन झाल्याची बातमी शेअर केली!

ज्या व्यक्तीने हा मेसेज तयार केला आहे तो त्याने विद्यार्थ्यांना दिशाभूल करण्याच्या हेतूने तयार केलेला असू शकतो.

2. गैरसमज पसरवण्यासाठी शेअर केलेली माहिती

लोकांची दिशाभूल करण्यासाठी शेअर केली गेलेली माहिती-बऱ्याचदा, पॉलिटिकल, आर्थिक किंवा सोशल फायद्यासाठी.

ती माहिती एका न्यूज साईट वर होती असे वाटत होते आणि म्हणून मला ती खरी वाटली....

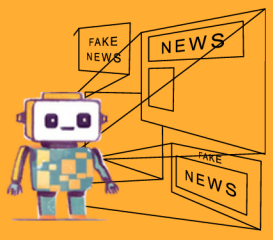
3. खोट्या बातम्या

जेव्हा खोटी माहिती न्यूज म्हणून शेअर केली जाते - आणि ते ही अगदी खरी वाटावी आणि दिसावी अश्याप्रकारे तयार करून.

.... कधी कधी एकच माहिती या तिन्ही प्रकारे शेयर केल्या जावू शकते!

ॲक्टीविटी

तुमच्या बघण्यात आलेली खोटी बातमी, गैरसमज पसरवण्यासाठीची माहिती किंवा चुकीची माहिती याची काही उदाहरणे लिहून काढा. तुम्हाला कसं कळले की ती माहिती खोटी आहे? तुम्हाला आधीपासून माहीत असलेल्या काही गोष्टी खरंच मदत करू शकतात!



तुम्ही एखादी माहिती/बातमी वेगवेगळ्या पद्धतींनी चेक करू शकता. एक सोपी आणि सहज लक्षात ठेवण्यासारखी पद्धत म्हणजे एसयूसीएस (SUCS) पद्धत, म्हणजे सोर्स, यूबीक्विटी, कॉंटेक्स्ट आणि सेकंड ओपीनियन. यामुळे तुम्ही ऑनलाईन खात्रीशीर माहितीच बघता आहात हे सुनिश्चित करण्यासाठी काय-काय गोष्टी तपासाव्यात हे जाणून घेण्यामध्ये मदत होईल. चला तर प्रत्येक स्टेप बारकाईने बघूया आणि या दोन न्यूज चेक करण्याचा प्रयत्न करूया!

https://economictimes.indiatimes.com/news/budget-2025

Home News Market Economy Politics Elections Blogs

द इकॉनॉमिक टाईम्स

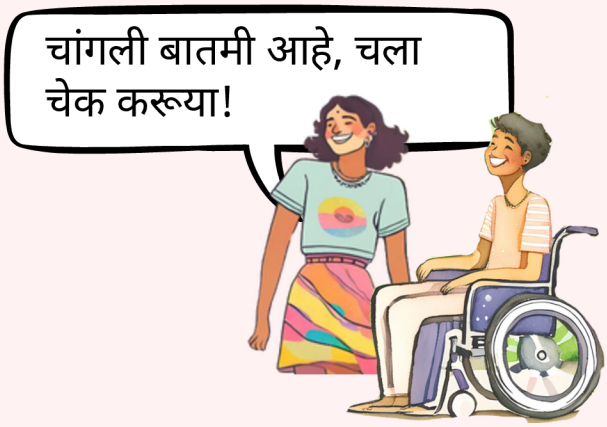
आरोग्य मंत्रालयाच्या निधीवरील नवीनतम अपडेट्स

डॉ. सोहिनी कुमार | शेवटचे अपडेट: २२ फेब्रुवारी २०२२

NATIONAL HEALTH MISSION
राष्ट्रीय स्वास्थ्य मिशन
Ministry of Health & Family Welfare

नवी दिल्ली: सत्ताधारी पक्ष येत्या राज्य निवडणुकांसाठी सज्ज होत असताना, आरोग्य मंत्रालयाने त्यांच्या राष्ट्रीय आरोग्य अभियानासाठी निधीत मोठी कपात केली आहे ज्यामुळे रुग्णालयांमध्ये पुरवठ्याची कमतरता असलेल्या ५०% राज्यांमध्ये परिस्थिती बदलू शकते. विरोधी पक्षाने....

लेखकाबद्दल:
डॉ. सोहिनी कुमार या स्कूल ऑफ इकॉनॉमिक्स अँड बिझनेसमध्ये प्राध्यापक आहेत आणि त्यांनी गेल्या दशकाहून अधिक काळ भारतीय आरोग्य प्रणाली आणि राजकारणाचा अभ्यास केला आहे.



http://economicsmadeeeazy123.biz/india-to-pay-foreign-

इकॉनॉमिक्समेडईझी

भारत आता खाजगी बँक खात्यांमधून फेडणार आंतरराष्ट्रीय कर्ज!

आंतरराष्ट्रीय देशांकडून घेतलेल्या कर्जामुळे भारत दिवसेंदिवस कर्जबाजारी होत चालला आहे आणि राष्ट्रीय संपत्ति झपाट्याने कमी होत चालली आहे. राज्यात निधीचा तुडवडा भासत आहे आणि हे भरून काढण्याचा एकमेव मार्ग म्हणजे नागरिकांच्या बँक खात्यांमधून मदत घेणे! खाजगी बँकांनी आधीच या उपक्रमात सहभागी न होण्याचे जाहीर केले असले तरी, स्टेट बँकांमधील कोणतीही खाती दुरुपयोग होण्यापासून सुरक्षित राहणार नाहीत.... (पुढे वाचा)

फोटो: भारतीय परराष्ट्र सचिव नवीन खाजगी बँकेच्या मालकांशी हस्तांदोलन करताना

सोर्स/माध्यम

सर्वात पहिले पाऊल म्हणजे एखाद्या बातमीचा किंवा माहितीचा सोर्स किंवा माध्यम चेक करणे. ते विश्वास ठेवण्याजोगे आहे का? तुम्ही त्या सोर्सवर विश्वास ठेवू शकता का?

म्हणजे मी हे चेक करायला हवं की ते कोणी पोस्ट केलंय? मला साधारणपणे माझ्या विश्वासातल्या मित्रांकडूनच न्यूज फॉरवर्ड केल्या जातात...

मला वाटतं महत्त्वपूर्ण आहे की माहितीचा मूळ स्त्रोत काय आहे - न्यूज आऊटलेट्स, रीसर्च स्टडीज किंवा स्टेटमेंट्स. मला वाटतं आपण हे देखील तपासायला हवं. पण कसं?

ही चेकलिस्ट वापरा. तुम्ही जर यातील बऱ्याच पर्यायांवर टिक करू शकलात, तर ही माहिती विश्वास ठेवण्याजोगी आहे. जर तुम्हाला शंका असेल, तर ती न्यूज फॉरवर्ड करू नका!

चला बघूया!

चेकलिस्ट

- ☐ ही वेबसाईट सुस्थापित न्यूज आऊटलेट, बारकाईने चेक केलेली किंवा प्रतिष्ठित संस्था आहे का?
- ☐ ही वेबसाईट व्यवस्थित चेक केलेली अचूक माहिती शेअर करण्यासाठी प्रसिद्ध आहे का?
- ☐ हे यूआरएल सुरक्षित आहे का (म्हणजे 'https' पासून सुरू होते का? का ही वेबसाईट ब्राऊझरने असुरक्षित म्हणून फ्लॅग केली आहे?
- ☐ वेबपेज स्पष्ट आणि उत्तमरित्या डिझाईन केलेले आहे का, का सतत त्यावर जाहिराती पॉपअप होत असतात, त्यामध्ये लिखाणातील चुका दिसत आहेत आणि डिझाईन पण एकसारखं दिसत नाहीये?
- ☐ लेखक सुशिक्षित आणि/किंवा विश्वस्त आहे का? त्यांनी या विषयाचा यापूर्वी अभ्यास केला आहे का आणि ते याबाबतीत प्रामाणिक आहेत का?

चला चेक करूया!

चला आपल्या लेखांकडे परत जाऊया. त्यांचे स्रोत विश्वसनीय आहेत का?

https://economictimes.indiatimes.com/news/budget-2025

Home Latest News Market Economy Politics Elections Blogs

द इकॉनॉमिक टाईम्स

आरोग्य मंत्रालयाच्या निधीवरील नवीनतम अपडेट्स

डॉ. सोहिनी कुमार | शेवटचे अपडेट: २२ फेब्रुवारी २०२२

NATIONAL HEALTH MISSION
राष्ट्रीय स्वास्थ्य मिशन
Ministry of Health & Family Welfare

नवी दिल्ली: सत्ताधारी पक्ष येत्या राज्य निवडणुकांसाठी सज्ज होत असताना, आरोग्य मंत्रालयाने त्यांच्या राष्ट्रीय आरोग्य अभियानासाठी निधीत मोठी कपात केली आहे ज्यामुळे रुग्णालयांमध्ये पुरवठ्याची कमतरता असलेल्या ५०% राज्यांमध्ये परिस्थिती बदलू शकते. विरोधी पक्षाने....

लेखकाबद्दल:
डॉ. सोहिनी कुमार या स्कूल ऑफ इकॉनॉमिक्स अँड बिझनेसमध्ये प्राध्यापक आहेत आणि त्यांनी गेल्या दशकाहून अधिक काळ भारतीय आरोग्य प्रणाली आणि राजकारणाचा अभ्यास केला आहे.

या वेबसाईटची यूआरएल https पासूनच सुरू होते

इकॉनॉमिक टाईम्स ही एक सुस्थापित न्यूज साईट आहे, जी चेक केलेली आणि अचूक माहिती पब्लिश करण्यासाठी प्रसिद्ध आहे

हे लेखक देखील या विषयावर लिहिण्यासाठी पात्र आहेत

एकंदर, वेब पेज स्पष्ट आणि उत्तम पद्धतीने डिझाईन केलेला आहे, त्यावर कोणत्याही जाहिराती, पॉपअप्स, किंवा लिखणातील चुका दिसत नाहीत

वेबसाईटची यूआरएल असुरक्षित आहे! ती http पासून सुरू होते ज्यात शेवटी s नाहीये, आणि त्यात स्पेलिंगच्या चुका आणि इतर विसंगती दिसत आहेत. आणि तिच्या शेवटी देखील .biz असे आहे.

ही वेबसाईट अविश्वसनीय आणि अनधिकृत आहे, आणि आपल्याला माहीत नाही की ती अचूक किंवा विश्वसनीय आहे का नाही!

या न्यूजचा कोणी लेखक पण नाही.

या वेबसाईट वर मोठ-मोठे पॉपअप्स आणि जाहिराती दिसत आहेत, आणि फॉर्मेटिंग आणि लिखाणात देखील चुका आहेत आणि इतर विसंगती देखील आहेत

http://economicsmadeeeazy123.biz/india-to-pay-foreign-

इकॉनॉमिक्समेडईझी

भारत आता खाजगी बँक खात्यांमधून फेडणार आंतरराष्ट्रीय कर्ज!

आंतरराष्ट्रीय देशांकडून घेतलेल्या कर्जामुळे भारत दिवसेंदिवस कर्जबाजारी होत चालला आहे आणि राष्ट्रीय संपत्ति झपाट्याने कमी होत चालली आहे. राज्यात निधीचा तुडवडा भासत आहे आणि हे भरून काढण्याचा एकमेव मार्ग म्हणजे नागरिकांच्या बँक खात्यांमधून मदत घेणे! खाजगी बँकांनी आधीच या उपक्रमात सहभागी न होण्याचे जाहीर केले असले तरी, स्टेट बँकांमधील कोणतीही खाती दुरुपयोग होण्यापासून सुरक्षित राहणार नाहीत.... (पुढे वाचा)

फोटो: भारतीय परराष्ट्र सचिव नवीन खाजगी बँकेच्या मालकांशी हस्तांदोलन करताना

टीप: टॅब्लॉइड्स, फ्लायर्स, मेसेज बोर्ड, सोशल मीडिया पोस्ट, ब्लॉग आणि वेबसाइट्स ज्यांबद्दल फारसे लोक ऐकत नाहीत ते अविश्वसनीय स्रोत आहेत!

ॲक्टीविटी

तुम्ही पाहिलेल्या तीन विश्वसनीय साईट्सची आणि 3 अविश्वसनीय साईट्सची नावे लिहा.

_____

_____

_____

_____

ही एक खूप उपयुक्त टीप आहे कारण आता तुम्ही लक्ष ठेवाल की मला कोणत्या माध्यमातून न्यूज आली आहे!

आता तुम्ही एक जबाबदार नेटीझन - बनत चालले आहात - पण सोर्सेस वरंच थांबून चालणार नाही!

यूबीक्विटी

यूबीक्विटी म्हणजे काहीतरी असे जे एकसारखं आहे किंवा सगळीकडे आढळणारं आहे. मिळालेली माहिती युनिक आहे का किंवा ती वेगवेगळ्या सोर्सेस द्वारे चेक केली जाऊ शकते का? अनेक विश्वस्त सोर्सेस वर त्याबद्दल दखल घेतली गेली आहे का आणि चेक केली गेली आहे का?

जरा थांब, मला हे समजले नाही. हे का गरजेचे आहे? खोट्या बातम्या कधी-कधी आगीसारख्या पसरतात नाही का?

खरंय: फक्त याकारणाने की अनेक वेबसाईट्स याबद्दल ठाम पणे सांगता आहेत, ती बातमी खरी होत नाही. पण काही बाबतीत - विशेषत: गैरसमज पासरवण्यासाठी शेअर केलेल्या माहिती संदर्भात - ती बनवलीच यासाठी जाते की त्यामुळे लोकं घाबरतील. अशी बातमी ऑनलाईन किंवा मेसेज मध्ये वाचायला मिळाल्याची कल्पना कर:

विचार कर: जर संपूर्ण देशात असं काही तरी भयानक घडत असेल, तर इतर न्यूज साईट्सने देखील याची दखल घेतलीच असती. राष्ट्रीय आणि आंतरराष्ट्रीय संस्थांनी यावर लगेच तपास सुरू केला असता , लोकांच्या तक्रारी नोंदवण्याची सुरुवात झाली असती, आणि अधिकृत स्टेटमेंट्स केली गेली असती....

आणि हे काहीच जर होत नसेल आणि ही न्यूज काही मोजक्याच अनोळखी ऑनलाईन स्पेसेस वर दिसत असेल, तर हे खोटं असू शकतं असं म्हणायला काहीच हरकत नाही..

धोका: 5जी नेटवर्क्स जगभरात कोविड-19 पसरवण्यास कारणीभूत!

मिठामध्ये सापडले जीवघेणे सायनाइड: भारतातील दुकानांमधून घरोघरी पोहोचते आहे विष

संदर्भ

तुमचं तुम्ही तपासून बघा की माहिती किंवा न्यूजचा संदर्भ ती जय संदर्भाने मांडली जाते आहे त्यामध्येसुसंगती आहे का.

चांगली कल्पना आहे!

आणखी एक महत्त्वाचा मुद्दा विसरून चालणार नाही:संपूर्ण माहिती ही कोणताही मुद्दा न वगळता, त्याचा टोन बदलून किंवा चुकीच्या पद्धतीने सांगितला जात नाही ना हे आपण सुनिश्चित करायला हवे.

चेकलिस्ट

- ☐ नावं, ठिकाणं आणि तारखा अचूक आहेत ना, का एखादी गोष्ट आहे त्यापेक्षा वेगळी सांगितली जाते आहे?
- ☐ माहिती अपडेट केलेली आहे का?
- ☐ संदर्भ पुराव्यांसकट स्पष्ट केलेला आहे का, का महत्त्वाची माहिती गहाळ झाली आहे?
- ☐ संबंधित व्यक्तींचे, ठिकाणाचे किंवा प्रसंगाचेच फोटो आणि व्हिडिओज माहिती मध्ये दिलेले आहेत ना?
- ☐ दिलेले फोटोज आणि व्हिडिओज नीट सादर केलेले आहेत ना, दिशाभूल करण्यासाठी ते क्रॉप, एडिट किंवा अल्टर तर केलेले नाहीत ?
- ☐ आपण परिस्थिती चांगल्या प्रकारे समजू शकू असा दृष्टिकोण यात चुकलेला तर नाही ना?

टीप: इतर सोर्सेस कडून संदर्भ जाणून घेण्यासाठी तुम्ही आहात त्या साईट वरून बाहेर पडा - शक्यतो, मूळ सोर्स बघा! त्या विषयावर सविस्तर माहिती वाचा!

संदर्भ बघताना, तुम्ही बघत असेलेले आर्टिकल, पोस्ट किंवा मेसेज यामध्ये पुरावे म्हणून संशोधन, रिपोर्ट्स, रेकॉर्डिंग्स किंवा कागदपत्रे याच्या लिंक्स दिलेल्या आहेत ना हे सुनिश्चित करा. यामध्ये तुम्हाला हे दिसते आहे का की ही माहिती कुठून मिळाली आहे? सर्व पुरावे विश्वास ठेवण्याजोगे आहेत का?

चला चेक करूया!

आपल्या आर्टिकल कडे वळू या. त्यात दिलेली माहिती, ती मांडण्याची पद्धत, संदर्भाशी संबंधित आहे का?

त्या आर्टिकल्स मध्ये ठिकाण आणि तारीख दिलेली आहे जी अपडेटेड आहे.

त्या आर्टिकल मध्ये पुराव्यासह संदर्भ दिलेला आहे, आणि इतर साईट्स वर देखील तीच माहिती दिसते आहे.

राष्ट्रीय आरोग्य मिशन संबंधी आर्टिकल मधील फोटो त्यातील महितीशी जुळतो आहे आणि तो फोटो अधिकृत असून त्यामध्ये कोणतेही एडिटिंग आणि अल्टरेशन केलेले नाही.

https://economictimes.indiatimes.com/news/budget-2025

Home Latest News Market Economy Politics Elections Blogs

द इकॉनॉमिक टाईम्स

आरोग्य मंत्रालयाच्या निधीवरील नवीनतम अपडेट्स

डॉ. सोहिनी कुमार **शेवटचे अपडेट: २२ फेब्रुवारी २०२२**

NATIONAL HEALTH MISSION
राष्ट्रीय स्वास्थ्य मिशन
Ministry of Health & Family Welfare

नवी दिल्ली: सत्ताधारी पक्ष येत्या राज्य निवडणुकांसाठी सज्ज होत असताना, आरोग्य मंत्रालयाने त्यांच्या राष्ट्रीय आरोग्य अभियानासाठी निधीत मोठी कपात केली आहे ज्यामुळे रुग्णालयांमध्ये पुरवठ्याची कमतरता असलेल्या ५०% राज्यांमध्ये परिस्थिती बदलू शकते. विरोधी पक्षाने....

लेखकाबद्दल:
डॉ. सोहिनी कुमार या स्कूल ऑफ इकॉनॉमिक्स अँड बिझनेसमध्ये प्राध्यापक आहेत आणि त्यांनी गेल्या दशकाहून अधिक काळ भारतीय आरोग्य प्रणाली आणि राजकारणाचा अभ्यास केला आहे.

दुसऱ्या आर्टिकल मध्ये तारीख, ठिकाण आणि लेखकाचे नाव दिलेले नाही.

कोणत्याही देशांशी किंवा बँकांशी दिलेल्या कर्जाचा संदर्भ दिलेला नाही! इतकी महत्त्वाची बातमी असून सुद्धा इतर कोणत्याही साईट्स वर ही माहिती पब्लिश केलेली नाही.

यामधील फोटो योग्य संदर्भात वापरला गेला नाही किंवा त्याचे कॅप्शन देखील चुकीचे आहे! हा फोटो तरुण व्यावसायिकांसाठी एक योजना सुरू करण्याबाबत ब्रिटिश आंतरराष्ट्रीय सचिव भारतीय परराष्ट्र व्यवहार मंत्र्यांशी भेटतानाचा आहे.

http://economicsmadeeeazy123.biz/india-to-pay-foreign-

इकॉनॉमिक्समेडईझी

भारत आता खाजगी बँक खात्यांमधून फेडणार आंतरराष्ट्रीय कर्ज!

आंतरराष्ट्रीय देशांकडून घेतलेल्या कर्जामुळे भारत दिवसेंदिवस कर्जबाजारी होत चालला आहे आणि राष्ट्रीय संपत्ति झपाट्याने कमी होत चालली आहे. राज्यां[illegible] निधीचा तुटवडा भासत आहे आणि हे [illegible]न काढण्याचा एकमेव मार्ग म्हणजे नागरिकांच्या बँक खात्यांमधून मदत घेणे! खाजगी बँकांनी आधीच या उपक्रमात सहभागी न होण्याचे जाहीर केले असले तरी, स्टेट बँकांमधील कोणतीही खाती दुरुपयोग होण्यापासून सुरक्षित राहणार नाहीत.... (पुढे वाचा)

फोटो: भारतीय परराष्ट्र सचिव नवीन खाजगी बँकेच्या मालकांशी हस्तांदोलन करताना

खाली आणखी काही बातम्या दिल्या आहोत: त्या दिशाभूल करणाऱ्या का आहेत हे तुम्ही ओळखू शकता का?

@citizensforum

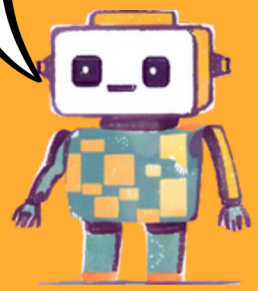
केंद्रीय रुग्णालयात आजचे शेवटचे 50 कोविड-19 वॅक्सिन सुपूर्द करण्यात आले. पुढचा एक आठवडा कोणतेही वॅक्सिन येणार नाहीत असे तज्ज्ञांनी सांगितले.

सेकंड ओपीनियन

अजूनही जर तुम्हाला दिलेल्या माहिती बद्दल विश्वास वाटत नसेल, तर एक सेंकड ओपीनियन घेतल्याने तुम्हाला नक्कीच मदत मिळेल - उदाहरणार्थ कुणी तज्ज्ञ किंवा ऑनलाईन रिसोर्स उदाहरणार्थ फॅक्ट चेकिंग वेबसाईट.

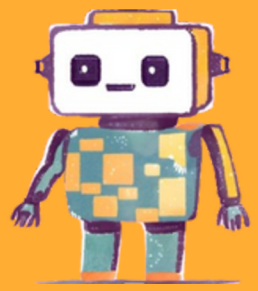
फॅक्ट-चेकिंग वेबसाईट? म्हणजे काय?!

फॅक्ट-चेकिंग वेबसाईट्स या इंटरनेट वर पसरलेल्या विशेषतः खोट्या आणि चुकीच्या बातम्या ओळखण्यासाठी काम करतात.



पण हे खोटं आहे हे त्या कसं ओळखतात?

प्रश्न चांगला आहे! प्रत्येक साईटची एक विशिष्ट पद्धत आहे, जी त्या वेबसाईट वर दिलेली असते. सामान्यतः, यामध्ये माहितीचे मूळ शोधण्यासाठी एक प्रगत वेब सर्चचा समावेश असतो....



ते मूळ सोर्स देखील शोधतात आणि वाचतात आणि स्थानिक अधिकाऱ्यांना किंवा त्या बातमी मध्ये दिसत असलेल्या लोकांना त्या बातमीची शहानिशा करण्या साठी संपर्क करतात ... खरं म्हणजे, तुम्ही पण एखाद्या तज्ज्ञाकडे सेंकड ओपीनियन साठी जावू शकता!

चला चेक करूया!

पुन्हा एकदा आपल्या आर्टिकल्स कडे वळूया. यामध्ये सेंकड ओपीनियन साठी कुठले स्त्रोत असू शकतात? तुम्ही कोणाशी संपर्क साधू शकता?

https://economictimes.indiatimes.com/news/budget-2025

Home News Market Economy Politics Elections Blogs

द इकॉनॉमिक टाईम्स

आरोग्य मंत्रालयाच्या निधीवरील नवीनतम अपडेट्स

डॉ. सोहिनी कुमार | शेवटचे अपडेट: २२ फेब्रुवारी २०२२

NATIONAL HEALTH MISSION
राष्ट्रीय स्वास्थ्य मिशन
Ministry of Health & Family Welfare

नवी दिल्ली: सत्ताधारी पक्ष येत्या राज्य निवडणुकांसाठी सज्ज होत असताना, आरोग्य मंत्रालयाने त्यांच्या राष्ट्रीय आरोग्य अभियानासाठी निधीत मोठी कपात केली आहे ज्यामुळे रुग्णालयांमध्ये पुरवठ्याची कमतरता असलेल्या ५०% राज्यांमध्ये परिस्थिती बदलू शकते. विरोधी पक्षाने....

लेखकाबद्दल:
डॉ. सोहिनी कुमार या स्कूल ऑफ इकॉनॉमिक्स अँड बिझनेसमध्ये प्राध्यापक आहेत आणि त्यांनी गेल्या दशकाहून अधिक काळ भारतीय आरोग्य प्रणाली आणि राजकारणाचा अभ्यास केला आहे.

हेल्थ मिनिस्ट्री वेबसाईट

टाईम्स ऑफ इंडिया शाळेतील शिक्षक

http://economicsmadeeeazy123.biz/india-to-pay-foreign-

इकॉनॉमिक्समेडईझी

भारत आता खाजगी बँक खात्यांमधून फेडणार आंतरराष्ट्रीय कर्ज!

आंतरराष्ट्रीय देशांकडून घेतलेल्या कर्जामुळे भारत दिवसेंदिवस कर्जबाजारी होत चालला आहे आणि राष्ट्रीय संपत्ति झपाट्याने कमी होत चालली आहे. राज्यात निधीचा तुडवडा भासत आहे आणि हे भरून काढण्याचा एकमेव मार्ग म्हणजे नागरिकांच्या बँक खात्यांमधून मदत घेणे! खाजगी बँकांनी आधीच या उपक्रमात सहभागी न होण्याचे जाहीर केले असले तरी, स्टेट बँकांमधील कोणतीही खाती दुरुपयोग होण्यापासून सुरक्षित राहणार नाहीत.... (पुढे वाचा)

फोटो: भारतीय परराष्ट्र सचिव नवीन खाजगी बँकेच्या मालकांशी हस्तांदोलन करताना

तीन विश्वसनीय फॅक्ट चेकिंग वेबसाईट्स बघा. त्यांची नावे, यूआरएल्स आणि व्हेरिफिकेशन प्रक्रिया शेअर करा:

लक्षात ठेवा: चुकीची माहिती खूप मोठे नुकसान करू शकते: यामुळे लोकांच्या जीवाला धोका निर्माण होऊ शकतो, मानसिक आरोग्य बिघडू शकते आणि लोकांमधील किंवा समाजातील नाते-संबंध आणि प्रतिष्ठेवर देखील विपरीत परिणाम होऊ शकतात.

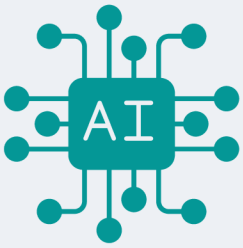

एसयूसीएस (SUCS) पद्धत खूपच उपयुक्त आहे.... पण मला खूपच लाजिरवाणे आणि अपराधी वाटते आहे की मी अशी चुकीची माहिती पसरवली. मी माझी चूक विसरू शकत नाही....
चुकीची माहिती ओळखण्यात सगळेच नेहमी यशस्वी होत नसतात, म्हणूनच तर ती इतकी कॉमन असते! मुद्दा एवढाच आहे की आपण चुकीची माहिती ओळखण्याची आपली क्षमता वाढवली पाहिजे, आणि सत्य समोर आले की आपले मत बदलले पाहिजे.
अमित दादा, मला खूप काळजी वाटते आहे! मला केवढे मेसेजेस आलेत. मी सगळ्याच मेसेजेसचे फॅक्ट-चेकिंग कसे काय करू शकतो? अक्खा एक दिवस जाईल त्यात!
हम्म....आपल्याला इंटरनेट वर कसं वाटतं याबद्दल जागरूक राहणे चांगले आहे. मी पण सध्या बऱ्याचदा इंटरनेट वर वाहवत जातो....
कुठेही हरवल्यासारखे न वाटता माहितीचा जबाबदार ग्राहक होण्याचे काही मार्ग येथे दिलेले आहेत!!
विश्वसनीय सोर्सेस कडून आलेल्या बातम्या वाचण्याची एक वेळ ठरवून घेणे.
हळू-हळू आपल्याला व्हेरिफिकेशन आपोआप यायला लागेल हे लक्षात ठेवणे!
फॅक्ट-चेकिंग बडी सोबत ठेवणे ज्याच्यासोबत तुम्ही सराव करू शकता आणि एकमेकांच्या चुका सुधारू शकता!
माहिती समजून घेण्यासाठी आणि कोणत्याही निष्कर्षावर येण्यासाठी वेळ घेणे, पण पूर्ण अचूकतेची खात्री झाल्याशिवाय ती फॉरवर्ड करू नका!

चुकीची माहिती आणि चुकीची माहिती कशी पसरते?

चुकीची माहिती आगीसारखी का पसरते यामागची कारणे समजून घेणे देखील महत्त्वाचे आहे. ही समस्या आपल्या सगळ्यांपेक्षा खूप मोठी आहे!

क्लिकबेट आणि खळबळजनक परिस्थिती निर्माण करण्यासाठी मुद्दाम केलेले प्रयत्न

आपल्याला क्लिक करण्यासाठी भरीस पाडण्यासाठी कंटेंट तयार केलेला असू शकतो - हा कंटेंट रोमांटिक पद्धतीने, अतिशयोक्तीपूर्ण पद्धतीने, तुम्हाला घाबरवण्यासाठी, उत्तेजना किंवा उत्सुकता निर्माण करण्यासाठी लिहिला गेलेला असू शकतो.



डीपफेक्स आणि फेरबदल केलेले कंटेंट

फोटोज आणि व्हिडिओज खरे वाटावे आणि लोकांना त्याद्वारे फसवता यावं यासाठी प्रचंड प्रमाणात एडिट केले जातात - कधी-कधी, त्याच्यामुळे फसवणूक होते किंवा लोकांनी कसं दिसावं याबद्दल अवास्तव अपेक्षा मांडल्या जातात.

पुष्टी करताना भेदभाव करणे

जी माहिती आपल्या मतांप्रमाणे नसते किंवा आपल्याला पटत नाही त्यापेक्षा जी माहिती आपल्याला पटते किंवा आपल्या मते योग्य असते त्यावर आपण पटकन विश्वास ठेवतो. त्यामुळे, फक्त आपल्याला पटलं आहे किंवा आपले मत त्यामध्ये दिलेल्या मतासारखेच आहे एवढ्या एका कारणास्तव आपण एखादी चुकीची माहिती देखील फॉरवर्ड करू शकतो.

वाढते ध्रुवीकरण

इंटरनेट वरील वाद-विवाद विकोपाला जाणारे असतात, कारण परस्परातील मतभेद वाढत चालले आहेत. अशा वातावरणात लोक चुकीची माहिती मुद्दाम पसरवण्यासाठी प्रोत्साहित होवू .

विश्वासार्हते बद्दल भेदभाव

आपला ज्यांच्यावर विश्वास नाही अशा व्यक्तींनी शेअर केलेल्या माहिती पेक्षा आपल्याला ज्या व्यक्तींवर विश्वास आहे त्यांनी शेअर केलेल्या माहितीवर आपण पटकन विश्वास ठेवतो - जसे उदाहरणार्थ शिक्षक, नातेवाईक किंवा मित्र. यामुळे आपण अडचणीत येऊ शकतो कारण यामध्ये न्यूज पेक्षा व्यक्तिच्या खरेपणावर भर देतो.

सोशल प्रूफिंग, बॉट्स आणि फेक प्रोफाईल्स

सोशल प्रूफिंग म्हणजे आपण प्रसिद्ध माहितीवर पटकन विश्वास करतो ज्यावर इतरांचा देखील विश्वास असतो.. हल्ली जास्त प्रमाणात बॉट्स आणि फेक प्रोफाईल्स याचा वापर करून पोस्ट्स लोकप्रिय केल्या जातात - जेणेकरून आपण त्यांच्यावर विश्वास ठेवू.

ऑनलाईन असताना जबाबदार आणि शोधक असणे

चुकीच्या माहिती पासून मुक्त असलेले इंटरनेट निर्माण करण्यासाठी आपण काय करू शकतो असं तुम्हाला वाटतंय?

_____

_____

_____

चुकीच्या माहिती पासून मुक्त असलेले इंटरनेट निर्माण करण्यासाठी आपण काय करू शकतो असं तुम्हाला वाटतंय?

हो! माहिती पडताळून बघताना मी पण अनेक गोष्टी वाचतो आणि नवीन गोष्टी शिकतो....

हे कसलं भन्नाट आहे! आता मला खात्री आहे की आपण यामध्ये हरवून न जाता आपल्याला हवं ते शोधू शकतो, तुम्हाला काय वाटतं....

लक्षात ठेवा, क्रिटीकल थिंकिंग चा अर्थ जे चुकीचे आहे त्यापासून लांब राहणे नाही एवढाच नाहीये, तर कोणत्याही निष्कर्षावर येताना फॅक्ट्स आणि मतं यामध्ये फरक देखील करता येणे हा देखील आहे.... ग्लिच आपल्याला समजावून सांगेल!

बऱ्याचदा, तुम्ही ऑनलाईन गोळा केलेली माहिती फॅक्ट्स आणि मतं याचं मिश्रण असते. कोणत्याही माहितीतील या दोन्ही बाजूंमध्ये फरक केल्याने तुमचा क्रिटीकल थिंकिंग करण्याचा प्रवास सोपा होईल.

फॅक्ट्स

बाहेर पाऊस पडतो आहे!

- याची पडताळणी केली जाऊ शकते
- निरीक्षण किंवा संशोधनाच्या आधारे
- हे निर्विवाद आहे

Vs

मतं

पावसामुळे सगळे दुःखी होतात!

- एक मत/दृष्टिकोण, याची पडताळणी होऊ शकत नाही, यावर चर्चा होऊ शकत नाही
- यामध्ये भेदभाव आणि चांगल्या/वाईट संकल्पना असू शकतात
- एका फॅक्ट बद्दल एखाद्या व्यक्तिला कसे वाटते हे सांगितले आहे

तुम्ही जगाचा अर्थ कसा लावता आणि तुम्हाला त्याबद्दल काय वाटते म्हणजे तुमचे मत असते. मतांवर चर्चा होऊ शकते, वाद-विवाद होऊ शकतात आणि त्यांचे अन्वेषण केले जावू शकते. जर ते फॅक्ट्सच्या उलट असतील, तर ते अवैध ठरतात

त्यामुळे सोर्सेस विश्वासार्ह आहेत आणि फॅक्ट्स स्पष्ट आहेतयाची खात्री करण्याबरोबरच, फॅक्ट्स आणि मतं यातील परस्पर संबंध काय आहे हे देखील आपण लक्षात घेतले पाहिजे, बरोबर?

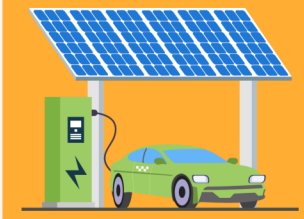
खूप छान माहिती दिलीस अमित दादा! थॅंक्स!

ॲक्टिव्हिटी

खाली दिलेल्या माहितीमध्ये तुम्ही फॅक्ट्सना सर्कल आणि मतांना अंडरलाईन करू शकाल का? हे करत असताना, ही मतं फॅक्ट्स वर आधारित आहेत का यावर विचार करा, आणि तुम्ही त्याच्याशी सहमत आहात का. तुम्ही खालील विषयावार आणखीन माहिती वाचू शकता आणि बघा तुमचा विचार बदलतो का!

स्ट्रॉबेरी हे एक असे फळ आहे ज्यामध्ये व्हिटॅमिन सी असते आणि ते सर्वात चविष्ट फळ आहे.

कुतुबमिनार नवी दिल्लीत आहे पण ते शहरातील इतर स्मारकांइतके सुंदर नाही.



इलेक्ट्रिक कार गॅसवर चालणाऱ्या वाहनांपेक्षा कमी उत्सर्जन निर्माण करतात, ज्यामुळे पर्यावरणाची काळजी घेणाऱ्या प्रत्येकासाठी ते स्पष्ट पर्याय बनतात.

अवकाश संशोधनावर पैसे खर्च करणे व्यर्थ असू शकते, परंतु त्यामुळे अविश्वसनीय तांत्रिक प्रगती झाली आहे!

दररोज वाचन केल्याने लक्ष केंद्रित करणे आणि शब्दसंग्रह सुधारण्यास मदत होऊ शकते, जरी काहींना वाटते की ऑडिओबुक तितकेच प्रभावी आहेत.

वैयक्तिकरित्या, हातात खरे पुस्तक धरण्याच्या भावनेपेक्षा काहीही चांगले नाही.

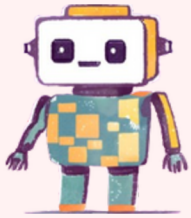
सोशल मीडिया अल्गोरिदम वापरकर्त्यांना व्यस्त ठेवणाऱ्या सामग्रीला प्राधान्य देतात, जे दर्शवते की ते आपल्या वर्तनात फेरफार करण्यासाठी डिझाइन केलेले आहेत.

एल्गोरिदम म्हणजे काय?

भरपूर पाऊस पडून गेला होता आणि प्रचंड गरम होत होतं, आणि शुभम एका झाडाखाली आईसक्रीम खात बसली होती. शुभम तिचा फोन बाहेर काढते आणि बातम्या वाचायला लागली, तिला वाटंत होते की आता तिला खोट्या बातम्या ओळखता येतात. ती जसं जसं पुढे वाचत जाते तिला काही तरी विचित्र जाणवतं.

हम्म, हे विचित्र आहे. मला माहितीये काल खूप मोठ्ठं वादळ आलं होतं, पण ऑनलाईन त्याबद्दल काहीच दिसत नाहीये. उलट माझे न्यूजफीड तर कॅफे रेकमेंडेशन्स ने भरलेले आहे.

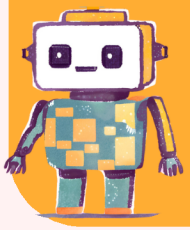
ते असं होतं कारण अल्गोरिदम्स तुम्ही काय आवडतं याचा अंदाज तुमच्या ॲक्टिव्हिटी वरून घेतात. तुम्ही अलीकडेच आसपासचे कॅफे शोधले असतील, तर अल्गोरिदम्स तुम्हाला त्याच गोष्टी अधिक दाखवतील!



आपण "हॅलो डिजिटल वर्ल्ड" या प्रकरणात इंटरनेटची तुलना एक रेल्वे स्टेशन बरोबर केली होती हे आठवते? एल्गोरिदम अगदी रेल्वेतल्या स्टेशन मॅनेजर सारखं काम करतं! कल्पना करा की तुम्ही एका ट्रेन मध्ये बसत आहात, आणि प्रत्येक स्टेशनवर पोहोचल्यावर, स्टेशन मास्टर बघत असतात की तुम्ही कुठे जात आहात. तुम्ही जर ओडीसा किंवा बंगालला जाण्यासाठी सारखी तीच ट्रेन घेत राहिलात तर स्टेशन मास्टरला वाटेल की तुम्हाला पूर्व भारत फिरायला आवडतं आहे. पुढच्या वेळेस ते तुम्हाला त्याच ठिकाणी जाण्यासाठी वेगवेगळ्या ट्रेन्स चे पर्याय सुचवतील कारण त्यांना वाटेल की तुम्हाला त्या भागात फिरायला आवडतं.

अगदी असेच जेव्हा तुम्ही इंटरनेट वापरता, एल्गोरिदम्स तुम्हाला काय आवडतं ते बघत असतात - उदाहरणार्थ तुम्ही बघत असलेले व्हिडिओज, तुम्ही बघितलेले पेजेस, किंवा तुम्ही शोधत असलेल्या गोष्टी. जर तुम्ही कुकिंग संबंधी व्हिडिओज शोधत असाल, तर एल्गोरिदम असं समजतं की तुम्हाला कुकिंग आवडतं आणि तुम्हाला वेगवेगळ्या रेसिपीज आणि फूड टिप्स रेकमेंड करतं.

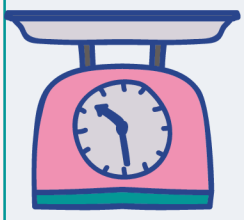
एल्गोरिदम्स तुमच्या ऑनलाईन ॲक्शन्सवर पाळत ठेवत असतात — उदाहरणार्थ, तुम्ही काय लाईक करता, कशावर कमेन्ट करता किंवा काय शेअर करता. या ॲक्शन्समुळे तुमच्या आवडी-निवडी सूचित केल्या जातात आणि प्लॅटफॉर्म्सना तुमचं फीड तयार करण्यात मदत होते. जर तुम्हाला गेमिंगच्या पोस्ट्स आवडत असतील, तर एल्गोरिदम गेमिंगसंबंधी कंटेंट, जाहिराती आणि पेजेस जास्त दाखवेल.



तुम्ही वापरत असलेल्या कंटेंटचा प्रकार—मग तो व्हिडिओ असो, लेख असो किंवा प्रतिमा असो—शिफारशींवर देखील प्रभाव पाडतो. अल्गोरिदम तुम्ही ज्या फॉरमॅटमध्ये सर्वात जास्त सहभागी होता त्यांना प्राधान्य देतात.

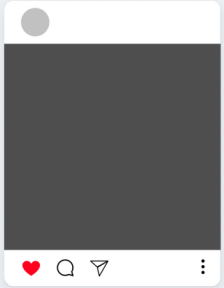
एल्गोरिदम्स कसे काम करतात?

तुम्ही एखाद्या विषयासाठी घालवलेला वेळ एल्गोरिदम्सना हे सूचित करतो की तुम्हाला कशाची आवड आहे. एखाद्या विशिष्ट कंटेंट वर तुम्ही जेवढा जास्त वेळ घालवाल, तितक्या त्याच कंटेंटच्या पोस्ट्स तुम्हाला जास्त दिसतील.



एल्गोरिदम्सचा आणखीन एक महत्त्वाचा घटक म्हणजे कंटेंटवेटिंग. ज्यामध्ये विविध प्रकारच्या पोस्ट्स आणि ॲक्टिव्हिटीजना स्कोअर दिला जातो. प्लॅटफॉर्म्स वर थेट अपलोड केलेल्या व्हिडिओजला एक्सटर्नल साईट्सवर जाण्याच्या लिंक्स पेक्षा प्राधान्य दिले जाते. उत्तम क्वालिटीच्या सोर्स मधील लिंक्सवर देखील जास्त वेट दिला जातो.

जशा जशा पोस्ट्स जुन्या होत जातात तशा तशा त्या मागे पडत जातात. ज्या पेजवर नवीन पोस्ट्स आणि चर्चा सुरू असतात त्याचे कंटेंट तुमच्या फीड मध्ये दिसण्याची शक्यता वाढते. काही काळासाठी जर तुम्ही एखाद्या पेज वर भेट दिली नसेल, तर ते नवीन असेल तरी त्यावरच्या पोस्ट्स दिसणे कमी होईल.

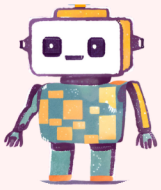


लक्षात ठेवा! एल्गोरिदम्स अश्या गोष्टींना प्राधान्य देते ज्या लक्ष वेधणाऱ्या असतात,ज्या गोष्टी खरोखर महत्त्वाच्या आहेत त्यांना नाही. ते नेहमी प्रसिद्ध कंटेंटलाच पुढे आणतात , जरी ते फार अचूक किंवा विश्वासार्ह नसले तरी, उदाहरणार्थ भडक हेडलाईन्स किंवा व्हायरल व्हिडिओज. याचा अर्थ असा की सगळ्यात आकर्षक वाटणार कंटेंट विश्वासार्ह असेलच असे नाही.

जरी एल्गोरिदम्स तुमचा ऑनलाईन अनुभव पर्सनलाईझ करत असले, तरी ते तुम्हाला फिल्टर बबल मध्ये अडकवू शकतात - असे ठिकाण जिथे तुम्हाला फक्त तुमच्या सध्याच्या आवडीचेच कंटेंट दिसेल. यामुळे तुमच्या नवीन संकल्पना आणि दृष्टिकोण माहिती करून घेण्याच्या क्षमतेला मर्यादा येतात. या बबल मधून बाहेर येण्यासाठी, वेगवेगळ्या विषयांचा अभ्यास करा आणि विविध कंटेंट बघत रहा - कधी तुम्हाला एखादी खूपच आश्चर्यकारक गोष्ट बघायला मिळेल सांगता येत नाही!

एल्गोरिदम्स कसे काम करतात?

एल्गोरिदम्स तुम्ही काशाप्रकारचे कंटेंट बघाल फक्त हेच नाही ठरवत, तर तुम्ही ब्राऊझ करत असताना कोणत्या जाहिराती पॉप अप होतील हे देखील ठरवतात. जाहिरातदार तुम्ही ऑनलाईन काय काय करता उदाहरणार्थ हिस्ट्री, क्लिक्स, आणि अगदी तुमचे लोकेशन याचा वापर करून खास तुमच्यासाठी बनवलेल्या जाहिराती डिझाईन करतात. हे आपण टप्प्याटप्प्याने समजून घेऊ:



ॲड टार्गेटिंग

एकदा जाहिराती तयार करून तुम्ही डेटा शोधण्याचा प्रयत्न करा, त्याचा अभ्यास करून ते समजून घ्या. जाहिरात तयार करणारे विशिष्ट ग्रूप्सशी संबंधित ॲड्स शोधण्यासाठी डेमोग्राफिक डेटाचे उदाहरण वय, लोकेशन, आणि आवडी-निवडी याचा वापर करतात.

ॲड पर्सनलायझेशन

एकत्रित डेटा वापरुन कंपनी तुमच्या आवडी-निवडी आणि तुमच्या सवयी यांच्या आधारे एक प्रोफाईल तयार करते. तुम्ही कोणत्या जाहिरातींवर क्लिक कराल याचा ते अंदाज घेतात आणि ज्या जाहिराती तुमच्या साठी सगळ्यात प्रासंगिक वाटतात त्या जाहिराती ते तुम्हाला दाखवतात. म्हणूनच, नवीन फोन बद्दल ऑनलाईन माहिती बघितल्यावर, अचानक तुम्हाला फोन केसेस, चार्जर्स, किंवा इयरफोन्स याच्या जाहिराती दिसायल लागतात.

जाहिरात तयार करणारे जो डेटा गोळा करतात त्यावर तुम्ही मर्यादा आणण्यासाठी काही पाऊले उचलू शकता आणि तुमच्या ऑनलाईन अनुभवावर पुन्हा एकदा तुमचे नियंत्रण आणू शकता. खाली काही उपाय दिले आहेत ज्याच्या आधारे तुम्ही काय शेअर करायचं आणि काय प्रायव्हेट ठेवायचं हे ठरवू शकता!

प्रायवसी सेटिंग्ज रिव्यू करा

लोकेशन ट्रॅकिंग किंवा पर्सन्लाइज्ड ॲड्स डिसेबल करण्याकरता सेटिंग्ज बदला

कुकीज आणि कॅशेज क्लिअर करा

जाहिरातदार वापरत असलेला डेटा रीसेट करण्यासाठी नियमितपणे कुकीज हटवा.

ॲड ब्लॉकर्स वापरा

ॲड्स ब्लॉक करा आणि तुमचा डेटा गोळा पासून ट्रॅकर्सना प्रतिबंधित करा.

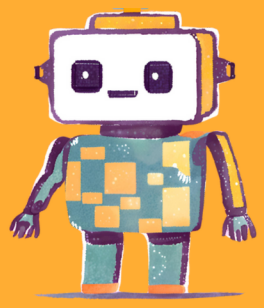
पर्सन्लाइज्ड ॲड्सच्या ऑप्शनमधून बाहेर पडा

तुमच्या ॲक्टीविटीज वर आधारित ॲड्सचा ऑप्शन रद्द करा. तुम्हाला ॲड्स दिसतील, पण त्या तुमची ब्राउजिंग हिस्ट्री पाहून त्यावरुन घेतलेल्या नसतील

अरे वा अल्गोरिदम कूल आहे पण जरा भीतीदायक आहे! आत्ता कळलं व्हिडिओचे सजेशन का बदलत राहतात. अल्गोरिदम जाहिराती पण ठरवतात का? मी एकदा शूज शोधत होतो तर आता सगळ्या त्याच्याच जाहिराती येतायत.

बरोबर! ती लक्ष्यित जाहिरात आहे, अल्गोरिदम तुमचा डेटा वापरण्याचा आणखी एक मार्ग!

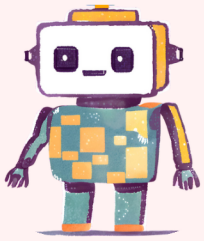
तुम्हाला तुमच्या न्यूजफीडमध्ये नेहमी जो तीन प्रकार चा कंटेन्ट दिसतो, तो लिहा. तुम्हाला ज्या विषयांमध्ये रस आहे नक्की तेच हे टॉपिक आहेत का की तुम्हाला असे वाटते की अल्गोरिदमने तुमच्यासाठी बबल तयार केला आहे? तुमच्या मित्राशी किंवा वर्गातल्या मित्राला याविषयी सांगा.



आर्टिफिशियल इंटेलिजन्स म्हणजे काय?

एआय कसं काम करतं?

आर्टिफिशियल इंटेलिजन्स अगदी तुमच्या असिस्टंटसारखं तुमचं सगळं काम करतो, तुमची कामं पटकन करतो, तुमचे प्रश्न सोडवतो, आणि तुमचा शिकण्याची प्रक्रिया सुद्धा मजेशीर करतो. तो माणसासारखा विचार करत नाही, किंवा त्याला काही भावना नसतात, पण ते रोजच्या अनेक कामात तुम्हाला भरपूर मदत करू शकतो. चला एआय तुम्हाला कशा प्रकारे मदत करू शकते ते पाहूया.



डेटाला फास्ट ॲक्सेस

एआय मोठ्या प्रमाणातील माहितीचे ॲनालिसिस काही सेकंदात करते. यामुळे एआय खास करून संशोधन आणि शिकण्याकरता उपयोगी आहे.

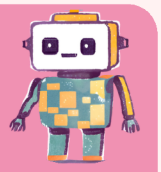
वेगवेगळ्या आयडिया डोक्यात येतात

नवीन कल्पनांचा विचार करताना तुम्हाला काही सुचतच नाही असं कधी झालं आहे का? एआय हे प्रोजेक्ट्ससाठी क्रिएटिव्ह पर्याय सुचवून आपल्याला मदत करतात. जणू काही तो आपला स्टडी पार्टनरच आहे.

भाषिक अनुवाद

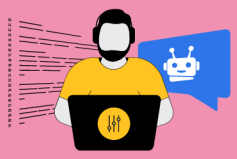
एआय टूल्स भाषेची बंधने तोडतात, त्यामुळे जगभरातील लोकांशी बोलणे किंवा अन्य भाषांमधील कंटेन्ट लगेच समजणे सोपे झाले आहे

एआय खूप उपयोगी आहे हे जरी खरं असलं तरी ते परफेक्ट नाहीये. ते वापरताना त्यातील चॅलेंजेस बद्दल आपल्याला माहिती पाहिजे.



एआय मधील बायस

एआय डेटावरून शिकते, आणि जर डेटा योग्य नसेल किंवा तो अपूर्ण असेल तर एआय कडून मिळणारे रिझल्ट अनफेअर असतील. याचा अर्थ त्याच्याकडून चुका होवू शकतात किंवा विशिष्ट मतांची बाजू घेतली जावू शकते.



उदाहरणार्थ

जर एआय टूल वेस्टर्न मीडियातील माहितीच्या आधारे ट्रेन केले गेले असेल तर भारतासह जगाच्या इतर भागातील कल्चरविषयी माहिती कळायला त्याला अवघड जाईल.

चुकीची माहिती

एआय एखादी माहिती खरी आहे असं दाखवते पण ती खरी नसते. त्याने दिलेली उत्तरे पॅटर्नवरून दिलेली असतात, फॅक्ट बेस्ड नाही.

उदाहरणार्थ

तुम्ही एआय टूलला इतिहासातील एखाद्या व्यक्तीविषयी विचारा, ते तुम्हाला त्या व्यक्तीचा चुकीचा संदर्भ दाखवेल किंवा जो प्रसंग कधी झालाच नाही तो दाखवेल.

प्रायवसीबद्दल काळजी

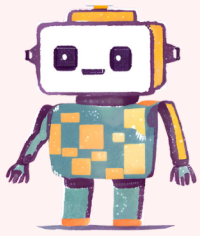
अनेक एआय टूल्स शिकण्यासाठी आणि सुधारणा करण्यासाठी डेटा गोळा करतात आणि ॲनलाईज करतात. यातून एआय आणखी स्मार्ट होते, पण आपली वैयक्तिक माहितीची प्रायवसी धोक्यात येते.

उदाहरणार्थ

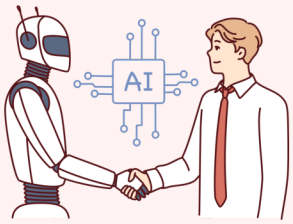
जर ॲपने तुमचं लोकेशन विचारलं, तर त्याला ती माहिती का हवी आहे आणि तुम्हाला ती माहिती द्यायची आहे की नाही याचा विचार करणं महत्त्वाचं आहे

एआय वापरण्याकरता ग्लिचचे गाईड

हे सगळं जड होतंय का समजायला? मी समजू शकतो. ही माहितीच भरपूर आहे आणि त्यामुळे गोंधळ होऊ शकतो. एआय जबाबदारीने कसे वापरायचे यावर या काही साध्यासोप्या टिप्स आहेत



एआय ला आपला पार्टनर करा, त्यावर अवलंबून राहू नका.



एआय हा तुमचा उत्तम असिस्टंट नक्कीच आहे, पण तो तुमच्या मौलिक संकल्पना, रचनात्मकता आणि क्रिटीकल थिंकिंग चा पर्याय नाहीये. एआय हे ब्रेन स्टॉर्म करायला किंवा सजेशन घेण्यात मदत करते, पण तुमच्या स्वत:च्या विचार करण्याच्या क्षमतेची आणि क्रिएटीविटीची जागा घेऊ शकत नाही

नेहमी फॅक्ट तपासून घ्या

एआय हे परफेक्ट नाही आणि बरेच वेळा चुकीची माहिती देते. एआय ने दिलेली माहिती बरोबर आहे की नाही हे पुस्तके, खात्रीच्या वेबसाइट यातून तपासून घ्या

त्याच्या मर्यादा लक्षात घ्या

एआय खूप स्मार्ट आहे, पण ते अगदी माणसासारखा विचार करत नाही. आपण जसे भावना जाणतो आणि सांस्कृतिक संदर्भांचा विचार करतो तसा ते करू शकत नाही. त्याला केवळ टूल म्हणूनच वापरा, त्याला एक्स्पर्ट समजू नका.

तर मी एआयचा वापर सुरुवातीचा मुद्दा म्हणून करावा, अंतिम उत्तर म्हणून नाही?

अगदी बरोबर! तो तुमचं काम हलकं करतो, परंतु तुमच्या क्रिटीकल थिंकिंगला पर्याय असू शकत नाही.

ॲक्टिविटी

जर तुमच्याकडे इंटरनेट नसेल तर

तुमच्यापैकी दोघे दोघे मिळून काम करा. आता तुमच्यापैकी एकाने एआय टूल वापरा आणि दुसऱ्याने ट्रॅडिशनल रिसर्च मेथड वापरा. तुमच्या आवडीच्या कोणताही विषय निवडा. त्यानंतर तुम्ही दोघांनी शोधून काढलेल्या माहितीची अचूकता, पूर्णता आणि विश्वासार्हता याची तुलना करा.

जर तुमच्याकडे इंटरनेटची सुविधा नसेल तर

एआय ने दिलेलं उत्तर पुन्हा लिहून काढा. त्यात अजून संदर्भ, उदाहरणे आणि तुमच्या स्वत:च्या आयडिया घाला आणि ते उत्तर आणखी समृद्ध आणि अचूक करा.

चॅप्टर रिकॅप

- ऑनलाईन माहितीच्या पुढील कॅटेगरीज करता येतात: व्हेरिफाईड आणि विश्वास ठेवता येईल अशी माहिती, मत आणि वैयक्तिक माहिती, चुकीची माहिती, मुद्दामून पसरवलेली चुकीची माहिती, आणि खोटी माहिती, किंवा विनोदी आणि मनोरंजक माहिती.

- मिसइन्फॉर्मेशन म्हणजे अशी माहिती जी कोणताही हेतू न ठेवता पसरवलेली चुकीची माहिती, तर डिसइन्फॉर्मेशन ही लोकांना फसवण्याकरता जाणूनबुजून तयार केलेली माहिती असते.

- तुम्ही एक साधी पद्धत वापरुन माहिती तपासून घेऊ शकता- एसयूसीएस (SUCS) पद्धत, म्हणजे सोर्स, यूबीक्विटी, कॉंटेक्स्ट आणि सेकंड ओपीनियन.

  - सोर्स: वेबसाईट रीलायेबल आणि प्रसिद्ध आहे का? यू आर एल सुरक्षित आहे का? पेजचे डिझाईन छान आहे का की त्यात खूप पॉप अप्स आहेत?
  - यूबीक्विटी: ही माहिती सर्वत्र सापडते का आणि इतर सोर्सकडून त्या माहितीची खात्री करून घेता येते आहे का?
  - संदर्भ: नावे, तारखा आणि ठिकाणे बरोबर आहेत का? त्यामध्ये सर्व संदर्भ आहेत का आणि अप टू डेट आहे का? दाखवली चित्रे आणि माहिती यात सुसंगतता आहे का?
  - इतरांना माहिती शेयर करताना देताना फॅक्ट कोणती आणि मत कोणते हे काळजीपूर्वक तपासा !

- लक्षात ठेवा: ज्या माहितीकडे सर्वांचे लक्ष जाते ती माहिती अल्गोरिदममध्ये पहिल्यांदा दाखवली जाते, मात्र ती बरोबर किंवा महत्त्वाची असते असे नाही.

- प्रायवसी सेटिंग रिव्यू करा, कुकीज आणि कॅशे क्लियर करा, ॲड ब्लॉकर वापरा, आणि पर्सनलाइज्ड ॲड्स डिसेबल करा जेणेकरून ॲड एजन्सीजना कमी माहिती मिळेल.

- एआय खूप कामाचे आहे, पण ते चुकीची माहिती देखील पुरवू शकते, एनकोड केलेले बायसेस किंवा पर्सनल मते दाखवू शकते आणि त्यामुळे प्रायवसी देखील धोक्यात येयेवू शकते! त्यामुळे एआय वापरताना फॅक्ट तपासून घ्यायला विसरू नका, त्याच्या मर्यादा लक्षात घ्या आणि त्याचा उपयोग फक्त कामाला मदत म्हणून करून घ्या, सगळे काम त्याच्यावर सोडू नका.

चॅप्टर ५: आज तुमचा दिवस नाही स्कॅमर्स! ऑनलाइन धोके ओळखणे आणि थांबवणे

आज ऊन पडलं आहे, आणि जसप्रीत आणि नूर जसप्रीतच्या घरी आहेत, दोघी मिळून काही नवीन बिया पेरत आहेत

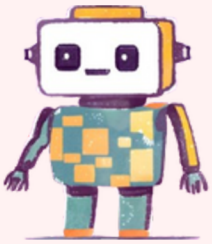
काल मी शुभमबरोबर थोडा वेळ होतो आणि ती मला अल्गोरिदम, एआय बद्दल आणि सिद्धार्थ आणि अमित दादाबरोबर काम करत असताना तिला समजलेल्या इतर काही रंजक गोष्टींबद्दल सांगत होती! ते मला रंजक वाटले, परंतु यामुळे मला हा विचार करण्यास भाग पाडले की असे आणखी किती आणि काय काय आहे ज्याबद्दल आपल्याला माहित नाही...

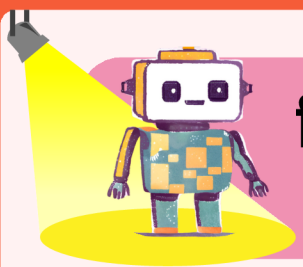
हे खरे आहे! इंटरनेट हे आकर्षक आहे, परंतु जेव्हा आपल्याला ते सुरक्षित आहे की विश्वासार्ह आहे हे माहित नसते तेव्हा ते नेव्हिगेट करणे देखील कठीण होऊ शकते.

मला असे वाटते की इंटरनेटवरील भीतीदायक आणि नको असणाऱ्या इंटरॅक्शनशी कसे डील करावे हे पटकन शिकता येईल अशा ठिकाणी जाता आलं तर ते आपल्या सर्वांसाठी खरोखर उपयुक्त ठरेल. तुला काय वाटतं?

ही आयडिया जबरदस्त आहे. मला वाटते ग्लिच आपल्याला यात मदत करू शकेल!

मी नक्कीच करू शकतो! चला काहीतरी धाडसी काम करूया! इंटरनेट वापरताना सुरक्षिततेसाठी ग्लिचच्या गाईडमध्ये तुमचे स्वागत आहे!





ग्लिच गाईड टूद गॅलेक्सी

इंटरनेट सुरक्षा

वैयक्तिक चॅनेलवर तुम्हाला आलेल्या धमक्या कशा ओळखाल?
येथे रेड फ्लॅगची चेकलिस्ट दिली आहे!

- त्यांनी वैयक्तिक माहिती किंवा संवेदनशील माहिती मागितली आहे का? (उदा: वय, पत्ता, फोन नंबर, शाळा, बँक खाते)
- मैत्रीपूर्ण संभाषणात त्यांनी खाजगी फोटो/ व्हिडिओची मागणी केली होती का?
- तुमचे संभाषण किंवा कृती इतरांपासून गुप्त ठेवण्यास त्यांनी तुम्हाला सांगितले होते का?
- त्यांनी खूप लवकर तुमचे जवळचे मित्र होण्याचा प्रयत्न केला, कॉम्प्लिमेंट्स किंवा भेटवस्तू दिल्या?
- त्यांनी अपमानास्प / दुखावणारे संदेश पाठवले का ज्यामुळे तुम्हाला असुरक्षित किंवा अपराधी वाटले?
- त्यांनी मोठी प्रॉमिसेस केली किंवा ऑफर दिली (उदा: लॉटरी, नोकरीची संधी)का?

धोके आणि असुरक्षित परिस्थिती टाळण्यासाठी काही सुरक्षा उपाय!

- अक्षरे, संख्या आणि स्पेशल कॅरॅक्टर यांच्या मिश्रणाने स्ट्रॉन्ग पासवर्ड तयार करा.
- 2-फॅक्टर ऑथेंटिकेशन लागू करा
- तुमच्या प्रोफाइलची विजिबिलिटी तुमच्या पसंतीनुसार सेट केली आहे याची खात्री करा - सार्वजनिक किंवा खाजगी!
- सार्वजनिक प्लॅटफॉर्मवर तुमचे पूर्ण नाव, पत्ता, फोन नंबर किंवा शाळेचे नाव यासारखी वैयक्तिक माहिती शेयर करणे टाळा.
- केवळ एन्क्रिप्टेड प्लॅटफॉर्मवर संवेदनशील तपशील (उदा. बँकेची माहिती)शेयर करा.
- अँटीव्हायरस सॉफ्टवेअर इन्स्टॉल करा आणि तुमच्या डिव्हाइसची फायरवॉल चालू आहे याची खात्री करा
- ईमेल किंवा मेसेजमधील तुम्हाला माहिती नसलेल्या अनोळखी लिंकवर क्लिक करू नका
- नेहमीपेक्षा वेगळी ॲक्टिविटी तपासण्यासाठी नियमितपणे तुमच्या खात्यावर लक्ष ठेवा.
- कोणत्याही ॲपला जास्त माहिती मिळू देणे टाळा. अनावश्यक परमिशन डिसेबल करा आणि जास्त परमिशन मागणाऱ्या ॲप्सपासून सावध रहा
- पॉप अप, बॅनर आणि व्हिडिओ ॲड्स रोखण्यासाठी आणि मालवेअरपासून वाचण्यासाठी ॲड ब्लॉकर्सचा वापर करा.
- सार्वजनिक ठिकाणचे वायफाय वापरणे टाळा आणि वापरात नसताना तुमचा ब्लूटूथ बंद ठेवा
- एक्सर्टनल हार्ड ड्राइव्हवर महत्त्वाच्या फाईल्स किंवा फोटोंच्या प्रती सेव्ह करा!

केस स्टडी: द ब्ल्यू व्हेल चॅलेंज

2016मध्ये ब्लू व्हेल चॅलेंज नावाचा ऑनलाइन ट्रेंड सोशल मीडिया आणि खासगी मेसेजिंग प्लॅटफॉर्मवर प्रसिद्ध झाला होता. हा एक सामान्य खेळ नव्हता- हा ऑनलाइन मॅनिपुलेशनचा एक प्रकार होता जो किशोरवयीन मुलांना लक्ष्य करतो, त्यांना 50 दिवसांत नुकसानकारक कृती करण्यास प्रवृत्त करतो. ऑनलाइन धमक्या, छळ आणि घोटाळे यामुळे वास्तविक आयुष्याचे नुकसान कसे होऊ शकते याचे एक उदाहरण म्हणून त्याकडे पाहिले जाते. .

सुरुवातीला हे चॅलेंज अनोळखी व्यक्तींकडून आमंत्रण म्हणून सगळीकडे पोहोचले - संदेश प्राप्तकर्त्यांना सांगितले गेले की त्यांना या प्रतिष्ठित खेळासाठी "निवडले" गेले आहे, ज्यामुळे उत्सुकता आणि रोमांच निर्माण झाला.खेळात कायम राहण्यासाठी , त्यांना अज्ञात "क्युरेटर" किंवा "गेम मास्टर" च्या सूचनांचे पालन करावे लागायचे जो त्यांना दैनंदिनटास्क देत होता . सुरुवातीला, बहुतेक कामे त्रासदायक वाटत नव्हती - व्हेलचे चित्र काढणे, भीतीदायक चित्रपट पाहणे किंवा अवेळी उठणे. परंतु कालांतराने, गेम खेळणाऱ्यांना धोकादायक जोखीम स्वीकारण्यास किंवा कुटुंब आणि मित्रांपासून स्वत: ला वेगळे करण्यास सांगितले गेले! गेम खेळणाऱ्यांवर दबाव आणण्यासाठी आणि त्यांना नियंत्रित करण्यासाठी वापरले जाणारे काही मार्ग असे होते:

- प्रायवसीचे उल्लंघन आणि ब्लॅकमेल- गेम द्वारे खेळणाऱ्यांचे पूर्ण नाव, पत्ता किंवा खाजगी छायाचित्रे यासारखी वैयक्तिक माहिती शेयर करण्यास भाग पाडले गेले. नंतर या माहितीचा वापर करून त्यांना धमकावले. 'तुम्ही कुठे राहता हे आम्हाला माहित आहे' किंवा 'तुम्ही गेम सोडून गेलात तर आम्ही तुमच्या कुटुंबाचं नुकसान करू' अशा संदेशांचा वापर स्पर्धकांना चॅलेंजमध्ये राहण्यासाठी आणि घाबरवण्यासाठी करण्यात आला. खोटी आश्वासनेही देण्यात आली.

- ऑनलाईन छळ आणि गुंडगिरी करणे- गेम खेळणाऱ्याने जेव्हा गेम सोडून जाण्याची इच्छा बोलून दाखवली तेव्हा त्यांना आक्रामक मेसेज आले, ज्यात त्यांना कमकुवत किंवा अपयशी म्हटले गेले. खेळाडूंना बनावट ऑनलाइन समुदायांमध्ये देखील जोडले गेले जेथे गेम खेळणाऱ्या लोकांना त्यांचे शौर्य दाखवण्यासाठी किंवा सिद्ध करण्यासाठी त्यांच्यावर दबाव आणण्यात आला.

- हॅकिंग अँड ट्रॅकिंग - काही खेळाडूंचा असा विश्वास होता की त्यांचे डिव्हाइस हॅक झाले आहेत, त्यांच्या स्क्रीनवर त्यांच्यावर नजर ठेवली जात असल्याचे इशारे येत होते, त्यामुळे खेळाडूंना आपण यामध्ये अडकलोय असे वाटत होते.

ब्लू व्हेल चॅलेंज आता तितकेसे खेळले जात नाही, परंतु नवीन ऑनलाइन धोके समोर येत आहेत. नीट माहिती असणे, मॅनिप्यूलेशन टॅक्टीक्स ओळखणे आणि इतरांची मदत घेणे डिजिटल जगात आपल्याला आणि इतरांना सुरक्षित ठेवू शकते.

ॲक्टीविटी

ब्लू व्हेल चॅलेंजसारख्या धोक्याला किंवा घोटाळ्याला बळी पडू नये म्हणून करता येतील अशा 3 गोष्टींची यादी करा:

1 . तुमची वैयक्तिक माहिती ऑनलाईन असणाऱ्या अनोळखी व्यक्तीशी कधीही शेयर करू नका. कोणत्याही खऱ्या गेम किंवा आव्हानामध्ये खाजगी माहितीची आवश्यकता असू शकत नाही.

2 . गुप्तता, धमक्या किंवा दबाव या धोक्याच्या सूचनांकडे लक्ष द्या. जर ऑनलाईन असणारी व्यक्ती तुम्हाला काही लपवून ठेवायला सांगत असेल, तुम्हाला इतरांपासून लांब राहायला किंवा काही अनुचित करायला सांगत असेल तर त्यांना ब्लॉक करा आणि त्यांच्याविषयी रिपोर्ट करा.

3 . जर तुम्ही कशामुळे अस्वस्थ होत असाल तर तुमचा ज्यांच्यावर विश्वास आहे त्यांच्याशी बोला. तुमच्या सुरक्षेपेक्षा कोणतेही चॅलेंज, ट्रेंड किंवा गेम महत्त्वाचा नाही. खरंतर तुम्ही कधीच एकटे नसता आणि तुम्हाला नेहमी मदत मिळू शकते.

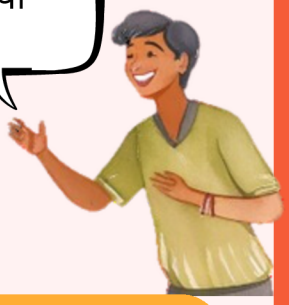
ऑनलाईन प्लॅटफॉर्मवरील हानीकारक कंटेन्ट रिपोर्ट करणे

ज्यांना धोक्यांपासून स्वतःचे संरक्षण करण्यासाठी त्वरित मार्गदर्शक हवा आहे त्यांच्यासाठी हा एक चांगला संदर्भ आहे! गुड जॉब, जसप्रीत आणि नूर!

धन्यवाद, अमित दादा!
मला अजूनही एक प्रश्न आहे. समजा आम्ही या सर्व स्टेप्स काळजीपूर्वक केल्या, परंतु तरीही आम्हाला असुरक्षित वाटणारे संदेश किंवा कंटेन्ट दिसतातच. अशा परिस्थितीत आम्ही काय करावं?

अरे, मी काल यावर एक व्हिडिओ बघत होतो! मला असे आढळले की बहुतेक ॲप्स आणि प्लॅटफॉर्ममध्ये रिपोर्टिंग आणि ब्लॉकिंग हे फीचर्स आहेत ती आपण वापरू शकतो.

अगदी बरोबर आहे, जसप्रीत! बहुतेक ऑनलाइन प्लॅटफॉर्म आणि मेसेजिंग ॲप्समध्ये छळ, धमक्या, तोतयागिरी आणि चुकीची माहिती यासारख्या हानिकारक कंटेन्टविषयी तक्रार करण्यासाठी बिल्ट- इन टूल्स असतात. रिपोर्टिंग करणे महत्वाचे आहे, कारण ते आपल्याला आणि आपल्या सभोवतालच्या इतरांना सुरक्षित ठेवण्यास मदत करते!



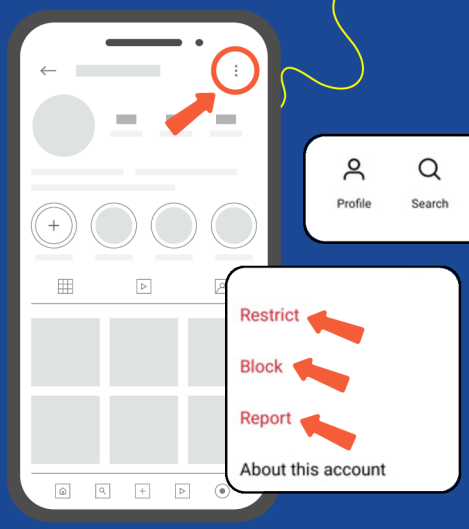
अशी सामग्री किंवा संदेश यांची रिपोर्टिंग करणे प्लॅटफॉर्मला गुन्हेगारांविरूद्ध कारवाई करण्यास मदत करते, ऑनलाइन गैरवर्तनापासून स्वत: चे आणि इतरांचे संरक्षण करते आणि हानिकारक सामग्री पसरण्यापासून प्रतिबंधित करते. रिपोर्टिंगमुळे नेहमीच त्वरित कारवाई होत नाही, परंतु एकाधिक वापरकर्त्यांकडून वारंवार रिपोर्ट केल्यास प्लॅटफॉर्म समस्येकडे लक्ष देतील ही शक्यता वाढू शकते.

ऑनलाइन प्लॅटफॉर्मवरील हानिकारक कंटेन्ट रिपोर्ट आणि ब्लॉक कसा करावा

अधिकांश प्लॅटफॉर्मवर हानिकारक कंटेन्ट किंवा चॅटची माहिती देणे खूप सोपे आहे. तुम्ही यातल्या काही साध्या सोप्या स्टेप्स तुम्ही करू शकता (लक्षात ठेवा की तुम्ही वापरत असलेल्या प्लॅटफॉर्मनुसार हे वेगळे असू शकतात, म्हणून तुम्हाला खात्री नसल्यास विश्वासातील मोठ्या व्यक्तीला किंवा मित्राला विचारा):

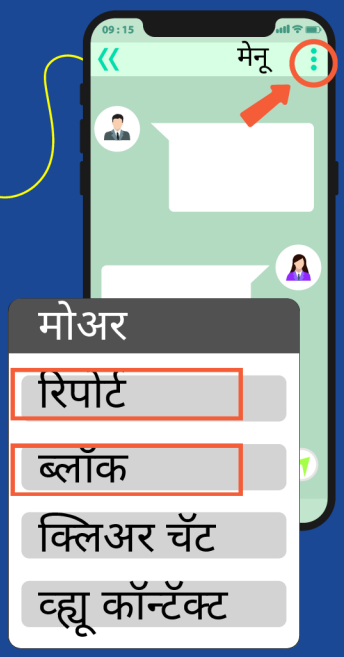
1. पुढील कारवाईची आवश्यकता असल्यास रिपोर्ट करण्यापूर्वी चॅट किंवा सामग्रीचा स्क्रीनशॉट घ्या. तुमच्या फोनवर स्क्रीनशॉट घेण्यासाठी पॉवर / होम बटण आणि व्हॉल्यूम बटण एकत्रित दाबा (हे मॉडेलनुसार वेगळे असू शकते)

2. मेनू ऑप्शनवर क्लिक करा. मेनूमधून "रिपोर्ट", "मोअर" किंवा "फाइंड सपोर्ट" निवडा. सर्वात अधिक जुळणारी कॅटेगरी निवडा (उदा. छळ, असत्य माहिती, तोतयागिरी, घृणा पसरवणारे भाषण इ.).



जर तुम्हाला बनावट खाते किंवा प्रोफाइल (तुमची किंवा तुमच्या ओळखीच्या एखाद्या व्यक्तीची तोतयागिरी करणारी एखादी व्यक्ती) रिपोर्ट करायची असेल, तर तुम्ही मेनू किंवा अधिक माहिती बटण शोधू शकता आणि "प्रोफाइलची तक्रार करा" वर क्लिक करू शकता.

बऱ्याच मेसेजिंग प्लॅटफॉर्मवर केवळ रिपोर्ट करण्याऐवजी "ब्लॉक अँड रिपोर्ट" करण्याचा पर्याय देखील आहे. यामुळे ती व्यक्ती पुन्हा तुमच्याशी संपर्क साधू शकणार नाही!



तुम्हाला एखादा विशिष्ट चॅट किंवा मेसेज याचा रिपोर्ट करायचा असल्यास, तुम्ही मेसेजचा टॅब दाबा आणि धरून ठेवा किंवा रिपोर्ट ऑप्शन शोधण्यासाठी संभाषण सेटिंग्ज तपासा (ते "मोअर" सेटिंग्ज मध्ये असू शकते)

3. रिपोर्ट सबमिट करा आणि अतिरिक्त सूचनांचे पालन करा. तुम्ही कंटेन्ट किंवा चॅट रिपोर्ट केल्यानंतर, ते काढून टाकण्याचा, अकाऊंटवर बंधने आणण्याचा किंवा त्याबद्दल चेतावणी देण्याचा निर्णय प्लॅटफॉर्म घेऊ शकतो. काही प्लॅटफॉर्म तुम्हाला तुमच्या रिपोर्टवर अपडेट्स देतील, तर काही कदाचित देणार नाहीत.

सायबर गुन्ह्यांची रिपोर्टिंग

नूरच्या फोनवर धमकीचा मेसेज येतो. ती घाबरते आणि प्लॅटफॉर्मवर रिपोर्ट करते आणि ब्लॉक करते! पण 5 मिनिटांतच तिला त्याच प्रोफाईलवरून वेगळ्या प्लॅटफॉर्मच्या माध्यमातून दुसरा मेसेज येतो.

मी प्लॅटफॉर्मवर अकाऊंट बद्दल रिपोर्ट केले, तरीही ते संदेश पाठवत आहेत! मला सुरक्षित वाटत नाही... मी आणखी काय करू शकते?

जर हे गंभीर असेल तर आपण सायबर क्राईम सेलला रिपोर्ट केले पाहिजे, असे मला वाटते. मी ऐकले आहे की ते ऑनलाइन धमक्या, छळ आणि डिजिटल फसवणूकचे केसेस हाताळतात. बरोबर ना अमित दादा?

बरोबर आहे! काही महत्त्वाच्या हेल्पलाईन्स तू आम्हाला सांगू शकशील का ग्लिच?

नक्की अमित दादा! तुम्ही cybercrime.gov.in सायबर गुन्ह्यांची तक्रार करू शकता किंवा त्वरित मदतीसाठी 1930वर कॉल करू शकता. आणि जर जेंडर संबंधित धोका असेल तर तुम्ही राष्ट्रीय महिला आयोगाच्या हेल्पलाइनवर 7827-170-170 वर संपर्क साधू शकता. ते ऑनलाइन छळ, ब्लॅकमेल आणि गैरवर्तनाच्या प्रकरणां संदर्भात सहाय्य करतात.

सायबर गुन्ह्याची माहिती देण्यासाठी सरकारी हेल्पलाईन

जर आपल्याला किंवा आपल्या ओळखीच्या एखाद्या व्यक्तीला ऑनलाइन गैरवर्तन, धमक्या, ब्लॅकमेल किंवा छळाला सामोरे जावे लागत असेल तर त्याची तक्रार करून कारवाई करा.

सायबर क्राईम सेल (नॅशनल सायबर क्राईम रिपोर्टिंग पोर्टल)

- वेबसाईट: cybercrime.gov.in
- हेल्पलाईन: 1930
- सायबर स्टॉकिंग, ऑनलाईन धमक्या, आयडेन्टिटी थेफ्ट हॅकिंग

राष्ट्रीय महिला आयोग (NCW)

- वेबसाईट: ncw.nic.in
- हेल्पलाईन: 7827-170-170
- महिलांना लक्ष्य करून त्यांच्यावर होणारे अत्याचार, ऑनलाईन छळ आणि अत्याचार

स्थानिक पोलिस स्टेशन

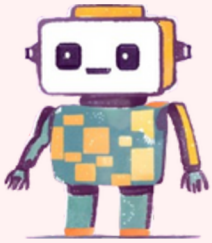
- फोन नंबर: 100
- तुमच्या जवळच्या पोलिस चौकीत सायबर क्राईमविरुद्ध तक्रार करता येते.
- तुम्ही एफ आय आर (FIR) देखील दाखल करू शकता.

चाइल्डलाईन इंडिया (लहान मुलांच्या सायबर सेफ्टीकरता)

- वेबसाईट: childlineindia.org
- हेल्पलाईन: 1098
- ऑनलाइन धमक्या, सायबर गुंडगिरी आणि बालकांसंबंधित इतर डिजिटल गुन्हे हाताळतात

ही माझ्यासाठी खरोखर उपयुक्त यादी आहे, धन्यवाद! समजा मी यापैकी एका नंबरवर कॉल केला किंवा त्यांच्या वेबसाईटवर गेलो. तर मी तक्रार कशी दाखल करू शकतो आणि माझ्याकडे कोणती माहिती असणे आवश्यक आहे?

काही गोष्टी लक्षात ठेवायला हव्यात. चला एक नजर टाकूया!



पायरी 1: पुरावे गोळा करा.

- धमक्या / संदेशांचे स्क्रीनशॉट घ्या किंवा यूआरएल सेव्ह करा.
- त्यांचे टाइमस्टॅम्प आणि आपल्याला संदेश पाठविणारा नंबर किंवा आयडी लिहून ठेवा

पायरी 2: तक्रार दाखल करा

- cybercrime.gov.in जाऊन रिपोर्ट करा. जर तुम्हाला नाव गुप्त ठेवायचे असेल तर तसे करता येते.
- जर तुला रिपोर्ट सबमिट करण्यास किंवा हेल्पलाइनवर कॉल करण्यास जमत नसेल तर एफआयआर दाखल करण्यासाठी आपल्या जवळच्या पोलिस स्टेशनला भेट द्या

पायरी 3: फॉलोअप करा

आपल्या तक्रारीच्या स्टेटसचा मागोवा ठेवा आणि आवश्यक असल्यास, स्वयंसेवी संस्था, कायदेतज्ज्ञ किंवा सपोर्ट करणाऱ्या संस्थांची मदत घ्या.

कृती : बघू या तुम्हाला काय लक्षात आहे

1. भारतात सायबर क्राईमची नोंद करताना कोणत्या प्रकारचे पुरावे अधिकाऱ्यांना सर्वात उपयुक्त ठरतात? अ) गुन्ह्याशी संबंधित कोणत्याही कागदपत्रांच्या फिजिकल कॉपीज

ब) स्क्रीनशॉट, ईमेल आणि फसव्या कंटेन्टच्या डिजिटल कॉपीज
क) फोन कॉलदरम्यान घटनेचे वर्णन
ड) गुन्हा झाला याची पुष्टी करण्या करता पीडित व्यक्तीच्या नातेवाईकांचे स्वाक्षरी केलेले प्रतिज्ञापत्र/ॲफीडेविट

२. बरोबर किंवा चूक : भारतातील सायबर गुन्ह्याची तक्रार करण्यासाठी पोलिस स्टेशनला प्रत्यक्ष भेट देणे आवश्यक आहे.

अ) बरोबर
ब) चूक

3. भारतातील सायबर गुन्ह्यांची माहिती देण्यासाठी हेल्पलाइन नंबर कोणता आहे?
अ) 100
ब) 112
क) 1930
ड) 1098

Activity, Continued

4. तुमचा मित्र तुम्हाला सांगतो की एक अनोळखी व्यक्ती त्यांची सायबर स्टॉकिंग करत आहे, ती त्यांना मेसेज करत असते आणि त्यांच्या ऑनलाइन ॲक्टीविटी ट्रॅक करत आहे..त्याकरता त्यांनी आधी काय केले पाहिजे?

अ) ॲपवर स्टॉकरला ब्लॉक करा आणि रिपोर्ट करा
ब) स्टॉकरला उत्तर द्या आणि त्यांना थांबायला सांगा.
क) सोशल मीडिया अकाऊंट ताबडतोब डिॲक्टिव्हेट करा आणि लोकेशन बंद करा
ड) परिस्थितीकडे दुर्लक्ष करा जेणेकरून स्टॉकरला तुमच्यात रस कमी होईल

5. खालीलपैकी कोणती कृती आपल्या सायबर सुरक्षेसाठी सर्वात जास्त धोका निर्माण करते?

अ) अनेक महत्त्वाच्या खात्यांमध्ये एकच मजबूत पासवर्ड वापरणे
ब) सार्वजनिक वाय-फायशी कनेक्ट होणे आणि संवेदनशील खात्यांमध्ये लॉग इन करणे
क) महत्त्वाच्या खात्यांवर टू-फॅक्टर ऑथेंटिकेशन (2एफए) एनेबल करणे
ड) फक्त सेवा वापरत असतानाच ब्लूटूथ आणि लोकेशन एनेबल करणे.

6. आपल्याहून मोठ्यांची मदत कधी घेणे उचित आहे?

अ) ऑनलाइन संदेशामुळे तुम्हाला अस्वस्थ किंवा असुरक्षित वाटते
ब) तुम्हाला तुमचे संभाषण आणि कृती इतरांपासून गुप्त ठेवण्यास सांगितले गेले आहे
क) आपल्याला ऑनलाइन नवीन मित्राकडून मोठ्या कॅश प्राइजची ऑफर मिळते
ड) वरील सर्व

- हिंसा किंवा त्रास देण्याची धमकी
- लैंगिक छळ किंवा पाठलाग
- हिंसा किंवा त्रास देण्याची धमकी
- तोतयागिरी, फसवणूक किंवा आयडेन्टीटी थेफ्ट

आपल्या संरक्षणासाठी कायदे

इंटरनेट ही एक पॉवरफुल स्पेस आहे जिथे आपण कनेक्ट होतो, शिकतो आणि शेयर करतो, परंतु खऱ्या जगाप्रमाणेच, आपले नुकसान होऊ नये याकरता इथेही कायदे आहेत. जर कोणी तुमच्याकडून काही चोरले, तुम्हाला धमकावले किंवा तुमच्या प्रायव्हसीवर अतिक्रमण केले आणि जरी गुन्हा ऑनलाइन झाला तरी तर त्यांना भारतीय कायद्यानुसार शिक्षा होऊ शकते.!

माहिती तंत्रज्ञान (आयटी) कायदा, 2000

आयटी कायदा हा भारताचा मुख्य सायबर कायदा आहे, जो लोकांना हॅकिंग, आयडेन्टीटी थेफ्ट आणि प्रायवसीच्या उल्लंघनापासून वाचवतो.

डेटा थेफ्ट(कलम 43)

जर कोणी तुमचे डिव्हाइस हॅक केले किंवा परवानगीशिवाय तुमचा डेटा चोरला तर त्यांना 1 कोटी रुपयांपर्यंत दंड होऊ शकतो.

आयडेन्टीटी थेफ्ट (सेक्शन 66सी)

दुसऱ्याचे नाव किंवा फोटो वापरून बनावट सोशल मीडिया प्रोफाइल तयार करणे बेकायदेशीर असून 3 वर्षांचा तुरुंगवास + ₹ 1 लाख दंडाची तरतूद आहे.

प्रायवसीचे उल्लंघन (सेक्शन 66ई)

संमतीशिवाय खाजगी छायाचित्रे किंवा व्हिडिओ शेअर करणे गुन्हा आहे., 3 वर्षांपर्यंत तुरुंगवास + ₹ 2 लाख दंड.

हॅकिंग (सेक्शन 66c)

बेकायदेशीरपणे एखाद्याचा संगणक किंवा सोशल मीडिया वापरणे, खराब करणे किंवा लॉक करणे याला 3 वर्षे तुरुंगवास + ₹ 5 लाख दंडाची शिक्षा होऊ शकते.

भारतीय दंड संहिता (आयपीसी), 1860

सायबर एक्स्टॉर्शन(सेक्शन 384)

पैसे दिले नाहीत म्हणून जर कोणी तुमचे खासगी चॅट किंवा फोटो लीक करण्याची धमकी दिली तर त्यांना सायबर खंडणी कायद्यांतर्गत शिक्षा होऊ शकते

ऑनलाईन स्टॉकिंग आणि हॅरॅसमेंट (सेक्शन 354डी)

ब्लॉक झाल्यानंतरही वारंवार मेसेज करणे, ट्रॅक करणे किंवा एखाद्याला ऑनलाइन त्रास देणे बेकायदेशीर आहे.

निनावी धमक्या (सेक्शन 507)

बनावट सोशल मीडिया अकाऊंट, बेनामी ईमेल किंवा मेसेजिंग ॲप्सच्या माध्यमातून आपली ओळख लपवत कोणी धमक्या पाठवत असेल तर त्यांना या कायद्यानुसार शिक्षा होऊ शकते.

आपल्या संरक्षणासाठी कायदे

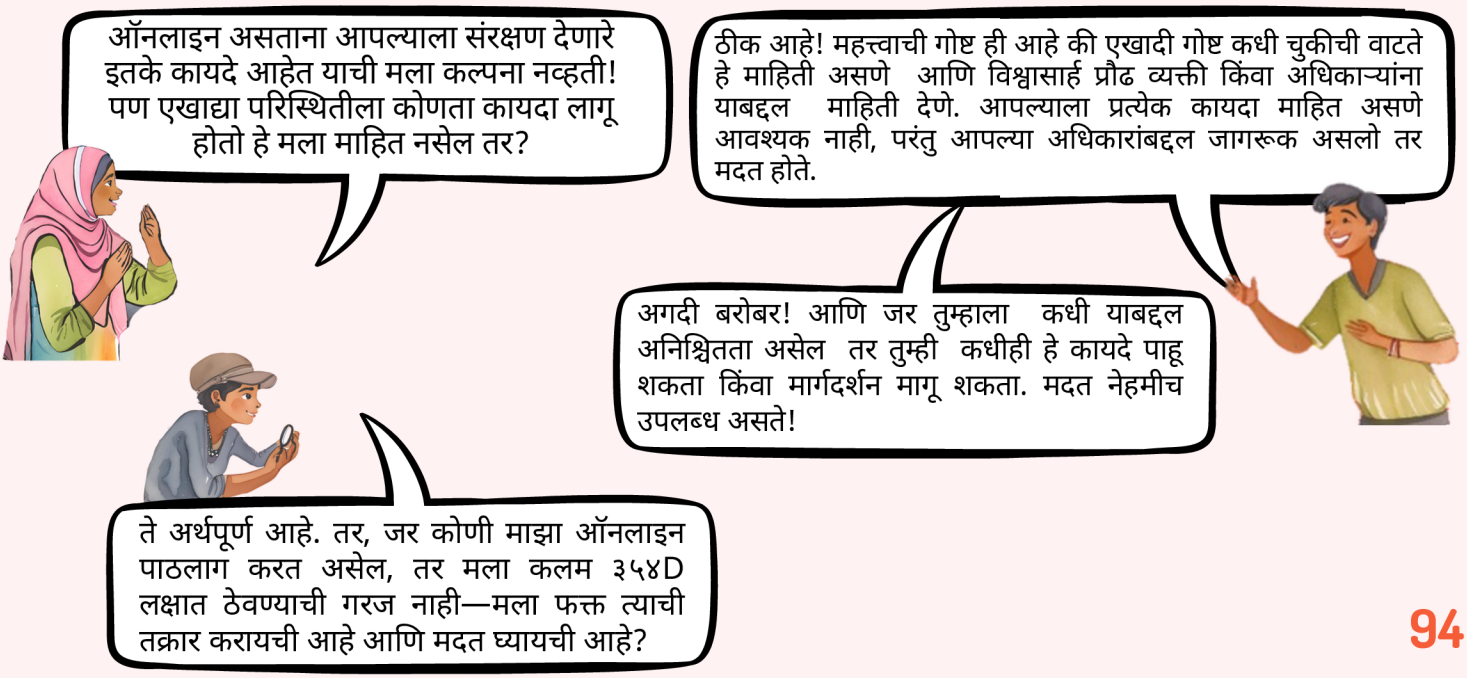
ग्राहक संरक्षण कायदा, 2019

हा कायदा ग्राहकांना ऑनलाइन फसवणूक, घोटाळे आणि अनुचित व्यवसाय पद्धतींपासून संरक्षण देतो. जर ऑनलाइन शॉपिंग वेबसाइटने सदोष उत्पादन परत करण्यास नकार दिला तर आपण या कायद्यांतर्गत तक्रार दाखल करू शकता.

ॲक्टिव्हिटी: कायद्यांची बरोबर जोडी जमवा!

खाली पाच वेगवेगळे ऑनलाइन गुन्हे आणि त्यांच्यापासून संरक्षण करण्यासाठी डिझाइन केलेले पाच कायदे दिले आहेत. प्रत्येक गुन्ह्याची योग्य कायद्याशी जोडी जमवा!

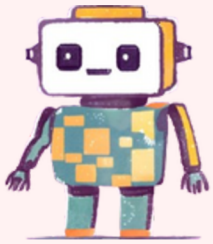
संमतीशिवाय खासगी फोटो लीक केला जातो	हॅकिंग
कोणीतरी तुमच्या कॉम्प्युटरमध्ये हॅक करून फाईल्स डिलीट करतो	ग्राहक संरक्षण कायदा
सदोष उत्पादनासाठी कंपनी आपल्याला रिफंड देण्यास नकार देते	आयडेन्टीटी थेफ्ट
अनोळखी व्यक्ती फेक अकाऊंटवरून धमक्या पाठवत असते	प्रायव्हसीचे उल्लंघन
कोणीतरी तुम्ही असल्याचे भासवून फेक प्रोफाइल तयार करतो	निनावी धमक्या



ऑनलाइन मदत शोधणे आणि इतरांना सपोर्ट देणे

इंटरनेट कनेक्ट होण्यासाठी, शिकण्यासाठी आणि मजा करण्यासाठी एक उत्तम जागा असू शकते-परंतु जेव्हा गोष्टी चुकतात तेव्हा काय होते? तुम्हाला कधीही असुरक्षित, भारावून गेल्यासारखे वाटत असेल किंवा व्यक्त होण्यासाठी एखाद्याची आवश्यकता असेल, तर मदत मिळवण्यासाठी एक कॉल करायचा आहे..

विश्वसनीय हेल्पलाइन, कौन्सिलर्स आणि संस्था आपल्याला सहाय्य करण्यास तयार आहेत, तुम्ही ऑनलाइन छळ, गुंडगिरी, त्रास याला सामोरे जात असाल किंवा मानसिक आरोग्याशी संघर्ष करत असाल. कुठून मदत घ्यावी आणि इतरांना कसा सपोर्ट करावा हे जाणून घेणे ऑनलाइन सुरक्षित राहण्याचा एक आवश्यक भाग आहे.



चाइल्ड लाइन इंडिया फाउंडेशन
गुंडगिरी, छळ, भावनिक समर्थन 1098 (टोल-फ्री) यावर लक्ष केंद्रित करते.

एनसीपीसीआर (राष्ट्रीय बाल हक्क संरक्षण आयोग)
बाल हक्कांचे उल्लंघन, गुंडगिरी, छळ
1800-121-2830 (टोल-फ्री) यावर लक्ष केंद्रित करते.

महिला हेल्पलाइन डब्ल्यूएचएल (निर्भया फंड, महिला व बाल विकास मंत्रालय
ऑनलाइन छळ, सुरक्षिततेची चिंता 181 (टोल-फ्री) यावर लक्ष केंद्रित करते.

एनसीडब्ल्यू (राष्ट्रीय महिला आयोग)
ऑनलाइन लैंगिक छळ, महिलांचे अधिकार यावर लक्ष केंद्रित करते.

AASRA हेल्पलाइन
आत्महत्या प्रतिबंध, भावनिक त्रास समर्थन 91-9820466726 यावर लक्ष केंद्रित करते.

iCALL
गोपनीय भावनिक समुपदेशन, मानसिक आरोग्य समर्थन यावर लक्ष केंद्रित करते.022-25521111 (सोमवार ते शनिवार, सकाळी 8 ते रात्री 10)

मानस फाऊंडेशन
मानसिक आरोग्य समर्थन, त्रास आणि गुंडगिरीसाठी समुपदेशन यावर लक्ष केंद्रित करते.
+91 97117 00069

बचपन बचाओ आंदोलन
बेपत्ता मुले, बालमजूर, तस्करी, गैरवर्तन 1800-102-7222 (टोल-फ्री, 24/7) यावर लक्ष केंद्रित करते.

इमोशनल फर्स्ट एड: त्रासात असताना स्वत:ला शांत करणे.

या हेल्पलाईन खरोखरच उपयुक्त आहेत! पण नूर, या क्षणी मला भीती वाटू लागली तर काय? मला शांत होण्यास मदत करण्यासाठी तुझ्याकडे काही टिप्स आहेत का? मला वाटते की मी सगळेकाही ठीक करण्याच्या प्रयत्नात इतका जास्त अडकतो की मला कसे वाटते याला किती महत्त्व आहे हे मी विसरतो.

तुझं म्हणणं मला समजलं! जेव्हा ऑनलाइन असताना धमकावणे किंवा वाद होणे असे काहीतरी तणावपूर्ण घडते, तेव्हा कसलाही विचार न करता प्रतिक्रिया देणे फार सोपे आहे. परंतु त्याऐवजी थोडा पॉज घेणे, आपल्या भावना मॅनेज करणे याचा नक्कीच उपयोग होतो. मी तुम्हाला काही सोप्या ट्रिक्स दाखवतो ज्यामुळे फरक पडू शकतो!

स्वत:ला शांत करण्याचे त्वरित उपाय: तुम्हाला सगळं सहन होत नसेल तर पुढील टेक्निक्स वापरुन पहा.

5-4-3-2-1 प्रत्यक्ष काय दिसते आहे ते पाहणे.

आजूबाजूला काय आहे ते पहा

5. वस्तू ज्या तुम्ही बघू शकता
4. वस्तू ज्यांना तुम्ही स्पर्श करू शकता
3. वस्तू ज्यांना तुम्ही ऐकू शकता
2. वस्तू ज्यांचा तुम्ही वास घेवू शकता
1. वस्तू ज्यांची तुम्हाला चव घेता येते.

तुमचे विचार लिहून काढणे

काय घडलं ते लिहून काढा, तुम्हाला कसं वाटलं आणि पुढे कोणती पावलं उचलता येतील ते लिहा.

आपले विचार कागदावर उतरवल्याने तुम्हाला भावनांवर विचार करण्यास, स्पष्टता मिळविण्यात आणि प्रतिक्रिया देण्यापूर्वी त्यावर विचार करून निर्णय घेण्यास मदत करते.

व्हिज्युअलायझेशन आणि खोल श्वास

पहिल्यांदा तर तुमचे डोळे बंद करा आणि तुम्ही शांत, सुरक्षित जागी आहात असं चित्र डोळ्यांसमोर आणा- अशी जागा जिथे आपल्याला पूर्णपणे आराम वाटतो. ती जागा म्हणजे शांत उद्यान, आरामदायक खोली किंवा शांत पर्वत असू शकते. तुमची सुरक्षित जागा कोठेही असू शकते ती तुम्हाला सुरक्षित, आरामशीर ठेवते आणि तुम्ही स्थिर होता...

आता, हळूहळू, खोल श्वास घ्या, त्या जागेची दृश्ये, ध्वनी आणि भावनांवर लक्ष केंद्रित करा. स्वत:ला या क्षणाचा पुरेपूर अनुभव घेऊ द्या.

ॲक्टिव्हिटी: स्वत: कसं शांत व्हायचं याचा प्लॅन ठरवा.

पुढच्या वेळी जेव्हा आपण भारावून जाल तेव्हा स्वत:ला शांत करण्याकरता कोणती ॲक्टिव्हिटी कराल?

आपली सुरक्षित जागा (वास्तविक किंवा कल्पित) कोठे आहे जेथे तुम्हाला आरामदायक वाटण्यास मदत मिळते?

कठीण प्रसंगी तुम्ही स्वत: ला पुन्हा पुन्हा काय बजावता ते वाक्य लिहा.
("मी बलवान आहे. हा क्षण निघून जाईल.)

वाह! हे किती उपयुक्त आहे - धन्यवाद नूर! मी स्वत:साठी नक्कीच एक भरणार आहे.
अशाच परिस्थितीत असलेल्या एखाद्या मित्राला कशी मदत करावी याबद्दल तुमच्याकडे काही सूचना आहेत का? फक्त त्यांना रिपोर्ट करा किंवा त्वरित कारवाई करण्यास सांगणे कधीकधी असंवेदनशील वाटू शकते आणि मला त्यांना चांगल्या प्रकारे सपोर्ट कसे करावे हे शिकायचे आहे!

तुमचे म्हणणे बरोबर आहे - एखादा मित्र ऑनलाइन गुंडगिरी, छळ किंवा नकारात्मकतेमुळे भावनिक आणि मानसिकदृष्ट्या संघर्ष करत असेल परंतु तो नेहमीच मदत मागू शकत नाही! अशीही शक्यता आहे की त्यांनी आधीच गुन्हा रिपोर्ट केला आहे परंतु तरीही त्यांना अस्वस्थ वाटत आहे. मला वाटते की आपल्या मित्रांना कसा सपोर्ट द्यावा हे जाणून घेणे खरोखर महत्त्वाचे आहे आणि यामुळे खूप मोठा बदल घडून येईल.

सोशल फर्स्ट एड: त्रासात असलेल्या मित्राचा उत्तम आधार कसे व्हायचे

ॲक्टिव लिसनिंग- जेव्हा एखादा मित्र त्यांच्या संघर्षाबद्दल तुम्हाला सांगतो, तेव्हा ताबडतोब उपाय सुचवू नका.. त्याऐवजी त्याला न थांबता बोलू द्या. त्याला त्याच्या भावना मोकळेपणाने व्यक्त करू द्या आणि तुम्ही त्या समजूनघ्या. कधीकधी हे माहिती असणे की कुणीतरी असे आहे जे कुठलेही जजमेंट न देता आपलं नीट ऐकून घेत आहे हे प्रत्यक्ष सल्ल्यापेक्षा ही दिलासा देणारे असते.

चेक इन आणि फॉलोअप - एक छोटा सा मॅसेज "हे, तू कसा आहेस? कसं काय चाललंय?" यामुळे खूप फरक पडू शकतो. जरी तो ठीक आहे असे म्हणत असला तरी फॉलोअप केले आणि चौकशी केली तर तुम्ही खरोखर त्याची काळजी करता हे दिसते. जर तो ऑनलाइन ताणतणाव, गुंडगिरी किंवा छळाचा सामना करत असेल तर अनौपचारिक बोलल्याने त्याला सपोर्ट मिळेल आणि त्याच्यावरचा ताण कमी होईल.

सीमा निश्चित करण्यात मदत करा - जर त्यांना ऑनलाइन छळ किंवा नकारात्मकतेचा सामना करावा लागत असेल तर त्यांच्या हे लक्षात आणून द्या की त्यांचे त्यांच्या स्पेस वर नियंत्रण आहे. धोकादायक यूजर्स ना ब्लॉक आणि रिपोर्ट करण्यासाठी तसेच त्यांच्या प्रायव्हसी सेटिंग्ज समायोजित करण्यास त्यांना प्रोत्साहित करा. त्यांना याबद्दल अनिश्चितता असल्यास याच्या प्रक्रियेबद्दल त्यांना मार्गदर्शन करण्याची ऑफर द्या.!

इंटरनेट सुरक्षा, प्रायवसी सेटिंग्ज आणि त्यांना ऑनलाइन टाईम मॅनेजमेंट करण्यात त्यांना मदत करण्यासाठी आपण या गाईडबुकची शिफारस देखील करू शकता. योग्य माहिती असली की तुम्हाला आणि तुमच्या सभोवतालच्या लोकांना सुरक्षित आणि हेल्दी डिजिटल अनुभव यावेत याकरतासक्षम करू शकते.

ॲक्टिव्हिटी:

आपण ऑनलाइन असताना तणावपूर्ण किंवा असुरक्षित परिस्थिती कशी हाताळता याकरता तयार असल्यास मोठा फरक पडू शकतो. आपल्याकडे योग्य साधने आणि सपोर्ट सिस्टिम आहे याची खात्री करण्यासाठी खालील चेकलिस्ट पूर्ण करा.

- [ ] यादीमधून किमान एक हेल्पलाइन निवडा आणि ती आपल्या फोनमध्ये सेव्ह करा किंवा सहज उपलब्ध असलेल्या ठिकाणी लिहा. एखाद्या संकटात लवकर कुठे मदत मिळवायची हे जाणून घेणे खूप उपयुक्त ठरू शकते.
- [ ] अश्या दोन व्यक्तींचा विचार करा ज्यांच्याकडे तुम्ही जावू शकता - हे कुटुंबातील सदस्य असू शकतात, शिक्षक, जवळचा मित्र यापैकी कोणीतरी असू शकतात. त्यांची नावे लिहा जेणेकरून संकटाच्या वेळी तुम्हाला आठवेल!
- [ ] कुठलीही एक कामिंग स्ट्रेटेजी निवडा, उदाहरणार्थ खोल श्वासोच्छवास घेणे , डायरी लिहिणे किंवा ग्राउंडिंग एक्सरसाईज. तुम्हाला सगळं जेव्हा असह्य होईल तेव्हा हे वापरण्याचा सराव करा!
- [ ] संकटात सापडलेल्या मित्राला मदत करण्यासाठी एका सोशल फर्स्ट एडचा सराव करा.

चॅप्टर उजळणी

- वैयक्तिक माहिती मागणाऱ्या , भेटवस्तू किंवा आश्वासने देणाऱ्या , फोटोंची मागणी करणाऱ्या किंवा आपले संभाषण गुप्त ठेवण्यास सांगणाऱ्या संदेशांपासून खूप सावधगिरी बाळगा!
- All messaging and social media platforms have mechanisms to report and block messages and profiles - you should always use these when in doubt!
- ऑनलाइन रिपोर्टिंग आणि ब्लॉक करणे पुरेसे वाटत नसल्यास, आपण सायबर क्राईम सेलकडे (पीएच. 1930 किंवा cybercrime.gov.in, किंवा आपल्या स्थानिक पोलिस स्टेशनसाठी 100) गुन्ह्याची तक्रार देखील करू शकता
- ऑनलाइन धमक्यांमध्ये हे समाविष्ट असू शकते: हिंसा किंवा नुकसान, लैंगिक छळ किंवा पाठलाग, संमतीशिवाय खाजगी फोटो शेयर करणे, तोतयागिरी , फसवणूक किंवा आयडेन्टीटी थेफ्ट
- आयटी कायदा 2000, भारतीय दंड संहिता 1860 आणि ग्राहक संरक्षण कायदा 2019 अंतर्गत अनेक कायदे आहेत जे डिजिटल सिटीझन या नात्याने तुझ्या अधिकारांची हमी देतात!
- सर्वात महत्वाचे म्हणजे तुम्ही एकटे नाही हे लक्षात ठेवा! तुमचे समर्थन करण्यासाठी बरेच प्रियजन आणि मित्र आहेत, म्हणून मदत मागा

चॅप्टर 6: क्लिक करा, स्क्रोल करा, श्वास घ्या: डिजिटल जगात मानसिक स्वास्थ्य

इंटरनेट ही एक भन्नाट जागा आहे- शिकण्याच्या, कनेक्ट होण्याच्या आणि स्वत:ला व्यक्त करण्याच्याअनेक संधी तिथे आहेत. परंतु खऱ्या आयुष्याप्रमाणे इथे देखील काही खास आव्हाने असू शकतात. ती आव्हाने ओळखणे, निरोगी ऑनलाइन सवयी लावून घेणे आणि सुरक्षित आणि कोणताही घोळ न होता आपल्या डिजिटल जगाचा जास्तीत जास्त फायदा घेणे महत्वाचे आहे.

मीरा रात्री उशीरा तिचा फोन स्क्रोल करत असते. तिला मित्रांचे रोमांचक अपडेट्स आणि मजेशीर व्हिडिओ दिसतात. पण तिला अस्वस्थ वाटणाऱ्या नकारात्मक बातम्या आणि कमेंट्सही दिसतात. दुसऱ्या दिवशी सकाळी ती उठते तेव्हा तिला थकल्यासारखं वाटतं.

मी फक्त स्क्रोल करत असतानाही मला इतका थकवा का जाणवतो? कंटेंटमुळे आहे फक्त... की सगळ्याचा अतिरेक झालाय?

तू बराच वेळ स्क्रोल करत आहेस असे दिसते. कधीकधी, ऑनलाइन असणे एखाद्या रोलरकोस्टरसारखे वाटू शकते- एका क्षणी आपले मनोरंजन केले जाते, दुसऱ्या क्षणी आपल्याला अशा गोष्टींचा फटका बसतो ज्यामुळे आपल्याला उदास वाटते. त्यामुळे थोडा वेळ थांबून आपल्याला कसे वाटत आहे हे पाहायला हवे.

होय, हे विचित्र आहे. काही गोष्टी मला हसवतात, पण मग मला काहीतरी त्रासदायक दिसतं आणि अचानक मला अस्वस्थ वाटतं.

तू शेवटचा ऑनलाइन कधी होता याचा विचार करा - केवळ सोशल मीडियावरच नव्हे तर कोणतेही ॲप किंवा वेबसाइट वापरत असशील तरी. मग ती बातमी असो, शॉपिंग असो किंवा बँकिंग ॲप्स, , तू इंटरनेटशी कसा संवाद साधतो त्याचा तुला कसे वाटते यावर परिणाम होऊ शकतो.

- बातम्या ब्राउझ केल्याने तुम्हाला माहिती मिळते पण त्यामुळे तुम्ही अस्वस्थ होता असे वाटले का?
- शॉपिंगने काही वेळ भारी वाटलं पण नंतर अपराधी वाटलं का?
- तुम्ही दिवसाच्या कोणत्या वेळेस ॲप किंवा वेबसाइटवर होता?

या घटकांचे विश्लेषण केल्याने याबद्दल अंतर्दृष्टी मिळू शकते की कुठल्या भावना तुमच्या इंटरनेट वापराला चालना देतात आणि त्या बदल्यात इंटरनेट तुमच्या मूडवर कसा परिणाम करते.

ॲक्टिव्हिटी:

इंटरनेट वेलबिइंग स्कोअरकार्ड

सूचना:

- खालील १० प्रश्नांची प्रामाणिकपणे उत्तरे द्या.
- प्रत्येक विधानासाठी, जर आपण ती कृती वारंवार करत असाल तर स्वत: ला 1 गुण द्या.

1. मी सकाळी सगळ्यात आधी माझा फोन (सोशल मीडिया, बातम्या, शॉपिंग ॲप्सपाहतो.
2. मला इतर बरंच कामे असली तरी स्क्रोल करणे थांबविणे कठीण जाते.
3. बातम्या वाचल्यानंतर किंवा ऑनलाइन अपडेट्स पाहिल्यानंतर मला तणाव किंवा चिंता वाटते.
4. मी माझ्या जीवनाची तुलना ऑनलाइन जे पाहतो त्याच्याशी करतो - मग ते लोक असोत, ट्रेंड्स असोत किंवा जीवनशैली असो
5. मला कशाचीही गरज नसतानाही मी ऑनलाइन शॉपिंग करतो, फक्त बरे वाटण्यासाठी.
6. जेव्हा मला उदास वाटते, कंटाळा येतो किंवा मला बाकी सगळं अंगावर येतं तेव्हा मी इंटरनेट वापरतो.
7. फक्त ब्राउझिंग किंवा स्क्रोल करत राहण्यासाठी मी उशीरापर्यंत जागलो आहे, आणि झोपेचा त्याग केला आहे.
8. संदेश, कमेंट्स किंवा सूचनांना त्वरित उत्तर देण्याचा मला ताण येतो .
9. ऑनलाइन असल्यामुळे मी वास्तविक जीवनातील कामे (छंद, शाळेचे काम, कौटुंबिक वेळ) देखील टाळली आहेत .
10. जेव्हा माझ्या पोस्टला पुरेसे लाइक्स, कमेंट्स मिळत नाहीत किंवा त्या कोणी फारशा पहात नाही तेव्हा मला अस्वस्थ वाटतं.

स्कोर विश्लेषण

- 0-3 गुण - छान! सोशल मीडियाशी तुझे निरोगी नाते आहे
- 4-6 गुण - संतुलित! तू ठीक आहेस, परंतु तू तुझ्या काही सवयींबाबत सावधगिरी बाळगू शकतोस
- 7-10 पॉईंट्स - तुझ्या सोशल मीडियाच्या वापरामुळे तुमच्या आरोग्यावर परिणाम होऊ शकतो. त्यामुळे रीसेट होण्याची वेळ आली आहे!

चिंतन आणि कृती

- तुझ्या स्कोअरबद्दल तुला काही आश्चर्य वाटलं का?
- तुझे डिजिटल जगातील स्वास्थ्य सुधारण्याकरता तू कोणते लहान बदल करू शकतोस?

तू कोणती स्टेटमेंट्स चेक केले आणि ते का केले याचा विचार कर. ते विशिष्ट प्लॅटफॉर्म, ॲप किंवा मूडशी संबंधित होते का? कधीकधी, काही ट्रिगर - उदाहरणार्थ लेट नाईट बोरडम किंवा तणाव - आपल्याला इंटरनेटचा अतिवापर करण्यास प्रवृत्त करतात. नंतर या चॅप्टरमध्ये आपण योग्य निवडी करण्याचे मार्ग शोधू

सिद्धार्थने दोन वर्षांपूर्वी डिजिटल चॅम्पियन्स प्रोग्राम पूर्ण केला आणि ऑनलाइन सुरक्षिततेबद्दल त्याच्या मित्रांसाठी तो मार्गदर्शक झाला. स्पाम शोधण्यापासून ते प्रायव्हसी कंट्रोल सेट करण्यापर्यंत, डिजिटल विश्वात जबाबदारीने कसे नेव्हिगेट करावे हे त्याला माहित होते. पण अलीकडे, त्याचे आई-वडील जरा अस्वस्थ झाले होते – सगळीकडे डिजिटल गुन्ह्यांच्या बातम्या येत होत्या आणि त्यांची चिंता वाढत होती. शेवटी एके दिवशी संध्याकाळी जेवताना सिद्धार्थने विचारलं,

आई, बाबा तुम्हाला कधी काळजी वाटते का की मी बराच वेळ इंटरनेट वापरतो म्हणून?

आमचा तुमच्यावर विश्वास आहे आणि आम्हाला माहिती आहे की तू इतके वर्षे सावधगिरीने इंटरनेट वापरत आहात. पण अलीकडे बातम्यांमध्ये चिंताजनक ट्रेंड पाहायला मिळत आहेत. आम्ही तुला घाबरवत नाही आहोत, पण तू सुरक्षित आणि सतर्क आहेस याची आम्हाला फक्त खात्री करून घ्यायची आहे - जसे आपण एखाद्या गर्दीच्या ठिकाणी करतो. त्या दिवशी मीराच्या आई-वडिलांशीही आम्ही याबद्दल बोलत होतो.

मग मी इंटरनेट अजिबात वापरू नये का? किंवा जेव्हा मी तुमच्या जवळ असेन तेव्हाच ते वापरायचे का?

अजिबात नाही—प्रवेश काढून घेणे हा उपाय नाही. चला काही सोपे, व्यावहारिक नियम बनवण्यासाठी एकत्र काम करूया जे तुमच्या स्वातंत्र्याचा आदर करण्याबरोबरच तुम्हाला सुरक्षित ठेवतील. आपण काही मर्यादा ठरवू शकतो आणि तुम्हाला कसे वाटते ते पाहू शकतो.

आपल्याला नेहमी इंटरनेट चा वापर कमी वेळा करायला का सांगितले जाते?

आपल्यापैकी अनेकांना हा प्रश्न पडतो की, मोठी माणसं का म्हणतात, "तो फोन खाली ठेवा?" हे केवळ स्क्रीन टाइमबद्दल नाही; स्क्रीनच्या मागे काय घडतंय याबद्दल आहे. सोशल मीडिया एक महासागर आहे अशी कल्पना करा - एक विशाल , रोमांचक आणि एक्सप्लोर करण्याच्या संधींनी परिपूर्ण असा. काही ठिकाणी गोष्टी स्पष्ट असतात जेथे तू शिकू शकतोस, कनेक्ट करू शकतोस आणि प्रगती करू शकतोस. पण कधी कधी आपण त्यात हरवून जाऊ शकतो. इंटरनेट आपल्याला व्यग्र ठेवण्यासाठी तयार केले गेले आहे- कंटेंट आणि नोटिफिकेशन सर्व सुधारित आणि पर्सनलाइज्ड केल्या आहेत, विशेषत: आपल्यासाठी. परंतु आपण ऑनलाइन किती वेळ घालवतो आणि आपण कशात गुंतत आहोत याबद्दल आपण जागरूक राहाणे आपल्या हातात आहे. आपला उद्देश पूर्णपणे डिस्कनेक्ट करणे नाही तर त्यावर नियंत्रण ठेवणे हे आहे - इंटरनेटचा अशा प्रकारे वापर करणे जे आपल्याला विचलित करण्याऐवजी आपल्या जीवनातील वॅल्यूज् वाढवतात.

चेकलिस्ट: जेव्हा सोशल मीडिया खूप जास्त होत आहे असे वाटते.

सिद्धार्थप्रमाणेच आपण सर्वांनी आपल्या इंटरनेट वापरासंदर्भात काही बेसिक गाईडलाईन्स ठरवून घेतली पाहिजेत. पण, पहिली पायरी म्हणजे काय सुरक्षित वाटते आणि काय नाही हे ओळखणे. स्वत:चे मूल्यांकन करण्याचे काही मार्ग येथे आहेत. जर खालीलपैकी कोणत्याही भावना तुम्ही अनुभवत असल्याचे लक्षात आले तर थोडा वेळ थांबण्याची आणि विचार करण्याची हीच वेळ आहे.

चिंताग्रस्त किंवा असुरक्षित वाटणे
शारीरिक चिन्हे: छातीत जडपणा वाटणे , अस्वस्थता किंवा मूड स्विंग्स असणे.

सतत तुलना
इतर लोक जे दाखवण्याचा प्रयत्न करतात त्याच्या आधारे तुम्ही तुमच्या आयुष्याचे मोजमाप करता.

संवादातून रागावणे किंवा दु:खी होणे
संभाषण किंवा कमेंट आपल्याला पूर्वीपेक्षा जास्त तणावग्रस्त करतात.

झोप कमी होणे
स्क्रोल किंवा फीड रिफ्रेश करताना तुम्ही उशिरापर्यंत जागे राहता.

डिस्कनेक्ट झाल्यासारखे वाटणे
"कनेक्टेड" असला तरीही तुम्हाला अधिक एकटेपणा जाणवतो.

लाइक्स आणि कमेंट्सचा अतिविचार
तू आपल्या डोक्यात प्रतिक्रियांचा विचार करत राहतोस

इमोशनल ड्रेनेज
ऑनलाइन राहिल्यानंतर तुम्हाला थकवा किंवा दमल्यासारखे जाणवते

लक्षात ठेवा, तुमच्या फोनला रिचार्ज करण्याची आवश्यकता आहे- तसेच तुम्हाला देखील! जर सोशल मीडियामुळे तुला उत्साही वाटण्यापेक्षा उदास वाटत असेल तर चला रीसेट करण्याचे आणि बरे वाटण्याचे मार्ग शोधूया

प्रत्येकाचा ऑनलाइन प्रवास वेगळा दिसतो- एका व्यक्तीसाठी जे लागू पडते ते दुसऱ्याला लागू पडत नाही. कनेक्ट होण्यासाठी आणि शिकण्यासाठी सोशल मीडिया उत्तम आहे, परंतु आपल्या डिजिटल जीवनाचा भौतिक जीवनाशी समतोल साधणे आवश्यक आहे. आपली सुधारणा, कनेक्शन आणि एकूणच सुधारणा होण्याकरता प्रत्यक्ष जीवनातील अनुभव आवश्यक आहेत आणि ते आपल्याला विशिष्ट मार्गाने आपल्याला तयार करतात.

माझ्या अनुभवाच्या आणि रिसर्चच्या आधारावर सोशल मीडियाशी सुदृढ नाते कसे निर्माण करायचे हे मी सांगतो

सोशल मीडियाशी सुदृढ नाते कसे निर्माण करायचे

1. पॉझिटिव आणि प्रेरणा देणारा कंटेन्ट वाचा किंवा पहा. खेळीमेळीचे संवाद साधून डिजिटल काइंडनेस चा सराव करा.
2. ॲप टाईमर चा उपयोग करून कोणती ॲप किती वेळ पाहता याचे लिमिट ठरवा.
3. जी ॲप तुम्हाला लगेच वापरायची नाही आहेत त्यांचे नोटिफिकेशन बंद ठेवा.
4. जेव्हा दुसरीकडे फोकस करायचा आहे किंवा ब्रेक हवा आहे तेव्हा 'Do Not Disturb' हे फीचर वापरा.
5. रात्री जागून स्क्रोलिंग टाळण्याकरता आणि घरी नो स्क्रीन झोन सेट करण्याकरता सोशल मिडियाचा वापर कमी करा
6. काहीही पोस्ट करण्यापूर्वी "One-Night Rule" चा वापर करा, यामध्ये तुम्ही काहीही पोस्ट करण्या आधी तुम्ही एक दिवस वाट पाहता.
7. जेव्हा इतरांच्या कृतीमुळे सोशल मीडिया स्ट्रेसफूल वाटतो तेव्हा तेथील संवाद कमी करा.
8. Mute, unfollow, आणि गरज वाटल्यास block करा.
9. मित्र, मैत्रीण, पार्टनर, शिक्षक कोणाशीतरी बोला.
10. लर्निंग आणि काहीतरी चांगलं पसरवण्याकरता सोशल मीडिया वापरा.

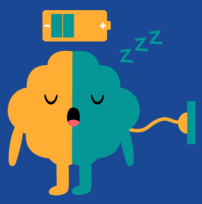
हॅप्पीनेस मेनू

लक्षात ठेवा, आपल्या स्क्रीनच्या बाहेर एक संपूर्ण जग आहे! जेव्हा इंटरनेट खूप अंगावर येतंय असं वाटतं तेव्हा एक पाऊल मागे घ्या - आपले जीवन केवळ पिक्सेल आणि नोटिफिकेशन नाही. श्वास घेण्यासाठी ताजी हवा आहे, खरी माणसं भेटायला आहेत आणि स्क्रोल करण्याशिवाय इतर अनेक अनुभव तुमची वाट बघत आहेत. तुमचे सर्वोत्तम क्षण केवळ ऑनलाइन नसतात. येथे एक हॅपीनेस मेनू आहे - सेरोटोनिन-बूस्टिंग ॲक्टिव्हिटीजची यादी ज्यामधून तुम्ही तुमचा मूड चांगल्या करण्यासाठी वापरू शकता आणि स्वत: ला आठवण करून देऊ शकता की आनंद ऑफलाइन देखील मिळतो!

- तुमच्या आवडत्या गाण्यावर डान्स करा
- निसर्गात फिरायला जा
- मित्राशी किंवा मैत्रिणीशी गप्पा मारायला फोन करा
- एखादा खेळ खेळा
- तुमचे विचार लिहून काढा
- पेंटिंग करा, डुडल किंवा एखादी कला जोपासा
- तुम्हाला उत्साह आणणारं म्युझिक लावा
- डीप मेडिटेशन किंवा ध्यान करा
- काही कुक करा किंवा बेक करा
- काहीही दयाळूपणाचे कृत्य करा
- सूर्यास्त पहायला जा
- तुमच्या आवडीच्या ठिकाणी जा
- तुमची गोल लिस्ट तयार करा
- निवांत वेळ काढून अंघोळ करा
- एखादं पुस्तक किंवा कविता वाचा
- तुम्ही भविष्यात कसे असाल असा विचार करून स्वत:ला पत्र लिहा.
- तुमचं घर आवरून घ्या
- एखाद्या कामासाठी स्वयंसेवा करा

वर लिस्ट केलेले उपक्रम ही केवळ काही उदाहरणे आहेत. मुख्य म्हणजे आपल्या स्वत:च्या गरजा समजून घेणे आणि आपला मूड आणि आनंदाकरता काय चांगले आहे हे ओळखणे. स्वत:ला हे विचारून सुरुवात करा

- कशामुळे मला चांगले आणि उत्साही वाटते?
- जेव्हा मला इंटरनेट कंटेन्टमुळे जड वाटतं तेव्हा मला शांत होण्यास कशाची मदत होते?
- कोणते उपक्रम मला आनंद देतात किंवा मला समाधान देतात?



एकदा आपण हे क्रियाकलाप ओळखले की त्यांना आपल्या दिनचर्येत समाविष्ट करा. कालांतराने, या सवयी आपल्याला ऑनलाइन आणि ऑफलाइन जीवनात संतुलन निर्माण करण्यात मदत करतील, सोशल मीडियालाने आपल्यावर नियंत्रण ठेवण्याऐवजी आपण त्याला नियंत्रणात ठेवत आहात याची खात्री करा.

आपल्या मेंटल हेल्थची काळजी घेणे याचा अर्थ आहे चढ-उतार हा जीवनाचा एक नैसर्गिक भाग आहे हे ओळखणे ऑनलाइन लाईफमध्ये ही. सोशल मीडिया हे शिक्षण, कनेक्शन आणि प्रेरणा यासाठीची एक स्पेस असू शकते, परंतु सोशल मीडिया सेल्फ डाऊट किंवा तुलना करण्याची स्थिती देखील आणू शकते. जेव्हा तू सतत दिसणाऱ्या रील्समधून स्क्रोल करत असतोस तेव्हा आपण जगाच्या मागे आहोत असे वाटणे साहजिक आहे - परंतु लक्षात ठेवा, आपण जे ऑनलाइन पाहतो ते बऱ्याचदा प्रत्यक्ष परिस्थितीचे काळजीपूर्वक तयार केलेले चित्र असते, ते खरे चित्र असतेच असे नाही.

चुकीची माहिती आणि चुकीच्या माहितीबद्दल आपण काय अभ्यास केला त्याचा विचार करा - जश्या खोट्या बातम्या पसरू शकतात, त्याचप्रमाणे काल्पनिक डिजिटल व्यक्तिमत्त्वदेखील . लोक नेहमी त्यांच्या आयुष्यातील सर्वोत्तम भाग शेयर करतात, ज्यामुळे गोष्टी जशा असतात त्यापेक्षा अधिक परिपूर्ण वाटतात. पण प्रत्येक पोस्टच्या मागे आपल्यासारखीच खरी व्यक्ती असते जिच्या जीवनात संघर्ष, असुरक्षितता आणि आव्हाने असतात.

स्वत:ला ही आठवण करून देणे महत्वाचे आहे की आपण जे पाहतो ते नेहमीच पूर्ण चित्र नसते. आपल्या वास्तविकतेची तुलना एखाद्या व्यक्तीच्या हायलाइट रीलशी करण्याऐवजी, तुम्हाला खरोखर आनंद आणि परिपूर्णता कशामुळे मिळते यावर लक्ष केंद्रित करा.

तुमच्या पोस्टवर लाईक्स आणि कमेंट्स किंवा तुमच्या फॉलोअर्सच्या संख्येपेक्षा तुमचा आनंद महत्त्वाचा आहे!

कालांतराने, मी शिकलो आहे की मी इंटरनेट कसे वापरतो याबद्दल जाणीवअसणे महत्वाचे आहे. मला असे वाटायचे की मला अद्ययावत राहण्यासाठी नेहमीच ऑनलाइन असणे आवश्यक आहे, परंतु मला जाणवले आहे की ते टिकाऊ नाही. आता, मी माझ्या ऑनलाइन वेळेबद्दल अधिक जागरूक राहण्याचा प्रयत्न करतो आणि सीमा निश्चित करतो जेणेकरून मी तिथेच अडकणार नाही. मित्र आणि कुटुंबियांसमवेत वेळ घालविणे, निसर्गाच्या सान्निध्यात असणे किंवा स्वत: साठी थोडा वेळ काढणे यासारख्या स्वत:ला रिचार्ज करण्यास मदत करणाऱ्या गोष्टींना माझ्या वेळापत्रकात स्थान असेल हे मी सुनिश्चित करतो. हे नेहमीच सोपे नसते, पण माझ्या हे लक्षात आले आहे की याचा दीर्घकालीन उपयोग आहे.

रीकॅप: क्लिक करा, स्क्रोल करा, श्वास घ्या!

आपल्याला ऑनलाइन कसे वाटते याकडे लक्ष द्या.

इंटरनेट मजेदार असू शकते, परंतु त्याचा आपल्या भावनांवर कसा परिणाम होतो हे लक्षात घेणे महत्वाचे आहे. ऑनलाइन राहिल्यानंतर आपल्याला चिंताग्रस्त, दु:खी किंवा थकल्यासारखे वाटत असल्यास, थांबणे आणि विश्रांती घेणे गरजेचे आहे.

ऑनलाइन आणि ऑफलाइन जीवनात निरोगी संतुलन शोधा.

जास्त वेळ ऑनलाइन घालवल्याने तुझ्या झोपेवर, मन:स्थितीवर आणि फोकसवर परिणाम होऊ शकतो. छंद जोपासणे, मित्रांसोबत वेळ घालवणे आणि आपल्या स्क्रीनपलीकडील जगाचा आनंद घेणे यासारख्या वास्तविक जीवनातील ॲक्टीविटीज करता वेळ ठेवा. .

तुमच्या हिताचे रक्षण करण्यासाठी स्पष्ट सीमा निश्चित करा.

अनावश्यक नोटिफिकेशन बंद करणे, सोशल मीडियासाठी वेळेची मर्यादा निश्चित करणे आणि रात्री उशिरा स्क्रोल करणे टाळणे यासारख्या छोट्या कृती आपल्याला आपल्या डिजिटल सवयींवर नियंत्रण ठेवण्यास मदत करतात.

लक्षात ठेवा, सोशल मीडिया म्हणजे संपूर्ण चित्र नाही

आपण ऑनलाइन जे पाहतो ते रिअल लाइफ नव्हे तर हायलाइट रील आहे. इतरांशी स्वत:ची तुलना करणे टाळा आणि आपल्या स्वत: च्या आयुष्यात आपल्याला आनंदी आणि परिपूर्ण कशामुळे करा येईलयावर लक्ष केंद्रित करा

एखादी गोष्ट चुकीची वाटत असेल तर इतरांशी संपर्क साधा

जर इंटरनेट कधीही अतिरेक करणारं किंवा असुरक्षित वाटत असेल तर आपल्या विश्वासातील एखाद्या व्यक्तीशी बोला. आपण एकटे नसतो आणि जेव्हा आपल्याला गरज असेल तेव्हा नेहमीच मदत उपलब्ध असते

चॅप्टर 7: ट्रेंडिंग फॉर चेंज: चांगल्यासाठी इंटरनेटचा वापर करणे

नूर नेहमीच इंटरनेटला फक्त शिकण्याची आणि मनोरंजनाची जागा मानत होती, पण तिचा दृष्टीकोन बदलू लागला होता. आता, जेव्हा ती तिच्या नागरिकशास्त्र विषयाच्या प्रकल्पावर काम करत होती, तेव्हा ऑनलाइन असणाऱ्या तरुणांच्या भूमिकेबद्दल करू - आणि ती जे काही शिकली आहे त्याआधारे ती आणखी चांगले कार्य कसे करू शकते याबद्दल विचार करू लागली.

डिजिटल नागरिक म्हणून जबाबदाऱ्या

नूर यांनी एक प्रस्तावना तयार केली ज्यात अश्या मुद्द्यांचा समावेश होता ज्याबद्दल कुठल्याही वाटाघाटी करण्याची शक्यता नाही. यांचा सर्व डिजिटल नागरिकांनी पालन केले पाहिजे असे तिला वाटत होते. तुझ्या तुमच्या मित्रांशी चर्चा करा आणि यामध्ये दोन गोष्टींची भर घाला ज्यांचा समावेश होणे गरजेचे आहे असे तुम्हाला वाटते.

आम्ही डिजिटल क्षेत्रातील नागरिक, आमच्या ऑनलाइन संवादात न्याय, स्वातंत्र्य आणि समानता राखण्याचा गंभीरपणे संकल्प करून, याद्वारे आमची वचनबद्धता जाहीर करतो.

- इतरांच्या हक्कांचा आणि मतांचा आदर करणे, प्रत्येकाचा आवाज सन्मानाने आणि निष्पक्षतेने ऐकला जाईल याची खात्री करणे;
- सर्व व्यक्तींच्या गोपनीयतेचा आदर करणे, घुसखोरी आणि गैरवापरापासून त्यांच्या वैयक्तिक स्पेसचे रक्षण करणे;
- शेयर केलेल्या माहितीची पडताळणी करणे, सत्याचा पाठपुरावा करणे आणि संभाषणातील एकवाक्यता टिकवणे
- डिजिटल स्पेसमध्ये आपल्या कृतींची जबाबदारी घेणे, उत्तरदायित्व आणि विश्वासाची संस्कृती जोपासणे;
- सभ्यता, सहानुभूती आणि परस्पर आदर ठेवून नेहमीच डिजिटल शिष्टाचाराचे पालन करणे
- _____
- _____

आपले हक्क आणि जबाबदाऱ्या या दोन्हींचा एकजुटीने वापर करताना, आपण एक सर्वसमावेशक, सुरक्षित आणि अर्थपूर्ण डिजिटल जग तयार करण्याचा प्रयत्न करू, जिथे प्रत्येक व्यक्ती स्वातंत्र्य, जबाबदारी आणि उद्देश्य यांच्याशी जोडला जाईल.

चेंजमेकर्स

नूर! डिजिटल नागरिकांसाठी तू तयार केलेली प्रस्तावना व्हायरल झाली! शाळेतले सगळेच याबद्दल बोलत असतात!

आमच्या नागरिकशास्त्राच्या वर्गात हक्क आणि जबाबदाऱ्यांबद्दल चर्चा झाली आणि काही लोकांनी डिजिटल नागरिकत्व हा विषय देखील काढला!

धन्यवाद मित्रांनो!

हे मस्तच आहे! फक्त आपल्या ग्रुप मध्येच नाही तर याच्या पलीकडे तुम्ही काय चर्चा करता हे बघून मला खूप आवडले.

मलिहा आबिदीसारखी? मी त्यांच्यापासून प्रेरित झालो आहे, आणि मी हाच विचार करत होतो की असे काहीतरी मी कसे सुरू करू शकेन ज्याचा प्रभाव देखील पडेल!

मला खात्री आहे की तुम्ही करू शकता! पण मलिहा आबिदी कोण आहेत आणि त्या काय करतात?

मलिहा आबिदी या २३ वर्षीय कलाकार आणि लेखिका आहेत. त्या कराचीची आहेत आणि सध्या ससेक्स विद्यापीठात न्यूरोसायन्सचे शिक्षण घेत कलेची आवड जोपासत आहेत विविध प्रकल्पांच्या माध्यमातून महिला सक्षमीकरणाचं काम वाढवत आहेत, त्यापैकी एक म्हणजे त्यांचे आगामी पुस्तक "पाकिस्तान फॉर वुमन".

हो! मला जी कार्ये महत्त्वाची वाटतात त्यात अधिक चांगली समज निर्माण करण्यात ऑनलाइन संसाधने उपयुक्त ठरली आहेत!

ते भारी आहे! तर लोक इंटरनेटचा वापर करून इतकं चांगलं काम करत आहेत!

शिकणे आणि वाढणे

- अनेक प्लॅटफॉर्म विद्यार्थ्यांना लर्निंग सपोर्ट देतात. यात शालेय विषयांचे स्टडी मटेरियल, बोर्ड व स्पर्धा परीक्षांची तयारी, ट्युशन, होमवर्क हेल्प अशा विविध प्रकारांचा समावेश होतो.

- ऑनलाइन सोर्सेस वापरून, ज्या विषयांबद्दल तुम्हाला खूप जाणून घ्यायचे आहे, त्यांविषयी केलेले संशोधन पाहून आणि संबंधित लोकांचे भिन्न दृष्टीकोन ऐकून आणखी जाणून घेऊ शकतो.

गेल्याच आठवड्यात सिद्धार्थने क्राऊडफंडिंगचा वापर करून मित्राच्या वैद्यकीय खर्चासाठी निधी गोळा केला होता. आम्ही एकमेकांसाठी उभे राहू शकतो आणि संगठित होवू शकतो!

समवयस्क आणि समुदाय वकिली

- सोशल मीडिया मोबिलायझेशन - कार्यकर्ते लोकप्रिय सोशल मीडिया आणि मेसेजिंग प्लॅटफॉर्मचा वापर संदेश वेगाने पसरविण्यासाठी, व्हायरल मोहिमा सुरू करण्यासाठी आणि मोठ्या प्रमाणात प्रेक्षकांना गुंतवून ठेवण्यासाठी करतात. हॅशटॅग, लाइव्ह व्हिडिओ आणि डिजिटल पेटीशन्स यामुळे चळवळीला जोर येतो, ज्यामुळे समर्थकांना एकत्र करणे आणि सार्वजनिक चर्चा करणे सोपे होते.

- कम्युनिटी कोऑर्डिनेशन अँड डायरेक्ट ॲक्शन - लॉजिस्टिक्सचे नियोजन करण्यासाठी, रिसोर्स शेयर करण्यासाठी आणि भागीदारांना एंगेज ठेवण्यासाठी आयोजक ऑनलाइन फोरम, मेलिंग लिस्ट आणि मेसेजिंग ॲप्सचा फायदा घेतात. क्राउडसोर्सिंग प्लॅटफॉर्म आणि डिजिटल साइन-अप यामुळे सामुहिक कृती करणे शक्य होते आणि त्यामुळे लोकांना सहाय्य करणे आणि निधी गोळा करणे शक्य होते.

चेंजमेकर्स

आपण ऑनलाइन किती शिकू शकतो आणि करू शकतो हे भारावून टाकणारं आहे, परंतु याचा अर्थ असा देखील आहे की ती याला एक उत्तम स्थान करण्याचीजबाबदारी आपली आहे, बरोबर?

हो, अगदी बरोबर! केवळ इंटरनेट वापरणेच नाही, तर आपण तिथे इतरांशी कसे संवाद साधतो त्यातही हे एक सकारात्मक स्थान राहील याची काळजी घे. घेतली पाहिजे.

आपण कुणाला काही पोस्ट करण्यापूर्वी किंवा उत्तर देण्यापूर्वी कुठल्या गोष्टींचा विचार करावा याची चेकलिस्ट बनवू शकतो

चांगलीआयडिया आहे ही! तुला माहित आहे की इंटरनेटबद्दल सर्वात चांगली गोष्ट ही आहे की अश्या लोकांकडून तुम्हाला ऐकायला मिळते जे आपण सहसा बातम्यांमध्ये किंवा टीव्हीवर पाहत नाही.

होय, परंतु मला हे देखील लक्षात आले आहे की काही लोकांचा अधिक ऑनलाइन द्वेष केला जातो. रिपोर्टिंग असो, बोलणं असो किंवा नुसतं सपोर्ट देणं असो, आपण काहीतरी करायला हवं, असं मला वाटतं.

प्रेमळ संभाषण

- ☐ ते प्रेमळ आहे का? (यामुळे कुणाला चांगलं वाटेल की वाईट?)
- ☐ हे आवश्यक आहे का? (मला खरंच हे सांगायची गरज आहे का?)
- ☐ हे आदरयुक्त आहे का? (मला कोणी असं सांगितलं तर चालेल का?)
- ☐ ते अचूक आहे का? (मी ही माहिती पडताळून पाहिली आहे का?)
- ☐ यामुळे गोपनीयतेचा आदर होत आहे का? (मी परवानगीशिवाय कोणाची वैयक्तिक माहिती शेअर करतो आहे का?)

समर्थन दर्शवणे

- आवाज उठवा - जर तुम्हाला सुरक्षित वाटत असेल तर हानिकारक कंटेन्टला फॅक्टस द्वारे उत्तर द्या किंवा शांतपणे त्याला प्रतिसाद द्या
- रिपोर्ट अँड ब्लॉक - हेट स्पीचची माहिती देण्यासाठी आणि पुढील नुकसान टाळण्यासाठी प्लॅटफॉर्मवरील टूल्स वापरा
- प्रेमळ व्यवहार करण्यास प्रोत्साहन द्या - आदरपूर्वक आणि सर्वसमावेशक चर्चेला प्रोत्साहन देऊन संभाषणाला अन्य दिशेला न्या.

संभाषण आणि कृती

याला काहीतरी अर्थ आहे!! आपण खऱ्या आयुष्यात जसे आहोत तसे आपण ऑनलाइन होऊ शकतो का? परंतु आपण काय बोलतो याबद्दल सावध गिरी बाळगण्या व्यतिरिक्त , इंटरनेट ही एक उत्तम जागा करण्यासाठी आपण खरोखर बरेच काही करू शकतो का?

हो! आयांचा अर्थ आहे की , आपण सर्व वेगवेगळ्या गटांचा भाग आहोत- आपले कुटुंब, शाळा, अगदी ऑनलाइन समुदाय देखील. आपण जे शिकलो ते येथे देखील आणण्याचे मार्ग असतील ना, बरोबर.

अगदी बरोबर! अशा काही गोष्टी आहेत ज्या आपण वेगवेगळ्या पातळ्यांवर करू शकतो - घरी, शाळांमध्ये, मित्र मंडळी मध्ये आणि अगदी मोठ्या ऑनलाइन स्पेसमध्ये देखील. याचा एकत्रित परिणाम होतो!

कृती

परिवर्तनाची सुरुवात घरातूनच होते!

- लहान भावंडांना किंवा कुटुंबातील सदस्यांना प्रायवसी सेटिंग्ज आणि डिजिटल वेलबिइंगबद्दल शिकवा.
- खोट्या बातम्या किंवा ऑनलाइन घोटाळे ओळखण्यासाठी पालकांची मदत करा.
- निरोगी स्क्रीन टाइम सवयींबद्दल एकमेकांशी संवाद साधण्याची सुरुवात करा

एक मित्र/मैत्रीण असावा

- हानिकारक जोक्स, सायबर गुंडगिरी किंवा अयोग्य कंटेन्ट पाहिल्यास त्याबद्दल आवाज उठवा.
- ज्यांना ऑनलाइन असुरक्षित किंवा तणावग्रस्त मित्रांना सहाय्य करा.
- जबाबदारीपूर्वक कंटेन्ट शेयर करण्यास प्रोत्साहन द्या-त्यांना फॅक्ट चेकिंग करण्याची आठवण करून द्या

शाळे मधील ॲम्बॅसॅडर

- डिजिटल काइन्डनेस कॅम्पेन आयोजित करा- जिथे विद्यार्थी एकमेकांसाठी सकारात्मक संदेश पोस्ट करतील.
- ऑनलाइन सुरक्षा आणि डिजिटल अधिकारांवर चर्चा करण्यासाठी अवेअरनेस क्लब सुरू करा.
- इंटरनेट जबाबदारीने कसे वापरावे यावर कार्यशाळा आयोजित करण्यासाठी आणि याकरता विद्यार्थ्यांमध्ये कोण ॲम्बॅसॅडर होईल हे ठरवण्या साठी , शिक्षकांबरोबर सहयोग करा.

समाजाशी संवाद

- ऑनलाइन घोटाळे आणि चुकीच्या माहितीबद्दल स्थानिक गटांमध्ये अवेअरनेस निर्माण करा
- शाळांमध्ये आणि अश्या ठिकाणी जेथे तरुण लोक जमतात तेथे मजबूत सायबर सुरक्षा धोरण याविषयी बोला.
- मानसिक आरोग्य, ऑनलाइन छळ आणि सपोर्ट नेटवर्क या बद्दल चे खात्रीशीर रिसोर्सेस शेयर करा.

या अप्रतिम आयडिया आहेत, शुभम. इंटरनेट जितके आपल्या ऑनलाइन अनुभवांना आकार देते, तितकेच आपण ही आपले ऑनलाइन भवितव्य घडवतो.

तुझं म्हणणे बरोबर आहे! मला जे करून पहायचं आहे त्याची माझ्याकडे एक आयडिया आहे नूर! पण मला थोडी मदत हवी आहे!

नक्कीच! उद्या दुपारी आपण भेटतोय हे मी सगळ्यांना सांगते!

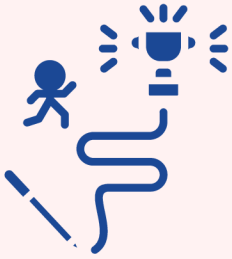
पुन्हा एकदा मित्र मैत्रिणी एकत्र भेटले. पण नुसतेच दुपारी टाइमपास करायला नाही. शुभमचं टीमसाठी एक मिशन होतं, आणि सगळे त्याबद्दल आणखी काही ऐकण्याची वाट पाहत होते.

शुभमने सर्वांना वर्कशीट आणि पेन दिले, तसेच त्यांच्या विचारांना चालना देण्यासाठी मिशन स्टेटमेंट सांगितले. 30 मिनिटांत त्यांनी काय केले हे पाहण्यासाठी खाली स्क्रोल करा! त्यांचा अंतिम ॲक्शन प्लॅन पाहण्यासाठी स्क्रॉल करत रहा.

सुरक्षानगरचे एजंट ,

तुमच्या समाजाला तुमची गरज आहे. कचरा आणि प्रदूषणाच्या वाढत्या धोक्यामुळे आपले रस्ते, आपली हवा आणि आपले भविष्य धोक्यात येत आहे. याकरता ॲक्शन घेण्याची ही वेळ आहे - आपल्या मित्रांना एकत्र करा, सर्वांना हे सांगा आणि उपाय करा. जनजागृती मोहिमेपासून ते स्वच्छता मोहिमेपर्यंत प्रत्येक कृती महत्त्वाची ठरते. मिशन स्पष्ट आहे: सुरक्षा नगर पुन्हा सुरक्षित आणि स्वच्छ ठेवा.

तुम्ही हे आव्हान पेलणार का? जर आपण बदल घडवून आणायलातयार असाल तर आत्ताच आपला ॲक्शन प्लॅन तयार करा!



ध्येय: सामुदायिक कृती आणि डिजिटल ॲड्वोकसीने सुरक्षा नगरची सुरक्षा आणि स्वच्छता पुन्हा स्थापित करा.

जागरुकतेसाठी 1 महिना + 2 साप्ताहिक स्वच्छता ड्राइव्ह + चालू असलेल्या सोशल मीडिया एंगेजमेंट.

शुभम - क्रिएटिव्ह डिझायनर

- कॅन्व्हा वापरून पोस्टर्स डिझाइन करायला शिका.
- ऑनलाइन आणि समाजात इतरांशी शेयर करण्यासाठी मोहिमेच्या हॅशटॅगसह आकर्षक चित्रे तयार करा.

रहीम - द रील मेकर

- प्रदूषण समस्या आणि सामुदायिक प्रयत्नांवर प्रकाश टाकणारे लघु रील चित्रपट आणि संपादन.
- जागरूकता पसरविण्यासाठी सोशल मीडियावर व्हिडिओ पोस्ट करा.

सुसान - कम्युनिटी कनेक्टर

- सुरक्षा नगर मेसेजिंग ग्रुप मॅनेज करा.
- शेजाऱ्यांना आमंत्रित करा, अपडेट्स शेयर करा आणि सर्वांना स्वच्छतेच्या कार्यक्रमांची आठवण करून द्या.

मीरा - सोशल मीडिया कॅप्टन

- एक डेडीकेटेड कॅम्पेन पेज तयार करा आणि चालवा (उदा., @CleanSuraksha).
- नियमितपणे प्रोग्रेस अपडेट, सक्सेस स्टोरीज आणि लोकांना यामध्ये योगदान कसे करता येईल याबद्दल पोस्ट करा.

सिद्धार्थ – संशोधक आणि खबऱ्या

- प्रदूषण, कचरा व्यवस्थापन आणि पर्यावरणपूरक पद्धतींबद्दल माहिती गोळा करा.
- माहितीपूर्ण पोस्ट लिहा आणि दैनंदिन जीवनातील कचरा कमी करण्याच्या टिप्स शेयर करा

नूर - इव्हेंट ऑर्गनायजर

- स्वच्छता मोहिमा आणि जनजागृती कार्यक्रमांचे नियोजन करा आणि कॉर्डीनेट करा.
- स्वयंसेवकांसाठी डिजिटल साइन-अप फॉर्म आणि वेळापत्रक तयार करा.

जसप्रीत - द हॅशटॅग हिरो

- #CleanSuraksha हॅशटॅगवर लक्ष ठेवा.
- सर्वांनी सामूहिक प्रयत्न करायचे आहेत ही भावना निर्माण करून, स्वत:चा स्वच्छतेचा उपक्रम शेयर करताना लोकांना हॅशटॅग वापरण्यास प्रोत्साहित करा.

आपले स्वत:चे ध्येय ठरवा आणि तुम्हाला महत्त्वाची वाटावी यासाठी ॲप्लक्शन प्लॅन डिझाइन करा!

मिशन

ध्येय

टाईमलाईन

ॲक्टीव्हिटीज

रोल आणि जबाबदाऱ्या

चॅप्टरची उजळणी

- डिजिटल नागरिक या नात्याने आपल्याकडे अधिकार आहेत आणि इतरांच्या हक्कांचा, मतांचा आणि गोपनीयतेचा आदर करणे या जबाबदाऱ्या आहेत

- इंटरनेटचा उपयोग चांगल्या कामासाठी एक पॉवरफूल फोर्स म्हणून केला जाऊ शकतो! जगात आपल्याला जे बदल व्हावेत असे वाटते त्यासाठी आपण त्याचा उपयोग करू शकतो!

- इंटरनेटचा उपयोग शिकण्यासाठी आणि प्रगती करण्याकरता, समुदाय आणि समवयस्क ग्रुप तयार करण्यासाठी आणि इतरांना समर्थन दर्शविण्यासाठी देखील केला जाऊ शकतो!

- स्वत:ला नेहमी विचारा, माझी कृती आणि शब्द दयापूर्ण आहेत का? ते आदरयुक्त आहेत का?

- परिवर्तनाची सुरुवात घरातूनच होते! आपण आपले कुटुंब आणि मित्रांशी संभाषण सुरू करू शकता, शाळेत या कार्याचा ॲम्बॅसॅडर होऊ शकता आणि आपल्या सभोवताली होणाऱ्या हानिकारक वर्तनाबद्दल आवाज उठवू शकता.

ग्रंथसूची

ग्रंथसूची

चॅप्टर 6

- मानसिक आरोग्य रिसोर्सेस
- तुमच्या वेळेच्या वापराचा समतोल राखण्यासाठी कमिटमेंट प्लॅनर
- मानसिक आरोग्याच्या समस्येशी झगडत असलेल्या मित्राला कसे ओळखावे आणि मदत कशी करावी

चॅप्टर 7

- Sमलिहा आबिदी यांची सुरक्षित मुलाखत
- सामुदायिक आरोग्य आणि विकासास प्रोत्साहन देण्यासाठी इंटरनेट आधारित साधने वापरणे
- डिजिटल सुरक्षा आणि नागरिकत्व' अभ्यासक्रम